BIOS Setup Utility

User Guide

For the Intel® Server Boards D50TNP, M50CYP, and D40AMP.

Rev. 1.07

January 2025

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

Document Revision History

Date	Revision	Changes
April 2021	1.0	• Initial release based on Intel® Server Boards D50TNP and M50CYP BIOS Setup Specification (revision 1.00).
December 2021	1.01	• Update based on Intel® Server Boards D50TNP, M50CYP, and D40AMP BIOS Setup Specification (revision 1.04). • Edits throughout the document to improve clarity and style.
December 2021	1.02	• Change IPMI Security Policy knob. • Update help text about PCIe Pll SSC knob. • Update help text about System Time knob. • Change PFR Unprovision string to PFR UnProvision. • Remove colon from PFR Status, PFR Lock Status, PFR Provision Status. • Change Select Owner EPOCH Input Type knob string. • Change Uncore Freq Scaling help text string. • Change AVX ICCP Pre-Grant Level knob string. • Add OS Native AER Support knob. • Add DBP-F knob. • Add PPR Type knob. • Remove L1 only option from PCIe ASPM Support (Global) setup knob. • Update Tool support table. • Correct spelling mistakes. • Add AMT related knobs. • Add Partial Mirror Mode option to Mirror Mode knob. • Add Partial Mirror size related knobs. • Add Mirror TAD0 knob. • Add TPM FW Update Knob.
July 2022	1.03	• Change console redirection default to disabled in the setup figure. • Add Max TME-MT Keys item description. • Add TPM FW item version description. • CCB3584: Add Redfish* HI BMC and Host LAN configuration knobs (Section 3.5.3). • Remove unnecessary description for Volatile Memory Mode item. • Add comments for console redirection three options. • CCB3692: Add Reset PCI Rebalance Data knob. • Add description for TPM FW update via `syscfg`.
October 2022	1.04	• CCB3694: Add Enable Custom Refresh Enable, Custom Refresh Rate. • Remove Hit Me, D2C and D2K three DFX releated knobs. • Add VROC section. • Update Memory RAS section information. • Add comments for MCTP bus owner and sw correctable error time window. • CCB3695: Expose 'Data Link Feature Exchange' in CYP/TNP BIOS SETUP interface. • Add comments for X2APIC and VT-d automicaly function. • Remove AHCI Capable (s)SATA Controller comments Note. • Add comments for exit air temp.
March 2023	1.05	• Remove SATA string in SATA/PCIe M.2 Volume Management Device. • Remove MCTP Broadcast Cycle knob due to no function. • Hidden MCTP Bus Owner knob since workaround for TNP to fix PMBUS fan failure issue. • Add a comment for PCIe ASPM Support(Global). • Replace "Intel Integrator Toolkit" with "Firmware Customization". • Update comments for X2APIC and VT-d.
November 2023	1.06	• Update NTB enabled behavior description in NTB note. • Remove PMem FastGo Configuration knob value Option 2 ~ Option 5. • Update Correctable Error Thershold default value to 500 and help text. • Update Current Configuration value string "1LM Full Mirror" to "Full Mirror". • Remove BMC User Configuration Privilege knob value Callback. • Add comment for PCIe M.2 Volume Management Device. • Add comment for Reset PCI Rebalance Data.

Date	Revision	Changes
January 2025	1.07	• Remove the comment related with 4096G of Memory Mapped I/O Size. • Update Adv MemTest Options Value range and help text, add support bit-20 and bit-21. • Hide 'Reset PCI Rebalance Data' option from BIOS SETUP UI, update comments about it can only be enabled via Firmware Customization.

Disclaimers

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

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

This document contains information on products, services and/or processes in development. All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications.

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

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

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

Table of Contents

List of Figures

List of Tables

1. Introduction

This user guide provides an overview of the features and functions offered by the embedded BIOS setup utility included in the Intel® Server Boards D50TNP, M50CYP, and D40AMP. These server boards are based on the 3rd Gen Intel® Xeon® Scalable processor family. The text-based setup utility controls the platform's built-in devices, the boot manager, and the error manager.

Use the BIOS setup utility 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.

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

The BIOS setup utility has the following features:

- **Localization:** The Intel® Server BIOS Toolkit is only available in English.
- **Console redirection:** The BIOS setup utility is functional via console redirection (refer to the *BIOS EPS for Intel® Server Boards D50TNP, M50CYP, and D40AMP,* Sections 3.16.5 and 7.4) over various terminal emulation standards. When this feature is enabled, the POST display is in purely in text mode due to redirection data transfer in a serial port data terminal emulation mode. This mode may limit some functionality for compatibility, for example, usage of colors or some keys or key sequences or support of pointing devices.
    - Setup screens are designed to be displayable in a 100-character x 31-line format, so they can work with console redirection. However, this screen layout should display correctly on any format with longer lines or more lines on the screen.
- **Password protection:** The BIOS Setup screen may be protected from unauthorized changes by setting an administrative password in the Security screen (refer to the *BIOS EPS for Intel® Server Boards D50TNP, M50CYP, and D40AMP*, Section 9.1). When an administrative password has been set, all selection and data entry fields in Setup screen (except System Time and Date) are grayed out. When grayed out, the user cannot change these fields unless the administrative password has been entered.

Note: If an administrative password has not been set, anyone who boots the system to the Setup screen has access to all selection and data entry fields in the screen and can change any of them. For more information about BIOS password protection, see the *BIOS EPS for Intel® Server Boards D50TNP, M50CYP, and D40AMP*, Section 9.1.

2. BIOS Setup Utility Operation

2.1 Setup Page Layout

The Setup screen layout is sectioned into four functional areas as defined in Figure 1. Each functional area is described in Table 1.

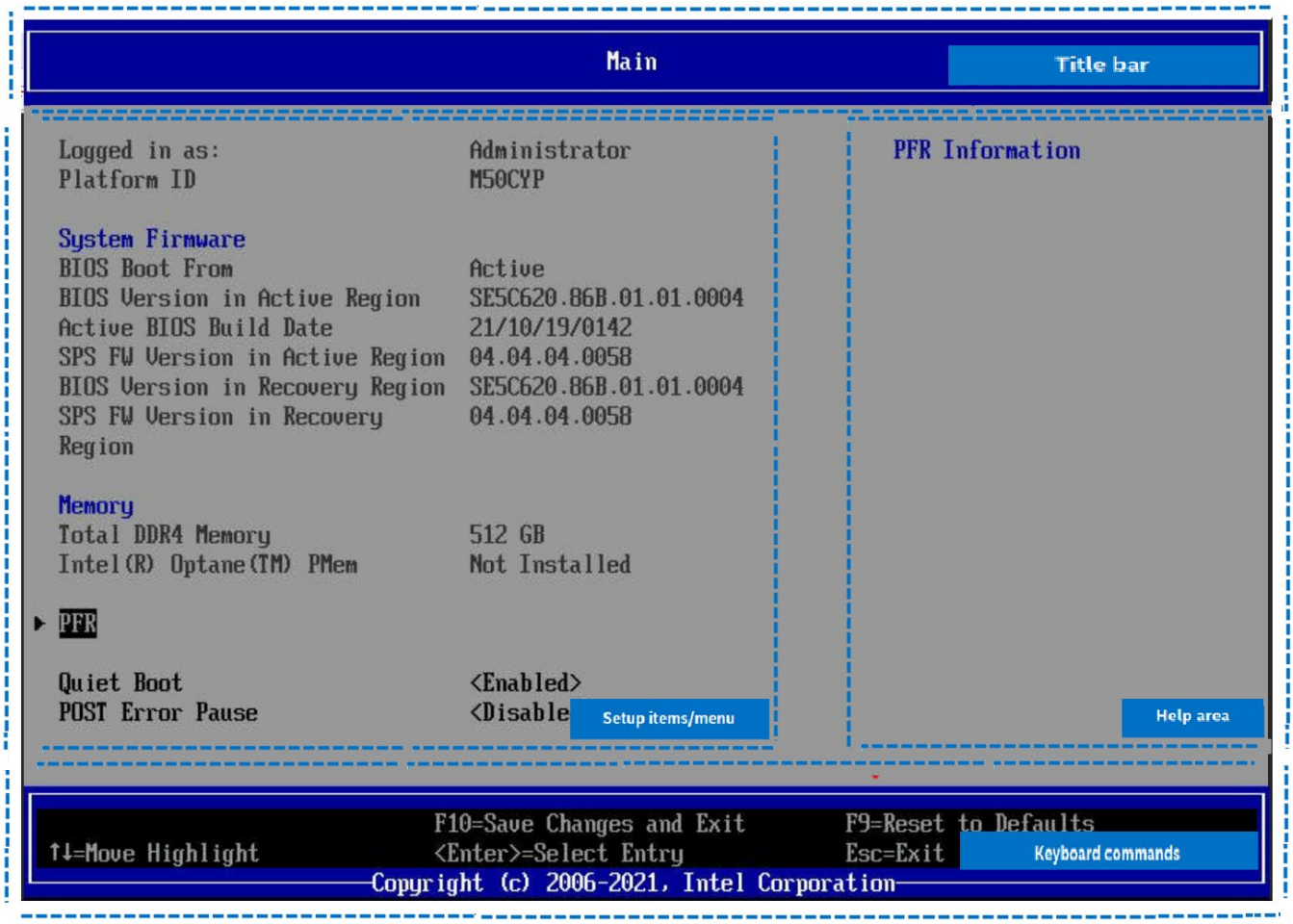


Figure 1. BIOS Setup Screen Layout

Table 1. BIOS Setup Page Layout

Functional Area	Description
Title bar	This area is at the top of the screen and displays tabs with the titles of the top-level pages or screens that can be selected. Use the **left** and **right arrow** keys to move from page to page through the tabs.
Page title	In a multi-level hierarchy of pages beneath one of the top-level tabs, this area is in the upper left corner of the page and identifies the specific page that the user is viewing. Use the **<ESC>** key to return to the higher level in the hierarchy, until the top-level page is reached.
Setup items/menu	This area is a set of control entries and informational items. The list is displayed in two columns. For each item in the list: • 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.
Help area	The item-specific help area is on the right side of the screen and contains help text specific to the highlighted setup item. Help information may include the meaning and usage of the item, allowable values, effects of the options, and other data.
Keyboard commands	The keyboard command area is at the bottom right of the screen and continuously displays help for keyboard special keys and navigation keys.

2.2 Enter BIOS Setup Utility

To enter the BIOS setup utility 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 next 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, the user must wait until the BIOS discovers the keyboard and beeps. The system does not read key pressing before the USB controller is initialized and the USB keyboard is activated.

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

The user could also cause a boot directly to the Setup screen 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 Utility

The user can use one of these methods to exit the BIOS setup utility:

1. By pressing the hotkey **<F10>**.
2. By selecting **<Save Changes and Exit>**.
3. By selecting **<Discard Changes and Exit>**.

No matter what changes are made or not, the system does cold reset after either of the above methods is 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 BIOS setup utility. These commands are always displayed.

Each setup menu page contains several features. Each feature is associated with a value field, except those items used solely 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 grayed out.

Table 2. BIOS Setup Utility Keyboard Command Bar

Key	Option	Description
<Enter>	Execute Command	Use the **<Enter>** key to activate submenus when the selected feature is a submenu, or to display a pick list if a selected option has a value field. Also, 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	Use the **<Esc>** key 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	Use the **up arrow** 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	Use the down arrow 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.

Key	Option	Description
<Tab>	Select Field	Use the **<Tab>** key 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	Use the **minus** key on the keypad to change the current item's value to the previous value. This key scrolls through the values in the associated pick list without displaying the full list.
<+>	Change Value	Use the **plus** key on the keypad to change the current menu item's value to the next value. This key scrolls through the values in the associated pick list without displaying the full list. **Note:** On 106-key Japanese keyboards, the plus key has a different scan code than the plus key on the other keyboards but has the same effect.

<F9>	Reset to Defaults	Press the **<F9>** key to cause 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> or 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	Press the **<F10>** key to cause 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> 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 Utility Screens

This section describes the BIOS setup utility screens through which the user can configure server platforms belonging to the Intel® Server Boards D50TNP, M50CYP, and D40AMP. These screens facilitate the configuration of options related to advanced features, security, server management, boot maintenance, error management, among others.

Each screen is presented including one or more screen images and a list of field descriptions detailing its items' contents. All the screen items are hyperlinked to their corresponding relevant field description.

These field description lists follow these guidelines:

- The text heading for field descriptions is the actual text displayed on the BIOS setup utility screen. The screen text in each figure is a hyperlink to its corresponding field description.
- The text shown as the value for each field description is the actual text displayed on the BIOS setup utility screen. The default values are shown in **bold**.
- The help text entry is the actual text that appears on the BIOS setup utility 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 utility 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 the 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 utility collection and organizes them into major categories. Each category has a hierarchy with a top-level screen from which lower-level screens can 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 another top-level screen, press the **up** or **down arrow** keys to traverse the tabs until the desired screen is selected.

The categories and their screens are listed in the following table, with links to the corresponding subsections in this document.

Table 3. Screen Map

Top-Level Categories	Second Level Screens	Third Level Screens
Main Screen	PFR	-
Advanced Screen	Processor Configuration	-
	Power & Performance	Uncore Power Management
		CPU P State Control
		Hardware P States
		CPU C State Control
	UPI Configuration	-
	Memory Configuration	Memory RAS and Performance Configuration
		Intel(R) Optane(TM) PMem BIOS Setting
	System Event Log	-
	Integrated I/O Configuration	PCIe* Slot Bifurcation Setting
		Processor PCIe* Link Speed
		Volume Management Device
		PCIe Misc. Configuration
		NTB Configuration
	Mass Storage Controller Configuration	SATA Port Configuration
	PCI Configuration	NIC Configuration
		UEFI Network Stack
		UEFI Option ROM Control
	Serial Port Configuration	-
	USB Configuration	-
	System Acoustic and Performance Configuration	-
Security Screen	-	-
Server Management Screen	Console Redirection	-
	System Information	-
	BMC LAN Configuration	User Configuration
Boot Manager Screen	-	-
Error Manager Screen	-	-

Top-Level Categories	Second Level Screens	Third Level Screens
Boot Maintenance Manager Screen	Advanced Boot Options	Secure Boot Configuration
		Https Boot Configuration
		Tls Auth Configuration
		Server CA Configuration
		Enroll Cert
	Add EFI Boot Option	-
	Delete EFI Boot Option	-
	Change Boot Order	-
Save & Exit Screen	-	-

3.2 Main Screen

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

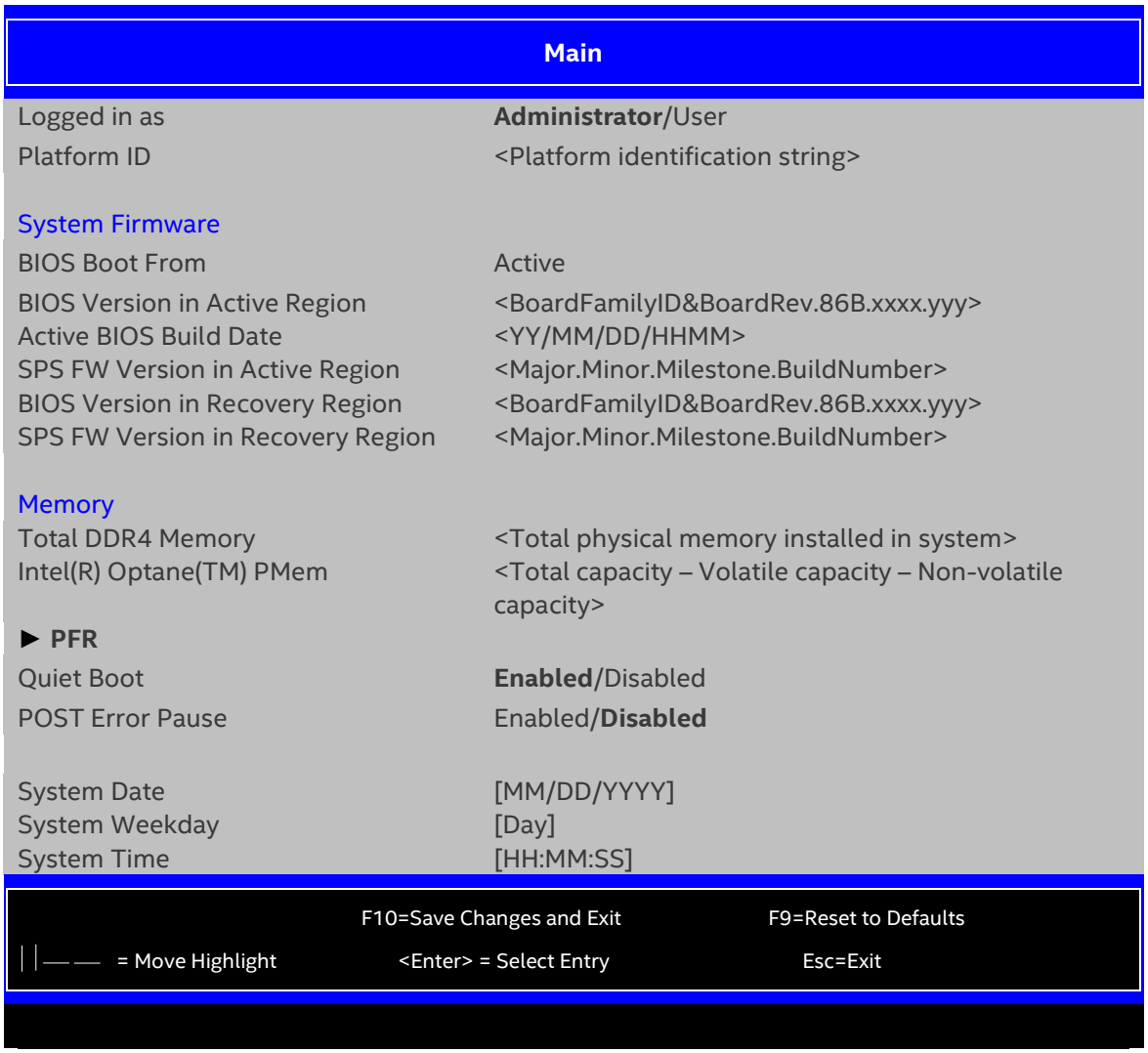


Figure 2. Main Screen

1. **Logged in as**

   Value: **Administrator**/User

   Help text: None.

   Comments: *Information only*. Displays the password level that setup is running in: Administrator or User. With no passwords set, Administrator is the default mode. For more information about BIOS password protection, refer to the *BIOS EPS for Intel® Server Boards D50TNP, M50CYP, and D40AMP*, 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 the POST.

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

   For a list of platform IDs and related product-specific information, refer to the *BIOS EPS for Intel® Server Boards D50TNP, M50CYP, and D40AMP*, Section 11.

   Back to: Main Screen – Screen Map

3. **BIOS Boot From**

   Value: **Active**

   Help text: None.

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

   Back to: Main Screen – Screen Map

4. **BIOS Version in Active Region**

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

   Help text: None.

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

   - BoardFamilyID – Identifies the server platform.
   - BoardRev – Define the level of debug output built into and enabled by the BIOS.
   - 86B – Identifies this BIOS as being a BIOS for Intel server boards.
   - xxxx – Major revision level of the BIOS.
   - yyy – Build Type and Minor revision of the BIOS.

   For full details on interpreting the BIOS ID string, see the *BIOS EPS for Intel® Server Boards D50TNP, M50CYP, and D40AMP*, Section 3.1.2.

   Back to: Main Screen – Screen Map

5. **Active BIOS Build Date**

   Value: < YY/MM/DD/HHMM >

   Help text: None.

   Comments: *Information only*. The date displayed is taken from the time stamp segment of the BIOS ID string and indicates the date when the currently installed primary BIOS was created (built). For full details about the BIOS ID string, refer to the *BIOS EPS for Intel® Server Boards D50TNP, M50CYP, and D40AMP*, Section 3.1.2.

   Back to: Main Screen – Screen Map

6. SPS FW Version in Active Region

Value: < Major.Minor.Milestone.BuildNumber >

Help text: None.

Comments: *Information only*. Detailed SPS FW information is in Intel® Management Engine – BIOS Interface Specification, CDI: 548530.

These segments are displayed:

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

Back to: Main Screen – Screen Map

7. BIOS Version in Recovery Region

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

Help text: None.

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

These segments are displayed:

- BoardFamilyID – Identifies the server platform.
- BoardRev – Define the level of debug output built into and enabled by the BIOS.
- `86B` – Identifies this BIOS as being a BIOS for Intel server boards.
- xxxx– Major revision level of the BIOS.
- yyy – Build Type and Minor revision of the BIOS.

For full details about interpreting the BIOS ID string, refer to the *BIOS EPS for Intel® Server Boards D50TNP, M50CYP, and D40AMP*, Section 3.1.2.

Back to: Main Screen – Screen Map

8. SPS FW Version in Recovery Region

Value: < Major.Minor.Milestone.BuildNumber >

Help text: None.

Comments: *Information only*. Detailed SPS FW information is in Intel® Management Engine – BIOS Interface Specification CDI: 548530.

These segments are displayed:

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

Back to: Main Screen – Screen Map

9. Total DDR4 Memory

Value: <Total physical DDR4 memory installed in the system>

Help text: None.

Comments: *Information only*. Displays the GB memory amount available in the system, in the form of installed DDR4 DIMMs. This item does not include Intel® Optane™ PMem information.

Back to: Main Screen – Screen Map

10. Intel(R) Optane(TM) PMem

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

Help text: None.

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

Back to: Main Screen – Screen Map

11. PFR

Value: None.

Help text: `PFR Information.`

Comments: None.

Back to: Main Screen – Screen Map

12. 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 the POST. For more information on the POST diagnostic screen, refer to the *BIOS EPS for Intel® Server Boards D50TNP, M50CYP, and D40AMP*, 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

13. POST Error Pause

Value: Enabled/**Disabled**

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

Comments: If enabled, the POST Error Pause option takes the system to the Error Manager to review the errors when major errors occur. Minor and fatal error displays are not affected by this setting. For more information, refer to the *BIOS EPS for Intel® Server Boards for D50TNP, M50CYP, and D40AMP*, Section 10.5.4.3.2.

Back to: Main Screen – Screen Map

14. 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 2020 and 2099.`

`Use the [Enter], [+] or [-] key to modify the selected field.`

`Use the [<-] or [->] key to select the previous or next field.`

Comments: This field initially displays the current system date. It can 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 – `01/01/2020`.

Back to: Main Screen – Screen Map

15. 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 01/01/2020 –`Wednesday`.

Back to: Main Screen – Screen Map

16. 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 can 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 system time is updated to match its own reset time, the update happens early during the POST.

Back to: Main Screen – Screen Map

3.2.1 PFR

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

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

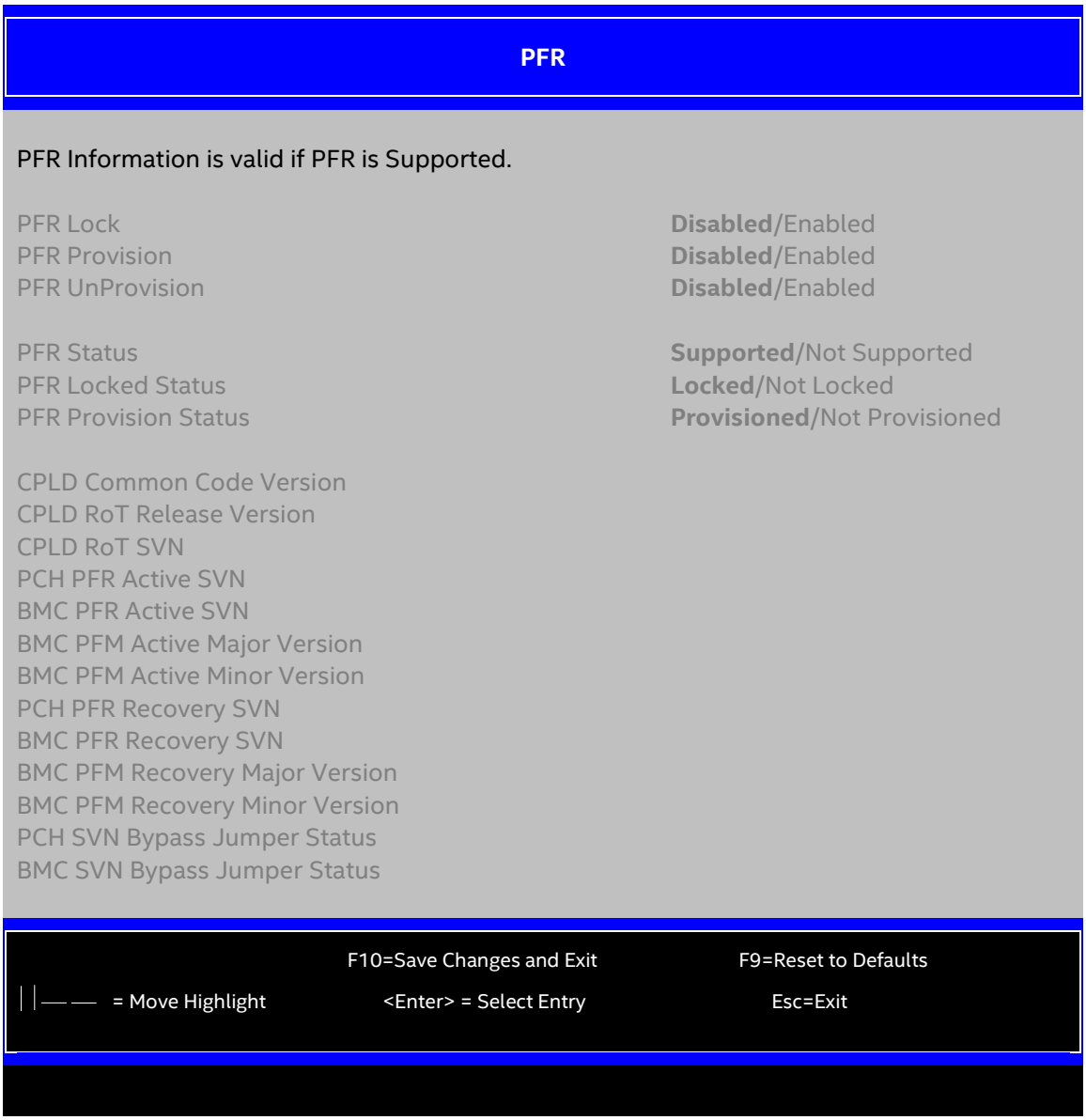


Figure 3. PFR Screen

1. PFR Lock

Value: Disabled/**Enabled**

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

Comments: PFR Lock is grayed out if it cannot be supported. If the PFR Locked Status is locked, the value changes to Disabled. PFR will be locked in production phase.

Back to: Advanced Screen – Screen Map

2. PFR Provision

Value: Disabled/**Enabled**

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

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

Back to: Advanced Screen – Screen Map

3. PFR UnProvision

Value: **Disabled**/Enabled

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

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

Back to: Advanced Screen – Screen Map

4. PFR Status

Value: Supported/Not Supported

Help text: None.

Comments: *Information only.* PFR Status updates during the BIOS POST, after getting the corresponding value back from PFR Mailbox Register.

Back to: Advanced Screen – Screen Map

5. PFR Locked Status

Value: Locked/Not Locked

Help text: None.

Comments: *Information only.* PFR Lock Status updates during the BIOS POST, after getting the corresponding value back from PFR Mailbox Register.

Back to: Advanced Screen – Screen Map

6. PFR Provision Status

Value: Provisioned/Not Provisioned

Help text: None.

Comments: *Information only.* PFR Provision Status updates during the BIOS POST, after getting the corresponding value back from PFR Mailbox Register.

Back to: Advanced Screen – Screen Map

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

Value: Information only

Help text: None.

Comments: *Information only.* These values update during the BIOS POST, after getting back the corresponding values from PFR Mailbox Register.

Back to: Advanced Screen – Screen Map

3.3 Advanced Screen

This screen provides an access point to configure several groups of advanced options. On this screen, the user can 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.

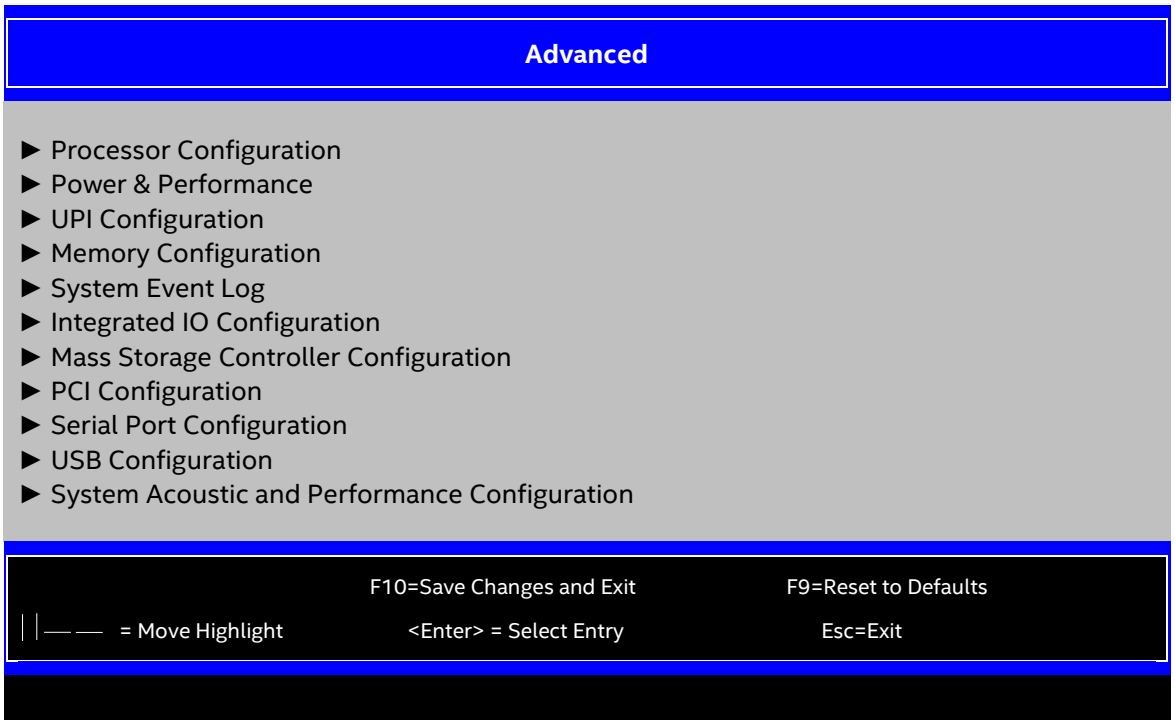


Figure 4. Advanced Screen

1. **Processor Configuration**

   Value: None.

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

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

   Back to: Advanced 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 UPI 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. **System Event Log**

   Value: None.

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

   Comments: *Selection only*. For more information on System Event Log settings, see Section 3.3.5.

   Back to: Advanced Screen – Screen Map

6. **Integrated IO Configuration**

   Value: None.

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

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

   Back to: Advanced Screen – Screen Map

7. **Mass Storage Controller Configuration**

   Value: None.

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

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

   Back to: Advanced Screen – Screen Map

8. **PCI Configuration**

   Value: None.

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

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

   Back to: Advanced Screen – Screen Map

9. **Serial Port Configuration**

   Value: None.

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

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

   Back to: Advanced Screen – Screen Map

10. USB Configuration

Value: None.

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

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

Back to: Advanced Screen – Screen Map

11. System Acoustic and Performance Configuration

Value: None.

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

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

All the information under System Acoustic and Performance Configuration page is grayed out if the IPMI Security Policy information on the 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

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 several processor options.

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

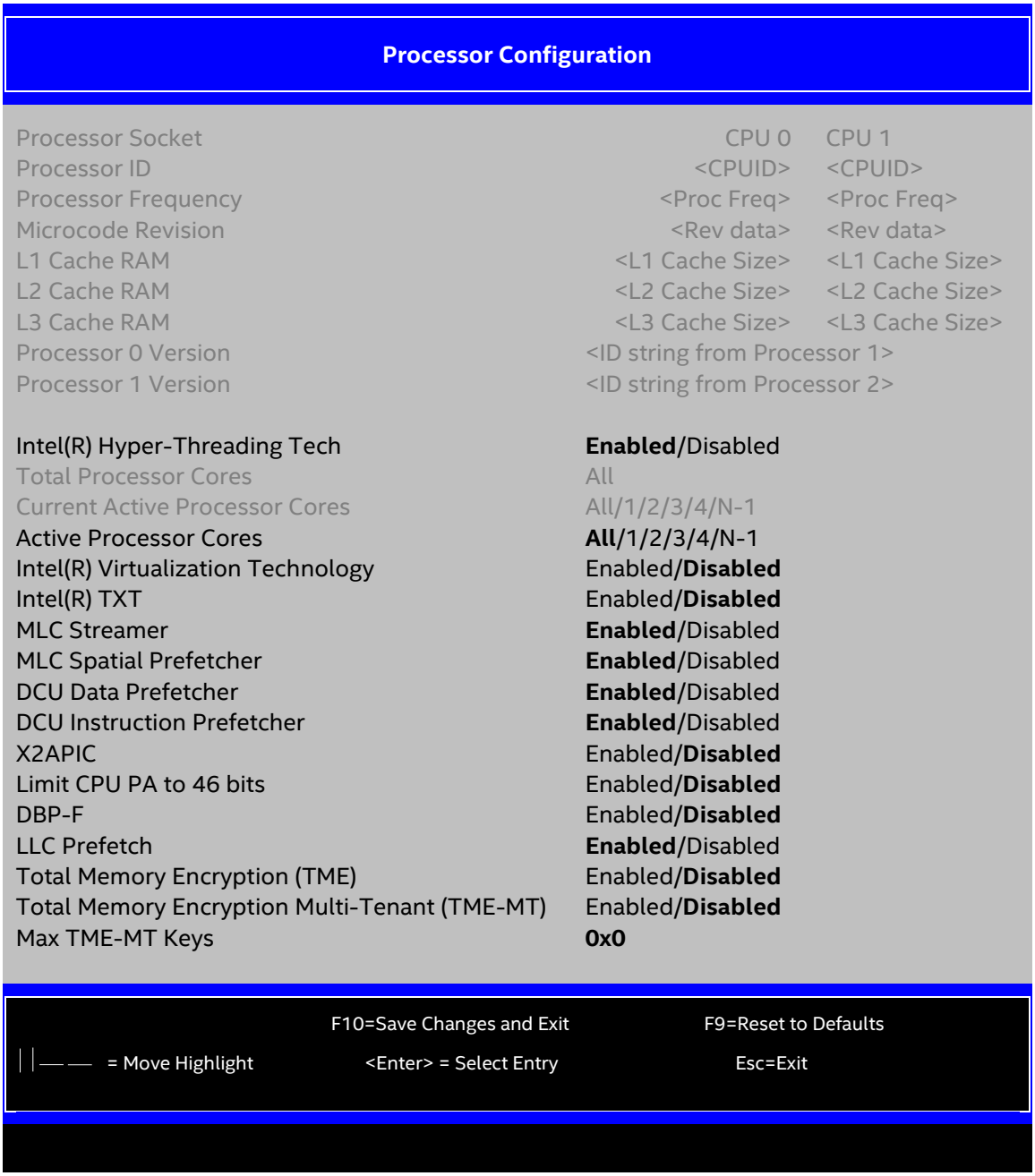


Figure 5. Processor Configuration Screen for Dual-Processor System – Page 1

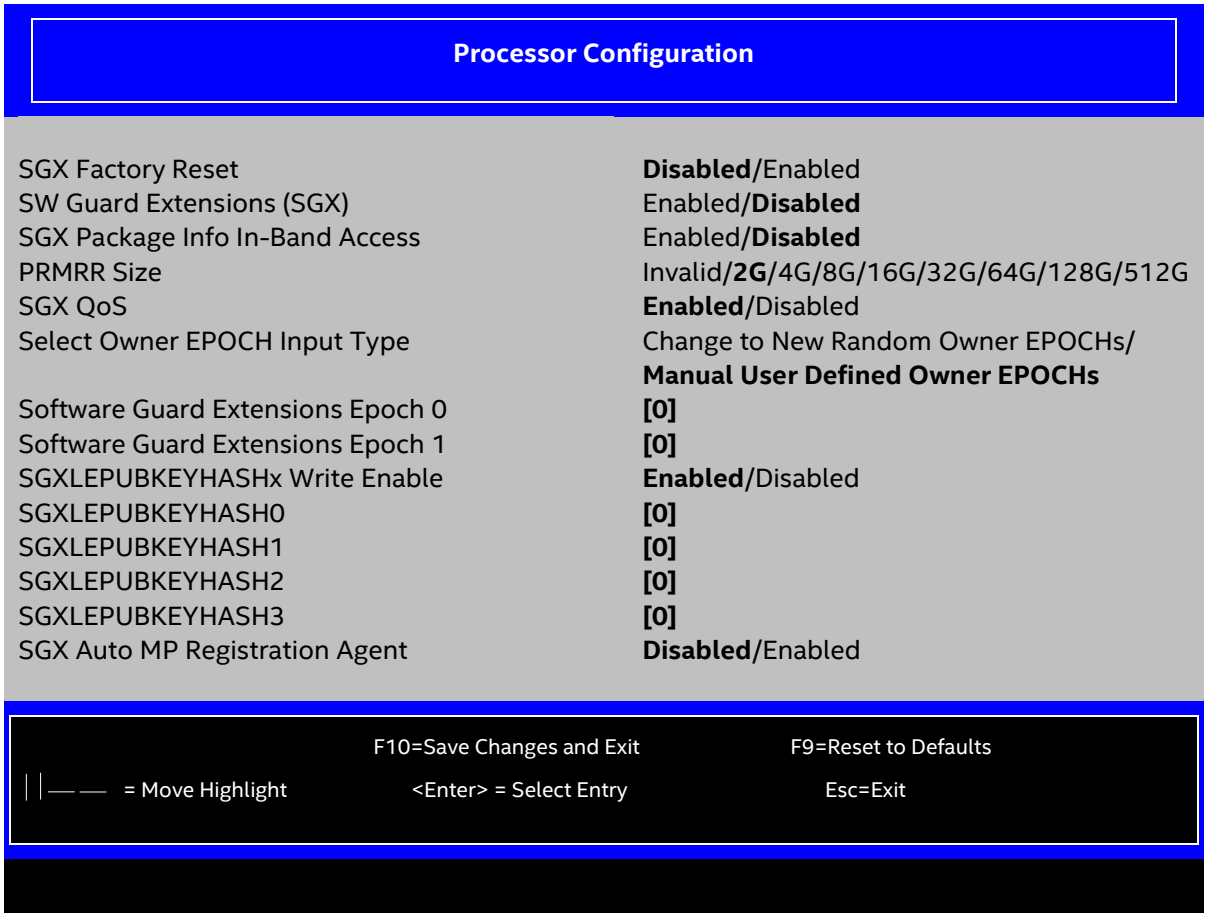


Figure 6. Processor Configuration Screen for Dual-Processor System – Page 2

1. **Processor Socket**

   Value: CPU 0 CPU 1

   Help text: None.

   Comments: *Information only*.

   Back to: Processor Configuration – Advanced Screen – Screen Map

2. **Processor ID**

   Value: <CPUID>

   Help text: None.

   Comments: *Information only*. Displays the processor signature value (from the CPUID instruction) identifying the processor type and the stepping. For more information about supported processors, refer to the *BIOS EPS for Intel® Server Boards D50TNP, M50CYP, and D40AMP*, Section 3.3.2.

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

   For the Intel® Server Boards D50TNP, M50CYP, and D40AMP, 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

3. **Processor Frequency**

   Value: <Current processor frequency>

   Help text: None.

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

   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 no processor is installed.

   Back to: Processor Configuration – Advanced Screen – Screen Map

4. **Microcode Revision**

   Value: <Microcode revision number>

   Help text: None.

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

   Single-socket boards have a single processor display. Two-socket and four-socket boards have a display column for each socket, showing `N/A` for empty sockets where no processor is installed.

   Back to: Processor Configuration – Advanced Screen – Screen Map

5. **L1 Cache RAM**

   Value: <L1 cache size>

   Help text: None.

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

   Single-socket boards have a single processor display. Two-socket and four-socket boards have a display column for each socket, showing `N/A` for empty sockets where no processor is installed.

   Back to: Processor Configuration – Advanced Screen – Screen Map

6. **L2 Cache RAM**

   Value: <L2 cache size>

   Help text: None.

   Comments: *Information only*. Displays the processor's L2 cache size in KB. Since L2 cache is not shared between cores . L2 cache RAM 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 no processor is installed.

   Back to: Processor Configuration – Advanced Screen – Screen Map

7. L3 Cache RAM

Value: <L3 cache size>

Help text: None.

Comments: *Information only*. Displays the processor's L3 cache size in KB. Since L3 cache is not shared between cores . L3 cache RAM 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 no processor is installed.

Back to: Processor Configuration – Advanced Screen – Screen Map

8. Processor 0 Version
Processor 1 Version

Value: <ID string from processor>

Help text: None.

Comments: *Information only*. Displays Brand ID string read from the processor through 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 no processor is installed.

Back to: Processor Configuration – Advanced Screen – Screen Map

9. Intel(R) Hyper-Threading Tech

Value: **Enabled**/Disabled

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

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

Comments: Provided that Intel® Hyper-Threading Technology (Intel® HT Technology) is supported by all the processors installed in the system, this option is visible.

Back to: Processor Configuration – Advanced Screen – Screen Map

10. Total Processor Cores

Value: All

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

Comments: *Information only*. The total processor cores value consists of the number of cores in the processor package. The displayed number of cores depends on the installed processor cores capability. This number may vary, according to different processor types.

Back to: Processor Configuration – Advanced Screen – Screen Map

11. Current Active Processor Cores

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

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

Comments: *Information only*. The current active number of cores, where N is the number of cores in the processor package. The displayed number of cores 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 value may be different from the number previously set by the user.

Note: The Intel® Management Engine (Intel® ME) can control the number of active cores independently of the Active Processor Cores BIOS setting.

During the POST, the BIOS calculates the Active Processor Cores disabled from BIOS setup utility and Intel® NM IPMI command, and add them together to disable the Active Processor Cores.

Back to: Processor Configuration – Advanced Screen – Screen Map

12. Active Processor Cores

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

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

`Note: According above 'Total Processor Cores', select value must < 'Total Processor Cores'.`

Comments: The number of cores that appear as selections depends on the number of cores available in the processors installed.

A board can have up to 4 processors, and each processor can have up to 28 cores. The same number of cores must be active in each processor package.

The “N” means the maximum cores on supported CPUs. Like the maximum of ICX is 56.

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

13. Intel(R) Virtualization Technology

Value: Enabled/**Disabled**

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

`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 the processors installed in the system support Intel® Virtualization Technology (Intel® VT). The software configuration installed on the system must support this feature so it can be enabled.

Note: To support Intel® Trusted Execution Technology (Intel® TXT), Intel® VT must be enabled. Before changing Intel® VT from Enabled to Disabled, the user must make sure

Intel® TXT is set to Disabled. This measure also applies when the settings are changed using Intel® Server Configuration Utility or Firmware Customization.

Back to: Processor Configuration – Advanced Screen – Screen Map

14. Intel(R) TXT

Value: Enabled/**Disabled**

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

Comments: Intel® TXT appears only with products and processors that have Intel® TXT capability. This option is only available when both Intel® VT and Intel® VT for Directed I/O (Intel® VT-d) are enabled and on models equipped with a Trusted Platform Module (TPM). The TPM must be active to support Intel® TXT.

For information about Intel® TXT support, refer to the *BIOS EPS for Intel® Server Boards D50TNP, M50CYP, and D40AMP*, Section 9.3.

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

Back to: Processor Configuration – Advanced Screen – Screen Map

15. MLC Streamer

Value: **Enabled**/Disabled

Help text: `MLC Streamer is a speculative prefetch unit within the processor(s).`

`Note: Modifying this setting may affect performance.`

Comments: MLC Streamer is normally enabled for best efficiency in L2 cache and memory channel use. However, disabling MLC Streamer can improve performance for some processing loads and on certain benchmarks.

For more information, refer to the *BIOS EPS for Intel® Server Boards D50TNP, M50CYP, and D40AMP*, Section 3.3.3.1.

Back to: Processor Configuration – Advanced Screen – Screen Map

16. MLC Spatial Prefetcher

Value: **Enabled**/Disabled

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

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

Comments: MLC Spatial Prefetcher is normally enabled, for best efficiency in L2 cache and memory channel use. However, disabling MLC Spatial Prefetcher can improve performance for some processing loads and on certain benchmarks.

For more information, refer to the *BIOS EPS for Intel® Server Boards D50TNP, M50CYP, and D40AMP*, Section 3.3.3.1.

Back to: Processor Configuration – Advanced Screen – Screen Map

17. DCU Data Prefetcher

Value: **Enabled**/Disabled

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

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

Comments: DCU Data Prefetcher is normally enabled for best efficiency in L1 data cache and memory channel use. However, disabling DCU Data Prefetcher can improve performance for some processing loads and on certain benchmarks.

For more information, refer to the *BIOS EPS for Intel® Server Boards D50TNP, M50CYP, and D40AMP*, Section 3.3.3.1.

Back to: Processor Configuration – Advanced Screen – Screen Map

18. DCU Instruction Prefetcher

Value: **Enabled**/Disabled

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

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

Back to: Processor Configuration – Advanced Screen – Screen Map

19. X2APIC

Value: Enabled/**Disabled**

Help text: `Enable/disable extended APIC support.`

Comments: The item is for the Intel® VT-d feature. With 2019 OS to verify Intel® VT-d enabling boot, X2APIC needs to be enabled. When X2APIC is changed from disabled to enabled, VT-d will be enabled automatically.

Note: This enabled VT-d automaticly when X2APIC is changed to enabled which will be not supported via Intel® Server Configuration Utility due to utility limation.

Back to: Processor Configuration – Advanced Screen – Screen Map

20. DBP-F

Value: Enabled/**Disabled**

Help text: `The DBP-F can be turned off by writing into the (MSR 792h [5:6] for CLX, CPX, and MSR 6Dh [2:3] for ICX).`

Comments: None.

Back to: Processor Configuration – Advanced Screen – Screen Map

21. Limit CPU PA to 46 bits

Value: Enabled/**Disabled**

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

Comments: This option is a workaround for the Intel® VT-d function due to an operating system issue. When booting with a 2019 OS, this item needs to be enabled for Intel® VT-d enabling boot. With 2020H1 operating system, keep the default value for Intel® VT-d enabling boot.

Back to: Processor Configuration – Advanced Screen – Screen Map

22. LLC Prefetch

Value: **Enabled**/Disabled

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

Comments: None.

Back to: Processor Configuration – Advanced Screen – Screen Map

23. Total Memory Encryption (TME)

Value: **Disabled**/Enabled

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

Comments: None.

Back to: Processor Configuration – Advanced Screen – Screen Map

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

Value: Enabled/**Disabled**

Help text: `Enable/Disable Total Memory Encryption Multi-Tenant (TME-MT).`

Comments: When TME is enabled, this item appears in setup. When the Limit CPU PA to 46 Bits is enabled, TME-MT is grayed out.

Back to: Processor Configuration – Advanced Screen – Screen Map

25. Max TME-MT Keys

Value: **0**

Help text: N/A

Comments: Maximum number of keys that are available for usage. `KeyID 0` is reserved as legacy TME key; `KeyID 1-63` = MKTME keys.

Back to: Processor Configuration – Advanced Screen – Screen Map

26. SGX Factory Reset

Value: **Disabled**/Enabled

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

Comments: When TME is enabled, Uma-Base Clustering is disabled, and memory population and SGX capabilities are supported, this item can appear in setup.

Back to: Processor Configuration – Advanced Screen – Screen Map

27. SW Guard Extensions (SGX)

Value: Enabled/**Disabled**

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

Comments: SGX can be shown normally. Enabling or disabling this field is possible only when TME is enabled, Uma-Based Clustering is disabled, and memory population and SGX capabilities are supported. When TME is enabled, even if hardware configuration is supported, this item is grayed out with the blue message: "SGX cannot be enabled due to unsupported configuration: mem or setup (valid options are UmaBasedClustering=All2All, NUMA=En, ADDDCEn=0)".

Back to: Processor Configuration – Advanced Screen – Screen Map

28. SGX Package Info In-Band Access

Value: Enabled/**Disabled**

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

Comments: When TME is enabled, Uma-Base Clustering is disabled, and memory population is supported, SGX Package Info In-Band Access can appear in setup.

Back to: Processor Configuration – Advanced Screen – Screen Map

29. PRMRR Size

Value: Invalid/**2G**/4G/8G/16G/32G/64G/128G/256G/512G

Help text: `Setting the PRMRR Size.`

Comments: When SGX is enabled, PRMRR Size appears in setup.

Note: During the POST, the BIOS SGX driver verifies the system hardware configuration to decide which PRMRR Size value settings are to be visible in the BIOS setup utility. So, some of the settings are visible in the BIOS setup utility.

Back to: Processor Configuration – Advanced Screen – Screen Map

30. SGX QoS

Value: **Enabled**/Disabled

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

Comments: When SGX is enabled, SGX QoS appears in setup.

Back to: Processor Configuration – Advanced Screen – Screen Map

31. Select Owner EPOCH Input Type

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

Help text: `There are two Owner EPOCH modes(Each EPOCH is 64-bit): change to new random owner epoch and manually entered by user. After generating new epoch via 'Change to New Random Owner EPOCHs', the selection reverts back to 'Manual User Defined Owner EPOCHs'.`

Comments: When SGX is enabled, Select Owner EPOCH input type appears in setup.

Back to: Processor Configuration – Advanced Screen – Screen Map

32. Software Guard Extensions Epoch 0

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

Help text: `Software Guard Extensions Epoch 0.`

Comments: When SGX is enabled, Software Guard Extensions Epoch 0 appears in setup.

Back to: Processor Configuration – Advanced Screen – Screen Map

33. Software Guard Extensions Epoch 1

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

Help text: `Software Guard Extensions Epoch 1.`

Comments: When SGX is enabled, Software Guard Extensions Epoch 1 appears in setup.

Back to: Processor Configuration – Advanced Screen – Screen Map

34. SGXLEPUBKEYHASHx Write Enable

Value: Disabled/**Enabled**

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

Comments: When SGX is enabled, SGXLEPUBKEYHASHx Write Enable appears in setup.

Back to: Processor Configuration – Advanced Screen – Screen Map

35. SGXLEPUBKEYHASH0

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

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

Comments: When SGX is enabled, SGXLEPUBKEYHASH0 appears in setup.

Back to: Processor Configuration – Advanced Screen – Screen Map

36. SGXLEPUBKEYHASH1

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

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

Comments: When SGX is enabled, SGXLEPUBKEYHASH1 appears in setup.

Back to: Processor Configuration – Advanced Screen – Screen Map

37. SGXLEPUBKEYHASH2

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

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

Comments: When SGX is enabled, SGXLEPUBKEYHASH2 appears in setup.

Back to: Processor Configuration – Advanced Screen – Screen Map

38. SGXLEPUBKEYHASH3

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

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

Comments: When SGX is enabled, SGXLEPUBKEYHASH3 appears in setup.

Back to: Processor Configuration – Advanced Screen – Screen Map

39. SGX Auto MP Registration Agent

Value: **Disabled**/Enabled

Help text: `The MP registration agent is responsible for register the platform.`

Comments: When SGX is enabled, SGX Auto MP Registration Agent appears in setup.

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 either for reduced power consumption or for increased performance.

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

The user has four profiles to choose from. When a power and performance profile is chosen, the system implements a defined list of setup option settings and internal (non-visible) settings.

For details on each of these power and performance profiles, refer to the *BIOS EPS for Intel® Server Boards D50TNP, M50CYP, and D40AMP*, Section 3.15.2.

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

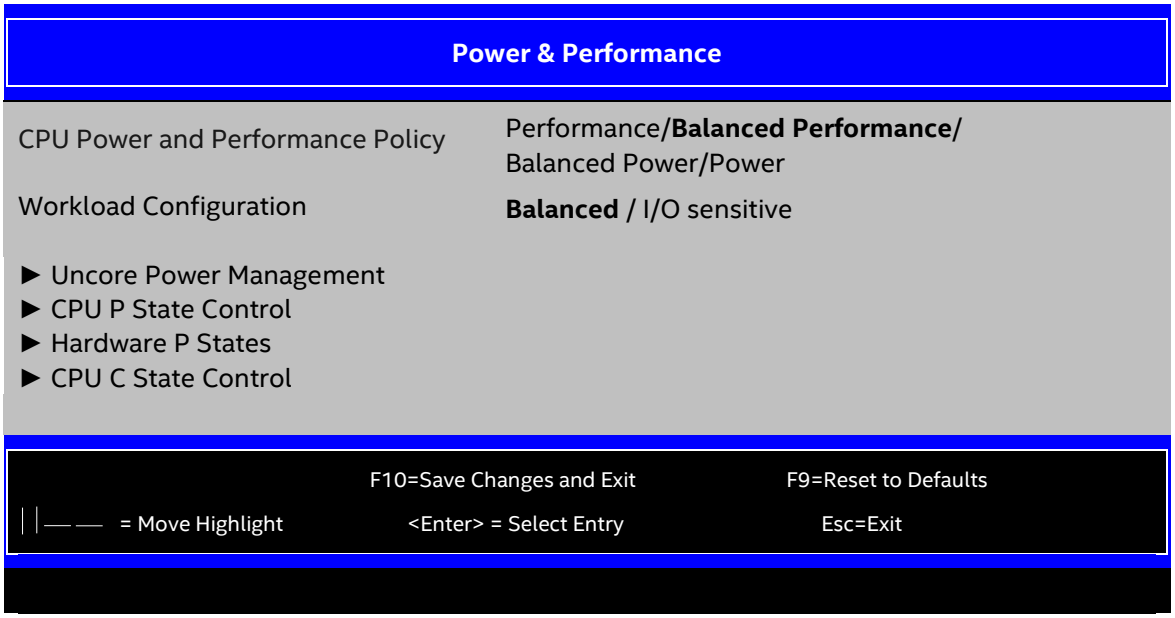


Figure 7. Power & Performance Screen

1. **CPU Power and Performance Policy**

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

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

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

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

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

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

   Comments: Choosing one of these four power and performance profiles implements several changes in BIOS settings, both visible settings in the setup screens and non-visible internal settings.

   For detailed lists of settings affected by each profile, see the *BIOS EPS for Intel® Server Boards D50TNP, M50CYP, and D40AMP*, Section 3.15.2.

   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 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 uncore voltage and frequency to be programmed independently. The uncore activity is monitored to optimize the frequency in real time. This option is visible only when Enhanced Intel SpeedStep® Technology is enabled by the BIOS. Workload Configuration is for dual-processor systems only.

   For more information, see the *BIOS EPS for Intel® Server Boards D50TNP, M50CYP, and D40AMP*, Section 3.15.2.

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

3. **Uncore Power Management**

   Value: None.

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

   Comments: *Selection only*. This option is only visible if Enhanced Intel SpeedStep® Technology is enabled. 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.

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

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 processors policy, which is optimized either for reduced power consumption or for increased performance.

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

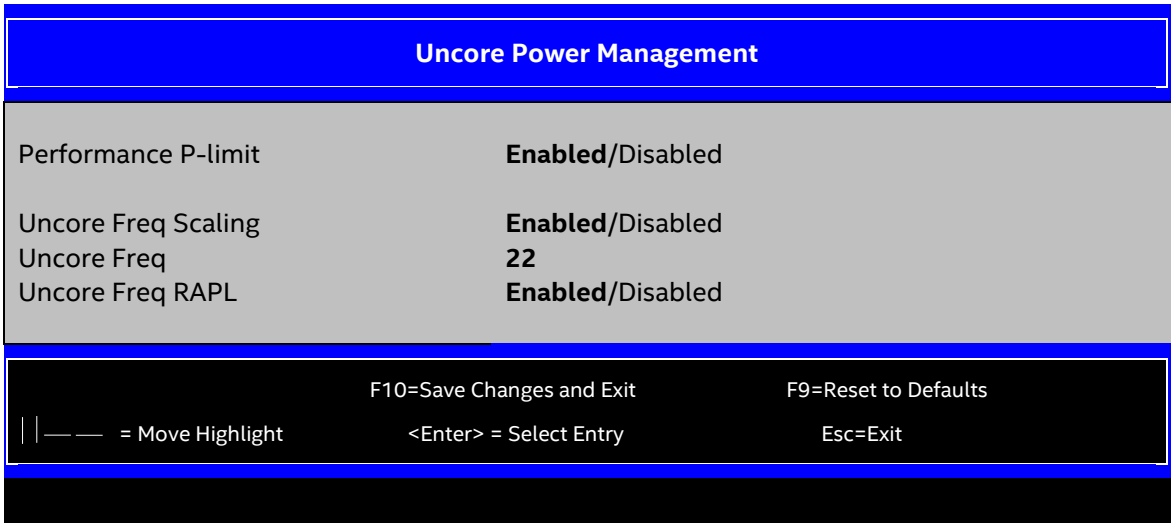


Figure 8. Uncore Power Management Screen

1. **Performance P-limit**

   Value: **Enabled**/Disabled

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

   Comments: This option is visible only if two processors are installed in the system. In a two-socket system, it can be desirable to have the two processors running at similar Uncore frequencies.

   The Performance P-limit feature does this by coordinating the frequency between the two sockets. This measure 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

2. **Uncore Freq Scaling**

   Value: **Enabled**/Disabled

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

   Comments: None.

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

3. **Uncore Freq**

   Value: 8/…/**22**

   Help text: `User input Uncore Frequency override MSR 0x620 MinClrRatio[14:8] & MaxClrRatio[6:0]\n\nIf input value > MAX_CLM_RATIO, then override with MAX_CLM_RATIO\n\nIf input value < MIN_CLM_RATIO, then override with MIN_CLM_RATIO`

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

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

4. **Uncore Freq RAPL**

   Value: **Enabled**/Disabled

   Help text: `Enable: BYPASS_CLM_RAPL_LIMIT = 0\n\nDisable: BYPASS_CLM_RAPL_LIMIT = 1`

   Comments: None.

   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 processors policy that is optimized either for reduced power consumption or for increased performance.

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

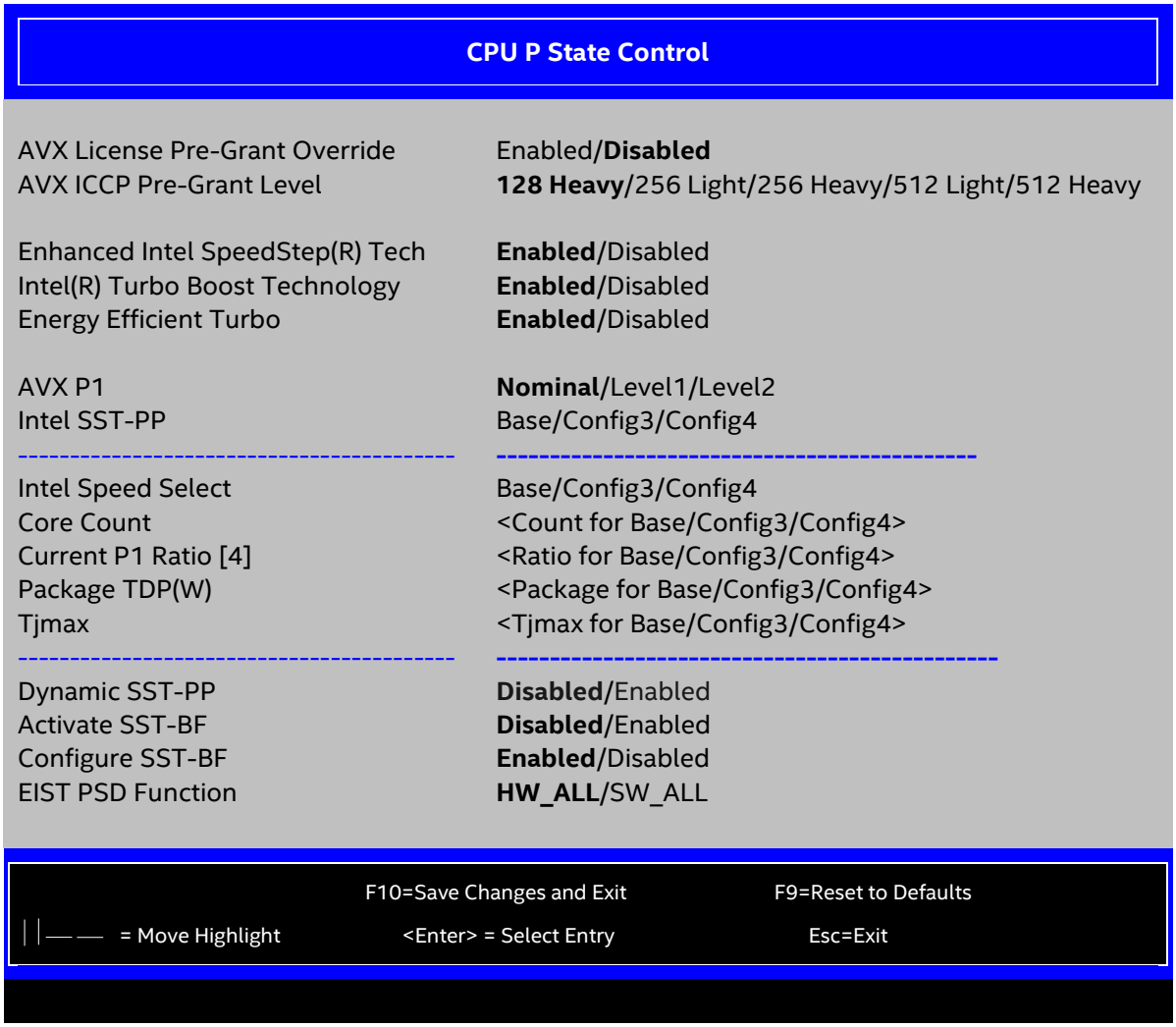


Figure 9. CPU P State Control Screen

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

   Value: Enabled/**Disabled**

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

   Comments: None.

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

2. **AVX ICCP Pre-Grant Level**

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

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

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

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

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

   Value: **Enabled**/Disabled

   Help text: `Enhanced Intel SpeedStep(R) Technology allows the system to dynamically adjust processor voltage and core frequency, which can result in decreased average power consumption and decreased average heat production.`

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

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

   This option is visible only if all the processors installed in the system support Enhanced Intel SpeedStep® Technology. For the Intel® Turbo Boost Technology option to be available, Enhanced Intel SpeedStep® Technology must be enabled.

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

4. **AVX P1**

   Value: **Nominal**/Level1/Level2

   Help text: `AVX P1 level selection.`

   Comments: None.

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

5. **Intel SST-PP**

   Value: **Base**/Config3/Config4

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

   Comments: This option is visible only if Enhanced Intel SpeedStep® Technology is enabled and the CPU supports this feature. If Dynamic SST-PP is enabled, this option gets hidden.

   In Base mode, it emerges Core count/Current P1 Ratio [4]/Package TDP (W).

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

6. **Intel Speed Select**

   Value: Base/Config3/Config4

   Help text: None.

   Comments: *Information Only*.

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

7. **Core Count**

   Value: Core count

   Help text: None.

   Comments: *Information Only*. Core Count shows the core count under each SST-PP mode.

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

8. **Current P1 Ratio [4]**

   Value: Current P1 Ratio [4]

   Help text: None.

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

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

9. **Package TDP(W)**

   Value: Package TDP (W)

   Help text: None.

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

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

10. **Tjmax**

    Value: Tjmax

    Help text: None.

    Comments: *Information Only*. It shows the Tjmax value under each SST-PP mode.

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

11. **Dynamic SST-PP**

    Value: **Disabled/**Enabled

    Help text: `Support Dynamic SST-PP Select.`

    Comments: This option is grayed out if Intel® Speed Select Technology - Performance Profile (Intel® SST-PP) is set to Base. Dynamic SST-PP only changes if Intel® SST-PP is set to Config1/Config2. If this option is enabled, Intel® SST-PP gets hidden in Setup screen.

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

12. **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 item is visible only if all the 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

13. **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: Visible only if all the 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

14. Activate SST-BF

Value: **Disabled**/Enabled

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

Comments: Visible only if the variable related to Prioritized Base Frequency Capable System (PBF Capable System) is not 0.

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

15. Configure SST-BF

Value: **Enabled**/Disabled

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

Comments: Visible only if the variable related to Prioritized Base Frequency Capable System (PBF Capable System) is not 0.

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

16. EIST PSD Function

Value: **HW_ALL**/SW_ALL

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

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

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.

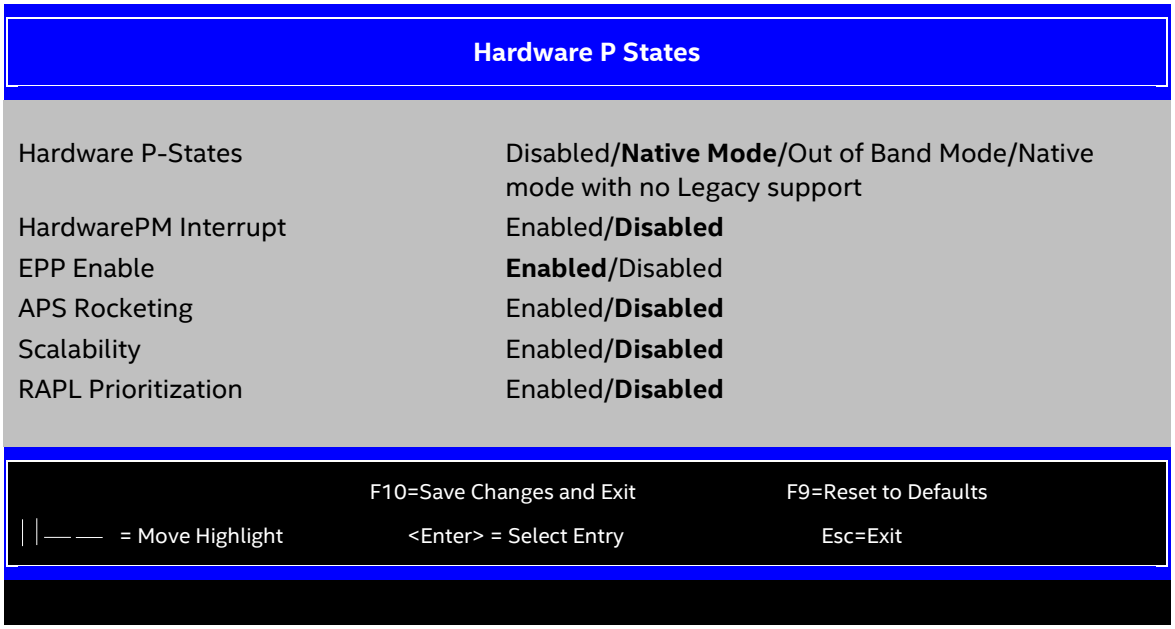


Figure 10. Hardware P States Screen

1. **Hardware P-States**

   Value: Disabled/**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. **HardwarePM Interrupt**

   Value: Enabled/**Disabled**

   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: **Enabled**/Disabled

   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: Enabled/**Disabled**

   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: Enabled/**Disabled**

   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: Enabled/**Disabled**

   Help text: `This knob controls whether RAPL balancer is enabled. When enabled, it activates per core power budgeting.`

   Comments: None.

   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.

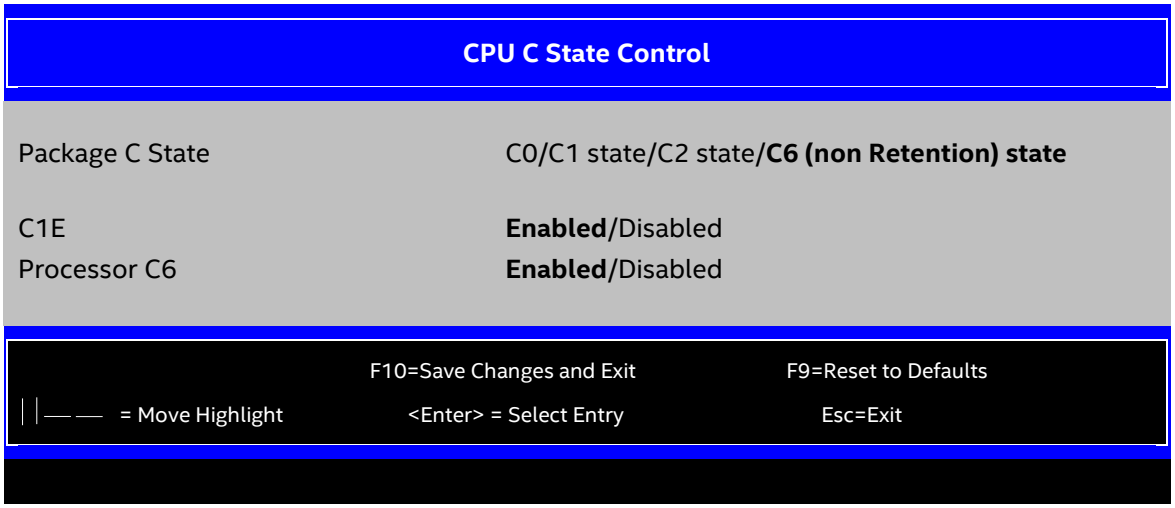


Figure 11. CPU C State Control Screen

1. **Package C State**

   Value: C0/C1 state/C2 state/**C6 (non Retention) state**

   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.

   `C6 retention state` and `No Limit` are hidden for ICX and ICXD.

   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: C1E is normally disabled but it 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: Processor C6 is normally enabled but it 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.

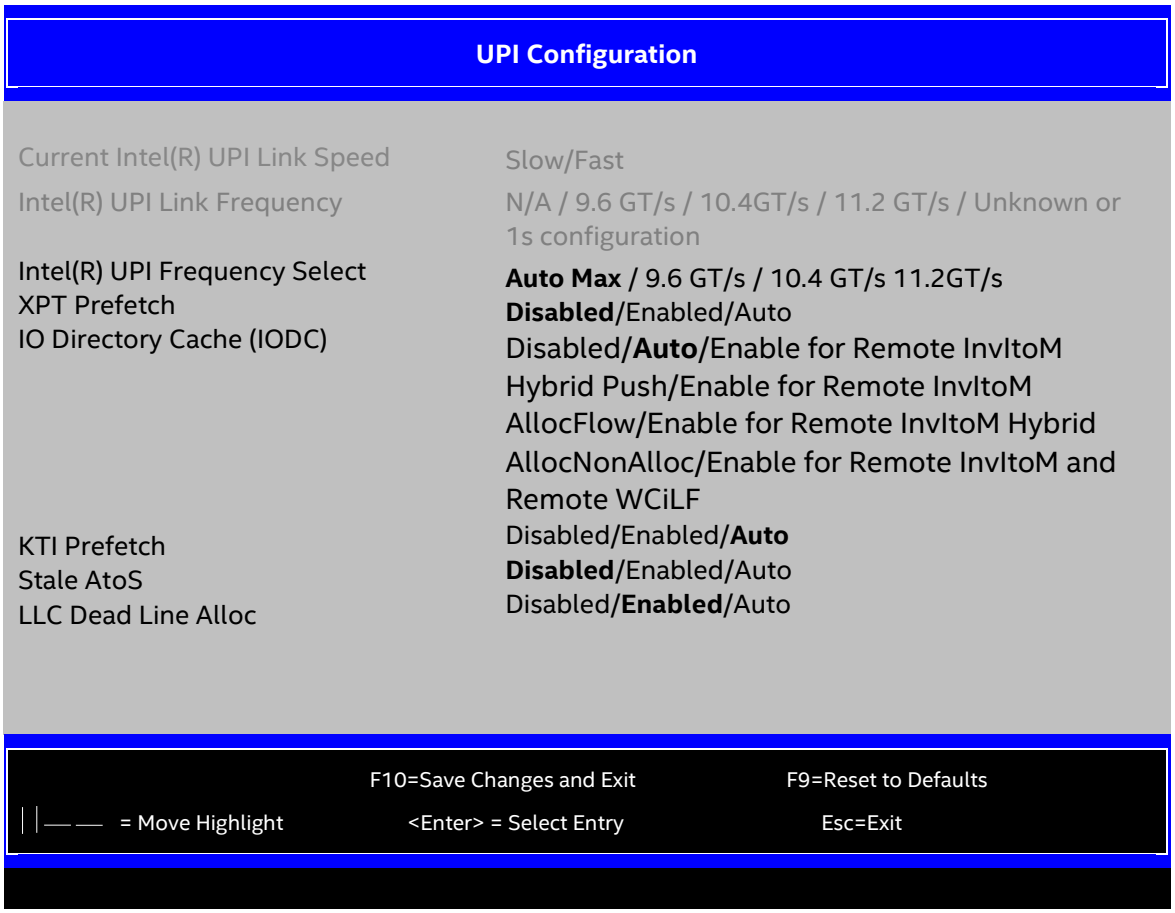


Figure 12. UPI Configuration Screen

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 must 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.

   Intel® UPI Link Speed must 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 / 9.6 GT/s / 10.4GT/s / 11.2 GT/s / Unknown or 1s configuration

   Help text: None.

   Comments: *Information only*. Only ICX CPU can support 11.2 GT/s. 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 /11.2 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: Only ICX CPU can support 11.2 GT/s, so 11.2 GT/s gets hidden with CPX CPU.

   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 and the previous value remains displayed.

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

   Back to: UPI Configuration – Advanced Screen – 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/**Auto**

   Help text: `KTI Prefetch.`

   Comments: None.

   Back to: UPI Configuration – Advanced Screen – Screen Map

7. **Stale AtoS**

   Value: **Disabled**/Enabled/Auto

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

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

   Back to: UPI Configuration – Advanced Screen – Screen Map

8. **LLC Dead Line Alloc**

   Value: Disabled/**Enabled**/Auto

   Help text: `Enable – opportunistically fill dead lines in LLC.`

   `Disable – never fill dead lines in LLC.`

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

   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 Boards D50TNP, M50CYP, and D40AMP, 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 slightly differs 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 can have RAS and performance options if they 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.

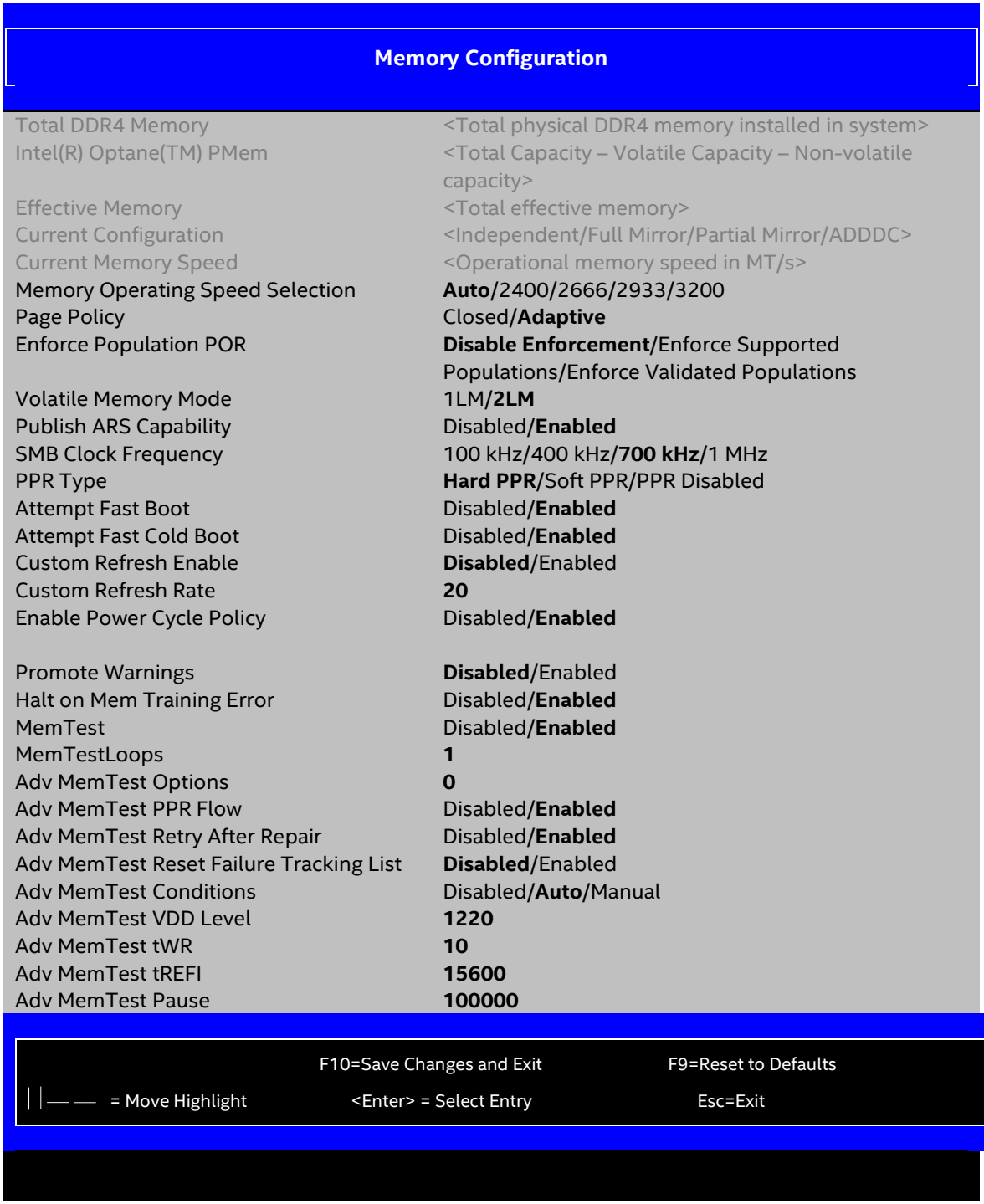


Figure 13. Memory Configuration Screen – Page 1

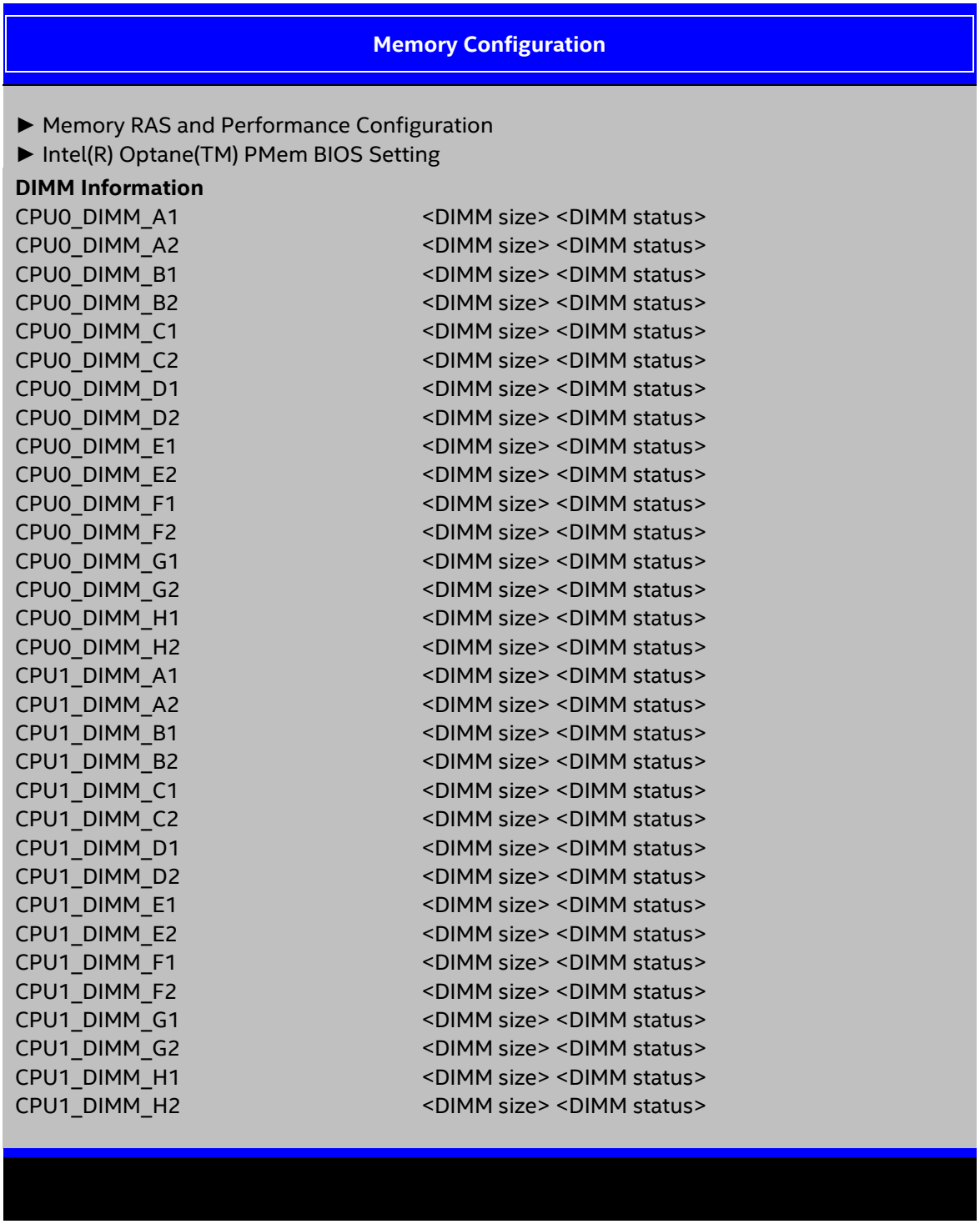


Figure 14. Memory Configuration Screen – Page 2

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 information on Intel® Optane™ PMem.

   Back to: Memory Configuration – Advanced Screen – Screen Map

2. **Intel(R) Optane(TM) PMem**

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

   Help text: None.

   Comments: *Information only*. Displays the current total Intel® Optane™ PMem capacity and volatile/persistent/block partition size. If there is no Intel® Optane™ PMem installed on the system, this message is displayed: `Not Installed`.

   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 operating system in MB or GB.

   The effective memory is the total physical memory minus the sum of all memory reserved for internal usage, RAS redundancy, and system management RAM (SMRAM).

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

   For more information on memory sizing, refer to the *BIOS EPS for Intel® Server Boards D50TNP, M50CYP, and D40AMP*, Section 3.4.8, especially Section 3.4.8.2.

   Back to: Memory Configuration – Advanced Screen – Screen Map

4. **Current Configuration**

   Value: **Independent**/Full Mirror/Partial Mirror/ADDDC

   Help text: None.

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

   - **Independent** – DIMMs are operating in Independent Channel Mode. This is the default configuration when there is no RAS Mode configured.
   - Full Mirror – Full Mirroring RAS Mode is configured and is operational.
   - Partial Mirror – Partial Mirroring RAS Mode is configured and is operational.
   - ADDDC – ADDDC mode is 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 2400 MT/s, 2666 MT/s, 2933 MT/s, and 3200 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**/2400/2666/2933/3200

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

   Comments: Allows the user to select a specific speed for the memory to operate. Only legitimate speeds 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 that is consistent with the installed DIMMs and processors.

   Back to: Memory Configuration – Advanced Screen – Screen Map

7. **Page Policy**

   Value: Closed/**Adaptive**

   Help text: `Select Page Policy.`

   Comments: None.

   Back to: Memory Configuration – Advanced Screen – Screen Map

8. **Enforce Population POR**

   Value: **Disable Enforcement**/Enforce Supported Populations/Enforce Validated Populations.

   Help text: `Enable Memory Population POR Enforcement. Selecting Enforce Validated Populations will only allow populations that have been validated.`

   Comments: When Disable Enforcement is selected, the Unified Extensible Firmware Interface (UEFI) must completely bypass this feature and proceed to memory decode without any additional population restrictions.

   When Enforce Supported Populations is selected, the UEFI must compare the current DIMM/PMem population against all configurations in the provided POR spreadsheet. When Enforce Validated Populations is selected, it must compare only against the configurations specified in the spreadsheet as validated. An error code record as memory population error shows in the setup Error Manager and logs to the system event log (BMC SEL).

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

   Back to: Memory Configuration – Advanced Screen – Screen Map

9. **Volatile Memory Mode**

   Value: 1LM/**2LM**

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

   Comments: None.

   Back to: Memory Configuration – Advanced Screen – Screen Map

10. Publish ARS Capability

Value: Disabled/**Enabled**

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

Comments: None.

Back to: Memory Configuration – Advanced Screen – Screen Map

11. SMB Clock Frequency

Value: 100 kHz/400 kHz/**700 kHz**/1 MHz

Help text: `Sets DDR4 SMBus Clock Frequencies For SPD Access. Current default is 700Khz.`

`Note: If Intel(R) Optane(TM) PMem is present, SMBus Clock Frequency is restricted to 400Khz regardless of this setting.`

Comments: None.

Back to: Memory Configuration – Advanced Screen – Screen Map

12. PPR Type

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

Help text: `Selects Post Package Repair Type - Hard / Soft / Disabled.`

Comments: None.

Back to: Memory Configuration – Advanced Screen – Screen Map

13. Attempt Fast Boot

Value: Disabled/**Enabled**

Help text: `Enable - Portions of memory reference code will be skipped when possible to increase boot speed on warm boots. Disable - Disables this feature. Auto - Sets it to the MRC default setting; current default is Enabled.`

Comments: None.

Back to: Memory Configuration – Advanced Screen – Screen Map

14. Attempt Fast Cold Boot

Value: Disabled/**Enabled**

Help text: `Enable - Portions of memory reference code will be skipped when possible to increase boot speed on cold boots. Disable - Disables this feature. Auto - Sets it to the MRC default setting; current default is Enabled.`

Comments: None.

Back to: Memory Configuration – Advanced Screen – Screen Map

15. Custom Refresh Enable

Value: **Disabled**/Enabled

Help text: `Enable/Disable a custom memory refresh rate.`

Comments: None.

Back to: Memory Configuration – Advanced Screen – Screen Map

16. Custom Refresh Rate

Value: **20**/.../80

Help text: `Refresh Rate in 0.1x units of the standard 7.8 usec interval. Valid range is 20 to 80 (i.e. 2x to 8x).`

Comments: This item will be displayed when customer refresh enable is enabled.

Back to: Memory Configuration – Advanced Screen – Screen Map

17. Enable Power Cycle Policy

Value: Disabled/**Enabled**

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

Comments: None.

Back to: Memory Configuration – Advanced Screen – Screen Map

18. Promote Warnings

Value: **Disabled**/Enabled

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

Comments: None.

Back to: Memory Configuration – Advanced Screen – Screen Map

19. Halt on Mem Training Error

Value: Disabled/**Enabled**

Help text: `Halt on Mem Training Error Disable/Enable.`

Comments: None.

Back to: Memory Configuration – Advanced Screen – Screen Map

20. MemTest

Value: Disabled/**Enabled**

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

Comments: None.

Back to: Memory Configuration – Advanced Screen – Screen Map

21. MemTest Loops

Value: 0/**1**/..../65535

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

Comments: None.

Back to: Memory Configuration – Advanced Screen – Screen Map

22. Adv MemTest Options

Value: **0**/1/..../4194303

Help text: `This option is a bit mask[21:0]: All 0 = disabled: bit-0=XMATS8, bit-1=XMATS16, bit-2=XMATS32, bit-3=XMATS64, bit-4=WCMATS8, bit-5=WCMCH8, bit-6=GNDB64, bit-7=MARCHCM64, bits[8:10]=Reserved, bit-11=TWR, bit-12=DATARET, bit-13=MATS8TC1, bit-14=MATS8TC2, bit-15=MATS8TC3, bit-16=SK-HYNIX, bit-17=SAMSUNG, bit-18=MICRON, bit-19=SCRAM_X2, bit-20=SAMSUNG2, bit-21=NANYA.`

Comments: None.

Back to: Memory Configuration – Advanced Screen – Screen Map

23. Adv MemTest PPR Flow

Value: Disabled/**Enabled**

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

Comments: None.

Back to: Memory Configuration – Advanced Screen – Screen Map

24. Adv MemTest Retry After Repair

Value: Disabled/**Enabled**

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

Comments: None.

Back to: Memory Configuration – Advanced Screen – Screen Map

25. Adv MemTest Reset Failure Tracking List

Value: **Disabled**/Enabled

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

Comments: None.

Back to: Memory Configuration – Advanced Screen – Screen Map

26. Adv MemTest Conditions

Value: Disabled/**Auto**/Manual

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

Comments: None.

Back to: Memory Configuration – Advanced Screen – Screen Map

27. Adv MemTest VDD Level

Value: 1080/.../**1220**/.../1320

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

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

Back to: Memory Configuration – Advanced Screen – Screen Map

28. Adv MemTest tWR

Value: **10**/.../26

Help text: `Specify tWR timing in units of tCK.`

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

Back to: Memory Configuration – Advanced Screen – Screen Map

29. Adv MemTest tREFI

Value: 3900/.../**15600**/.../32767

Help text: `Specify tREFI (refresh rate) timing in units of tCK.`

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

Back to: Memory Configuration – Advanced Screen – Screen Map

30. Adv MemTest Pause

Value: 0/.../**100000**/.../512000

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

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

Back to: Memory Configuration – Advanced Screen – Screen Map

31. Memory RAS and Performance Configuration

Value: None.

Help text: `View/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

32. Intel(R) Optane(TM) PMem BIOS Setting

Value: None.

Help text: `View/Configure Intel(R) Optane(TM) persistent memory information and BIOS settings.`

Comments: *Selection only*. For more information on BIOS settings for Intel® Optane™ PMem, see Section 3.3.4.2.

Back to: Memory Configuration – Advanced Screen – Screen Map

33. DIMM Information

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

Value: <DIMM size><DIMM status>

Help text: None.

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

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

- Installed & Mapped out – There is a DDR4 DIMM installed and mapped out in this slot.
- 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 in the Installed & Operational state, the DIMM size in GB of that DIMM is displayed. This value represents the physical size of the DIMM, regardless of how it is counted in the effective memory size.

Notes:

For DIMM_XY, X denotes the channel identifier A-P, while 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 number depends on the board features.

If the DIMM is a PMem, 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 PMem devices.

The BIOS setup utility displays DIMM size - `xx GB value` by truncating decimal value. For example: 491.7 GB is displayed in the BIOS setup utility as 491 GB.

The Intel® Server Boards D50TNP, M50CYP, and D40AMP can have DIMMs A1 and A2 to L1 and L2 (maximum two CPUs, six channels, two DPC). Each project can have a different DIMM slot topology, this document just gives a general design. The user must adjust per the DIMM schematic to tune.

For details about different board configurations, refer to *the BIOS EPS for Intel® Server Boards D50TNP, M50CYP, and D40AMP*, Sections 3.4.4.1 and 12.

Back to: Memory Configuration – Advanced Screen – Screen Map

3.3.4.1 Memory RAS and Performance Configuration

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

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

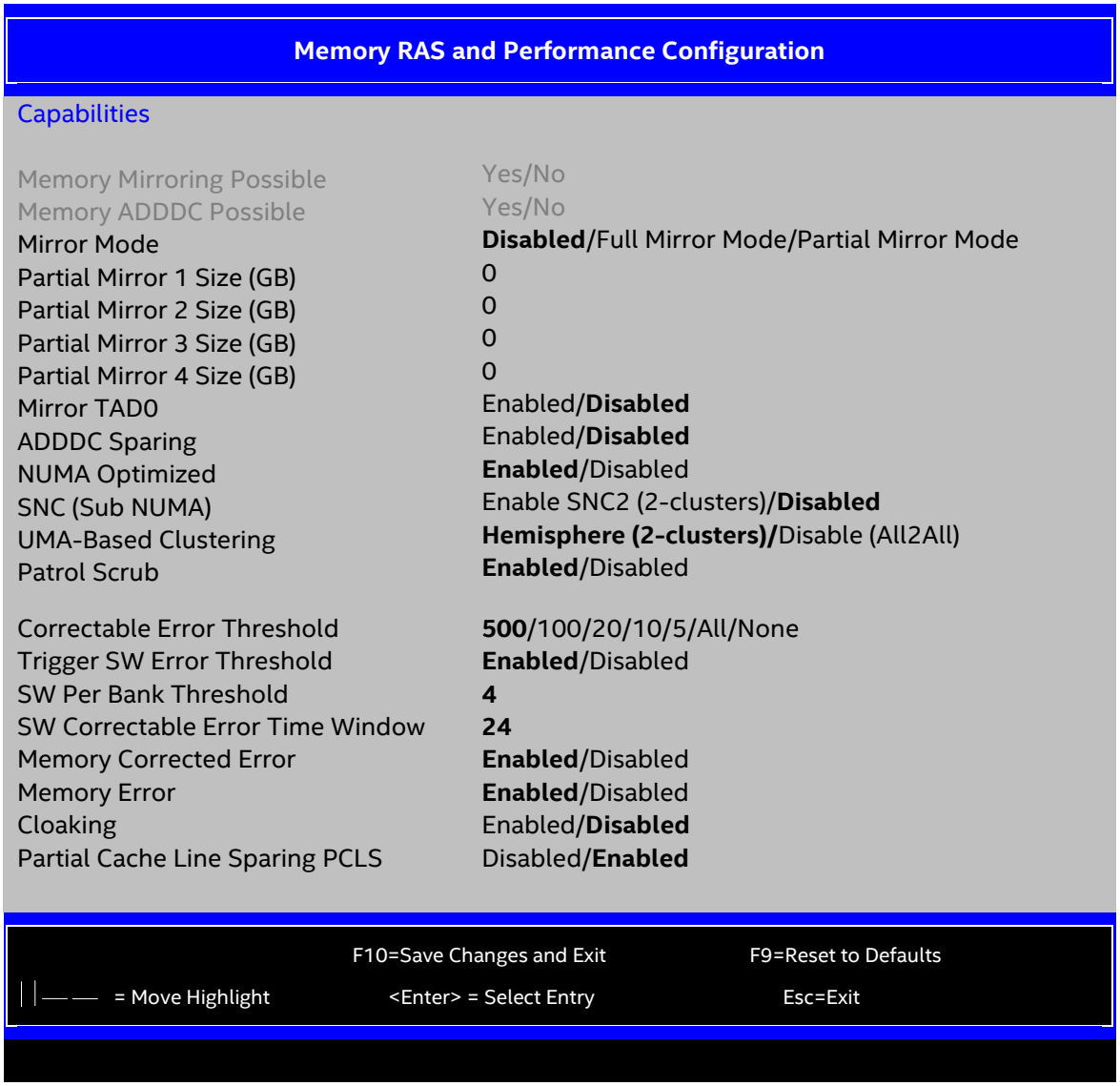


Figure 15. Memory RAS and Performance Configuration Screen

1. **Memory Mirroring Possible**

   Value: Yes/No

   Help text: None.

   Comments: *Information only.* Displays whether the current DIMM configuration can perform memory mirroring. For memory mirroring to be possible, DIMM configurations on all the paired channels must be identical between the channel pair (Mirroring Domain).

   For details about mirroring configurations, refer to the *BIOS EPS for Intel® Server Boards D50TNP, M50CYP, and D40AMP*, Section 3.4.3 and Section 3.4.4.

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

2. **Memory ADDDC Possible**

   Value: Yes/No

   Help text: None.

   Comments: *Information only.* Displays whether the current DIMM configuration can perform 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

3. **Mirror Mode**

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

   Help text: `Allows the user to select the Mirror Mode to be applied for the next boot.`

   Comments: This setting is shown when the current CPU supports mirror mode, the DIMM population meets mirror requirements, and no spare or lockstep is enabled. This item is grayed out when Intel® Software Guard Extensions (Intel® SGX) is enabled.

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

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

   Value: **0**

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

   Comments: Must set Mirror Mode to Partial Mirror Mode at first. This knob will be hidden when the OS requests the mirroring region with the methods.

   Note: Once OS requests the mirroring region, Clear CMOS is needed to make the request from OS to BIOS.

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

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

   Value: **0**

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

   Comments: Must set Mirror Mode to Partial Mirror Mode at first. This knob will be hidden when the OS requests the mirroring region with the methods.

   Note: Once OS requests the mirroring region, Clear CMOS is needed to make the request from OS to BIOS.

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

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

   Value: **0**

   Help text: `Allows the user to select the Mirror Mode to be applied for the next boot.`

   Comments: Must set Mirror Mode to Partial Mirror Mode at first. This knob will be hidden when the OS requests the mirroring region with the methods.

   Note: Once OS requests the mirroring region, Clear CMOS is needed to make the request from OS to BIOS.

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

7. **Partial Mirror 4 Size (GB)**

   Value: **0**

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

   Comments: Must set Mirror Mode to Partial Mirror Mode at first. This knob will be hidden when the OS requests the mirroring region with the methods.

   Note: Once OS requests the mirroring region, Clear CMOS is needed to make the request from OS to BIOS.

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

8. **Mirror TAD0**

   Value: Enabled/**Disabled**

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

   Comments: This setting is shown when the current CPU supports mirror mode, the DIMM population meets mirror requirements, and no spare or lockstep is enabled. This item is grayed out when Intel® Software Guard Extensions (Intel® SGX) is enabled. This knob will not be effective when the OS requests the mirroring region with the methods.

Note: Once OS requests the mirroring region, Clear CMOS is needed to make the request from OS to BIOS.

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

9. ADDDC Sparing

Value: Enabled/**Disabled**

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

Comments: This setting is hidden if x8 data width DIMMs are installed or if mirror mode or mirror TAD0 or memory sparing are not disabled. This setting is grayed out when Intel® SGX is enabled.

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

10. NUMA Optimized

Value: **Enabled**/Disabled

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

Comments: This option is hidden only for boards that have just one SNC-incapable socket installed.

When enabled, the SRAT and SLIT ACPI tables are provided, showing the locality of systems resources, especially memory.

This information allows a NUMA Aware operating system to optimize the processor threads used by processes that can benefit by having the best access to those resources.

For more information, refer to the *BIOS EPS for Intel® Server Boards D50TNP, M50CYP, and D40AMP*, Section 3.4.4.6.

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

11. SNC (Sub NUMA)

Value: ICX: Enable SNC2 (2-clusters)/**Disabled**

Help text: `SNC disable will support 1-cluster (XPT/KTI Prefetch enable) 4-IMC way interleave. SNC2 Enable supports 2-clusters SNC and 2-way IMC interleave. Enable SNC2 will gray out UmaBasedClustering knob.`

Comments: This feature is similar to COD on previous generations. It produces more NUMA objects under ACPI. The major difference is that SNC LLC is unified, and COD LLC is separated.

SNC (Sub NUMA) enables the two-cluster SNC. Two-way interleave of IMC Interleaving focuses to one cluster.

If there are DIMMs on both MCs, SNC (Sub NUMA) enables the SNC and sets one-way interleave. This action enables SNC2 (two clusters).

SNC4 removes from ICX POR. And when CPU available core number is less than 12, this item is grayed out.

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

12. UMA-Based Clustering

Value: **Hemisphere (2-clusters)**/Disable (All2All)

Help text: `UMA Based Clustering options include Disable (ALL2ALL), Hemisphere (2-cluster), and Quadrant (4 cluster, not supported on ICX). These options are only valid when SNC is disabled. If SNC is enabled, UMA-Based Clustering is automatically disabled by BIOS.`

Comments: When UMA-Based Clustering is disabled and TME is enabled, Intel® SGX setup can be enabled.

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

13. 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) it encounters. To correct those ECC errors, Patrol Scrub writes back the corrected data to memory.

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

14. Correctable Error Threshold

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

Help text: `Threshold value for logging Correctable Errors (CE) - Threshold of 500 (default) logs 500th CE, "All" logs every CE, and "None" means no CE logging.`

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 item is also the CE threshold used when Rank Sparing RAS Mode is configured.

When a CE threshold crossing occurs in Rank Sparing Mode on a channel that is in the redundant state, it causes a sparing failover (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

15. Trigger SW Error Threshold

Value: **Enabled**/Disabled

Help text: `Enable or Disable Sparing trigger SW Error Match Threshold`

Comments: None.

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

16. SW Per Bank Threshold

Value: **4**

Help text: `SW Per Bank Correctable Error Threshold (1 - 0x7FFF) used for bank level information`

Comments: This option appears only when Trigger SW Error Threshold is enabled.

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

17. SW Correctable Error Time Window

Value: **24**

Help text: `SW Correctable Error time window based interface in Hour (0 – 24)`

Comments: This option appears only when Trigger SW Error Threshold is enabled. Value 0 means disabled which no time window function.

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

18. Memory Corrected Error

Value: **Enabled**/Disabled

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

Comments: None.

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

19. Memory Error

Value: **Enabled**/Disabled

Help text: `Enable/Disable Memory Error.`

Comments: None.

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

20. Cloaking

Value: Enabled/**Disabled**

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

Comments: None.

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

21. Partial Cache Line Sparing PCLS

Value: Disabled/**Enabled**

Help text: `Enable/Disable PCLS Sparing.`

Comments: None.

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

3.3.4.2 Intel(R) Optane(TM) PMem BIOS Setting

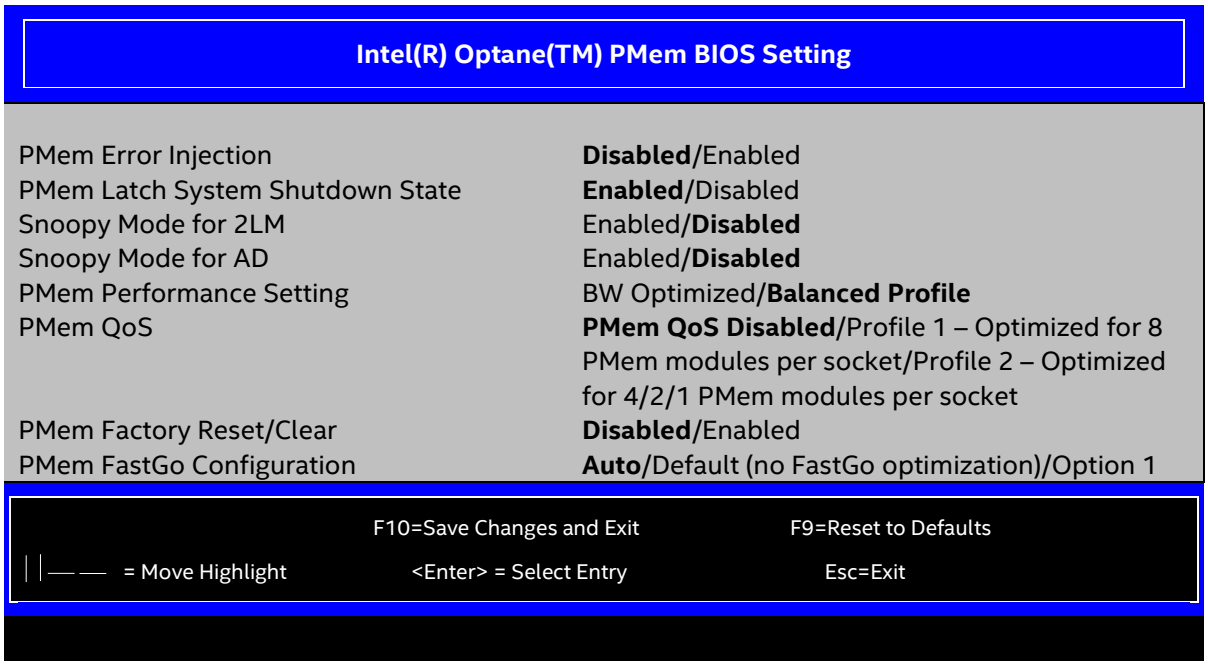


Figure 16. Intel® Optane™ PMem BIOS Setting Screen

1. **PMem Error Injection**

Value: **Disabled**/Enabled

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

Comments: None.

Back to: Intel(R) Optane(TM) PMem BIOS Setting – Memory Configuration – Advanced Screen – Screen Map

2. **PMem Latch System Shutdown State**

Value: Disabled/**Enabled**

Help text: `Latch System Shutdown State.`

Comments: None.

Back to: Intel(R) Optane(TM) PMem BIOS Setting – Memory Configuration – Advanced Screen – Screen Map

3. **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: Intel(R) Optane(TM) PMem BIOS Setting – Memory Configuration – Advanced Screen – Screen Map

4. Snoopy Mode for AD

Value: **Disabled**/Enabled

Help text: `Enables new AD specific feature to avoid directory updates to PMem memory from non-NUMA optimized workloads.`

Comments: None.

Back to: Intel(R) Optane(TM) PMem BIOS Setting – Memory Configuration – Advanced Screen – Screen Map

5. PMem Performance Setting

Value: BW Optimized/**Balanced Profile**

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

Comments: Balanced Profile (Default): Is optimized for Memory mode by allowing the controller to switch more often between DRAM and Intel® Optane™ PMem so that eviction transactions in DRAM can execute faster. BW Optimized: Arbitrates between DRAM and Intel® Optane™ PMem to maximize DRAM bandwidth on the memory bus.

Back to: Intel(R) Optane(TM) PMem BIOS Setting – Memory Configuration – Advanced Screen – Screen Map

6. PMem QoS

Value: **PMem QoS Disabled**/Profile 1 – Optimized for 8 PMem modules per socket/ Profile 2 – Optimized for 4/2/1 PMem modules per socket.

Help text: `Prevents DDR4 BW drop in presence of concurrent DDRT BW.`

Comments: If no Intel® Optane™ PMem DIMM is installed, this item gets hidden.

Back to: Intel(R) Optane(TM) PMem BIOS Setting – Memory Configuration – Advanced Screen – Screen Map

7. PMem Factory Reset/Clear

Value: **Disabled**/Enabled

Help text: `Enable\Disable Factory Reset/Clear.`

Comments: None.

Back to: Intel(R) Optane(TM) PMem BIOS Setting – Memory Configuration – Advanced Screen – Screen Map

8. PMem FastGo Configuration

Value: **Auto**/Default (no FastGo optimization)/Option 1

Help text: `Select PMem QoS Configuration Profiles.`

Comments: None.

Back to: Intel(R) Optane(TM) PMem BIOS Setting – Memory Configuration – Advanced Screen – Screen Map

3.3.5 System Event Log

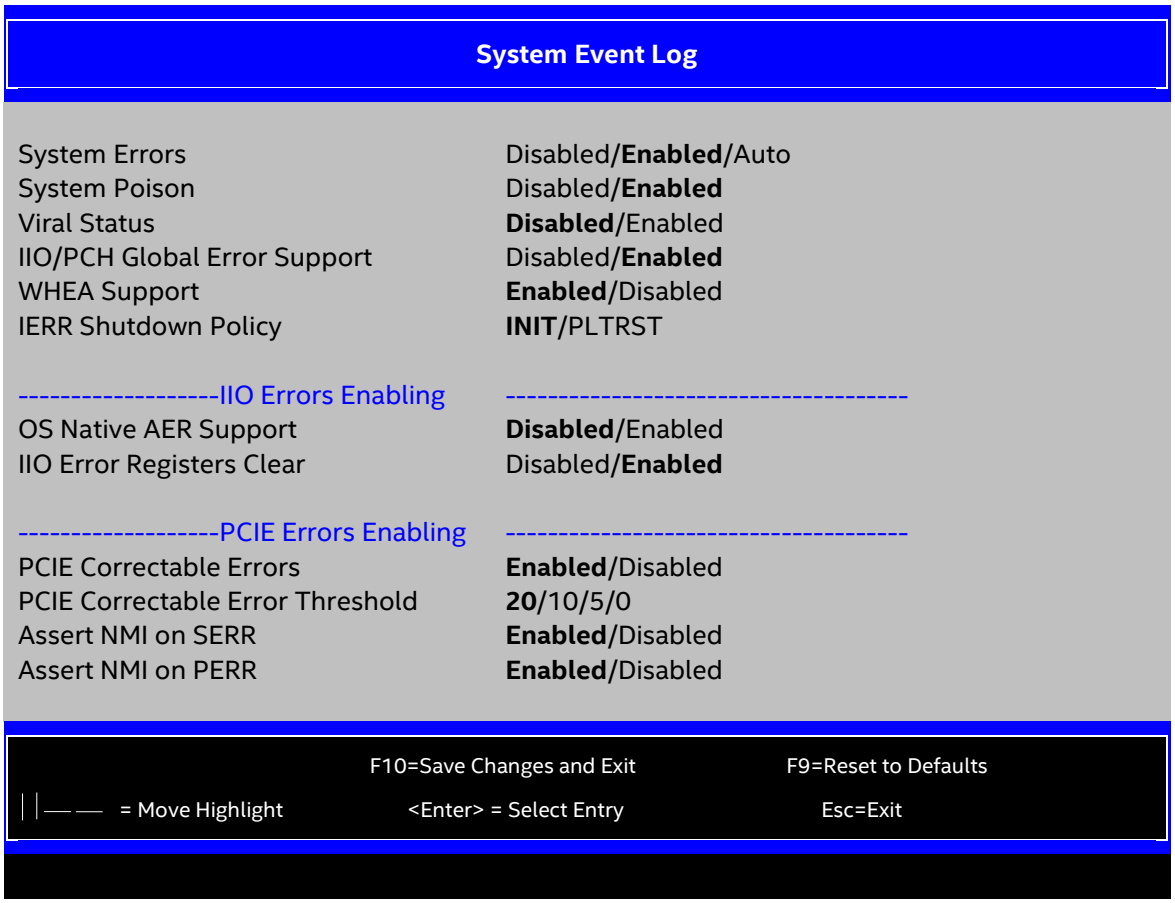


Figure 17. System Event Log Screen

1. **System Errors**

   Value: Disabled/**Enabled**/Auto

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

   Comments: None.

   Back to: System Event Log – Advanced Screen – Screen Map

2. **System Poison**

   Value: Disabled/**Enabled**

   Help text: `Enable/Disable System Poison.`

   Comments: This item gets hidden if System Errors is set to Disabled or Auto. If SGX is enabled, System Poison gets grayed out. If this item is disabled, Poisoned TLP Received error and Poisoned TLP Egress Blocked error will be masked and not reported.

   Back to: System Event Log – Advanced Screen – Screen Map

3. **Viral Status**

   Value: **Disabled**/Enabled

   Help text: `Enable/Disable Viral.`

   Comments: Viral Status is grayed out when System Poison is disabled, or System Errors is set to Disabled or Auto.

   Back to: System Event Log – Advanced Screen – Screen Map

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

   Value: Disabled/**Enabled**

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

   Comments: This item gets hidden when System Errors is set to Disabled or Auto.

   Back to: System Event Log – Advanced Screen – Screen Map

5. **WHEA Support**

   Value: **Enabled**/Disabled

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

   Comments: None.

   Back to: System Event Log – Advanced Screen – Screen Map

6. **IERR Shutdown Policy**

   Value: **INIT**/PLTRST

   Help text: `Allows to configure Shutdown Policy Select in General Interrupt Register. Available modes are INIT and PLTRST.`

   Comments: None.

   Back to: System Event Log – Advanced Screen – Screen Map

7. **OS Native AER Support**

   Value: **Disabled**/Enabled

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

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

   Back to: System Event Log – Advanced Screen – Screen Map

8. **IIO Error Registers Clear**

   Value: Disabled/**Enabled**

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

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

   Back to: System Event Log – Advanced Screen – Screen Map

9. **PCIE Correctable Errors**

   Value: **Enabled/**Disabled

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

   `[Disabled] - Processor & PCH PCIe correctable error logging is disabled.`

   Comments: None.

   Back to: System Event Log – Advanced Screen – Screen Map

10. **PCIE Correctable Error Threshold**

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

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

    Comments: None.

    Back to: System Event Log – Advanced Screen – Screen Map

11. **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: None.

    Back to: System Event Log – Advanced Screen – Screen Map

12. **Assert NMI on PERR**

    Value: **Enabled**/Disabled

    Help text: `On PERR, generate an NMI and log an error.`

    `Note: This option is only active if the Assert NMI on SERR option has [Enabled] selected.`

    Comments: None.

    Back to: System Event Log – Advanced Screen – Screen Map

3.3.6 Integrated I/O Configuration

The Integrated I/O Configuration screen allows the user to configure the Integrated I/O used for onboard devices inside the processors.

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

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

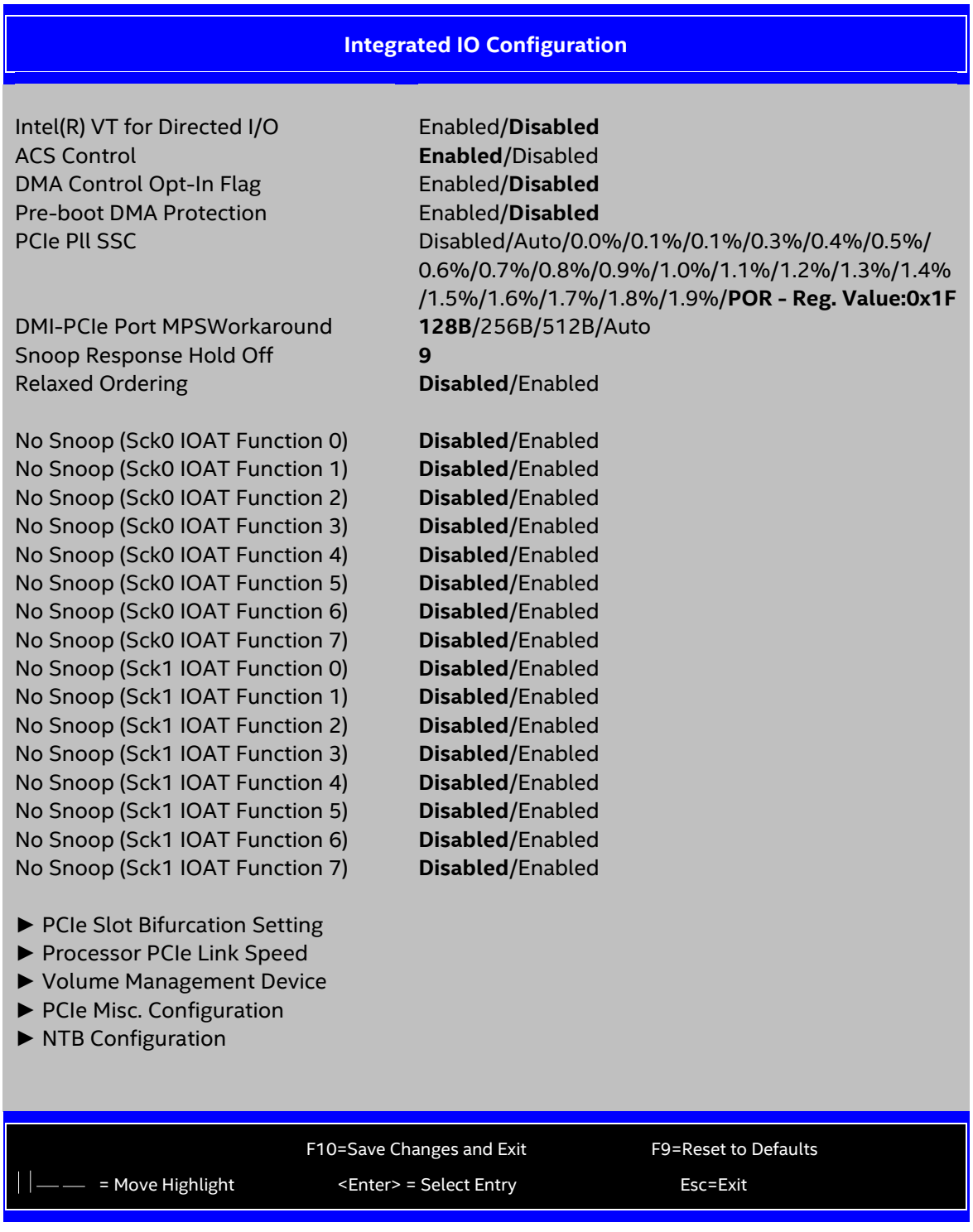


Figure 18. Integrated I/O Configuration Screen

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

   Value: Enabled/**Disabled**

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

   `Report the I/O device assignment to VMM through DMAR ACPI Tables.`

   Comments: This option is visible only if all the processors installed in the system support Intel® VT-d. The software configuration installed in the system must support this feature so it can be enabled.

   Note: Limit CPU PA to 46-bits setup knob must be enabled before enabling this function to boot to 2019 Windows* operating system. When booting to 2020H1 operating system, there is no need to enable Limit CPU PA to 46-bits setup knob. When VT-d is changed from enabled to disabled, X2APIC also need to be disabled if it is enabled.

   Back to: Integrated I/O Configuration – Advanced Screen – Screen Map

2. **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 appears only when Intel® VT-d is enabled.

   Back to: Integrated I/O Configuration – Advanced Screen – Screen Map

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

   Value: Enabled/**Disabled**

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

   Comments: This option is grayed out when Intel® VT-d is disabled.

   Back to: Integrated I/O Configuration – Advanced Screen – Screen Map

4. **Pre-boot DMA Protection**

   Value: Enabled/**Disabled**

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

   Comments: This option appears only when Intel® VT-d is enabled. The Pre-boot DMA protection is not supported with NVMe by VROC UEFI driver when it is enabled.

   Back to: Integrated I/O Configuration – Advanced Screen – Screen Map

5. **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 I/O Configuration – Advanced Screen – Screen Map

6. **DMI-PCIe Port MPSWorkaround**

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

   Help text: `Set Maxpayload size to 256B if possible.`

   Comments: None.

   Back to: Integrated I/O Configuration – Advanced Screen – Screen Map

7. **Snoop Response Hold Off**

   Value: **9**

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

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

   Back to: Integrated I/O Configuration – Advanced Screen – Screen Map

8. **Relaxed Ordering**

   Value: **Disabled**/Enabled

   Help text: `Relaxed Ordering Enable/Disable.`

   Comments: None.

   Back to: Integrated I/O Configuration – Advanced Screen – Screen Map

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

   Value: **Disabled**/Enabled

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

   Comments: None.

   Back to: Integrated I/O Configuration – Advanced Screen – Screen Map

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

    Value: **Disabled**/Enabled

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

    Comments: None.

    Back to: Integrated I/O Configuration – Advanced Screen – Screen Map

11. **No Snoop (Sck0 IOAT Function 2)**

    Value: **Disabled**/Enabled

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

    Comments: None.

    Back to: Integrated I/O Configuration – Advanced Screen – Screen Map

12. No Snoop (Sck0 IOAT Function 3)

Value: **Disabled**/Enabled

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

Comments: None.

Back to: Integrated I/O Configuration – Advanced Screen – Screen Map

13. No Snoop (Sck0 IOAT Function 4)

Value: **Disabled**/Enabled

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

Comments: None.

Back to: Integrated I/O Configuration – Advanced Screen – Screen Map

14. No Snoop (Sck0 IOAT Function 5)

Value: **Disabled**/Enabled

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

Comments: None.

Back to: Integrated I/O Configuration – Advanced Screen – Screen Map

15. No Snoop (Sck0 IOAT Function 6)

Value: **Disabled**/Enabled

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

Comments: None.

Back to: Integrated I/O Configuration – Advanced Screen – Screen Map

16. No Snoop (Sck0 IOAT Function 7)

Value: **Disabled**/Enabled

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

Comments: None.

Back to: Integrated I/O Configuration – Advanced Screen – Screen Map

17. No Snoop (Sck1 IOAT Function 0)

Value: **Disabled**/Enabled

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

Comments: None.

Back to: Integrated I/O Configuration – Advanced Screen – Screen Map

18. No Snoop (Sck1 IOAT Function 1)

Value: **Disabled**/Enabled

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

Comments: None.

Back to: Integrated I/O Configuration – Advanced Screen – Screen Map

19. No Snoop (Sck1 IOAT Function 2)

Value: **Disabled**/Enabled

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

Comments: None.

Back to: Integrated I/O Configuration – Advanced Screen – Screen Map

20. No Snoop (Sck1 IOAT Function 3)

Value: **Disabled**/Enabled

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

Comments: None.

Back to: Integrated I/O Configuration – Advanced Screen – Screen Map

21. No Snoop (Sck1 IOAT Function 4)

Value: **Disabled**/Enabled

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

Comments: None.

Back to: Integrated I/O Configuration – Advanced Screen – Screen Map

22. No Snoop (Sck1 IOAT Function 5)

Value: **Disabled**/Enabled

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

Comments: None.

Back to: Integrated I/O Configuration – Advanced Screen – Screen Map

23. No Snoop (Sck1 IOAT Function 6)

Value: **Disabled**/Enabled

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

Comments: None.

Back to: Integrated I/O Configuration – Advanced Screen – Screen Map

24. No Snoop (Sck1 IOAT Function 7)

Value: **Disabled**/Enabled

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

Comments: None.

Back to: Integrated I/O Configuration – Advanced Screen – Screen Map

25. PCIe Slot Bifurcation Setting

Value: None.

Help text: `View/Configure PCIe Slot Bifurcation setting.`

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

Note: This configuration page is only visible on the Intel® Server Boards D50TNP, M50CYP, and D40AMP.

Back to: Integrated I/O Configuration – Advanced Screen – Screen Map

26. Processor PCIe Link Speed

Value: None.

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

Comments: *Selection only*. For more information on Processor PCIe* Link Speed, see Section 3.3.6.2.

Back to: Integrated I/O Configuration – Advanced Screen – Screen Map

27. 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, see Section 3.3.6.3.

Back to: Integrated I/O Configuration – Advanced Screen – Screen Map

28. PCIe Misc. Configuration

Value: None.

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

Comments: *Selection only*. For more information on PCIe* miscellaneous configuration, see Section 3.3.6.4.

Back to: Integrated I/O Configuration – Advanced Screen – Screen Map

29. NTB Configuration

Value: None.

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

Comments: *Selection only*. For more information on NTB Configuration, see Section 3.3.6.4.

Back to: Integrated I/O Configuration – Advanced Screen – Screen Map

3.3.6.1 PCIe* Slot Bifurcation Setting

Each board from the Intel® Server Boards D50TNP, M50CYP, and D40AMP have different risers and options for PCIe* Slot Bifurcation.

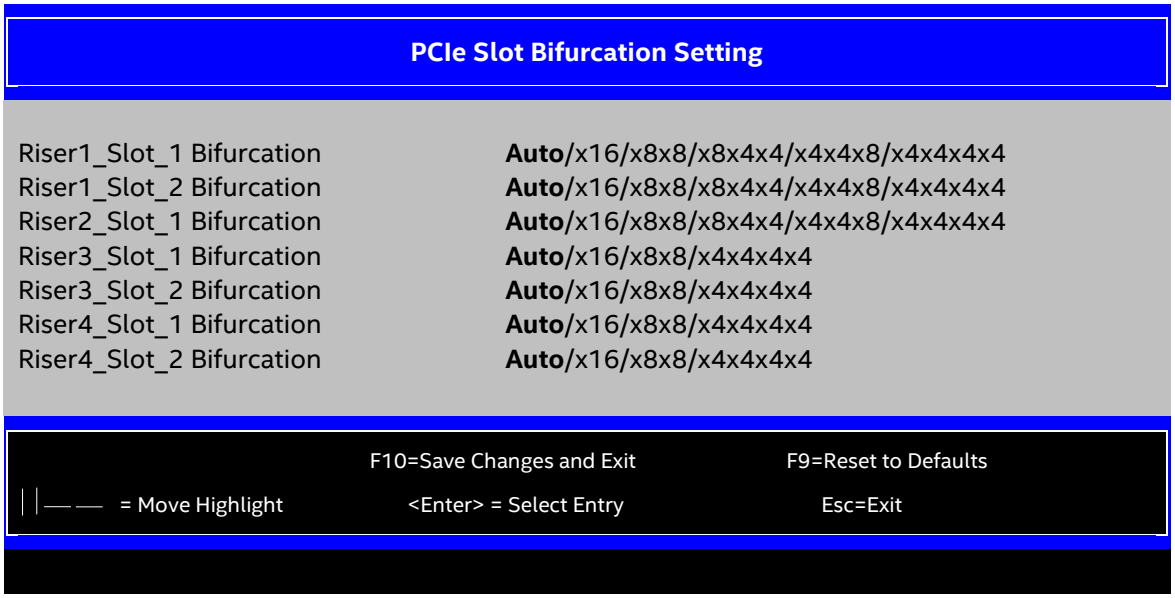


Figure 19. PCIe* Slot Bifurcation Setting Screen – Intel® Server Board D50TNP

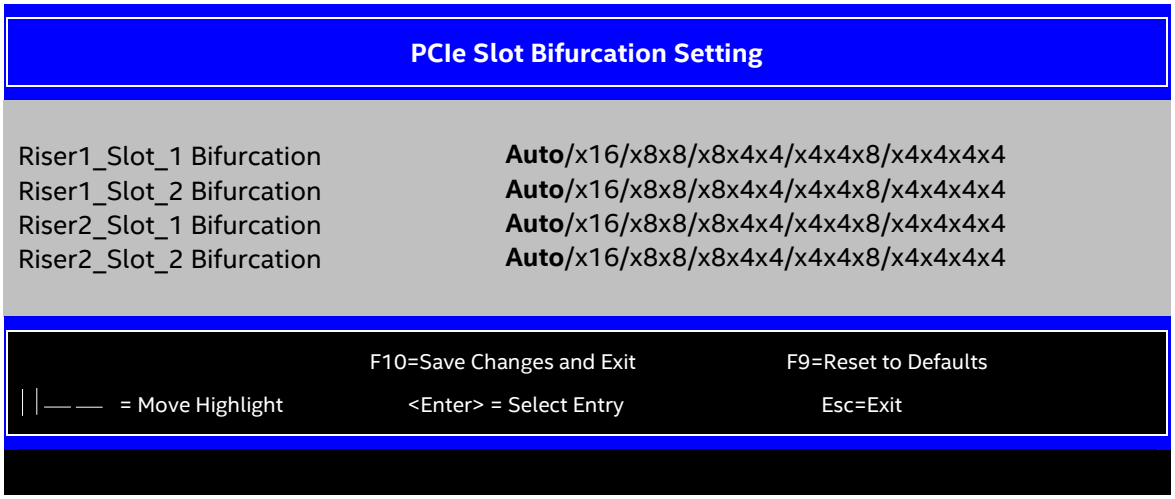


Figure 20. PCIe* Slot Bifurcation Setting Screen – Intel® Server Board M50CYP

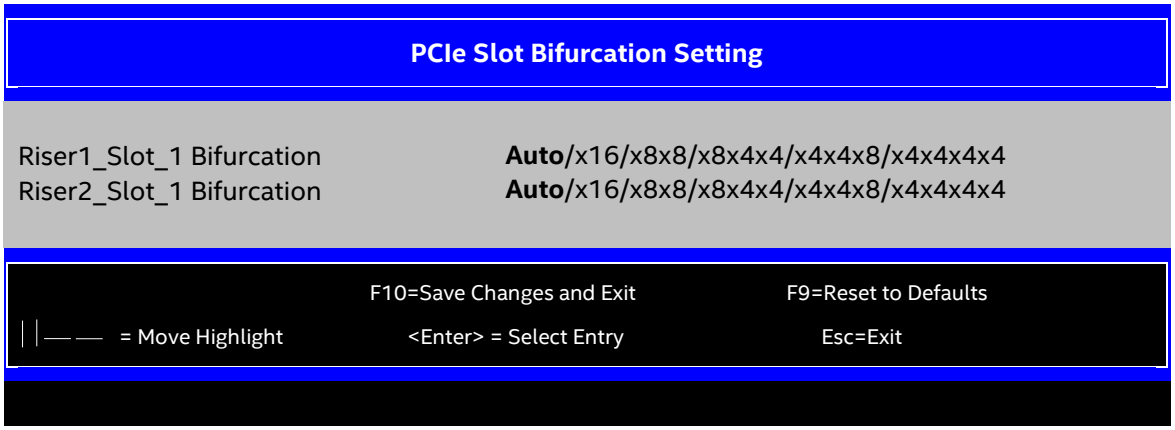


Figure 21. PCIe* Slot Bifurcation Setting Screen – Intel® Server Board D40AMP

1. **RiserX_Slot_X Bifurcation**

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

   Help text: Selects PCIe Port Bifurcation for selected riser slot(s).

   Comments: Due to Astera* retimers embedded in Intel® Server Board D50TNP's risers 3 and 4, those bifurcation settings apply on PCIe* root ports and Astera* devices. Risers 3 and 4 from the Intel® Server Board D50TNP only support Auto/x16/x8x8/x4x4x4x4 options.

   Note: Each setup item displays if a x16 riser is plugged.

   Back to: PCIe* Slot Bifurcation Setting – Integrated I/O Configuration – Advanced Screen – Screen Map

3.3.6.2 Processor PCIe* Link Speed

The Processor PCIe* Link Speed configuration screen allows the 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 user can also select the target link speed as Gen1, Gen2, Gen3, or Gen4 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 20.

The IIO supports 64 PCIe* lanes and 4 DMI lanes. The DMI lanes can also be strapped to operate in PCIe* mode, which is displayed as PCIe* Port 00. The 64 PCIe* lanes are grouped in 4. Each port can be bifurcated as 2x8, or 4x4, or any combination thereof, which is displayed as PCIe* Ports 1a, 1b, 1c, or 1d.

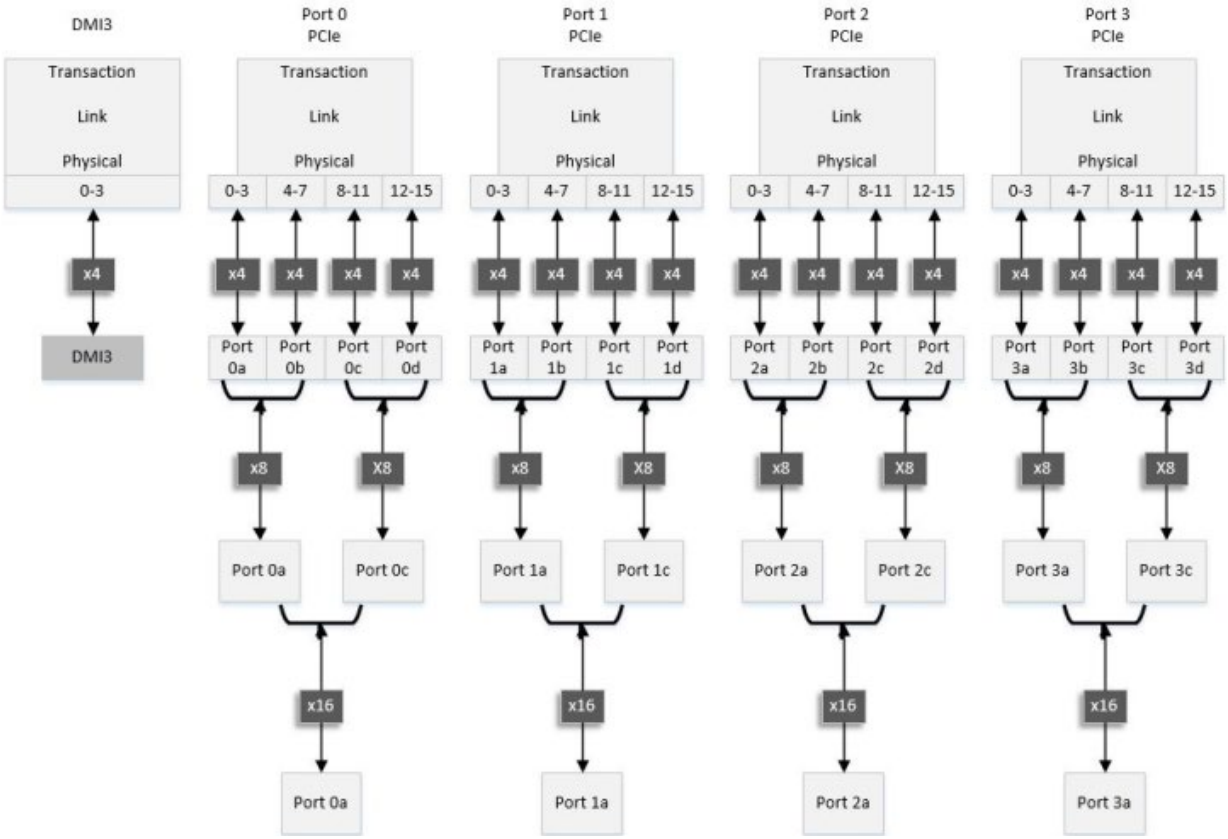


Figure 22. IIO PCIe* Lane Partitioning

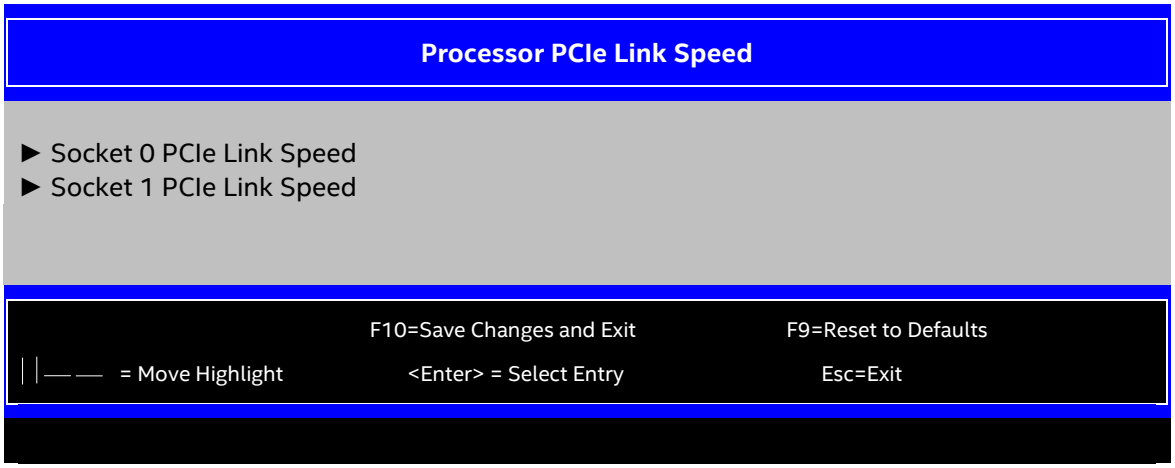


Figure 23. Processor PCIe* Link Speed Screen

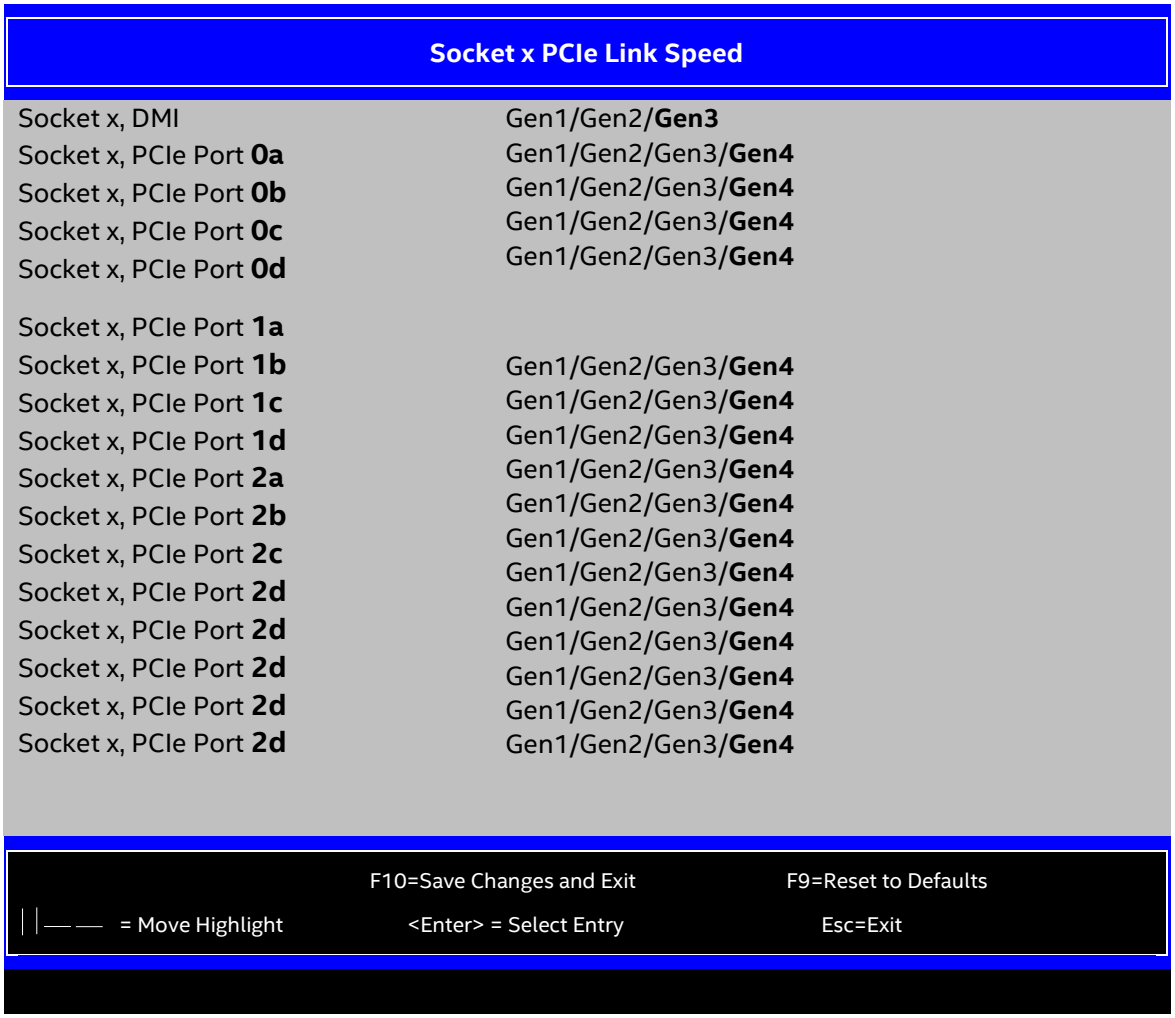


Figure 24. Processor Socket x PCIe* Link Speed Screen

1. **Socket x, DMI**

   Value: **Gen3/**Gen2/Gen1

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

   Comments: DMI port supports Gen1, Gen2, and Gen3 speeds. This option is available only when there is a corresponding PCIe* slot implemented on the specific board.

   Note: For Socket 0 in Intel® Server Boards D50TNP, M50CYP, and D40AMP, the DMI is already connected to PCH. So, it should not be visible.

   Back to: Processor PCIe* Link Speed – Integrated I/O Configuration – Advanced Screen – Screen Map

2. **Socket x, PCIe Port 0a**
3. **Socket x, PCIe Port 0b**
4. **Socket x, PCIe Port 0c**
5. **Socket x, PCIe Port 0d**
6. **Socket x, PCIe Port 1a**
7. **Socket x, PCIe Port 1b**
8. **Socket x, PCIe Port 1c**
9. **Socket x, PCIe Port 1d**
10. **Socket x, PCIe Port 2a**
11. **Socket x, PCIe Port 2b**
12. **Socket x, PCIe Port 2c**
13. **Socket x, PCIe Port 2d**
14. **Socket x, PCIe Port 3a**
15. **Socket x, PCIe Port 3b**
16. **Socket x, PCIe Port 3c**
17. **Socket x, PCIe Port 3d**

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

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

    Comments: PCIe* port supports 1.0 (2.5 GT/s), 2.0 (5 GT/s), and 3.0 (8 GT/s) speeds. Although ICX SP supports Gen4 speed. Those options for PCIe* ports are available only when there is a corresponding PCIe* slot implemented on the specific board.

    Back to: Processor PCIe* Link Speed – Integrated I/O Configuration – Advanced Screen – Screen Map

3.3.6.3 Volume Management Device

Volume Management Device is an enhanced feature to support NVMe* storage devices. Such enhanced feature manages attached PCIe* SSD device access and hot plug. Volume Management Device can also work with Intel® Virtual RAID on CPU (Intel® VROC) or SATA RAID to create a PCIe* SSD RAID volume.

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

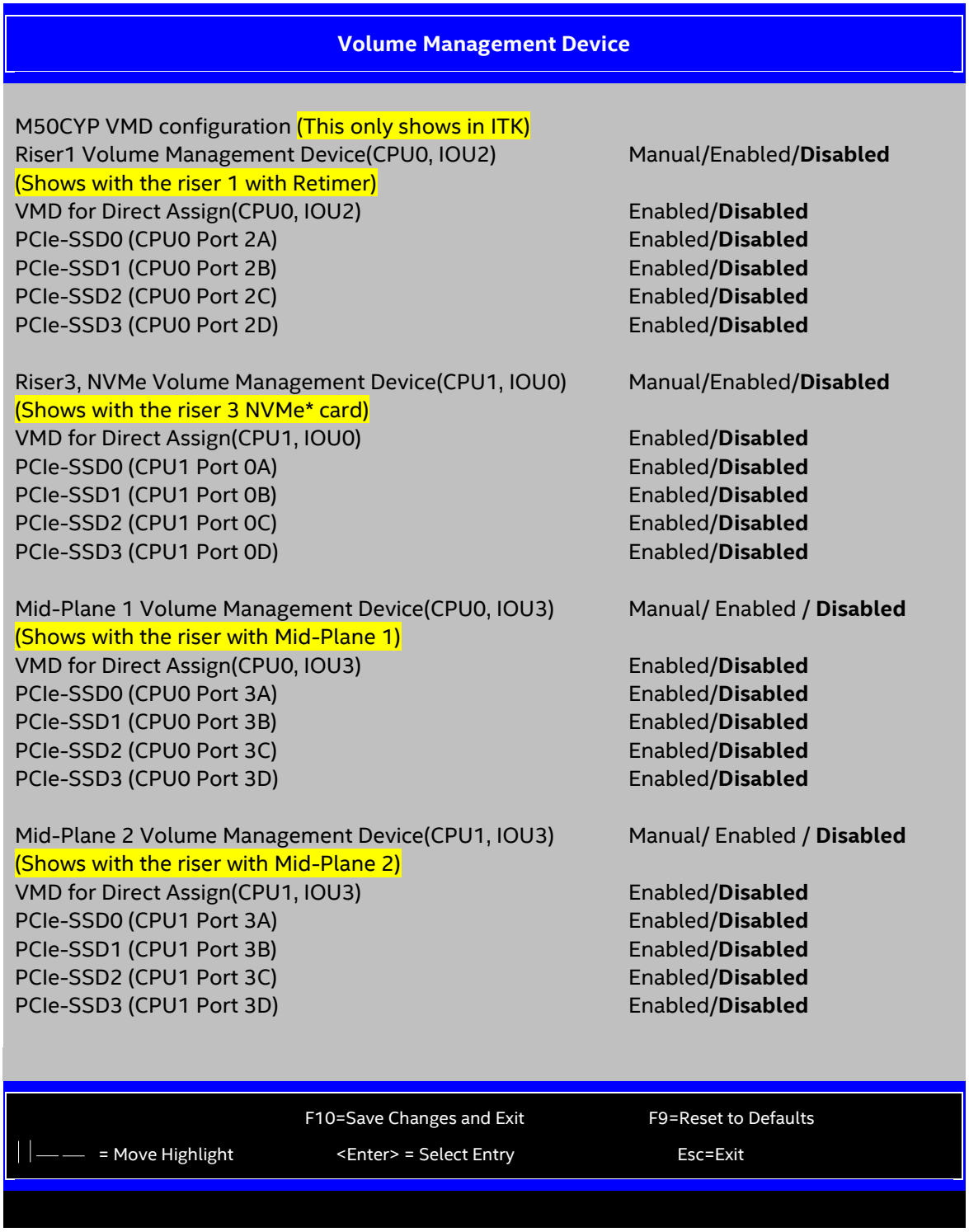


Figure 25. Volume Management Device Screen – Intel® Server Board M50CYP – Page 1

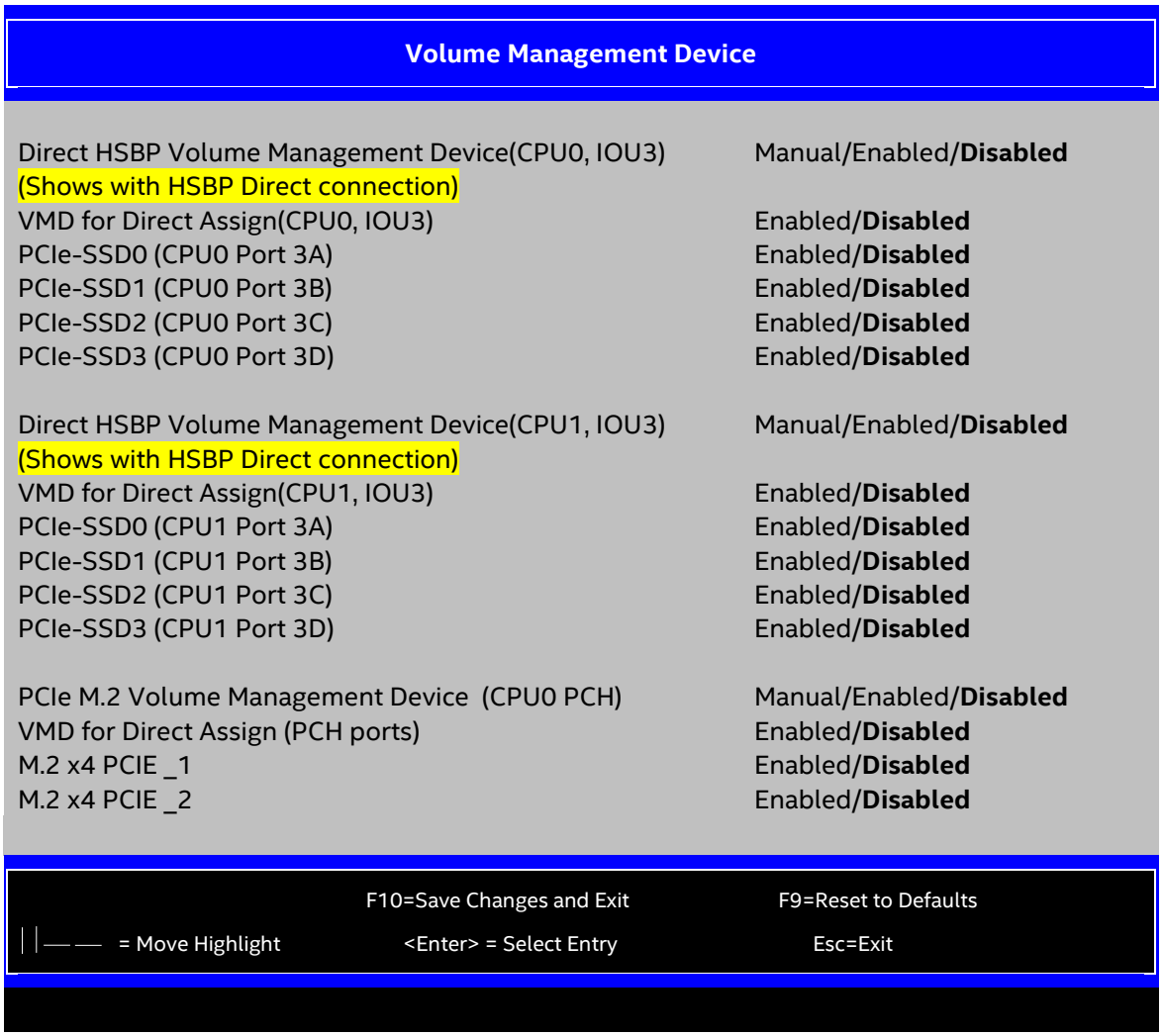


Figure 26. Volume Management Device Screen – Intel® Server Board M50CYP – Page 2

Figure 27. Volume Management Device Screen – Intel® Server Board D50TNP

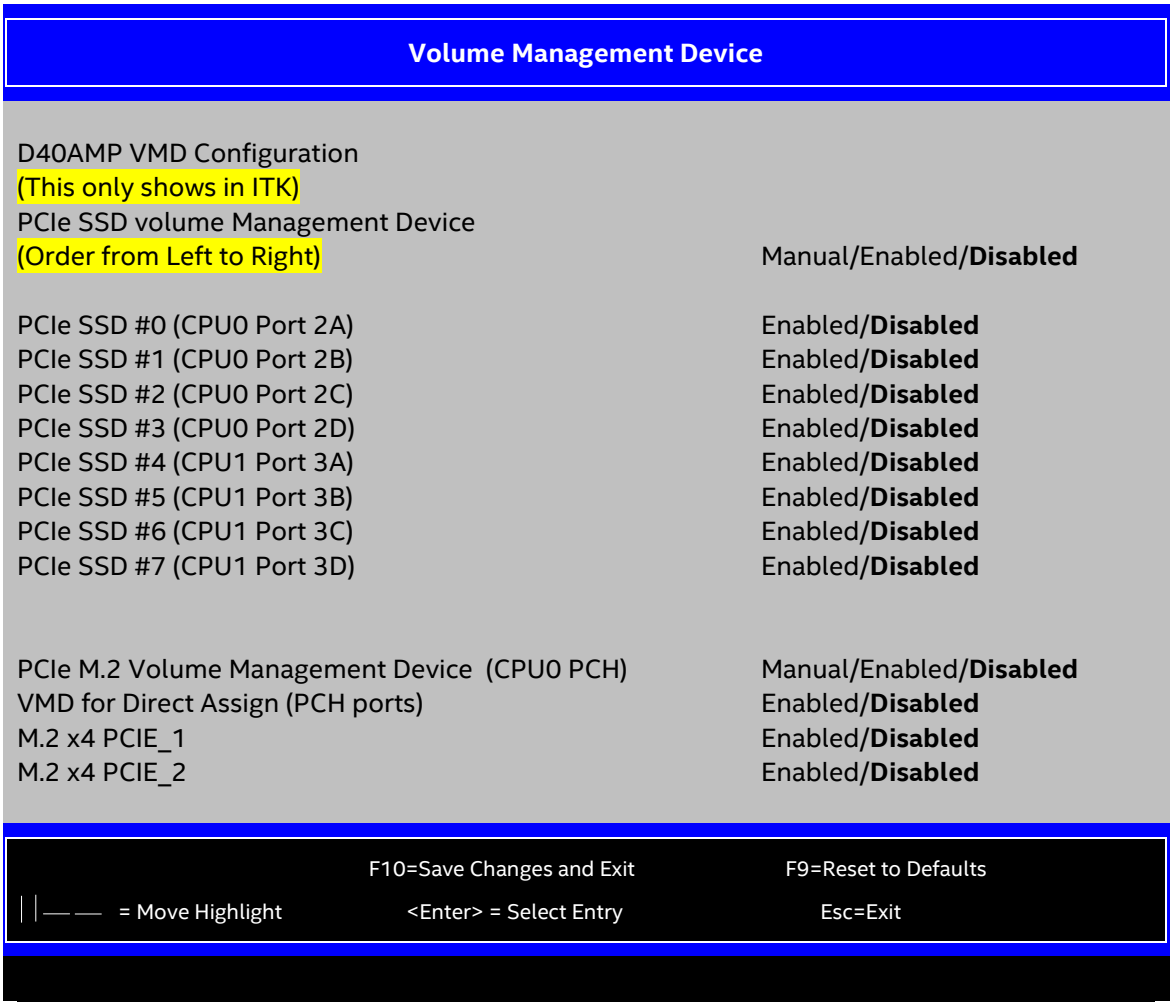


Figure 28. Volume Management Device Screen – Intel® Server Board D40AMP

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

For Intel® Server Board D50TNP

Ruler SSD Volume Management Device (order from left to right)

2U Riser Volume Management Device (order from right to left)

For Intel® Server Board M50CYP

Riser1, Volume Management Device (CPU0, IOU2) (shows with riser 1 with retimer).

Riser3, NVMe* Volume Management Device (CPU1, IOU0) (shows with the riser 3 NVMe* card).

Mid-Plane 1, Volume Management Device (CPU0, IOU3) (shows with the riser with Mid-Plane 1).

Mid-Plane 2, Volume Management Device (CPU1, IOU3) (shows with the riser with Mid-Plane 2).

Direct HSBP Volume Management Device (CPU0, IOU3) (shows with HSBP Direct connection).

Direct HSBP Volume Management Device (CPU1, IOU3) (shows with HSBP Direct connection).

For Intel® Server Board D40AMP

PCIe* SSD Volume Management Device (order from left to right)

Value: Manual/Enabled/**Disabled**

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

`[Enabled] – All specified VMD ports are forced to enable.`

`[Disabled] – All specified VMD ports are forced to disable.`

Comments: The following are some examples, according to the value assigned to Ruler SSD Volume Management Device.

- Manual – Exposes RSSD #0~#15 options selection respectively.
- Enable – Grays out RSSD #0~#15 and forces all child options value as Enabled.
- Disabled – Grays out RSSD #0~#15 and forces all child options value as Disabled.

Global set up option to enable or disable VMD support for this system. The setup can be different, based on the system configuration for SKUs.

For Intel® Server Board M50CYP, the display of VMD setup options relies on ID detection of riser/Mid-plane/Direct HSBP ID. Refer to Figure 25 for more information.

For Intel® Server Board D50TNP, the setup options depend on the SKU. For instance, EDSFF SKU supports a maximum of 16 VMD ports; on left front and right front in 2U riser, only 2 VMD ports are supported. Refer to Figure 27 for more information.

For Intel® Server Board D40AMP, the setup options depend on the SKU. For instance, U.2 SKU supports a maximum of 6 VMD ports; E1.L SKU supports a maximum of 8 VMD ports. Refer to Figure 28 for more information.

Back to: Volume Management Device – Integrated I/O Configuration – Advanced Screen – Screen Map

2. **VMD for Direct Assign**

   Value: Enabled/**Disabled**
   Help text: `Enable/Disable VMD for Direct Assign`
   Comments: Enable or disable VMD for Direct Assign for the corresponding PCIe* root port. This option is show/hide-based on this SKU's board design, only the capable root port has the visible option.

   Back to: Volume Management Device – Integrated I/O Configuration – Advanced Screen – Screen Map

3. **PCIe-SSD0 (CPU0 Port 2A)**
   PCIe-SSD1 (CPU0 Port 2B)
   PCIe-SSD2 (CPU0 Port 2C)
   PCIe-SSD3 (CPU0 Port 2D)
   RSSD#0 (CPU0 Port 0A)
   RSSD#1 (CPU0 Port 0B)

   Value: Enabled/**Disabled**

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

   Comments: Enable or disable VMD support for the corresponding PCIe* root port. This option is shown or hidden based on the SKU's board design. Only capable root ports have the Visible option.

   Back to: Volume Management Device – Integrated I/O Configuration – Advanced Screen – Screen Map

4. **PCIe M.2 Volume Management Device (CPU 0 PCH)**

   Value: Enabled/**Disabled**
   Help text:
   ```
   [Manual] – All specified VMD ports can be selected to enable or disable alone.
   [Enabled] – All specified VMD ports are forced to enable.
   [Disabled] – All specified VMD ports are forced to disable.
   ```
   Comments: Enable or disable VMD for Direct Assign for the corresponding PCIe* root port. This option is show/hide-based on this SKU's board design, only the capable root port has the visible option.

   Back to: Volume Management Device – Integrated I/O Configuration – Advanced Screen – Screen Map

5. **VMD for Direct Assign (PCH ports)**

   Value: Enabled/**Disabled**
   Help text: `Enable/Disable VMD for Direct Assign(PCH ports)`
   Comments: Enable or disable VMD for Direct Assign for the corresponding PCH PCIe* root port. This option is hidden when a SATA M.2 SSD installed on corresponding M.2 slot. If user install 2 SATA M.2 SSD on both M.2 slots, all PCIe M.2 Volume Management Device options will be hidden.

   Back to: Volume Management Device – Integrated I/O Configuration – Advanced Screen – Screen Map

6. **M.2 x4 PCIE_1**
   M.2 x4 PCIE_2

   Value: Enabled/**Disabled**

   Help text: `Configuration PCH root port: Enable - VMD ownership root port.`

   Comments: Enable or disable VMD support for the corresponding PCH PCIe* root port. This option is hidden when a SATA M.2 SSD installed on corresponding M.2 slot. If user install 2 SATA M.2 SSD on both M.2 slots, all PCIe M.2 Volume Management Device options will be hidden.

   Note: This section lists all the setup options. For detailed setup items per SKU, see the figures in Section 3.3.6.3.

   Back to: Volume Management Device – Integrated I/O Configuration – Advanced Screen – Screen Map

3.3.6.4 PCIe Misc. Configuration

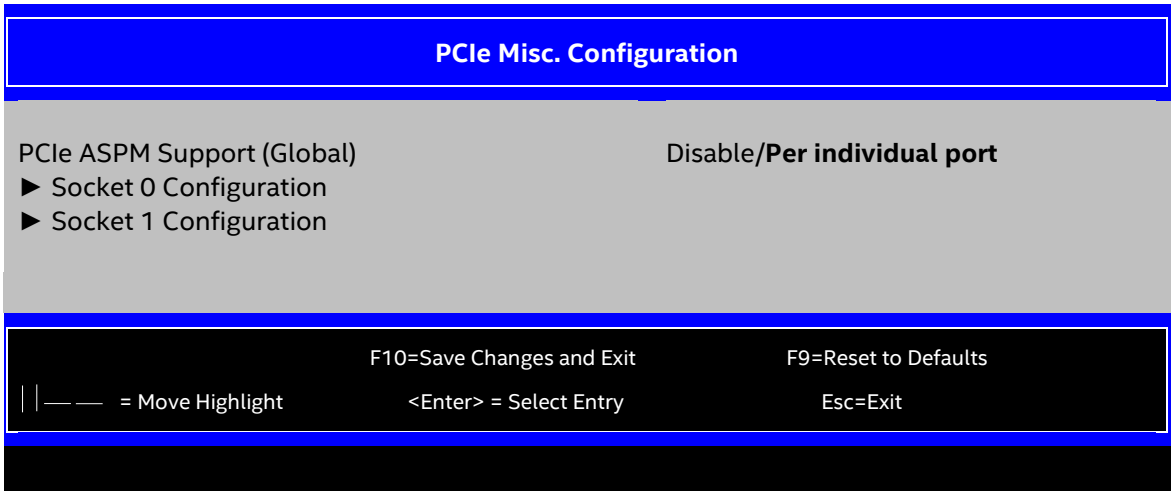


Figure 29. PCIe* Misc. Configuration Screen

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

   Value: Disabled/**Per individual port**

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

   Comments: This knob only control PCIe per port ASPM on socket. PCIe M.2 on PCH port will set L1 only by default.

   Back to: PCIe Misc. Configuration – Integrated I/O Configuration – Advanced Screen – Screen Map

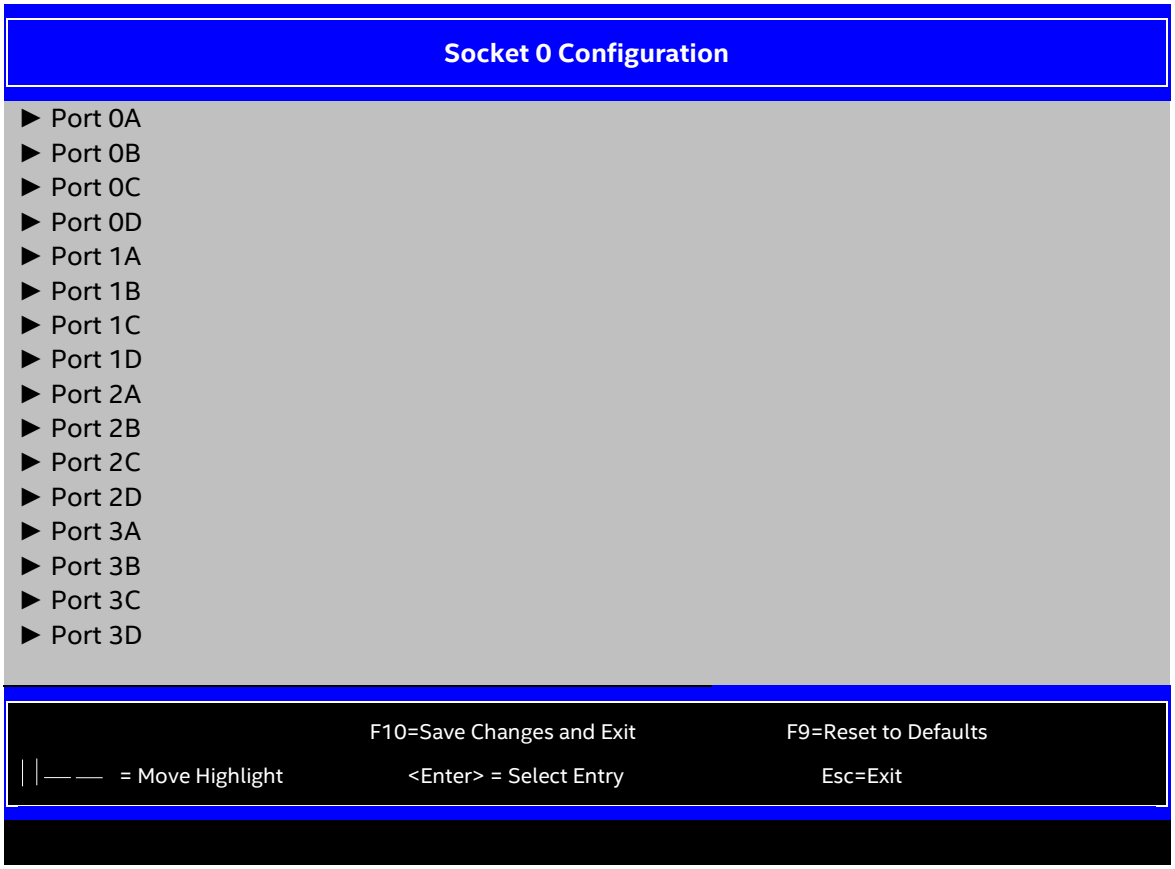


Figure 30. PCIe* Misc. Socket 0 Configuration Screen

1. **Port 0A/0B/0C/0D ----3A/3B/3C/3D**

   Value: Enabled/**Disabled**
   Help text: `Settings related to PCI Express Port 0A（or 0B/0C/0D ---3A/3B/3C/3D）`
   Comments: None.
   Back to: PCIe Misc. Configuration – Integrated I/O Configuration – Advanced Screen – Screen Map

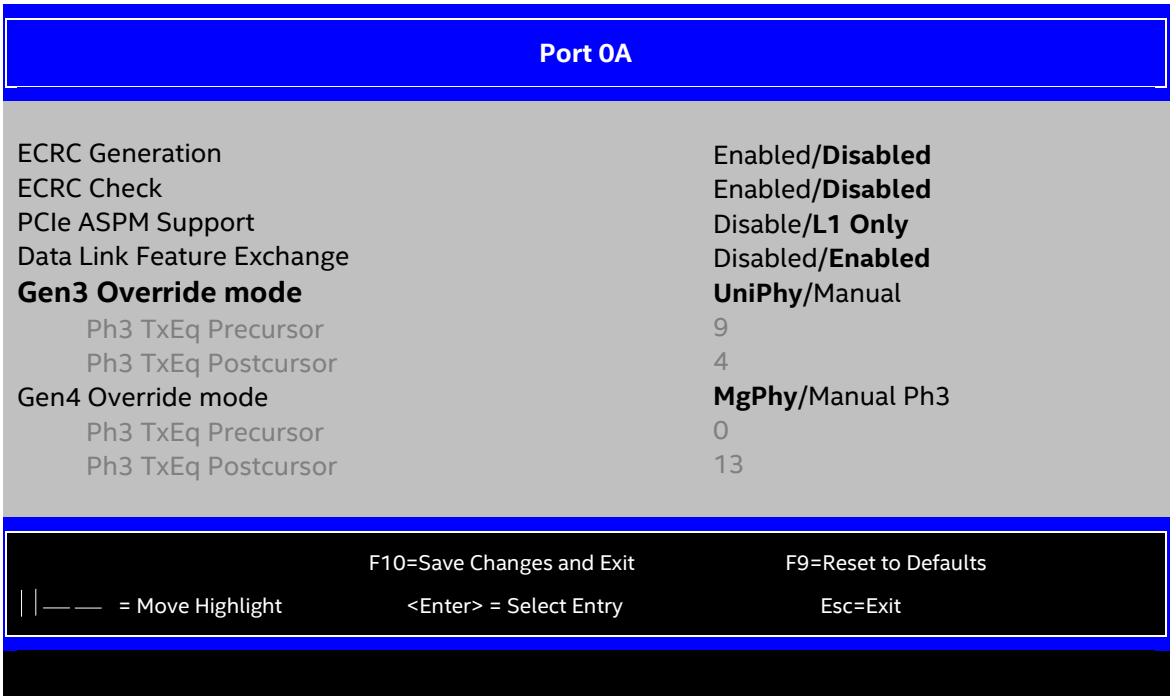


Figure 31. PCIe* Misc. Port 0A Screen

1. **ECRC Generation**

   Value: Enabled/**Disabled**
   Help text: `Enable or Disable ECRC Generation (Error Capabilities and Control Register).`
   Comments: None.
   Back to: PCIe Misc. Configuration – Integrated I/O Configuration – Advanced Screen – Screen Map

2. **ECRC Check**

   Value: Enabled/**Disabled**
   Help text: `Enable or Disable ECRC Check (Error Capabilities and Control Register).`
   Comments: None.
   Back to: PCIe Misc. Configuration – Integrated I/O Configuration – Advanced Screen – Screen Map

3. **PCIe ASPM Support**

   Value: **L1 only**/Disable
   Help text: `Allow for selecting target PCIe ASPM as disable, L1 support.`
   Comments: It gets grayed out when Global ASPM support is disabled.
   Back to: PCIe Misc. Configuration – Integrated I/O Configuration – Advanced Screen – Screen Map

4. **Data Link Feature Exchange**

   Value: Disabled/**Enabled**
   Help text: `Enable/Disable data link feature negotiation in the Data Link Feature Capabilities (DLFCAP) register.`
   Comments: None.
   Back to: PCIe Misc. Configuration – Integrated I/O Configuration – Advanced Screen – Screen Map

5. **Gen3 Override mode**

   Value: Manual/**UniPhy**
   Help text: `Set specific TxEq overrides in PCIe features.`
   Comments: None.
   Back to: PCIe Misc. Configuration – Integrated I/O Configuration – Advanced Screen – Screen Map

6. **Gen4 Override mode**

   Value: Manual Ph3/**MgPhy**
   Help text: `Set specific TxEq overrides in PCIe features.`
   Comments: None.
   Back to: PCIe Misc. Configuration – Integrated I/O Configuration – Advanced Screen – Screen Map

7. **Ph3 TxEq Precursor**

   Value: **9**
   Help text: `Override Ph3 TXEQ register.`
   Comments: The value is displayed as decimal, and the maximum value is 63. For Gen3 Override mode, is 9 by default. For Gen4 Override mode, is 0 by default. It does not get grayed out when Gen3/Gen4 Override mode is set to Manual.
   Back to: PCIe Misc. Configuration – Integrated I/O Configuration – Advanced Screen – Screen Map

8. **Ph3 TxEq Postcursor**

Value: **4**
Help text: `Override Ph3 TXEQ register.`
Comments: The value is displayed as decimal, and the maximum value is 63. For Gen3 Override mode, is 4 by default. For Gen4 Override mode, is 13 by default. It does not get grayed out when Gen3/Gen4 Override mode is set to Manual.
Back to: PCIe Misc. Configuration – Integrated I/O Configuration – Advanced Screen – Screen Map

3.3.6.5 NTB Configuration

NTB Configuration

NTB PCIe Port 1a on CPU socket 0	**Transparent Bridge**/NTB to NTB
Enable NTB Bars	**Disabled**/Enabled
Enable SPLIT BARs	**Disabled**/Enabled
Imbar1 Size	[12–51, **22** is Default]
Imbar2_0 Size	[12–39, **12** is Default]
Imbar2_1 Size	[12–39, **12** is Default]
Imbar2 Size	[12–51, **22** is Default]
Embar1 Size	[12–51, **22** is Default]
Embar2_0 Size	[12–39, **12** is Default]
Embar2_1 Size	[12–39, **12** is Default]
Embar2 Size	[12–51, **22** is Default]
Crosslink Control Override	**DSD/USP** / USD/DSP
NTB PCIe Port 2a on CPU socket 0	**Transparent Bridge**/NTB to NTB
Enable NTB Bars	**Disabled**/Enabled
Enable SPLIT BARs	**Disabled**/Enabled
Imbar1 Size	[12–51, **22** is Default]
Imbar2_0 Size	[12–39, **12** is Default]
Imbar2_1 Size	[12–39, **12** is Default]
Imbar2 Size	[12–51, **22** is Default]
Embar1 Size	[12–51, **22** is Default]
Embar2_0 Size	[12–39, **12** is Default]
Embar2_1 Size	[12–39, **12** is Default]
Embar2 Size	[12–51, **22** 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 32. NTB Configuration Screen – Page 1

Figure 33. NTB Configuration Screen – Page 2

1. **M50CYP: NTB PCIe* Port 1a on CPU socket 0**
   NTB PCIe* Port 2a on CPU socket 0
   NTB PCIe* Port 0a on CPU socket 1
   NTB PCIe* Port 1a on CPU socket 1
   NTB PCIe* Port 2a on CPU socket 1
   D50TNP: NTB PCIe* Port 2a on CPU socket 0
   NTB PCIe* Port 1a on CPU socket 1
   NTB PCIe* Port 2a on CPU socket 1
   D40AMP: NTB PCIe* Port 3a on CPU socket 0
   NTB PCIe* Port 2a on CPU socket 1

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

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

   Comments: This option selects the configuration mode for PCIe* ports 0A, 1A, 2A, 3A to support the NTB configuration.

   Note: When NTB is enabled, 'PCIe Pll SSC' setting will be ignored, and SSC function will be disabled automatically. NTP-RP mode is not supported in the Intel® Server Boards D50TNP, M50CYP, and D40AMP.

   Back to: Volume Management Device – Integrated I/O 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: When enabled, this option allows the BIOS to program NTB BAR registers with default values. If disabled, the BIOS does not program NTB BARs registers and the task is left to drivers. This option appears only when the NTB PCIe* port is not configured as Transparent Bridge.

   Back to: Volume Management Device – Integrated I/O 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 is enabled, the 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 appears only when Enable NTB Bars is enabled.

   Back to: Volume Management Device – Integrated I/O Configuration – Advanced Screen – Screen Map

4. **Imbar1 Size**

   Value: [12–51, **22** is Default]

   Help text: `[IMBAR1SZ] Used to set the prefetchable Imbar1 size on primary side of NTB. Value range <12...51> representing BAR sizes <4KB ... 128PB>.`

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

   Back to: Volume Management Device – Integrated I/O Configuration – Advanced Screen – Screen Map

5. **Imbar2_0 Size**

   Value: [12–39, **12** is Default]

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

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

   Back to: Volume Management Device – Integrated I/O Configuration – Advanced Screen – Screen Map

6. **Imbar2_1 Size**

   Value: [12–39, **12** is Default]

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

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

   Back to: Volume Management Device – Integrated I/O Configuration – Advanced Screen – Screen Map

7. **Imbar2 Size**

   Value: [12–51, **22** is Default]

   Help text: `[IMBAR2SZ] Used to set the prefetchable Imbar2 size on primary side of NTB. Value range <12...51> representing BAR sizes <4KB ... 128PB>.`

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

   Back to: Volume Management Device – Integrated I/O Configuration – Advanced Screen – Screen Map

8. **Embar1 Size**

   Value: [12–51, **22** is Default]

   Help text: `[EMBAR1SZ] Used to set the prefetchable Embar1 size on secondary side of NTB. Value range <12...51> representing BAR sizes <4KB ... 128PB>.`

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

   Back to: Volume Management Device – Integrated I/O Configuration – Advanced Screen – Screen Map

9. Embar2_0 Size

Value: [12–39, **12** is Default]

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

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

Back to: Volume Management Device – Integrated I/O Configuration – Advanced Screen – Screen Map

10. Embar2_1 Size

Value: [12–39, **12** is Default]

Help text: `Used to set the prefetchable Embar2_1 size on Secondary side of NTB. Value < than 12 or > 29 (39 for BIOS supporting > 4G PCI) disables BAR.`

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

Back to: Volume Management Device – Integrated I/O Configuration – Advanced Screen – Screen Map

11. Embar2 Size

Value: [12–51, **22** is Default]

Help text: `[EMBAR2SZ] Used to set the prefetchable Embar2 size on secondary side of NTB. Value range <12...51> representing BAR sizes <4KB ... 128PB>.`

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

Back to: Volume Management Device – Integrated I/O 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 NTB port's crosslink configuration.

Crosslink Control Override appears only when the NTB PCIe* Port is configured as NTB to NTB.

For more details about this item, refer to the *BIOS EPS for Intel® Server Boards D50TNP, M50CYP, and D40AMP*, Section 3.7.1.

Back to: Volume Management Device – Integrated I/O Configuration – Advanced Screen – Screen Map

13. NTB Link Train by BIOS

Value: No/Yes/**Auto**

Help text: `This knob enables or disables the BIOS to train the NTB link.`

Comments: None.

Back to: Volume Management Device – Integrated I/O Configuration – Advanced Screen – Screen Map

3.3.7 Mass Storage Controller Configuration

The Mass Storage Controller Configuration screen allows the user to configure the mass storage controllers integrated into the server board on which the BIOS is executing. This screen 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.

Two SATA port configurations are offered in this screen, representing the SATA controller and the sSATA controller with SATA drive support and redundant array of independent disks (RAID) support. When applicable, this screen also includes informational displays of two SATA controller configurations and SATA drive information. If an Intel® Storage Module is detected, the type of storage module is displayed as information only.

For detailed information about mass storage in the Intel® Server Boards D50TNP, M50CYP, and D40AMP, refer to the *BIOS EPS for Intel® Server Boards D50TNP, M50CYP, and D40AMP*, Section 3.7. For details on the storage configurations supported by the different server boards, refer to the *BIOS EPS for Intel® Server Boards D50TNP, M50CYP, and D40AMP*, Section 11.

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

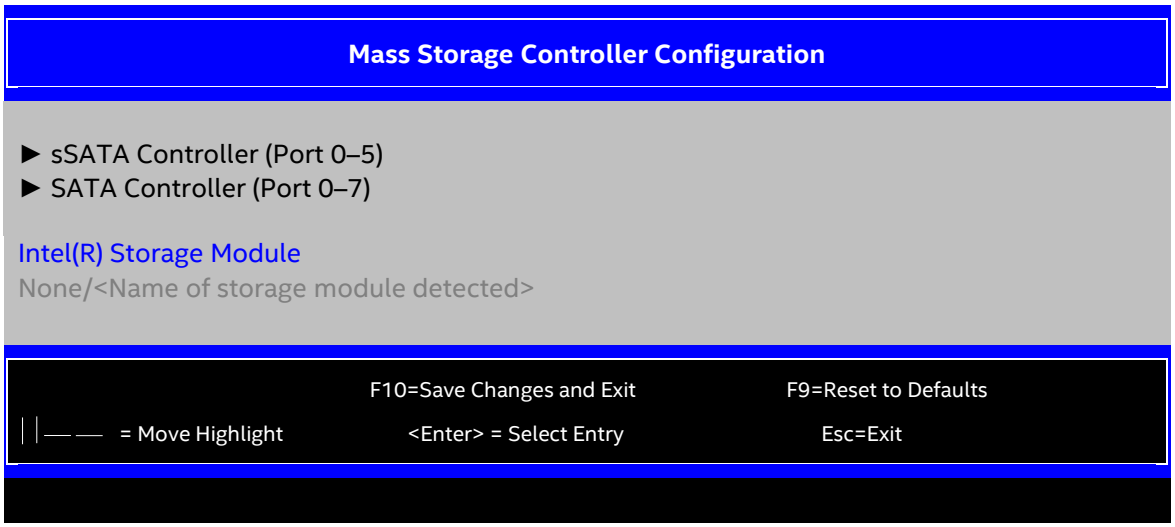


Figure 34. Mass Storage Controller Configuration Screen

1. **sSATA Controller (Port 0–5)**

   Value: None.

   Help text: `Configure the sSATA Port 0-5 and view current disk drive information.`

   Comments: *Selection only*. For more information on SATA Port configuration settings, see Section 3.3.7.1.

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

2. **SATA Controller (Port 0–7)**

   Value: None.

   Help text: `Configure the SATA Port 0-7 and view current disk drive information.`

   Comments: *Selection only*. For more information on SATA Port configuration settings, see Section 3.3.7.1.

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

3. **Intel(R) Storage Module**

   Value: None/<Name of storage module detected>

   Help text: None.

   Comments: *Information only*. This item displays the product name of the Intel® Storage Module installed, which helps in identifying drivers, support, documentation, and others. If no module is detected, then `None` is displayed.

   For details about Intel® Storage Modules support, refer to the *BIOS EPS for Intel® Server Boards D50TNP, M50CYP, and D40AMP*, Section 3.7.5.

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

3.3.7.1 SATA Port Configuration

The SATA Port Configuration screen allows the user to configure the AHCI-capable controllers integrated into the server board on which the BIOS is executing. Two onboard controllers are available, the AHCI SATA controller and the AHCI sSATA controller with SATA drive and RAID support. When applicable, this screen also provides informational displays on AHCI controller configuration and SATA drive information.

Note: Due to limitations of Intel® Server Configuration Utility (cannot change two options with the same name), the user must make sure that all SATA options have different names.

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

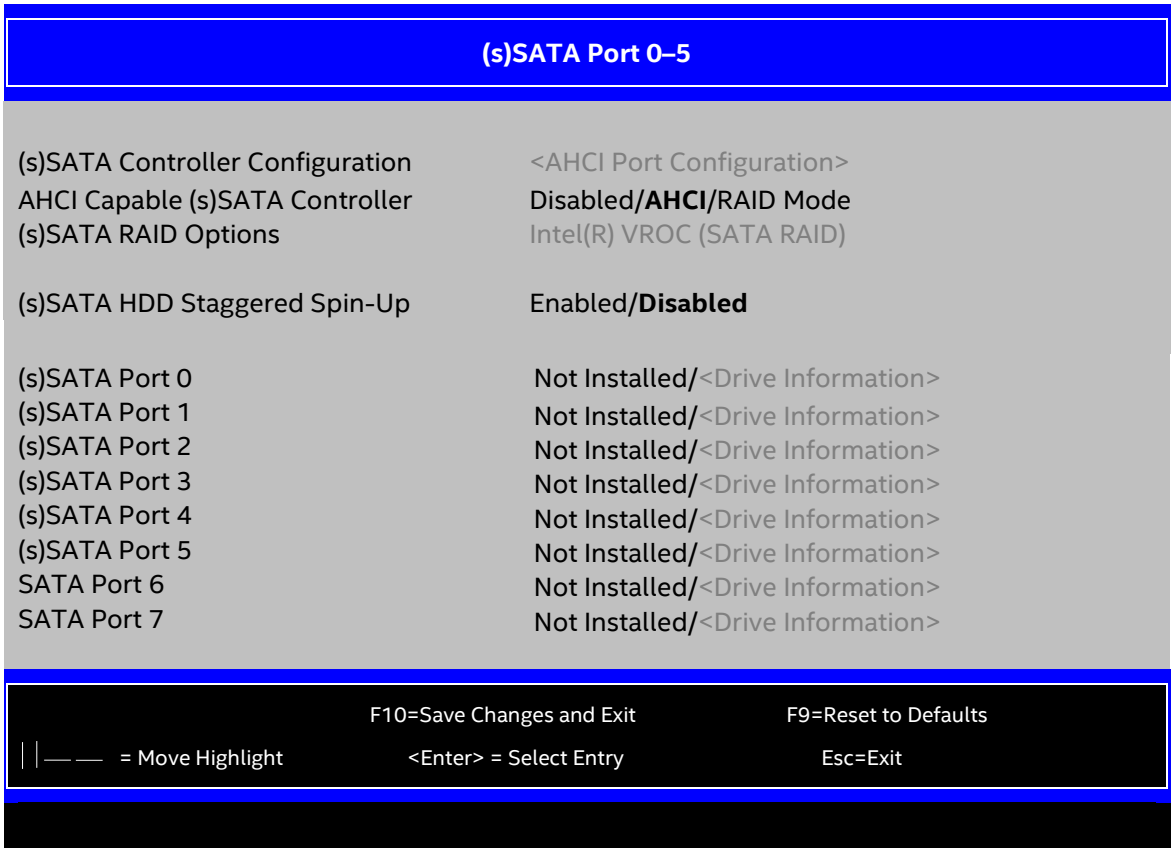


Figure 35. SATA Port Configuration Screen

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

   Value: Controller is disabled/<AHCI port configuration>

   Help text: None.

   Comments: *Information only*. This item is a display showing the capability of the onboard AHCI-capable SATA controller, if the controller is enabled. The controller configuration is one of the following states:

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

   This information is also displayed during the POST in the POST Diagnostic screen. Refer to the *BIOS EPS for Intel® Server Boards D50TNP, M50CYP, and D40AMP*, Section 4.2.

   The number of SATA ports available from the integrated AHCI-capable SATA controller is dependent on the specific server board installed in the system. Different server board designs expose different SATA port configurations.

   If no M.2 is attached, the screen shows `Controller is disabled` for a board belonging to the Intel® Server Board M50CYP. For Intel® Server Board D50TNP, the controller is disabled and hidden.

   The platform ID (board ID) is displayed in the Main screen, and the corresponding SATA port configuration can be found in the *BIOS EPS for Intel® Server Boards D50TNP, M50CYP, and D40AMP*, Section 11.

   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 the *BIOS EPS for Intel® Server Boards D50TNP, M50CYP, and D40AMP*, Section 11.

   If the SATA controller is disabled, the SATA ports do not operate, and any installed SATA devices are unavailable. RAID Mode provides host-based RAID support on the onboard SATA ports. RAID levels supported and required drivers depend on the RAID stack selected.

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

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

   Value: **Intel(R) VROC (SATA RAID)**

   Help text: `- Intel(R) VROC (SATA RAID): Provides pass-through drive support. Also provides host based RAID 0/1/10/5 support. Uses Intel(R)VROC (SATA RAID)iastor drivers.`

   Comments: This option appears only when the SATA Controller is enabled, and RAID Mode is 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 there is not a RAID Volume previously created that is compatible with the RAID stack selected, the user must click **Save and Exit** and reboot to create a RAID Volume.

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

4. **(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-up and this option does not affect them.

   (s)SATA HDD Staggered Spin-Up is visible only when the SATA controller is enabled and AHCI or RAID is selected as the operational SATA mode.

   Staggered spin-up is necessary if there are enough HDDs attached to the system to cause a marked startup power demand surge when all the drives start to spin-up together. The power demand is greater just as the drive spinning is started. To avoid possible issues, the overall startup power demand can be leveled off by activating each drive at a slightly different time. This staggered activation assures that 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 drives spinning starts. 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

5. **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 of the disk drive installed on a particular port.

   This drive information line is repeated for the SATA ports for the two onboard AHCI-capable SATA controllers.

   However, for any given board, only the ports that are physically populated on the board are shown. That is, a board that only implements the two 6 GB/s ports 0 and 1 only shows those two ports in this drive information list.

   When the SATA operational mode is RAID Mode, this section for drive information does not appear.

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

3.3.8 PCI Configuration

The PCI Configuration screen allows the user to configure the PCI memory space used for add-in and onboard adapters, configure video options, and configure onboard adapter options. This screen also includes a selection option to go to the NIC Configuration screen.

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

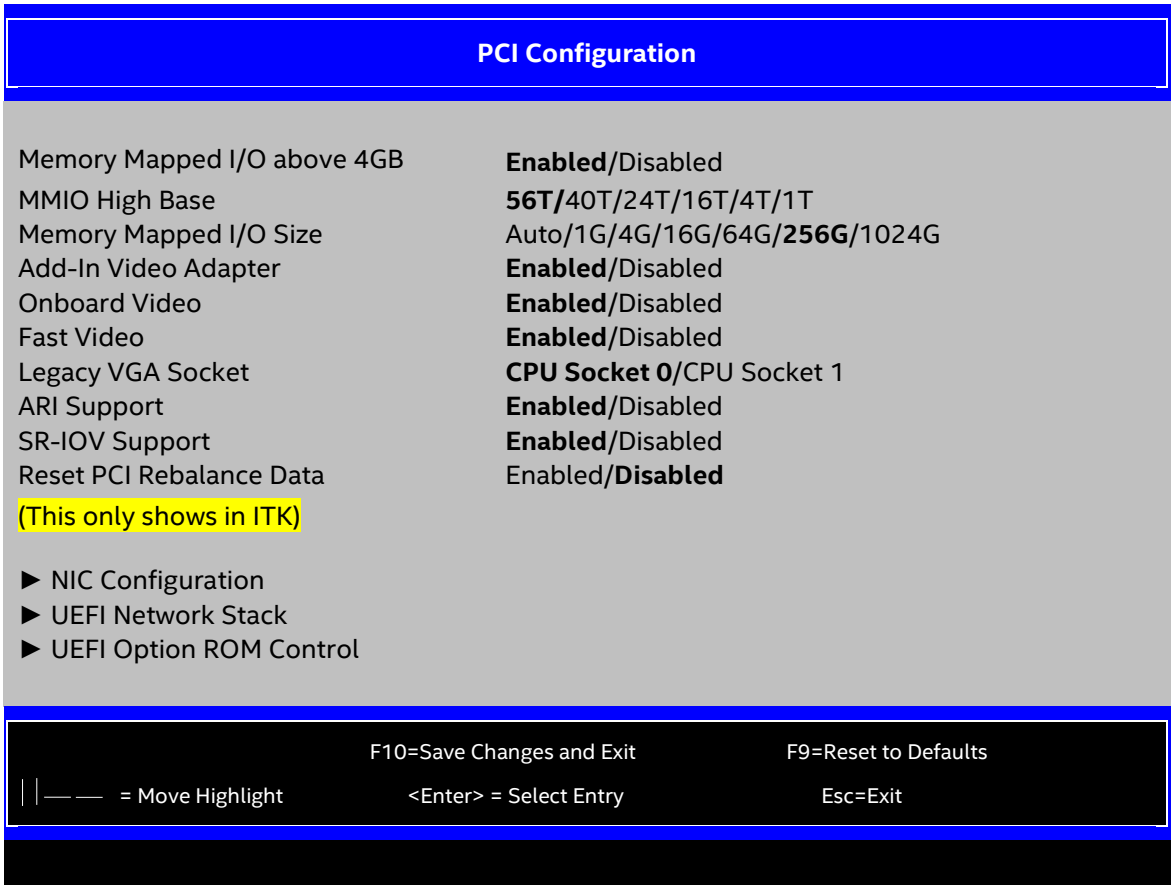


Figure 36. PCI Configuration Screen

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. The 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 4 GB.`

   Comments: When Memory Mapped I/O above 4 GB option is enabled, this option sets the preserved MMIO size as PCI/PCIe* Memory Mapped I/O for devices capable of 64-bit addressing. }

   The Auto setting automatically calculates the required MMIO size of all add-in PCIe* devices and tries to assign sufficient resources for each device.

   This option is grayed out when Memory Mapped I/O above 4 GB option is disabled.

   Note: The system does not work normally if the system requested memory mapped I/O size is greater than the chosen value (1 GB/4 GB/16 GB/64 GB). This behavior is expected due to MMIO resources 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 the Legacy VGA Socket option set to CPU Socket 0 and there is no add-in video card in any PCIe* slot connected to CPU Socket 0, this option is set to Disabled, grayed out, and unavailable.

   If the Legacy VGA Socket option set to CPU Socket 1 and there is no add-in video card in any PCIe* slot connected to CPU Socket 1, this option is set to Disabled, grayed out, and unavailable.

   If the Legacy VGA Socket option is set to CPU Socket 0 with both Add-in Video Adapter and Onboard Video enabled, the onboard video device works as primary video device while the add-in video adapter works 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 0, and the Legacy VGA Socket option is set to CPU Socket 0, then this Onboard Video option is available to be set by default as Disabled.

If there is an add-in video card installed on a PCIe* slot connected to CPU Socket 1, and the Legacy VGA Socket option is set to CPU Socket 1, this option is grayed out and unavailable, with a value set to Disabled.

In such scenario, Onboard Video gets disabled by default because it is connected to CPU Socket 0 and is not functional when CPU Socket 1 is the active path for video. When Legacy VGA Socket is set back to CPU Socket 0, this option becomes available again and is set to its default value of Enabled.

Note: This option does not appear on some models. For product-specific information, refer to the *BIOS EPS for Intel® Server Boards D50TNP, M50CYP, and D40AMP*, Section 11.

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 appears only when Onboard Video is Enabled.

Comments: None.

Back to: PCI Configuration – Advanced Screen – Screen Map

7. Legacy VGA Socket

Value: **CPU Socket 0**/CPU Socket 1

Help text: `Determines whether Legacy VGA video output is enabled for PCIe slots attached to Processor Socket 0 or 1. Socket 0 is the default.`

Comments: This option is necessary when using an add-in video card on a PCIe* slot attached to CPU Socket 1, due to a limitation of the processor IIO.

The legacy video device can be connected through either socket but there is a setting that requires it to be set only on one of the two. This option allows the switch to using a video card in a slot connected to CPU Socket 1.

Legacy VGA Socket does not appear unless the BIOS is running on a board that has one processor installed on CPU Socket 1. The board can also have a video card installed in a PCIe* slot connected to CPU Socket 1.

This option is grayed out as unavailable and set to CPU Socket 0 unless a processor is installed on CPU Socket 1 and a video card is installed in a PCIe* slot connected to CPU Socket 1.

When this option is active and is set to CPU Socket 1, then both Onboard Video and Dual Monitor Video are set to Disabled and grayed out as unavailable. These items get grayed out because the Onboard Video is a PCIe* device connected to CPU Socket 0 and is unavailable when the Legacy VGA Socket is set to Socket 1.

Back to: PCI Configuration – Advanced Screen – Screen Map

8. **ARI Support**

   Value: **Enabled**/Disabled

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

   Comments: None.

   Back to: PCI Configuration – Advanced Screen – Screen Map

9. **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

10. **Reset PCI Rebalance Data**

    Value: Enabled/**Disabled**

    Help text: `Select whether to reset PCI rebalance data.`

    Comments: This knob is enabled once. It is necessary to previously disable the SR-IOV Support option. After successfully resetting the PCI rebalance data, this knob gets changed back to disabled and the system triggers a warm reset. To prevent user enable this knob via BMC Web Console, the BIOS hides this knob. User can only enable this knob via Firmware Customization.

    Back to: PCI Configuration – Advanced Screen – Screen Map

11. **NIC Configuration**

    Value: None.

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

    Comments: *Selection only*. For more information on NIC Configuration settings, see Section 3.3.8.1.

    Note: This field cannot support Intel® Server Configuration Utility changes with the `/bcs` command and cannot support Firmware Customization. For Intel® Server Boards D50TNP, M50CYP and D40AMP that do not have onboard ports, this page does not exist.

    Back to: PCI Configuration – Advanced Screen – Screen Map

12. **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 3.3.8.2.

    Back to: PCI Configuration – Advanced Screen – Screen Map

13. **UEFI Option ROM Control**

    Value: None.

    Help text: `View/Configure UEFI Oprom control settings.`

Comments: *Selection only*. For more information on UEFI Option ROM Control settings, see Section 3.3.8.3.

Note: This field cannot support Intel® Server Configuration Utility changes with the `/bcs` command and cannot support Firmware Customization.

Back to: PCI Configuration – Advanced Screen – Screen Map

3.3.8.1 NIC Configuration

The NIC Configuration screen allows the user to configure the network interface card (NIC) controller options for the BIOS POST. It also displays the NIC MAC addresses currently in use. This screen manages built-in network controllers 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.

Usually, one onboard NIC is built into the baseboard, although in some cases two onboard NICs are present. Several types of NICs are available to be 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 matches the number of ports the onboard NIC presents.

Note: The fields on the NIC Configuration screen do not support Intel® Server Configuration Utility changes with the `/bcs` command and do not support Firmware 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 Boards D50TNP, M50CYP, and D40AMP, the NIC controller feature can be disabled/enabled only under UEFI mode. Also, for this feature to be supported, the onboard NIC must be the Intel® C620 PCH Integrated 10 Gigabit Ethernet Controller.

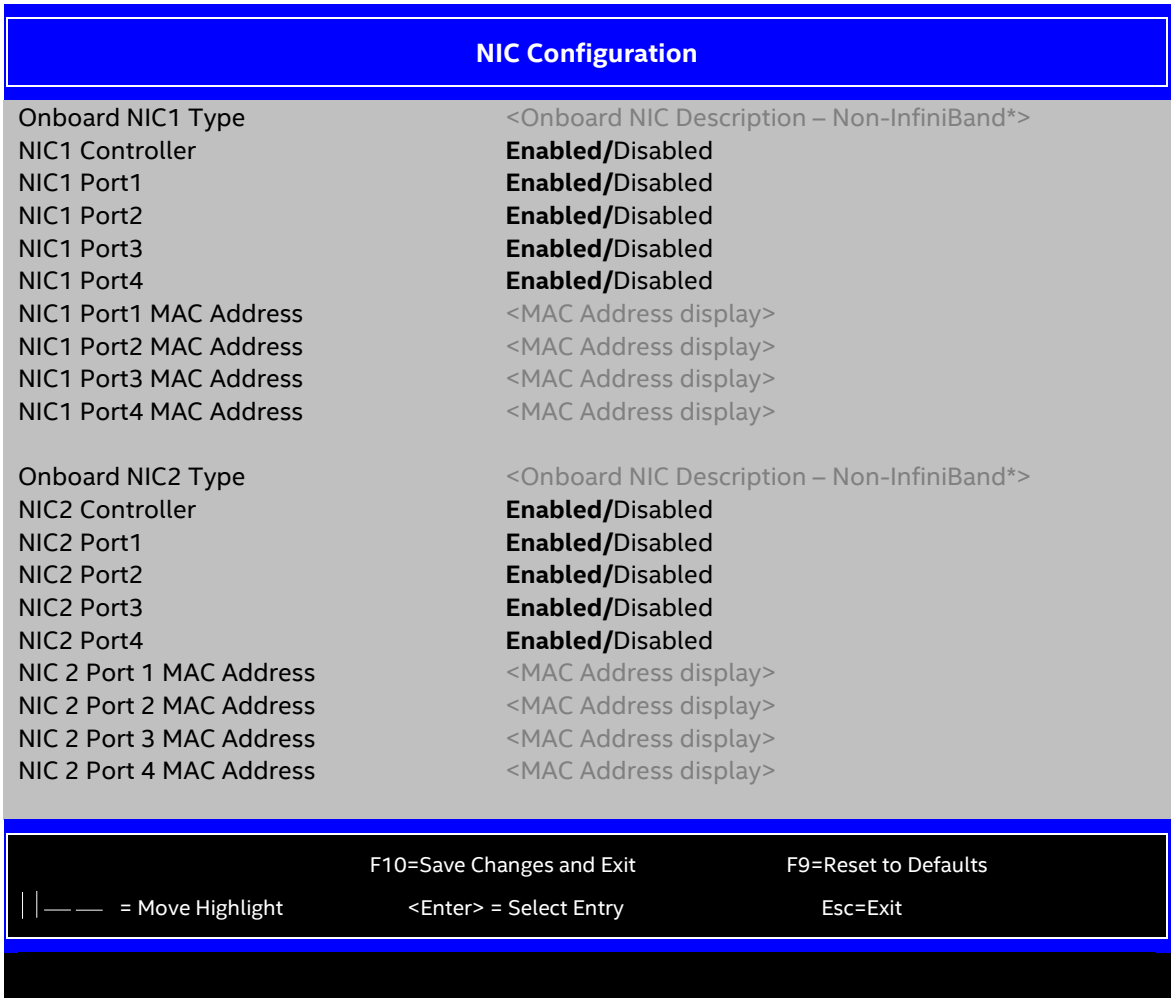


Figure 37. NIC Configuration Screen

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

Value: <Onboard NIC description>

Help text: None.

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

This NIC description is:

- `Intel(R) X550 Single-Port 10 Gigabit RJ-45 Controller`

Each one of these onboard NICs is followed by a section including a group of options that are specific to the NIC type. If a board only has one onboard NIC, the second NIC type and following options section do not appear.

The Intel® Server Board D50TNP only supports an Intel® Ethernet Controller X550 (up to 10 GbE) built in on the baseboard and one NIC port. So, the NIC1 Controller option design for this NIC port allows enabling/disabling.

By default, the Intel® Server Board M50CYP does not support NIC controllers built in on the baseboard.

For details about the NIC hardware configuration for a specific board, refer to the *BIOS EPS for Intel® Server Boards D50TNP, M50CYP, and D40AMP*, Section 11.

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.

When a controller is disabled, its 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 the associated port PXE options. The NIC <n> Port <x> PXE option and the MAC address displays 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 the *BIOS EPS for Intel® Server Boards D50TNP, M50CYP, and D40AMP*, Section 11, or the corresponding board-specific technical product specification.

The Intel® Server Board D50TNP only supports an Intel® Ethernet Controller X550 (up to 10 GbE) built in on the baseboard and one NIC port. But it cannot support the port disable feature, so it is hidden.

By default, the Intel® Server Board M50CYP board does not support NIC controllers built in on the baseboard.

Note: If the onboard NIC is the Intel® C620 PCH Integrated 10 Gigabit Ethernet Controller, NIC port Enable/Disable setup option is supported only under the 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 hexadecimal digits of the network controller's MAC address of Port1–Port4, 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, its corresponding port MAC address does not appear.

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

3.3.8.2 UEFI Network Stack

The UEFI Network Stack screen provides access to network devices while executing in the UEFI boot services environment. This stack follows the *Unified Extensible Firmware Interface Specification*, version 2.3.1.

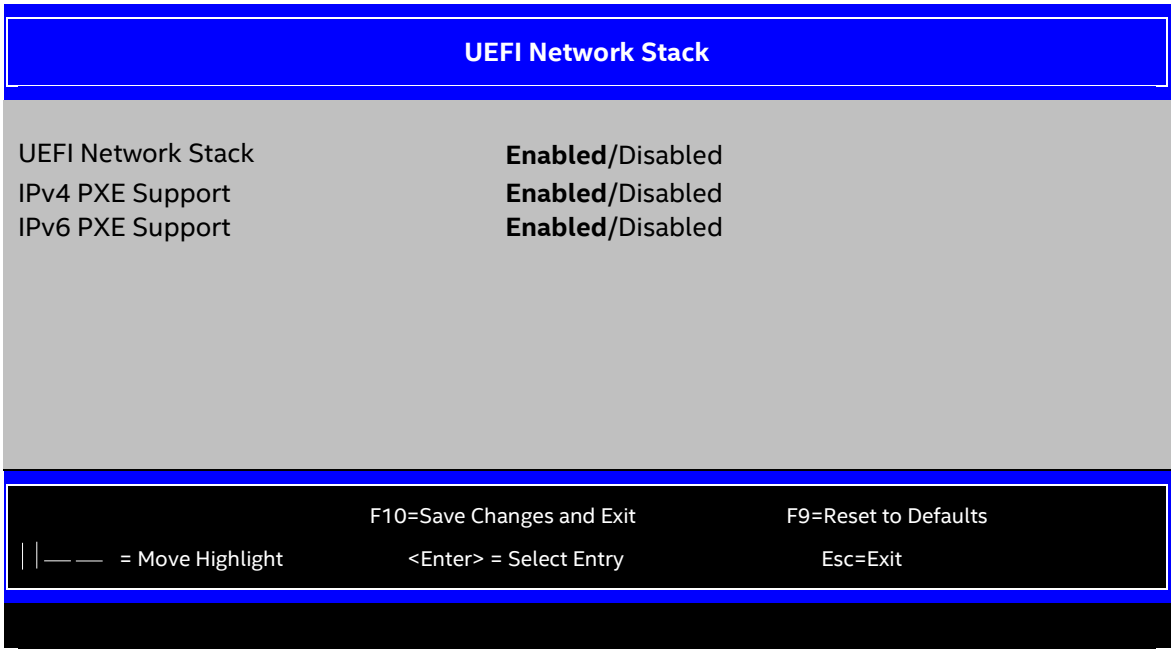


Figure 38. UEFI Network Stack Screen

1. **UEFI Network Stack**

   Value: **Enabled**/Disabled

   Help text: `Enable or Disable the whole UEFI Network Stack.`

   Comments: Disabling the UEFI Network Stack deactivates the network protocols defined in the *Unified Extensible Firmware Interface Specification*, version 2.3.1.

   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 the built-in 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 the built-in UEFI PXE functionality.

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

3.3.8.3 UEFI Option ROM Control

The UEFI Option ROM Control configuration screen is brought by the EFI PCI Option ROM compliant with the specification document (version 2.3.1) for the Human Interface Infrastructure (HII). Those configuration settings are provided by third-party PCI device provider and not controlled directly by the BIOS.

The BIOS parses the HII package provided by the EFI PCI Option ROM and groups them with their ClassID into this screen.

Four ClassID groups are designed:

- Network controller.
- Storage controller.
- Fiber channel.
- 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 Intel® Server Configuration Utility changes with the `/bcs` command and do not support Firmware Customization.

To identify each option ROM with the physical device's location, the BIOS attaches the SlotID to them. The SlotID is designed based on various products' configuration, which covers:

- Onboard devices.
- I/O modules.
- Storage modules.
- Riser slots.

How to translate the SlotID into the physical address is defined in Table 4.

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
Switch slot	00 – reserved	4	0:F = 16 switch	0:F = 16 possible slots per switch

Figure 39 is an example for the UEFI Option ROM Control screen. The contents change according to the system configuration.

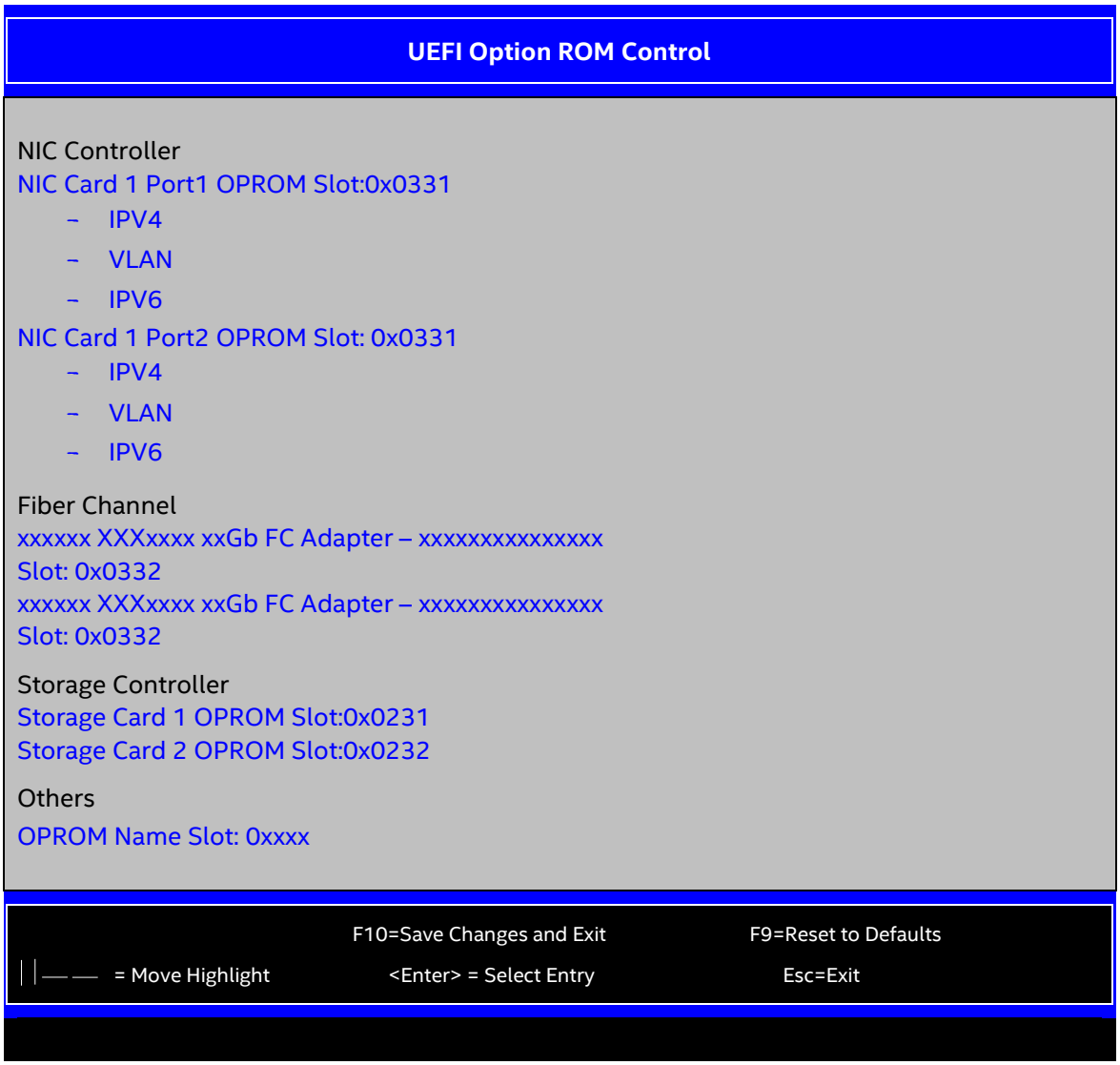


Figure 39. UEFI Option ROM Control Screen

Note: This document does NOT describe configuration items brought by EFI PCI Option ROMs, since their appearance depends on the PCI device vendor, which is out of the baseboard BIOS scope.

3.3.9 Serial Port Configuration

The Serial Port Configuration screen allows the user to configure the Serial A port. In legacy Industry Standard Architecture (ISA) nomenclature, these are ports COM1 and COM2, respectively.

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

The primary usage for these serial ports is to enable serial console redirection and serial-over-LAN (SOL) capabilities. Either port can be used for Serial Console Redirection, but SOL is only supported on Serial A. For more information on console redirection, see Section 3.5.1.

Note: The Serial Port B is not supported by the Intel® Server Boards D50TNP and D40AMP.

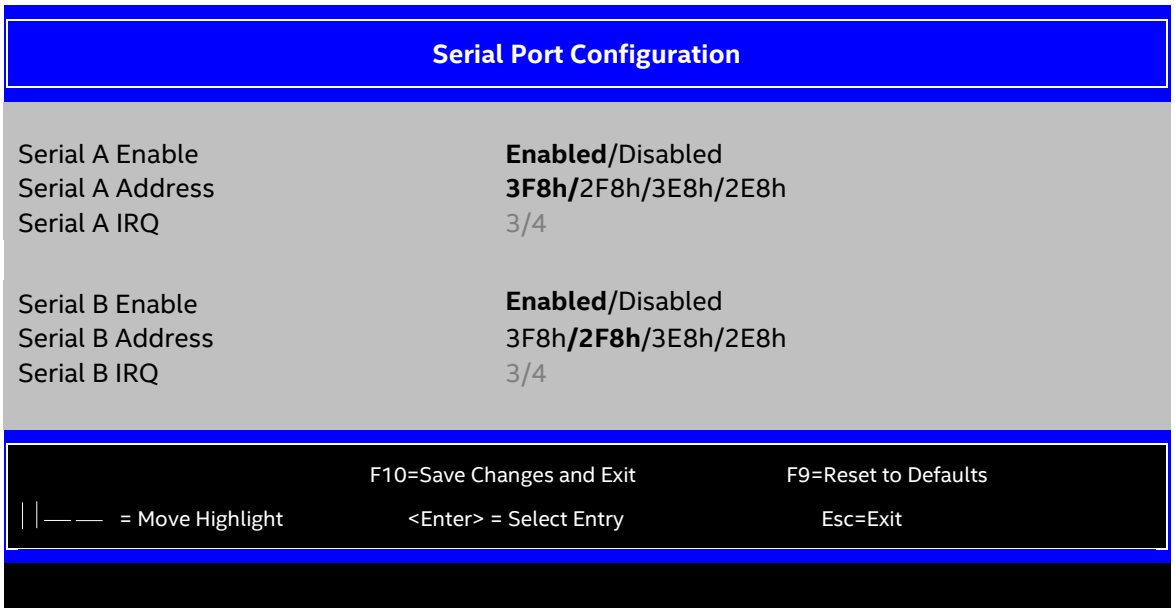


Figure 40. Serial Port Configuration Screen

1. **Serial A Enable**

   Value: **Enabled**/Disabled

   Help text: `Enable or Disable Serial port A.`

   Comments: Serial Port A can be used for either serial-over-LAN or serial console redirection.

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

2. **Serial A Address**

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

   Help text: `Select Serial port A base I/O address.`

   Comments: Legacy I/O port address. This field does not appear when Serial A Port enable/disable option 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

3. **Serial A IRQ**

   Value: 3/**4**

   Help text: `Select Serial port A interrupt request (IRQ) line.`

   Comments: Legacy interrupt request (IRQ). This field does not appear when Serial A Port enable/disable option does not appear.

   This item is grayed out because AST2500 UART* IRQ is fixed under ESPI Mode, and such option does not support Firmware Customization on the Intel® Server Boards D50TNP, M50CYP, and D40AMP.

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

4. **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

5. **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 the Serial B Address cannot be set to the same value.

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

6. **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 IRQ. This item is grayed out because AST2500 UART* IRQ is fixed under ESPI Mode, and such option does not support Firmware Customization on the Intel® Server Boards D50TNP, M50CYP, and D40AMP.

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

3.3.10 USB Configuration

The USB Configuration screen allows the user to configure the available USB controller options.

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

Each USB mass storage device may be set to allow the media emulation for which it is formatted, or an emulation may be specified. Particularly for USB flash memory devices, 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 sized less than 528 MB is forced to FDD emulation. Otherwise, if it is 528 MB or greater in size, it is forced to HDD emulation.

Note: Hot-plugged USB devices during the POST are detected, enumerated, and work under the operating system environment; but they are not displayed on this screen nor enumerated as bootable devices. The USB Internal Ports are not supported by the Intel® Server Boards D50TNP and D40AMP.

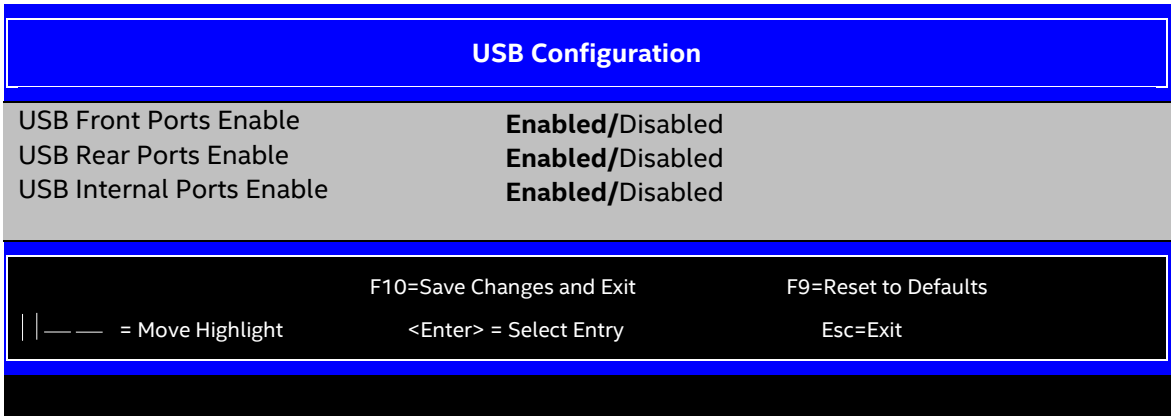


Figure 41. USB Configuration Screen

1. **USB Front Ports Enable**

   Value: **Enabled**/Disabled

   Help text: `Enable or disable the USB Front Ports.`

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

   Back to: USB Configuration – Advanced Screen – Screen Map

2. **USB Rear Ports Enable**

   Value: **Enabled**/Disabled

   Help text: `Enable or disable the USB Rear Ports.`

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

   Back to: USB Configuration – Advanced Screen – Screen Map

3. **USB Internal Ports Enable**

   Value: **Enabled**/Disabled

   Help text: `Enable or disable the USB Internal and BMC Ports.`

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

   Back to: USB Configuration – Advanced Screen – Screen Map

3.3.11 System Acoustic and Performance Configuration

The System Acoustic and Performance Configuration screen allows the user to configure the thermal control behavior of the system. Specifically, the parameters used in the system's fan speed control algorithms.

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

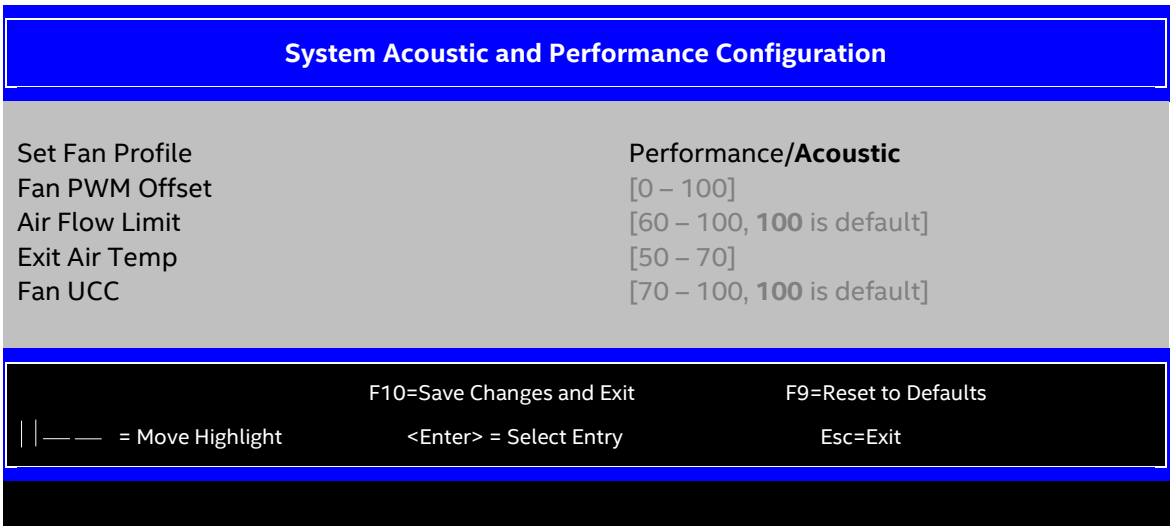


Figure 42. System Acoustic and Performance Configuration Screen

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 the fan speeds when necessary. This measure 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 first attempts to control thermal conditions by throttling memory to reduce the heat production. This measure 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 Intel® Server Configuration Utility/Intel® Server Information Retrieval Utility support is needed, get this setting from the BMC via IPMI, and not from the BIOS variable via `/bcs`. This option is required to support Firmware Customization.

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

2. Fan PWM Offset

Value: [Entry Field 0–100]

Help text: `Valid Offset 0-100. This number is added to the calculated PWM value to increase Fan Speed.`

Comments: This value is a percentage by which the calculated fan speed is increased. The user can apply a positive offset that results in increasing the minimum fan speeds.

At each system boot, the BIOS queries the BMC for the current PWM offset setting and displays its value in the BIOS setup utility.

This PWM offset setting is specified through the BIOS setup utility and is applicable to both Intel server chassis and third-party chassis. However, the BMC firmware owns the PWM offset setting. Only if a user changes the BIOS setting for the PWM offset does the BIOS send the new setting to the BMC.

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

Note: If Intel® Server Configuration Utility/Intel® Server Information Retrieval Utility support is needed, get this setting from the BMC via IPMI, and not from the BIOS variable via `/bcs`. This option does not support Firmware Customization.

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 the BMC immediately.

The 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.

This setup knob is hidden in *D50TNP*.

Table 5. Set FSC Parameter and Get FSC Parameter Commands for Airflow 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 Intel® Server Configuration Utility/Intel® Server Information Retrieval Utility support is needed, get this setting from the BMC via IPMI, and not from the BIOS variable via `/bcs`. This option does not support Firmware Customization.

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

4. Exit Air Temp

Value: [Entry Field 50–70]

Help text: `Exit Air temperature. BIOS valid range 50-70. This is to give MAX exit air temperature to BMC.`

Comments: On each boot, the BIOS reads the value from the BMC, as the BMC owns the policy. So, default setting is gotten from the BMC through an IPMI command.

If the user changes the value at setup, the BIOS sends the value to the BMC immediately. If the BMC has no response when reading, the 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 6. 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 Intel® Server Configuration Utility/Intel® Server Information Retrieval Utility support is needed, get this setting from the BMC via IPMI, and not from the BIOS variable via `/bcs`. This option does not support Firmware Customization.

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, but for total domain.

If the user changes the value at Setup, the BIOS sends the value to the BMC immediately. If the BMC has no response when reading, the 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 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. The BIOS uses domain 0 value for setup item.

Note: If Intel® Server Configuration Utility/Intel® Server Information Retrieval Utility support is needed, get this setting from the BMC via IPMI, and not from the BIOS variable via `/bcs`. This option does not support Firmware Customization.

Back to: System Acoustic and Performance 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 TPM security settings for boards that support TPM.

Note: The user must activate the TPM to enable Intel® Trusted Execution Technology (Intel® TXT) on the 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 passwords to:

- Have from 8 through 14 characters in length.
- Contain at least one case-sensitive alphabetical character.
- Contain at least one numeric character.
- Contain at least and one special character.

The user gets a warning when a password that does not meet the strong password criteria is set. But the password is accepted.

For further security, the BIOS optionally can require a power-on password to be entered early during the POST to boot the system. When the Power On Password option is enabled, the POST is halted soon after power-on, while the BIOS queries for a power-on password. Either the administrator or the user password can be entered for a power-on password.

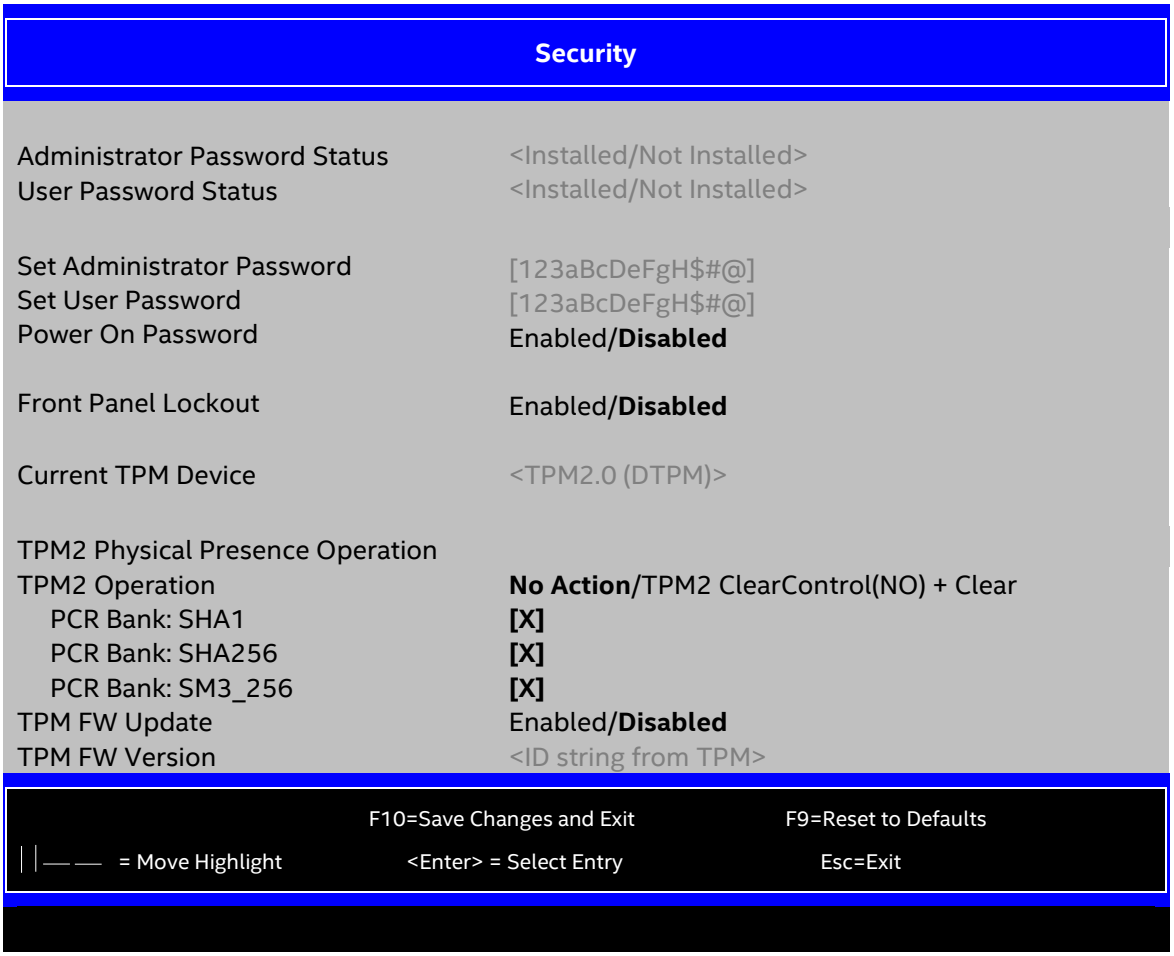


Figure 43. Security Screen

1. **Administrator Password Status**

   Value: <Installed/Not Installed>

   Help text: None.

   Comments: *Information only*. Indicates the status of the administrator password.

   Note: This field does not support Intel® Server Configuration Utility display with the `/bcs` command.

   Back to: Security Screen – Screen Map

2. **User Password Status**

   Value: <Installed/Not Installed>

   Help text: None.

   Comments: *Information only*. Indicates the status of the user password.

   Note: This field does not support Intel® Server Configuration Utility display with the `/bcs` command.

   Back to: Security Screen – Screen Map

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: An 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 can be used to allow the BIOS to complete the 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, alphabetical,
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 that does not meet the strong password criteria is entered, 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, see the *BIOS EPS for Intel® Server Boards D50TNP, M50CYP, and D40AMP*, Section 9.1.

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

Back to: Security Screen – 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 is previously set. This option protects setup settings and boot choices. The user password only allows limited access to the setup options, and no choice of boot devices.

   When Power On Password protection is enabled, the user password can be used to allow the BIOS to complete the 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 the previous field description, Number 3).

   For full details on BIOS password protection, refer to the *BIOS EPS for Intel® Server Boards D50TNP, M50CYP, and D40AMP*, Section 9.1.

   Note: This field does not support Intel® Server Configuration Utility changes with the `/bcs` command. However, the Intel® Server Configuration Utility `/bap` command can be used to set the user password.

   Back to: Security Screen – 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 the power-on and the BIOS asks for a password before continuing the POST and booting. Either the administrator or user password can be used.

   If an administrator password is not set, this option is grayed out and unavailable. Removing the administrator password also disables this option.

   Back to: Security Screen – 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 – Screen Map

7. **Current TPM Device**

   Value: TPM2.0 (DTPM)

   Help text: None.

   Comments: *Information only*. Shows the current TPM device. If the current TPM device is DTPM, TPM2.0 (DTPM) is shown. If there is no TPM device, this information is not shown.

   Back to: Security Screen – Screen Map

8. **TPM2 Operation**

   Value: **No Action**/TPM2 ClearControl(NO) + Clear

   Help text: `Select one of the supported operations to change TPM2 state.`

   Comments: Any TPM2 operation selected requires the system to perform a hard reset to become effective. For information about TPM support, refer to the *BIOS EPS for Intel® Server Boards D50TNP, M50CYP, and D40AMP*, Section 9.2.

   Back to: Security Screen – Screen Map

9. **PCR Bank: SHA1**

   Value: [Checkbox]

   Help text: `TCG2 Request PCR Bank: SHA1`

   Comments: Use the checkbox to select the **TPM Active PRC Bank**. Any TPM2 Operation selected requires the system to perform a hard reset to become effective. For information about TPM support, refer to the *BIOS EPS for Intel® Server Boards D50TNP, M50CYP, and D40AMP*, Section 9.2.

   Back to: Security Screen – Screen Map

10. **PCR Bank: SHA256**

    Value: [Checkbox]

    Help text: `TCG2 Request PCR Bank: SHA256`

    Comments: Use the checkbox to select the **TPM Active PRC Bank**. Any TPM2 Operation selected requires the system to perform a hard reset to become effective. For information about TPM support, refer to the *BIOS EPS for Intel® Server Boards D50TNP, M50CYP, and D40AMP*, Section 9.2.

    Back to: Security Screen – Screen Map

11. PCR Bank: SM3_256

Value: [Checkbox]

Help text: `TCG2 Request PCR Bank: SM3_256`

Comments: Use checkbox to select the TPM active PRC bank. Any TPM2 Operation selected requires the system to perform a hard reset to become effective. For information about TPM support, refer to the *BIOS EPS for Intel® Server Boards D50TNP, M50CYP, and D40AMP*, Section 9.2.

Back to: Security Screen – Screen Map

Notes:

TPM2 Operation, PCR Bank: SHA-1 and PCR Bank: SHA256 appear only on the boards equipped with a TPM. SM3_256 only works on a TPM module with SM3 capability (like iPC AXXTPMCHNE8).

The user must keep one PCR Bank checked when a PCR bank modification is done, otherwise the warning message shows up like: “Warning – Need one PCR Bank active. Press ENTER to continue...”. See the *BIOS EPS for Intel® Server Boards D50TNP, M50CYP, and D40AMP*, Section 11 for product-specific information about TPM availability.

TPM2 Operation, PCR Bank: SHA-1 and PCR Bank: SHA256 options do not support BIOS customization utilities (Intel® Server Configuration Utility nor Firmware Customization). This setting can be changed only within the setup menus of the target system.

---

12. TPM FW Update

Value: Enabled/**Disabled**

Help text: `Enable/disable Update TPM firmware.`

Comments: None.

Back to: Security Screen – Screen Map

13. TPM FW Version

Value: ID String for TPM

Help text: `Show current TPM FW Version.`

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

Back to: Security Screen – Screen Map

3.5 Server Management Screen

The Server Management screen allows the user to configure several server management features. This screen also provides an access point to the screens for configuring console redirection, displaying system information, and controlling the BMC LAN configuration.

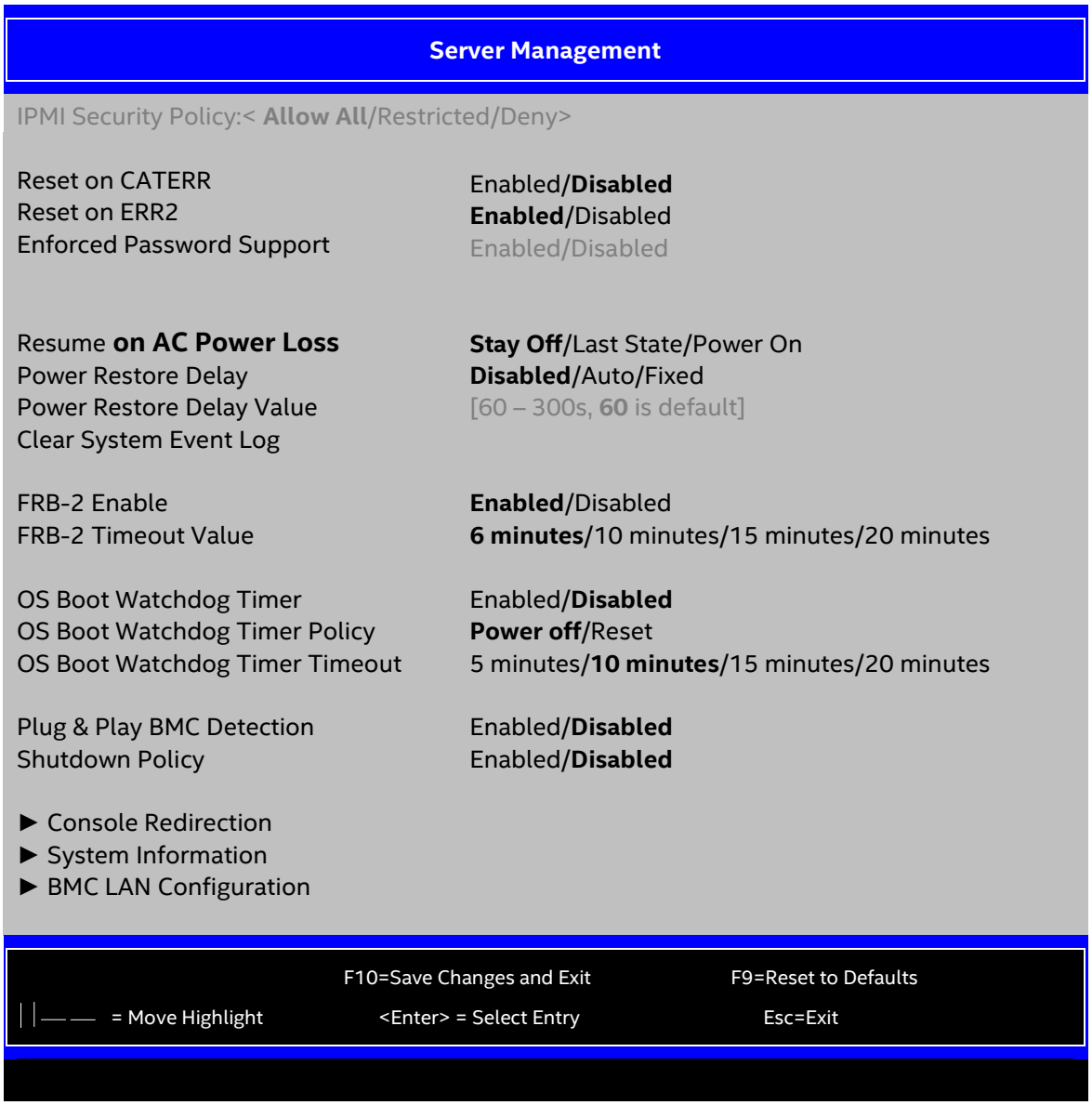


Figure 44. Server Management Screen

1. **IPMI Security Policy**

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

   Help text: None.

   Comments: *Information only*. This option shows the IPMI Security Policy information the BMC is set to be functioning with and if it is functioning in any mode out of Allow All, Restricted, and Deny All. This information is suppressed if the BMC is functioning on any Unknown state.

   Back to: Server Management Screen – Screen Map

2. **Reset on CATERR**

   Value: **Enabled**/Disabled

   Help text: `When enabled system gets reset upon encountering Catastrophic Error (CATERR); when disabled system does not get reset on CATERR.`

   Comments: This option controls whether the system is reset when the catastrophic error `CATERR#` signal is held asserted, rather than just pulsed to generate a system management interrupt (SMI). A CATERR indicates that the processor has encountered a fatal hardware error.

   Note: If this option is disabled, the result can be a system hang for certain error conditions, possibly causing the system to be unable to update the system status LED or log an error to the SEL before hanging.

   Back to: Server Management Screen – Screen Map

3. **Reset on ERR2**

   Value: **Enabled**/Disabled

   Help text: `When enabled system gets reset upon encountering ERR2 (Fatal error); when disabled system does not get reset on ERR2.`

   Comments: This option controls whether the system is reset if the BMC's ERR2 monitor times out. Such timeout error means that the ERR2 signal is continuously asserted long enough to indicate that the SMI handler is not able to service the condition.

   Note: If this option is disabled, the result can be a system hang for certain error conditions, possibly causing the system to be unable to update the system status LED or log an error to the SEL before hanging.

   Back to: Server Management Screen – Screen Map

4. **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: None.

   Back to: Server Management Screen – Screen Map

5. 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 followed by the BMC 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 the 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 the POST, 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.

Notes:

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

For Intel® Server Configuration Utility, this setting must come from the BMC via IPMI but not from the BIOS variable via `/bcs`.

Back to: Server Management Screen – Screen Map

6. **Power Restore Delay**

Value: **Disabled**/Auto/Fixed

Help text: `Allows a delay in powering up after a power failure, to reduce peak power requirements. The delay can be fixed or automatic between 60-300 seconds.`

Comments: When the AC power resume policy (see previous field description Number 5) is either Power On or Last State, this option allows a delay to be taken after AC power is restored, before the system actually begins to power up.

This delay can be either a fixed time or an automatic time. For the automatic delay, the BIOS selects a randomized 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 the systems drawing 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 the 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. What it means is that the BMC starts to power on the host with no delay after it finishes the BMC's IPMI stack initialization. A delay occurs, which time depends on how long the BMC needs to boot after AC power is restored.

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

Notes:

This option applies only to the power-on when AC is applied. It has no effect on powering the system up using the power button on the front panel. A DC power-on using the power button is not delayed.

If Intel® Server Configuration Utility/Intel® Server Information Retrieval Utility support is needed, this setting must come from the BMC via IPMI but not from the BIOS variable via `/bcs`.

For additional information about BIOS/BMC power control, refer to the *BIOS EPS for Intel® Server Boards D50TNP, M50CYP, and D40AMP*, Section 7.1.3.

Back to: Server Management Screen – Screen Map

7. 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 the 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 Intel® Server Configuration Utility/Intel® Server Information Retrieval Utility support is needed, get this setting from the BMC via IPMI but not from the BIOS variable via `/bcs`.

Back to: Server Management Screen – Screen Map

8. 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 measure gives the user the time/date when the log was cleared.

After selected, a confirmation popup 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

9. 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 the POST. When the BMC watchdog timer is used as a fault resistant booting level 2 (FRB-2) timer, it is initially set to allow six minutes for the 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 the POST is paused with the **<Pause>** key.

For more information on FRB-2 timer operation, refer to the *BIOS EPS for Intel® Server Boards D50TNP, M50CYP, and D40AMP*, Sections 3.16.4, 6.1.1.1, and 10.7.3.2.

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

10. FRB-2 Timeout Value

Value: **6 minutes**/10 minutes/15 minutes/20 minutes

Help text: `If FRB-2 enabled, this is the timeout value that BIOS will use to configure the FRB-2 timer.`

Comments: This option controls FRB-2 timer threshold if the BMC watchdog timer detects what appears to be a hang during the POST. This value is optionally set to 6/10/15/20 minutes for the POST to complete.

For more information on FRB-2 timer operation, refer to the *BIOS EPS for Intel® Server Boards D50TNP, M50CYP, and D40AMP*, Sections 3.16.4, 6.1.1.1, and 10.7.3.2.

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

11. 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 the 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 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 the *BIOS EPS for Intel® Server Boards D50TNP, M50CYP, and D40AMP*, Sections 3.16.4, 6.1.1.2, and 10.7.3.3.

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

12. 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

13. 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

14. 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

15. Shutdown Policy

Value: Enabled/**Disabled**

Help text: `Enable/Disable Shutdown Policy.`

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

Back to: Server Management Screen – Screen Map

16. 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

17. 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

18. 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 mode is kept 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 Super I/O in the BMC. However, if console redirection is to be coordinated with serial-over-LAN (SOL), the user must know that SOL is only supported through serial port A.

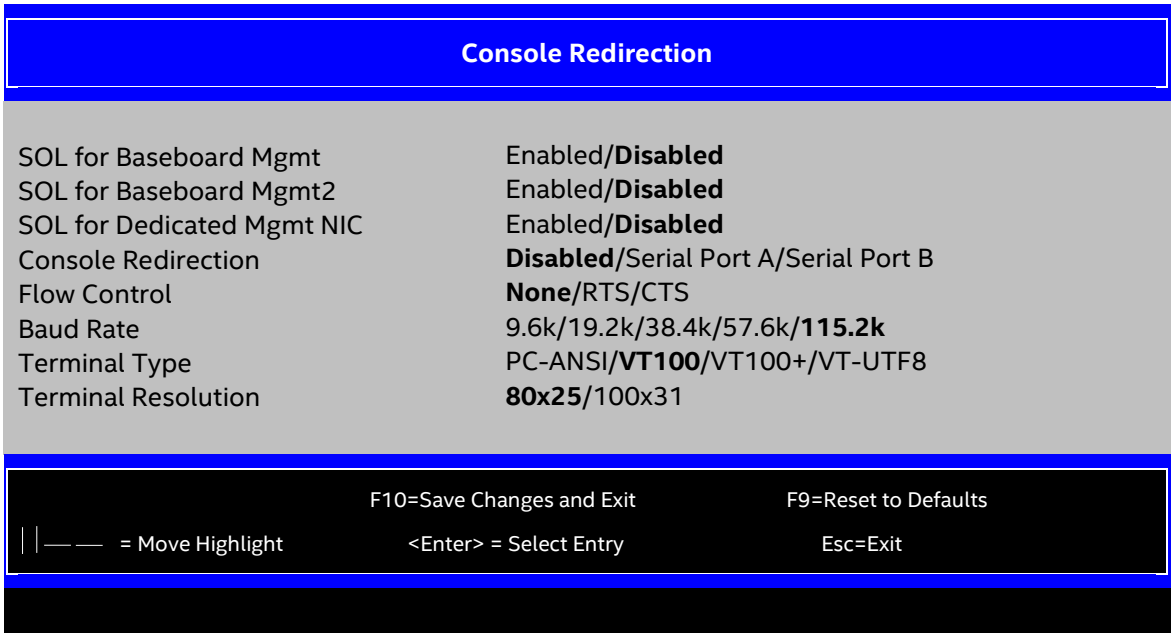


Figure 45. Console Redirection Screen

1. **SOL for Baseboard Mgmt**

   Value: Enabled/**Disabled**

   Help text: `Enable/disable Serial Over LAN feature for Baseboard Management Lan.`

   `[Advance>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 Intel® Server Configuration Utility/Intel® Server Information Retrieval Utility support is needed, get this setting from the BMC via IPMI but not from the BIOS variable via `/bcs`. This field does not support Firmware 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. [Advance>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 Intel® Server Configuration Utility/Intel® Server Information Retrieval Utility support is needed, get this setting from the BMC via IPMI, and not from the BIOS variable via `/bcs`. This field does not support Firmware Customization. Not all boards have this item, its presence depends on the board features.

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.`

   `[Advance>Serial Port Configuration>Serial A Enable] needs be enabled before enabling this option.`

   Comments: This option controls whether the BMC enables or disables the SOL feature on each LAN channel of the system following the IPMI 2.0 Specification. This feature could be re-enabled using the specific IPMI command.

   For more information, refer to the *BIOS EPS for Intel® Server Boards D50TNP, M50CYP, and D40AMP*, 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, options related to console redirection 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 Intel® Server Configuration Utility/Intel® Server Information Retrieval Utility support is needed, get this setting from the BMC via IPMI, and not from the BIOS variable via `/bcs`. This field does not support Firmware 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. 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. The three options are exposed in the BIOS configuration page from the Integrated BMC Web Console. If the board does not support serial port B but customer selects this option, the function still is disabled.

   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 built-in character encoding used by PC-compatible applications and emulators.

   For more information about character encoding, refer to the *BIOS EPS for Intel® Server Boards D50TNP, M50CYP, and D40AMP*, Section 7.4.

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

8. **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 screen serves the sole purpose of displaying information, the user cannot change any setting through the System Information screen.

To access this screen from the front page, select **Server Management** > **System Information**. Press the **<Esc>** key to return to the Server Management screen.

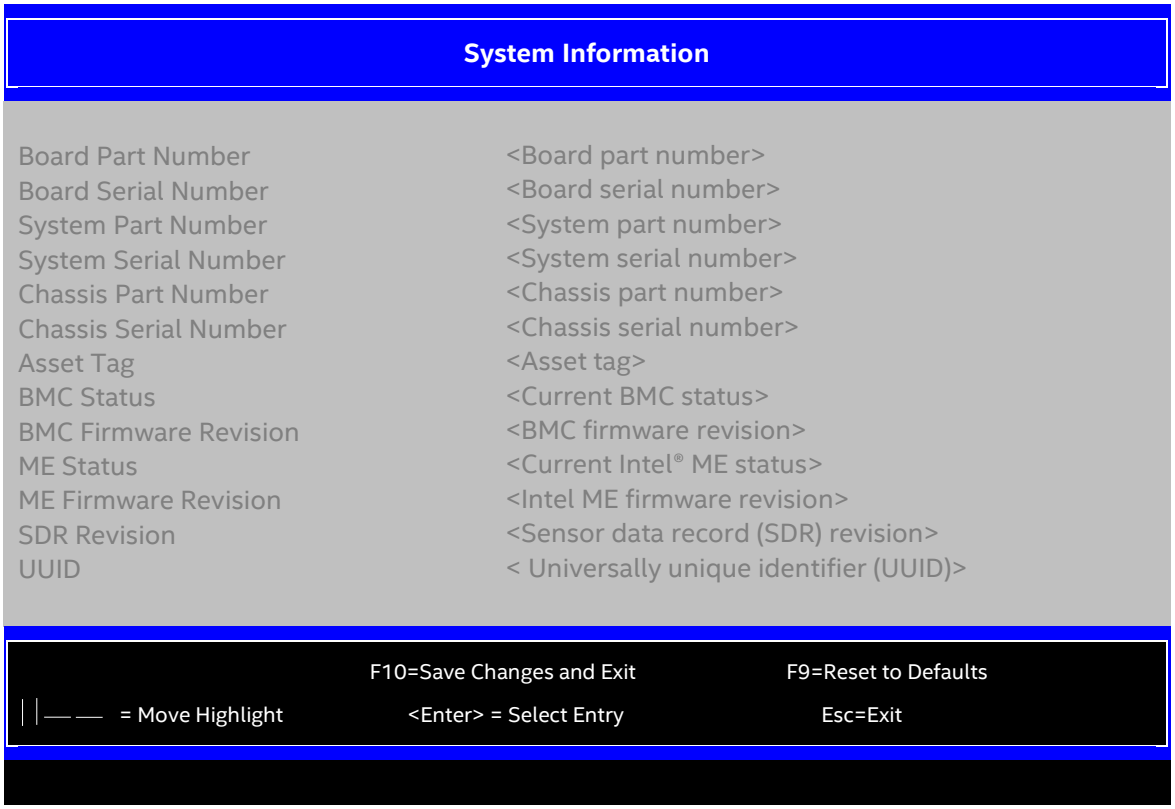


Figure 46. System Information Screen

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: *Information only*. This option indicates the BMC status, either 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(R) Management Engine (Intel(R) ME) status>

Help text: None.

Comments: *Information only*. This option indicates the Intel® ME status, either functional or failed.

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

11. ME Firmware Revision

Value: <Intel(R) 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: 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, also to manage the 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 (DMN) module can be installed in the server system. In that case, the LAN settings for the DMN module can 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 scenario is true for both the Baseboard LAN configuration and the Dedicated Server Management NIC Module.

IP addresses for either IPv4 or IPv6 addressing can be assigned by static IP addresses manually typed in, or by dynamic IP addresses supplied by a Dynamic Host Configuration Protocol (DHCP) server. IPv6 addressing can also be provided by stateless autoconfiguration that does not require a DHCP server.

The BMC LAN Configuration screen is unusual in that the LAN configuration parameters are maintained by the BMC itself. Because of this peculiarity, 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 changes are saved. If changes are discarded, any accumulated changes from this screen are disregarded and lost.

At the top of this page, two different messages can be displayed. The options are controlled accordingly, depending on the IPMI Security Policy information on Server Management screen.

These messages can be displayed:

- 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.
- 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.

Currently, only an NCSI-supported LAN embedded in a baseboard can function as BMC LAN. The setup options of IPv4 and IPv6 are exposed accordingly.

Note: If Intel® Server Configuration Utility/Intel® Server Information Retrieval Utility support is needed, all these settings under the BMC LAN Configuration must be gotten from the BMC via IPMI but not from the BIOS variable via `/bcs`. The fields on this screen do not support Firmware Customization.

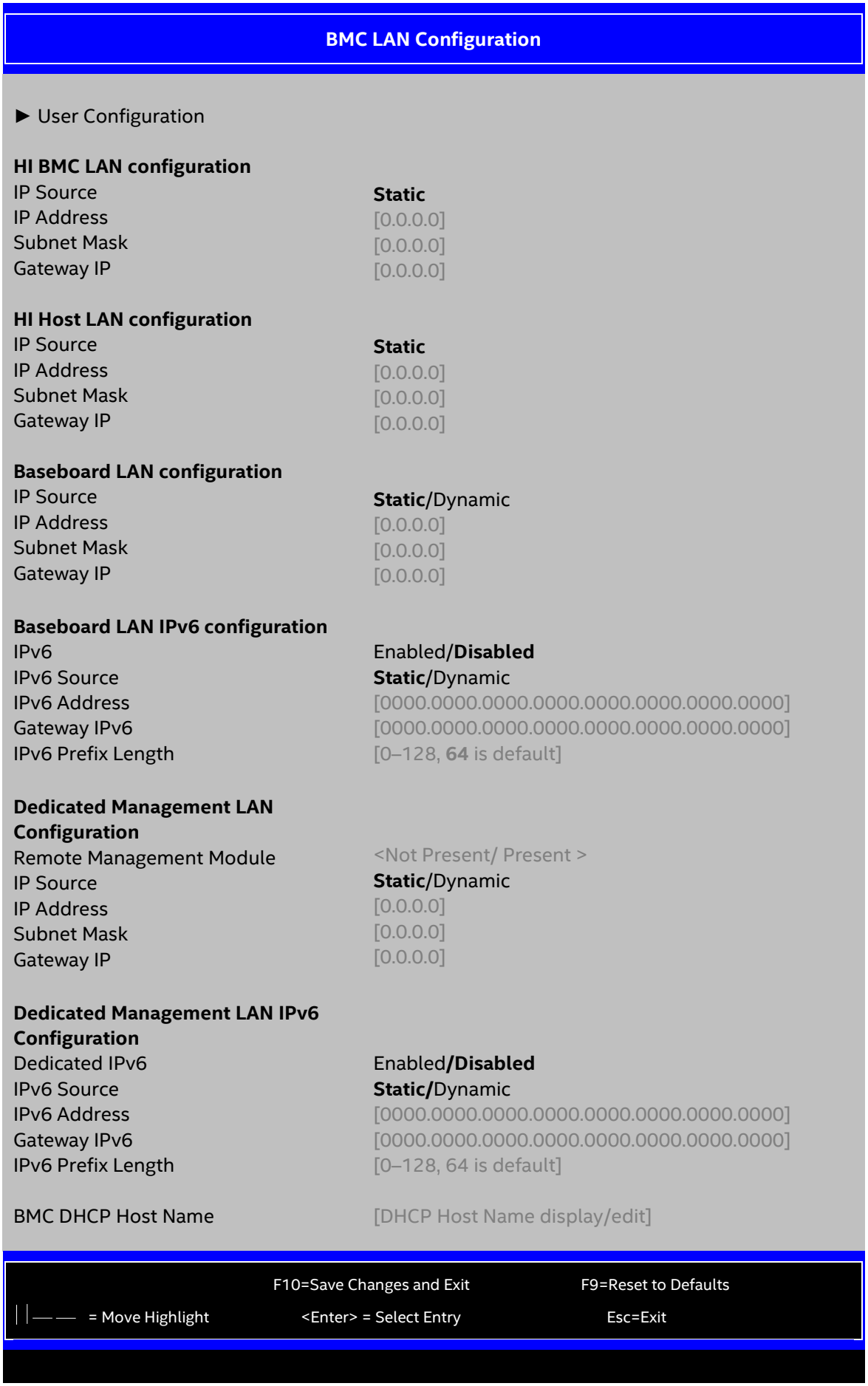


Figure 47. BMC LAN Configuration Screen

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 the 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**

   Help text: `None.`

   Comments: *Information only.* This specifies the IP source for IPv4 addressing for the Redfish* BMC LAN connection. There is a separate IP Source field for the HI BMC LAN configuration.

   When IPv4 addressing is used, the initial value for this field is acquired from the BMC.

   This option gets grayed out if the IPMI Security Policy information on the 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 Redfish* BMC LAN. There is a separate IPv4 address field for the HI BMC LAN configuration.

   When IPv4 addressing is used, the initial value for this field is acquired from the BMC.

   This option gets grayed out if the IPMI Security Policy information on the 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 Redfish* BMC LAN. There is a separate IPv4 Subnet Mask field for the HI BMC LAN configuration.

   When IPv4 addressing is used, the initial value for this field is acquired from the BMC.

   This option gets grayed out if the IPMI Security Policy information on the 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 Redfish* BMC LAN. There is a separate IPv4 addressing gateway IP field for the HI BMC LAN configuration.

   When IPv4 addressing is used, the initial value for this field is acquired from the BMC.

   This option gets grayed out if the IPMI Security Policy information on the 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. **IP Source**

   Value: **Static**

   Help text: `None.`

   Comments: *Information only.* This specifies the IP source for IPv4 addressing for the Redfish* Host LAN connection. There is a separate IP Source field for the HI Host LAN configuration.

   When IPv4 addressing is used, the initial value for this field is configured by the user.

   This option gets grayed out if the IPMI Security Policy information on the 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. **IP Address**

   Value: [Entry Field 0.0.0.0, **0.0.0.0 is default**]

   Help text: `View/Edit IP Address. Press <Enter> to edit.`

   Comments: This specifies the IPv4 address for the Redfish* Host LAN. There is a separate IPv4 address field for the HI Host LAN configuration.

   When IPv4 addressing is used, the initial value for this field is configured by the user.

   This option gets grayed out if the IPMI Security Policy information on the 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. Subnet Mask

Value: [Entry Field 0.0.0.0, **0.0.0.0 is default**]

Help text: `View/Edit Subnet Mask. Press <Enter> to edit.`

Comments: This specifies the IPv4 addressing subnet mask for the Redfish* Host LAN. There is a separate IPv4 Subnet Mask field for the HI Host LAN configuration.

When IPv4 addressing is used, the initial value for this field is configured by the user.

This option gets grayed out if the IPMI Security Policy information on the 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 IP

Value: [Entry Field 0.0.0.0, **0.0.0.0 is default**]

Help text: `View/Edit Gateway IP. Press <Enter> to edit.`

Comments: This specifies the IPv4 addressing gateway IP for the Redfish* Host LAN. There is a separate IPv4 addressing gateway IP field for the HI Host LAN configuration.

When IPv4 addressing is used, the initial value for this field is configured by the user.

This option gets grayed out if the IPMI Security Policy information on the 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. 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 item specifies the IP source for IPv4 addressing for the baseboard LAN. A separate IP Source field is available for the Dedicated Management LAN Configuration.

When IPv4 addressing is used, the initial value for this field is acquired from the BMC. This BMC setting determines whether the other baseboard LAN IPv4 addressing fields are display-only (when Dynamic) or can be edited (when Static).

When IPv6 addressing is enabled, this field is grayed out and inactive.

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

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

11. IP Address

Value: [Entry Field 0.0.0.0, **0.0.0.0 is default**]

Help text: `View/Edit IP Address. Press <Enter> to edit.`

Comments: This item specifies the IPv4 address for the baseboard LAN. A separate IPv4 Address field is available for the Dedicated Management LAN Configuration.

When IPv4 addressing is used, the initial value for this field is acquired from the BMC. The IP Source setting determines whether this field is display-only (when Dynamic) or can be edited (when Static).

When IPv6 addressing is enabled, this field is grayed out and inactive.

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

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

12. Subnet Mask

Value: [Entry Field 0.0.0.0, **0.0.0.0 is default**]

Help text: `View/Edit Subnet Mask. Press <Enter> to edit.`

Comments: This item specifies the IPv4 addressing subnet mask for the baseboard LAN. A separate IPv4 Subnet Mask field is available for the Dedicated Management LAN Configuration.

If IP Source is set to Static, the default value of Subnet Mask is `0.0.0.0`. If a cable is connected, and IP Source is set to be Dynamic, the default value of Subnet Mask that comes from the BMC must be `255.255.255.0`.

When IPv4 addressing is used, the initial value for this field is acquired from the BMC. The IP Source setting determines whether this field is display-only (when Dynamic) or can be edited (when Static). When IPv6 addressing is enabled, this field is grayed out and inactive.

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

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

13. Gateway IP

Value: [Entry Field 0.0.0.0, **0.0.0.0 is default**]

Help text: `View/Edit Gateway IP. Press <Enter> to edit.`

Comments: This item specifies the IPv4 addressing gateway IP for the baseboard LAN. A separate IPv4 Gateway IP field is available for the Dedicated Management LAN Configuration.

When IPv4 addressing is used, the initial value for this field is acquired from the BMC.

The IP Source setting determines whether this field is display-only (when Dynamic) or can be edited (when Static). When IPv6 addressing is enabled, this field is grayed out and inactive.

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

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

14. 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 can 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 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

15. 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 item specifies the IP source for IPv6 addressing for the baseboard LAN configuration. A separate IPv6 Source field is available for the Dedicated Management LAN Configuration.

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

When IPv6 addressing is enabled, the initial value for this field is acquired from the BMC. This BMC setting determines whether the other baseboard LAN IPv6 addressing fields are display-only (when Dynamic or Auto) or can be edited (when Static).

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

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

16. **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 item specifies the IPv6 address for the baseboard LAN. A separate IPv6 Address field is available 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 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

17. **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 item specifies the gateway IPv6 address for the baseboard LAN. A separate Gateway IPv6 address field is available 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 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

18. 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 item specifies the IPv6 prefix length for the baseboard LAN. A separate IPv6 Prefix Length field is available 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 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

19. Remote Management Module

Value: <Not Present/Present>

Help text: None.

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

When the Management Module is not present at all, the fields for Dedicated Management LAN Configuration are not visible.

When IPv6 is Disabled, the IPv4 configuration fields are visible, and the IPv6 configuration fields are not visible.

When IPv6 is Enabled, the IPv4 fields are grayed out and inactive, while the IPv6 Configuration fields are visible.

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

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.

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

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

20. 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 item specifies the IP source for IPv4 addressing for the DMN LAN connection. A separate IP Source field is available for the baseboard LAN configuration.

When IPv4 addressing is used, the initial value for this field is acquired from the BMC. This BMC setting determines whether the other DMN LAN IPv4 addressing fields are display-only (when Dynamic) or can be edited (when Static).

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

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

21. 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 item specifies the IPv4 address for the DMN LAN. A separate IPv4 Address field is available for the baseboard LAN configuration.

When IPv4 addressing is used, the initial value for this field is acquired from the BMC.

The IP Source setting determines whether this field is display-only (when Dynamic) or can be edited (when Static).

When IPv6 addressing is enabled, this field is grayed out and inactive.

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

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

22. 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 item specifies the IPv4 addressing subnet mask for the DMN LAN. A separate IPv4 Subnet Mask field is available for the baseboard LAN configuration.

If IP Source is set to Static, the default value of Subnet Mask is `0.0.0.0`. If a cable is connected, and IP Source is previously set to be Dynamic, the default value of Subnet Mask that comes from the BMC must be `255.255.255.0`.

When IPv4 addressing is used, the initial value for this field is acquired from the BMC.

The IP Source setting determines whether this field is display-only (when Dynamic) or can be edited (when Static).

When IPv6 addressing is enabled, this field is grayed out and inactive.

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

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

23. 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 item specifies the IPv4 addressing gateway IP for the DMN LAN. A separate IPv4 Gateway IP field is available for the baseboard LAN configuration.

When IPv4 addressing is used, the initial value for this field is acquired from the BMC.

The IP Source setting determines whether this field is display-only (when Dynamic) or can be edited (when Static).

When IPv6 addressing is enabled, this field is grayed out and inactive.

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

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

24. Dedicated IPv6

Value: Enabled/**Disabled**

Help text: `Enable/Disable Dedicated IPv6.`

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

When this option is set to Disabled, all other IPv6 fields are not visible for DMN (if installed).

When IPv6 addressing is set to Enabled, all IPv6 fields for the Dedicated Management DMN become visible, and all IPv4 fields for Dedicated LAN are grayed out and inactive.

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

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

25. 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 item specifies the IP source for IPv6 addressing for the DMN LAN configuration. A separate IPv6 Source field is available 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. This BMC setting determines whether the other DMN LAN IPv6 addressing fields are display-only (when Dynamic or Auto) or can be edited (when Static).

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

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

26. 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 item specifies the IPv6 address for the DMN LAN. A separate IPv6 Address field is available 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 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

27. 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 item specifies the gateway IPv6 address for the DMN LAN. A separate Gateway IPv6 Address field is available 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 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

28. 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 item specifies the IPv6 prefix length for the DMN LAN. A separate IPv6 Prefix Length field is available 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 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

29. 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 can be edited whenever at least one of the IP Source or IPv6 Source options is set to Dynamic.

This item displays 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 IPv4/IPv6 Source fields are set to Dynamic, then this BMC DHCP Host Name field is grayed out and inactive.

This page gets grayed out if the IPMI Security Policy information on Server Management screen is shown as IPMI Security Policy: 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.

Note: This form option is not configurable and 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.

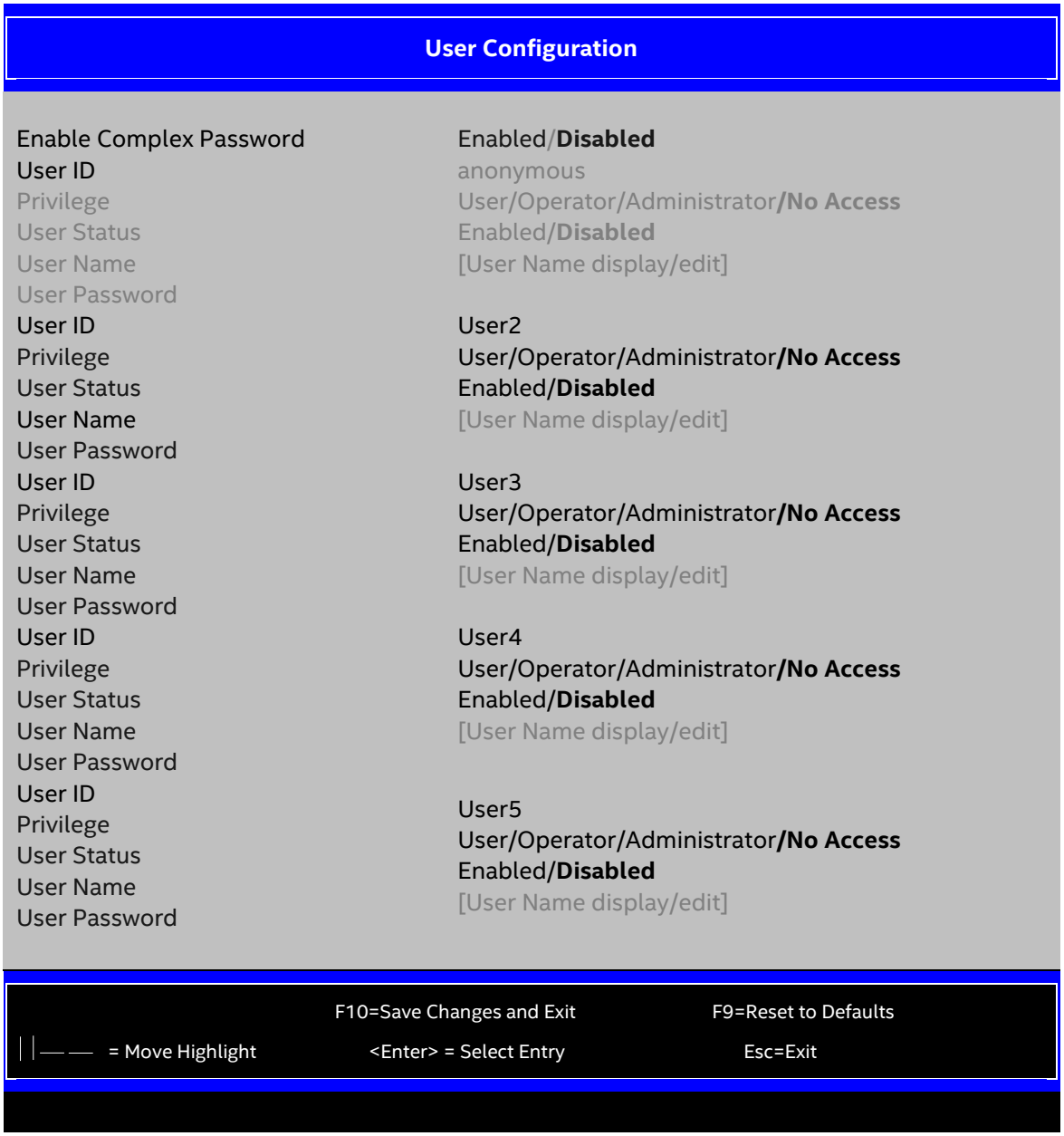


Figure 48. User Configuration Screen

1. **Enable Complex Password**

   Value: Enabled/**Disabled**

   Help text: `When enabled User password should match the complexity criteria. 8 to 20 characters & Must Contain Letters (Both Upper & Lower case), Numbers(0-9) and Special Characters & Cannot be the same as the username or username in reverse order & Have at least two new characters when compared with previous password.`

   Comments: The default status setting is Disabled.

   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. The anonymous is not available to modify from the legacy BMC side, gray out as information display only.

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

3. **Privilege**

   Value: User/Operator/Administrator/**No Access**

   Help text: `View/Select user privilege. All users must be set to a privilege other than No Access and enabled for IPMI messaging before they can be used on any channel.`

   Comments: The level of privilege that is assigned for a user ID affects which functions that user can 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: 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 null/blank always. Since user names are unique, no other users can be named *null* nor like 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. No display is available.

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

Note: Privilege and User Status gray out if User Name is empty or not configured. This measure is needed for security reasons. The right step is to change the User Name first and then reboot to make it work. After that, Privilege and User Status setting can be modified.

3.6 Boot Maintenance Manager Screen

The Boot Maintenance Manager screen contains all bootable media encountered during the 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 the POST is used to boot the system. The same device continues to be used to reboot the system until the boot device configuration is changed (that is, a change in which boot devices are present) or until the system is powered down and booted in a cold power-on boot.

Notes:

USB devices can be hot plugged during the POST, they are detected and "beeped". Such hot-plugged USB devices are enumerated and displayed on the USB Configuration Setup screen. However, these hot-plugged USB devices are not enumerated as bootable devices, depending on when during the POST they are hot plugged. If they are recognized before the enumeration of bootable devices, they appear as boot devices, if appropriate. If they are recognized after the enumeration, they do not appear as bootable devices on the Boot Maintenance Manager screen, the Boot Manager screen, nor the Boot Menu.

A USB key (USB flash drive) can be formatted to emulate either a floppy drive or a hard drive and appear in that boot device class. Although it can be formatted as a CD-ROM drive, it is not detected as such and is treated as a hard disk drive appearing in the list of available hard drives.

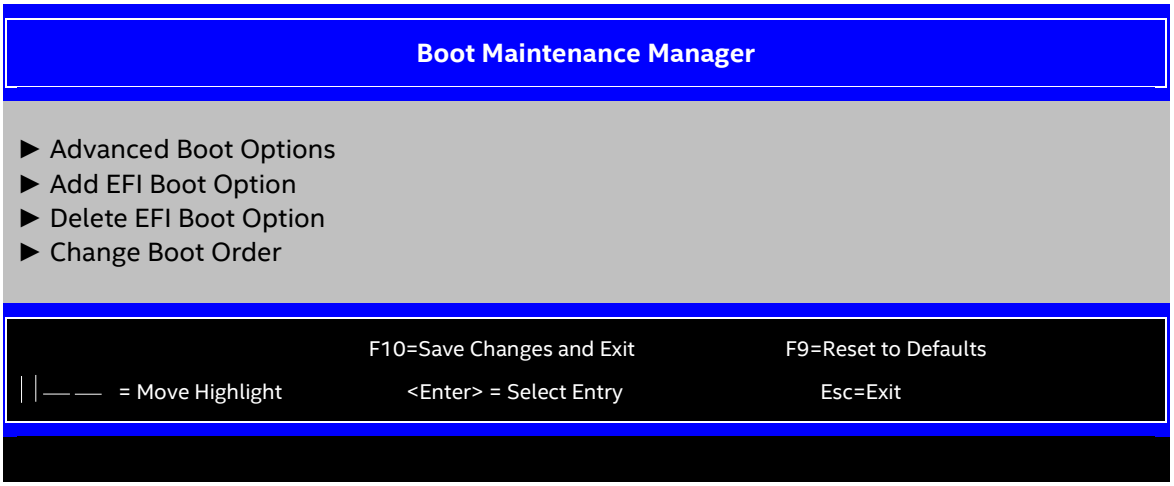


Figure 49. Boot Maintenance Manager Screen

1. **Advanced Boot Options**

   Value: None.

   Help text: `Set the Advanced Boot Options in this group.`

   Comments: *Selection only*. For more information on Advanced Boot Options, see Section 3.6.1.

   Back to: Boot Maintenance Manager Screen – Screen Map

2. Add EFI Boot Option

Value: None.

Help text: `Add a new EFI boot option to the boot order.`

Comments: *Selection only*. For more information on Add EFI Boot Option, see Section 3.6.2.

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

Note: This field does not support Intel® Server Configuration Utility changes with the `/bcs` command. However, the Intel® Server Configuration Utility `/bbo` or `/bbosys` commands can be used to set boot order. This field does not support Firmware Customization.

Back to: Boot Maintenance Manager Screen – Screen Map

3. Delete EFI Boot Option

Value: None.

Help text: `Remove an EFI boot option from the boot order.`

Comments: *Selection only*. For more information on Delete EFI Boot Option settings, see Section 3.6.3.

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

Notes:
This field does not support Intel® Server Configuration Utility changes with the `/bcs` command. However, the Intel® Server Configuration Utility `/bbo` or `/bbosys` commands can be used to set boot order. This field does not support Firmware Customization.

For the boot option added by the BIOS BDS, it can be deleted in this menu, and it can be added again at the end of boot order in the next BIOS POST.

Back to: Boot Maintenance Manager Screen – Screen Map

4. Change Boot Order

Value: None.

Help text: `Set the Boot Order in this group.`

Comments: *Selection only*. For more information on Change Boot Order settings, see Section 3.6.4.

Note: This field does not support Intel® Server Configuration Utility changes with the `/bcs` command. However, the Intel® Server Configuration Utility `/bbo` or `/bbosys` commands can be used to set boot order. This field does not support Firmware 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.

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

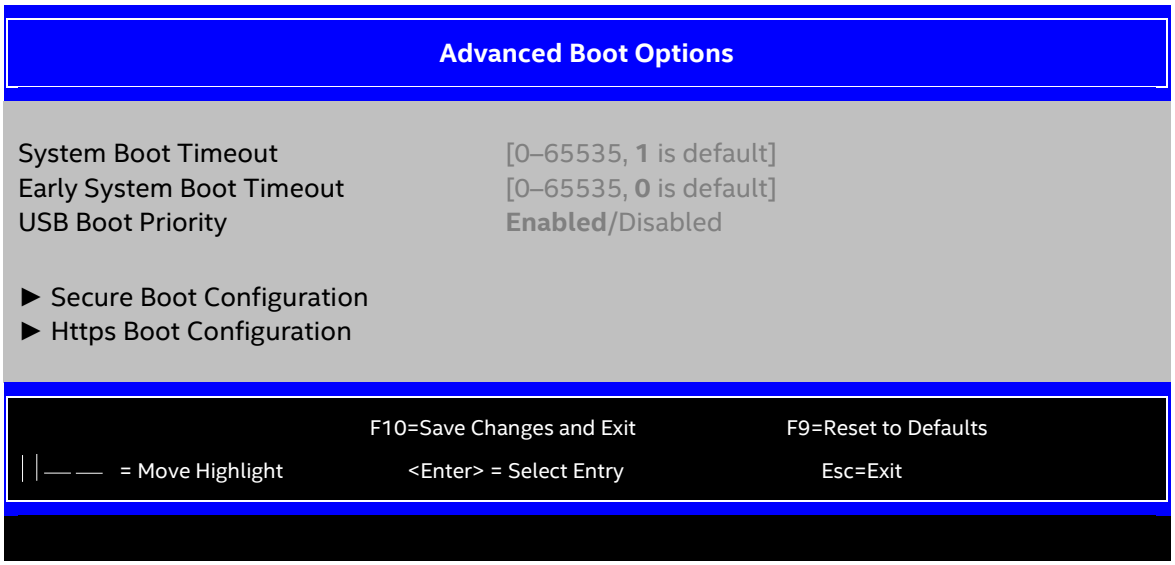


Figure 50. Advanced Boot Options Screen

1. **System Boot Timeout**

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

   Help text: `The number of seconds BIOS will pause at the end of POST to allow the user to press the [F2] key for entering the BIOS Setup Utility.`

   `Valid values are 0-65535. 1 is the default. A value of 65535 causes the system to go to the Boot Manager menu and wait for user input for every system boot.`

   Comments: After entering the desired timeout in seconds, press the **<Enter>** key to register that timeout value to the system. The timeout value entered takes effect on the next boot.

   This timeout value is independent of the FRB-2 setting for BIOS boot failure protection. The FBR-2 countdown is suspended during the time that the boot timeout countdown is active.

   If the **<Pause>** key is pressed while the boot timeout is active, the boot timeout countdown is suspended until the pause state is dismissed and a 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.

   The BIOS cannot support any key that is pressed while 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. **USB Boot Priority**

   Value: **Enabled**/Disabled

   Help text: `If enabled, newly discovered USB devices are moved to the top of their boot device category.`

   `If disabled, newly discovered USB devices are moved to the bottom of their boot device category.`

   Comments: None.

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

4. **Secure Boot Configuration**

   Value: None.

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

   Comments: None.

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

5. **Https Boot Configuration**

   Value: None.

   Help text: `Set the Https Boot Configuration Options in this group.`

   Comments: None.

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

3.6.1.1 Secure Boot Configuration

The Secure Boot Configuration screen allows the user to configure the UEFI secure boot.

To access this screen from the front page, select **Boot Maintenance Manager** > **Advanced Boot Options** > **Secure Boot Configuration**. Press the **<Esc>** key to return to the Advanced Boot Options screen.

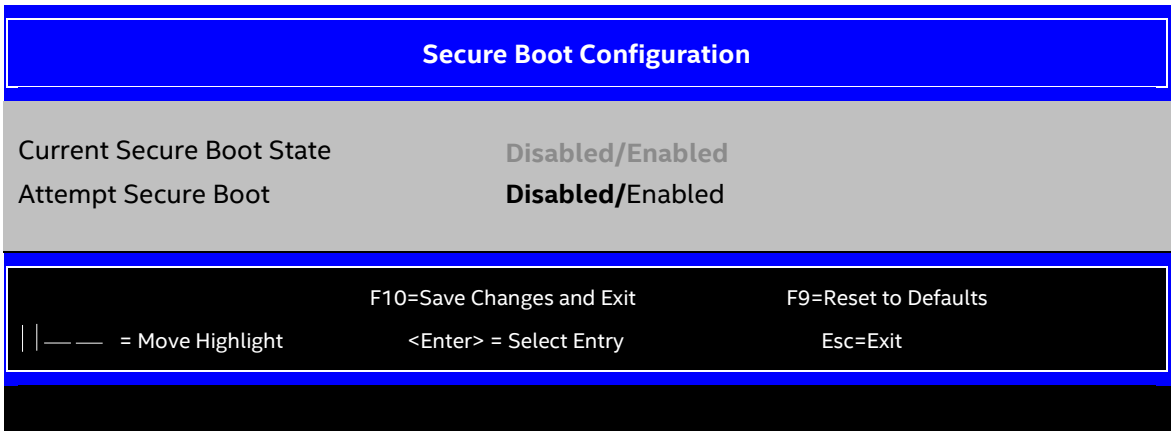


Figure 51. Secure Boot Configuration Screen

1. **Current Secure Boot State**

   Value: Disabled/Enabled

   Help text: `Current Secure Boot state: enabled or disabled.`

   Comments: *Information only*. Displays the current secure boot state. A platform reset is required after enabling or disabling the BIOS UEFI secure boot feature in the Attempt Secure Boot option described below.

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

   Back to: Secure Boot Configuration – 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, during a platform reset after this option is turned to Enabled. The BIOS provisions the default keys automatically if the corresponding key is not present.

Notes:

The product BIOS ships a default set of `PK`, `KEK`, `db`, and `dbx` in the BIOS release images. The BIOS provisions the keys for the first-time user to successfully enable this option. After `PK`, `KEK`, `db`, and `dbx` are provisioned, the user must use Intel® Server Configuration Utility to update these keys using digitally signed payloads (according to the *Unified Extensible Firmware Interface Specification*, version 2.3.1). When a new BIOS capsule release contains new keys (if the private key is compromised or there is a known security vulnerability):

- If the user has already done the provision, the new keys are NOT provisioned, and old keys still take effect. Using Intel® Server Configuration Utility to update keys with signed payload is mandatory.
- If the user has not yet done the provision (never enabled the UEFI secure boot before), the new keys are provisioned and take effect.

This option is protected by BIOS administrator password as basic security level. A more advanced security level requires that platform physical presence policy to be applied, so that the secure boot feature control option can be changed. Therefore, Current Secure Boot State is not always successfully changed after a platform reset if the advanced security check fails.

For Intel® Server Configuration Utility related support, Secure Boot just supports proprietary solution defined in the *Intel® Server Configuration Utility User Guide*. The user can use Intel® Server Configuration Utility `/sboot` to attempt to change current secure boot enable or disable status. The BIOS does not support other commands for general setup options, such as `/s` or `/bcs` command.

Back to: Secure Boot Configuration – Advanced Boot Options – Boot Maintenance Manager Screen – Screen Map

3.6.1.2 Https Boot Configuration

The Https Boot Configuration allows the user to configure the options for Https Boot Configuration.

To access this screen from the front page, select **Boot Maintenance Manager** > **Advanced Boot Options** > **Https Boot Configuration**. Press the **<Esc>** key to return to the Advanced Boot Options screen.

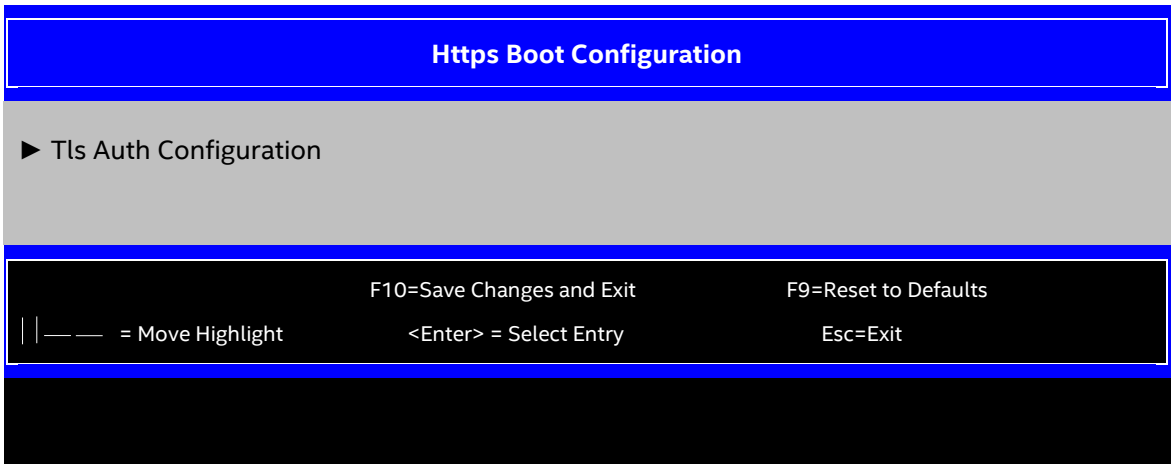


Figure 52. Https Boot Configuration Screen

1. Tls Auth Configuration

Value: None.

Help text: `Press <Enter> to select Tls Auth Configuration.`

Comments: None.

Back to: Https Boot Configuration – Advanced Boot Options – Boot Maintenance Manager Screen – Screen Map

3.6.1.3 Tls Auth Configuration

The Https Boot Configuration screen allows the user to configure Tls Auth Configuration.

To access this screen from the front page, select **Boot Maintenance Manager** > **Advanced Boot Options** > **Https Boot Configuration** > **Tls Auth Configuration**. Press the **<Esc>** key to return to the Advanced Boot Options screen.

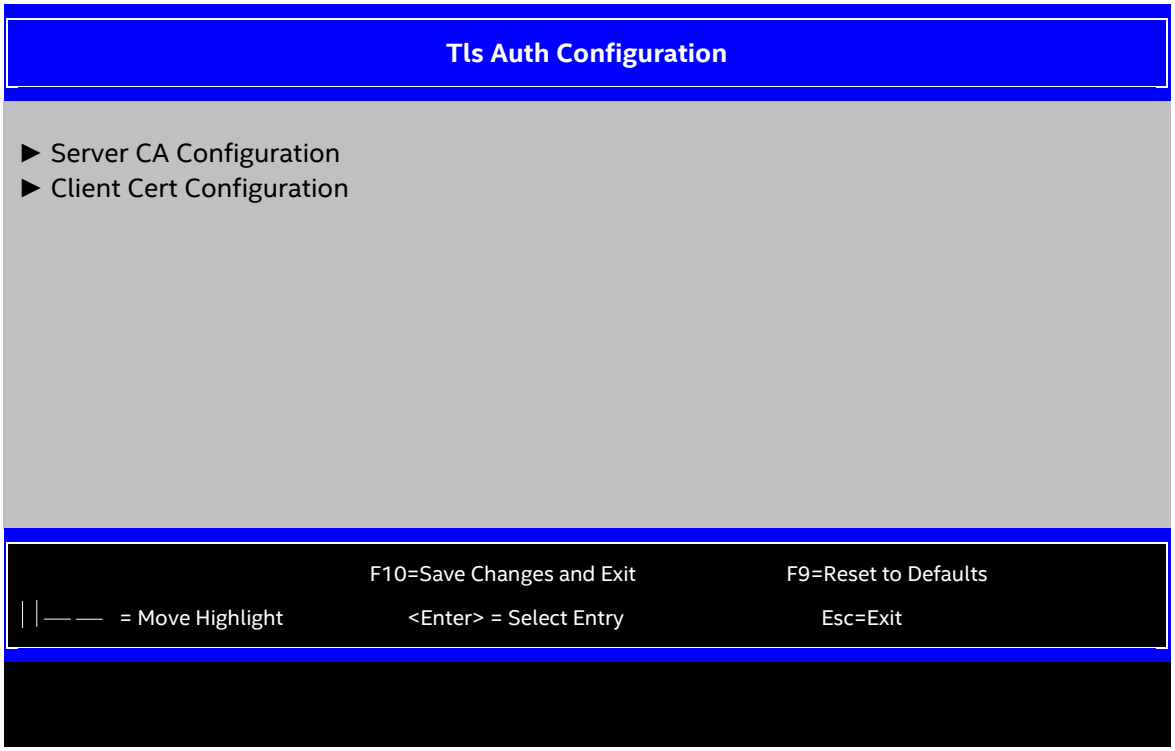


Figure 53. Tls Auth Configuration Screen

1. **Server CA Configuration**

Value: None.

Help text: `Press <Enter> to configure Server CA.`

Comments: None.

Back to: Tls Auth Configuration – Https Boot Configuration – Advanced Boot Options – Boot Maintenance Manager Screen – Screen Map

2. **Client Cert Configuration**

Value: None.

Help text: `Client cert configuration is unsupported currently.`

Comments: Currently unsupported.

Back to: Tls Auth Configuration – Https Boot Configuration – Advanced Boot Options – Boot Maintenance Manager Screen – Screen Map

3.6.1.4 Server CA Configuration

The Https Boot Configuration screen allows the user to access and modify Server CA Configuration.

To access this screen from the front page, select **Boot Maintenance Manager** > **Advanced Boot Options** > **Https Boot Configuration** > **Tls Auth Configuration** > **Server CA Configuration**. Press the **<Esc>** key to return to the Advanced Boot Options screen.

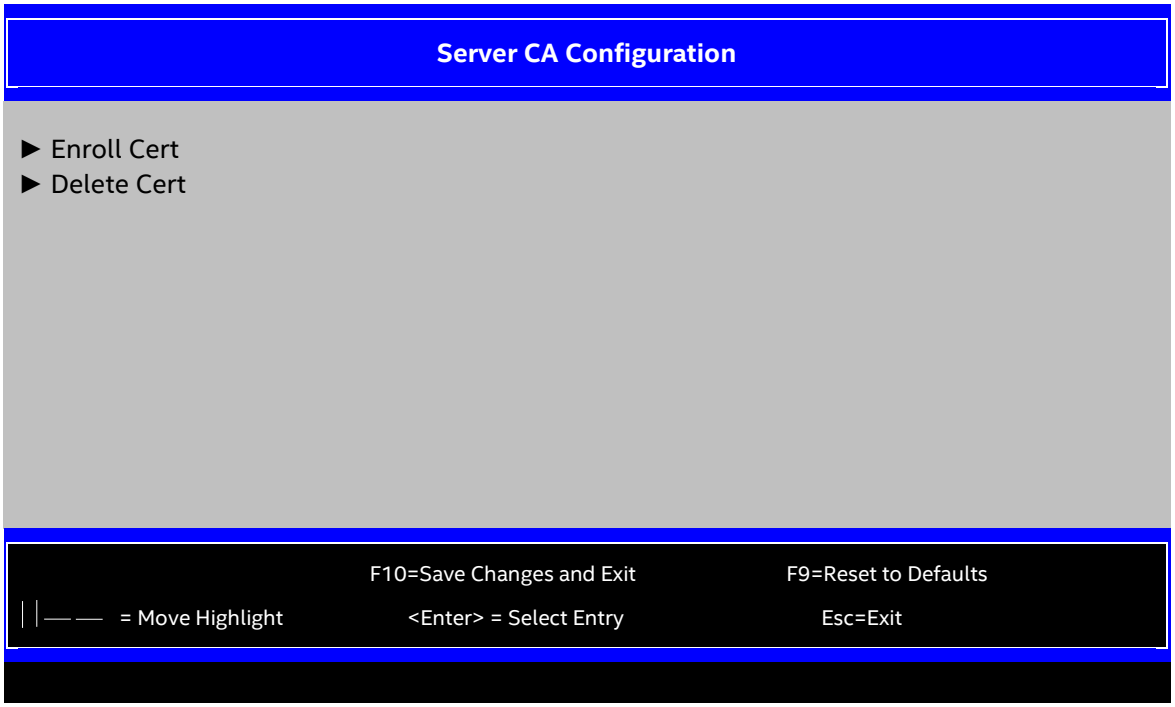


Figure 54. Server CA Configuration Screen

1. **Enroll Cert**

Value: None.

Help text: `Press <Enter> to enroll cert.`

Comments: None.

Back to: Server CA Configuration – Tls Auth Configuration – Https Boot Configuration – Advanced Boot Options – Boot Maintenance Manager Screen – Screen Map

2. **Delete Cert**

Value: None.

Help text: `Press <Enter> to delete cert.`

Comments: None.

Back to: Server CA Configuration – Tls Auth Configuration – Https Boot Configuration – Advanced Boot Options – Boot Maintenance Manager Screen – Screen Map

3.6.1.5 Enroll Cert

The Https Boot Configuration screen allows the user to access and modify Server CA Configuration.

To access this screen from the front page, select **Boot Maintenance Manager** > **Advanced Boot Options** > **Https Boot Configuration** > **Tls Auth Configuration** > **Server CA Configuration** > **Enroll Cert**. Press the **<Esc>** key to return to the Advanced Boot Options screen.

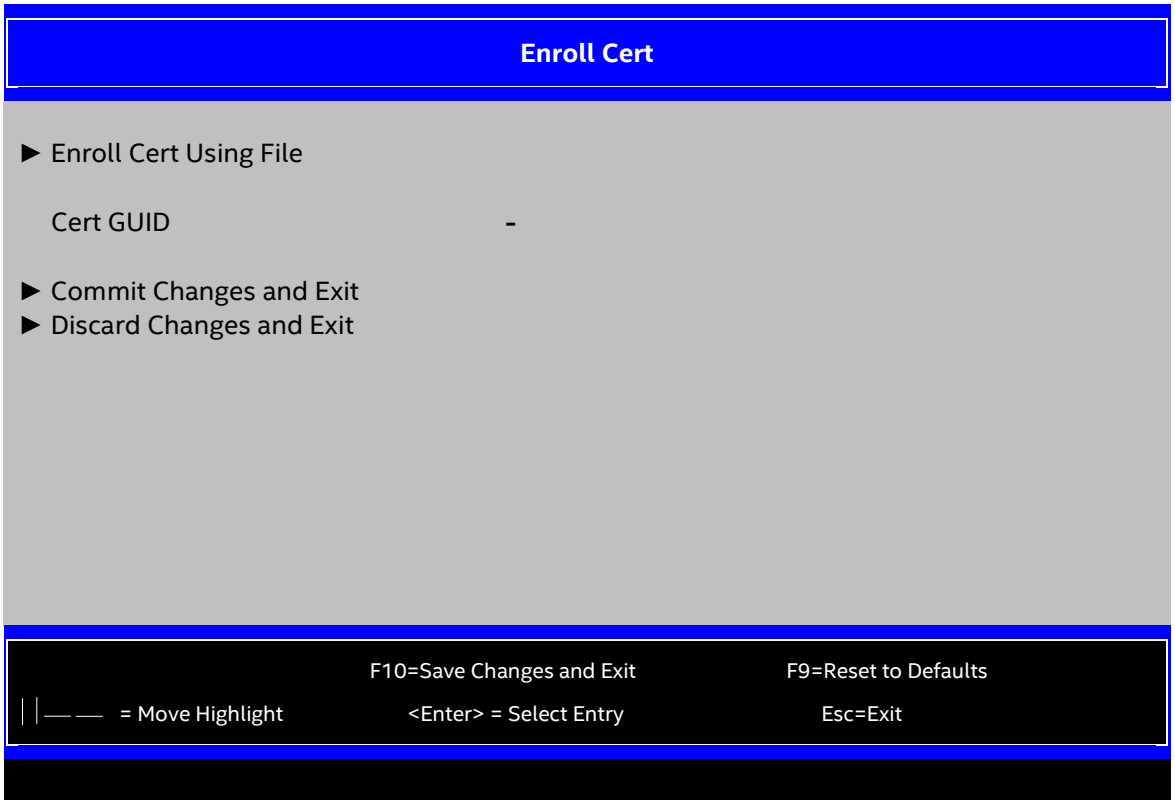


Figure 55. Enroll Cert Screen

1. **Enroll Cert Using File**

Value: None.

Help text: `Enroll Cert Using File`

Comments: None.

Back to: Enroll Cert – Server CA Configuration – Tls Auth Configuration – Https Boot Configuration – Advanced Boot Options – Boot Maintenance Manager Screen – Screen Map

2. **Cert GUID**

Value: -

Help text: `Input digit character in 11111111-2222-3333-4444-1234567890ab format.`

Comments: None.

Back to: Enroll Cert – Server CA Configuration – Tls Auth Configuration – Https Boot Configuration – Advanced Boot Options – Boot Maintenance Manager Screen – Screen Map

3. Commit Changes and Exit

Value: None.

Help text: `Commit Changes and Exit.`

Comments: None.

Back to: Enroll Cert – Server CA Configuration – Tls Auth Configuration – Https Boot Configuration – Advanced Boot Options – Boot Maintenance Manager Screen – Screen Map

4. Discard Changes and Exit

Value: None.

Help text: `Discard Changes and Exit.`

Comments: None.

Back to: Enroll Cert – Server CA Configuration – Tls Auth Configuration – Https Boot Configuration – Advanced Boot Options – Boot Maintenance Manager Screen – Screen Map

3.6.2 Add EFI Boot Option

The Add EFI Boot Option screen allows the user to add an EFI boot option to the boot order. The Internal EFI Shell boot option is permanent and cannot be added or deleted.

To access this screen from the front page, select **Boot Maintenance Manager** > **Add EFI Boot Option**. Press the **<Esc>** key to return to the Boot Maintenance Manager screen.

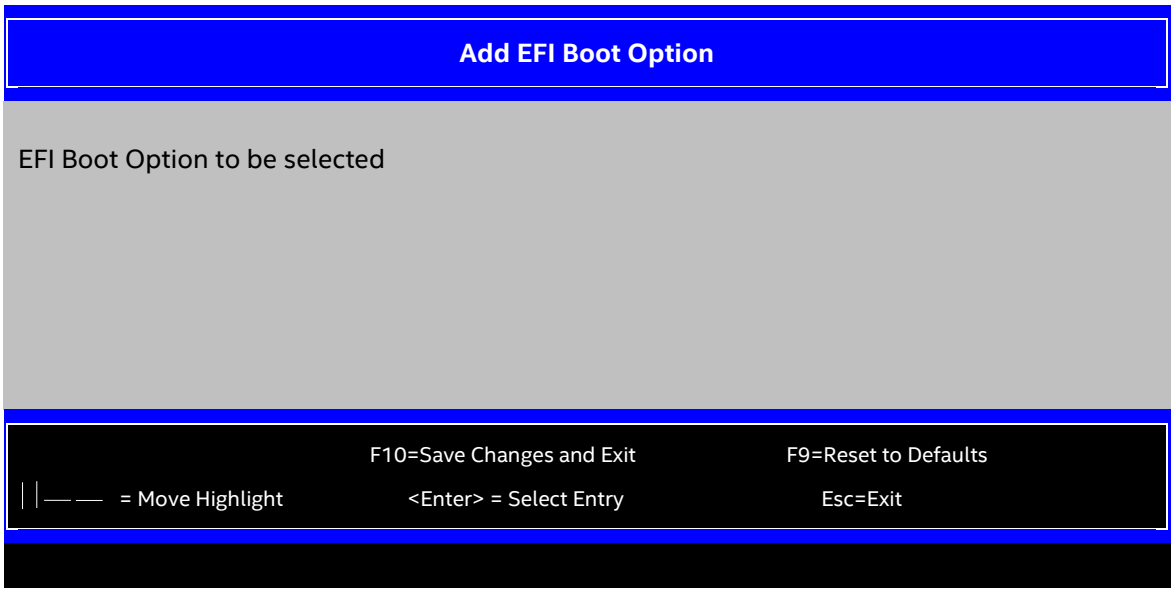


Figure 56. Add EFI Boot Option Screen

1. **EFI Boot Option to be selected**

   Value: None.

   Help text: None.

   Comments: *Selection only*. This item lists the current EFI devices paths enumerated by the BIOS during the POST, for the user to select the EFI Boot Option.

   Back to: Add EFI Boot Option – Boot Maintenance Manager Screen – Screen Map

3.6.3 Delete EFI Boot Option

The Delete EFI Boot Option screen allows the user to remove an EFI boot option from the boot order. The Internal EFI Shell boot option is not listed since it is permanent and cannot be added or deleted.

To access this screen from the front page, select **Boot Maintenance Manager** > **Delete EFI Boot Option**. Press the **<Esc>** key to return to the Boot Maintenance Manager screen.

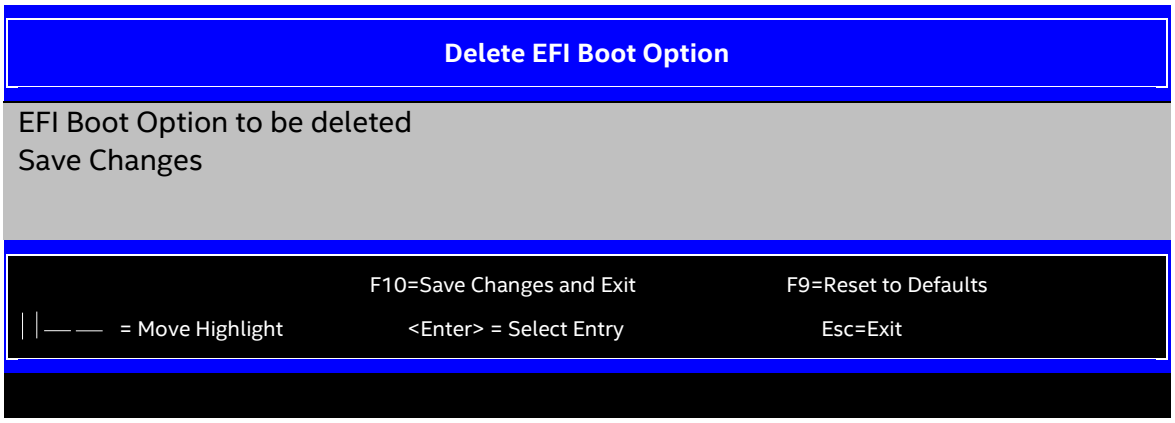


Figure 57. Delete EFI Boot Option Screen

1. **EFI Boot Option to be deleted**

   Value: [Checkbox]

   Help text: `Select one to delete.`

   Comments: Use the checkbox to select the EFI boot option to be deleted. This item does not allow a user to delete the EFI shell.

   Back to: Delete EFI Boot Option – Boot Maintenance Manager Screen – Screen Map

3.6.4 Change Boot Order

The Change Boot Order screen allows the user to configure the desired order in which the UEFI boot devices are to be tried sequentially.

To access this screen from the front page, select **Boot Maintenance Manager** > **Delete EFI Boot Option**. Press the **<Esc>** key to return to the Boot Maintenance Manager screen.

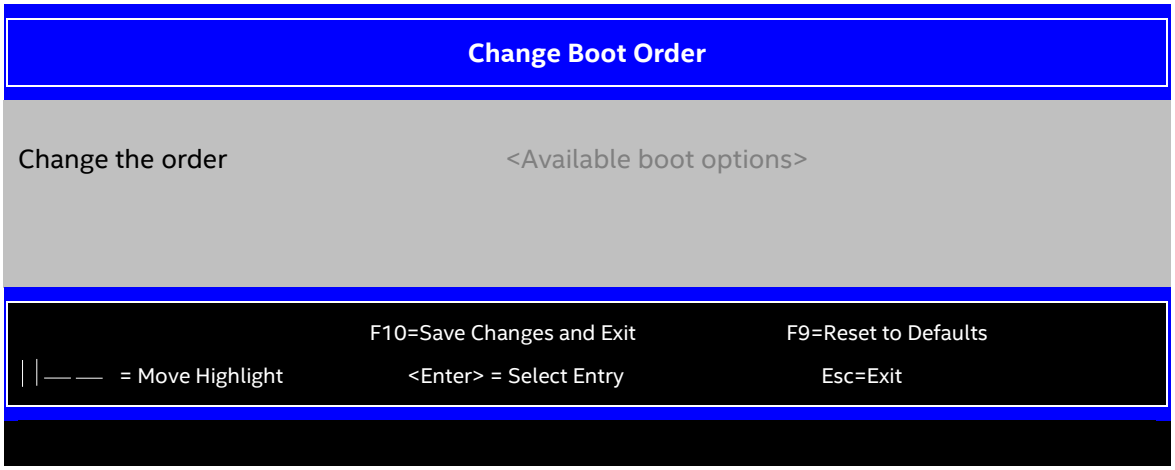


Figure 58. Change Boot Order Screen

1. **Change the order**

   Value: <Available boot options>

   Help text: `Use [Enter] key and [Up Arrow] or [Down Arrow] to select the booting device. Use [+] or [-] key to move up/down the selected field.`

   Comments: None.

   Back to: Change Boot Order – Boot Maintenance Manager Screen – 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 to immediately boot the system. No predetermined order is set for listing bootable devices, they are simply listed in order of discovery. The Internal EFI Shell option is always available, regardless of any other bootable device availability.

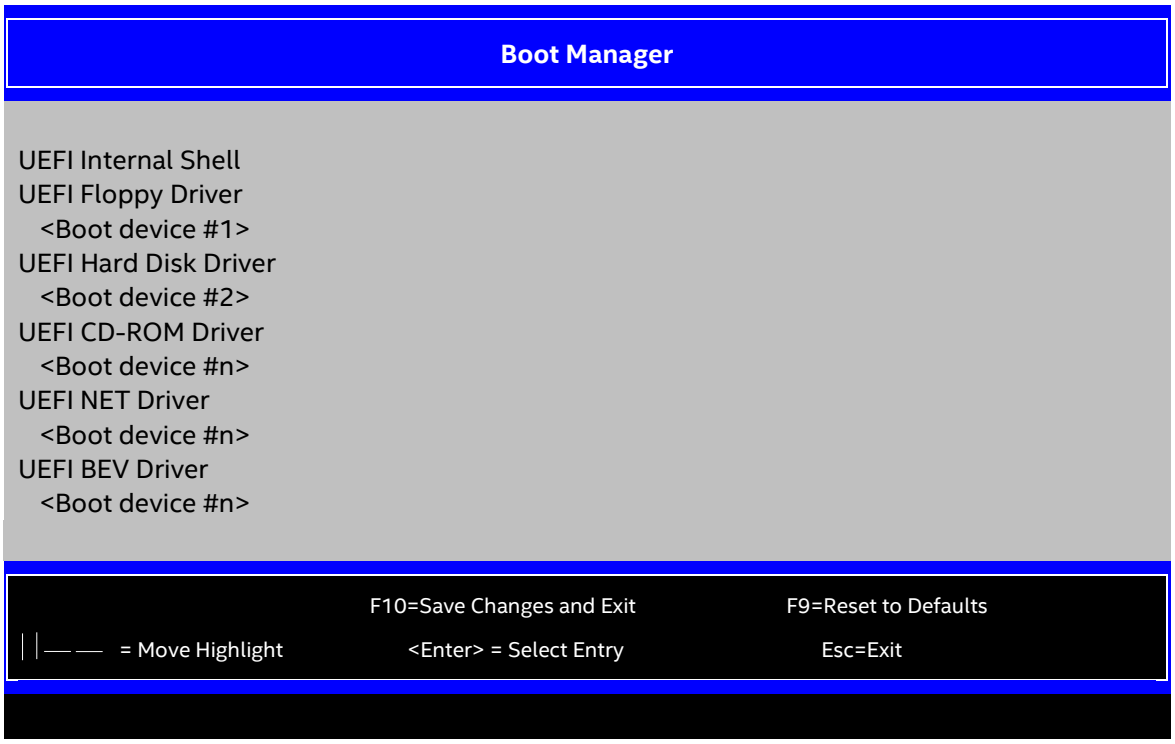


Figure 59. Boot Manager Screen

1. **UEFI Internal Shell**

   Value: None.

   Help text: `Select this option to boot now.`

   `Note: This list is not the system boot option order. Use the Boot Maintenance Manager menu to view and configure the system boot option order.`

   Comments: The EFI shell is always present in the list of bootable devices.

   Note: This field does not support Intel® Server Configuration Utility changes with the `/bcs` command. However, the Intel® Server Configuration Utility `/bbo` or `/bbosys` commands can be used to set boot order.

   Back to: Boot Manager Screen – Screen Map

2. **<Boot device #1>**
3. **<Boot device #2>**
4. **<Boot device #n>**

Value: None.

Help text: `Select this option to boot now.`

`Note: This list is not the system boot option order. Use the Boot Maintenance Manager menu to view and configure the system boot option order.`

Comments: These are names of bootable devices discovered in the system. The system user can choose any of them to initiate a one-time boot from it. Booting from any device in this list does not permanently affect the defined system boot order.

These bootable devices are not displayed in any specified order, particularly not in the system boot order established by the Boot Maintenance Manager screen. This item is just a list of bootable devices in the order in which they are enumerated.

Note: This field does not support Intel® Server Configuration Utility changes with the `/bcs` command. However, the Intel® Server Configuration Utility `/bbo` or `/bbosys` commands can be used to set boot order.

Back to: Boot Manager Screen – Screen Map

3.8 Error Manager Screen

The Error Manager screen displays any POST error codes encountered during the BIOS POST, along with help text to explain the meaning of the error code. This screen is used only to display information.

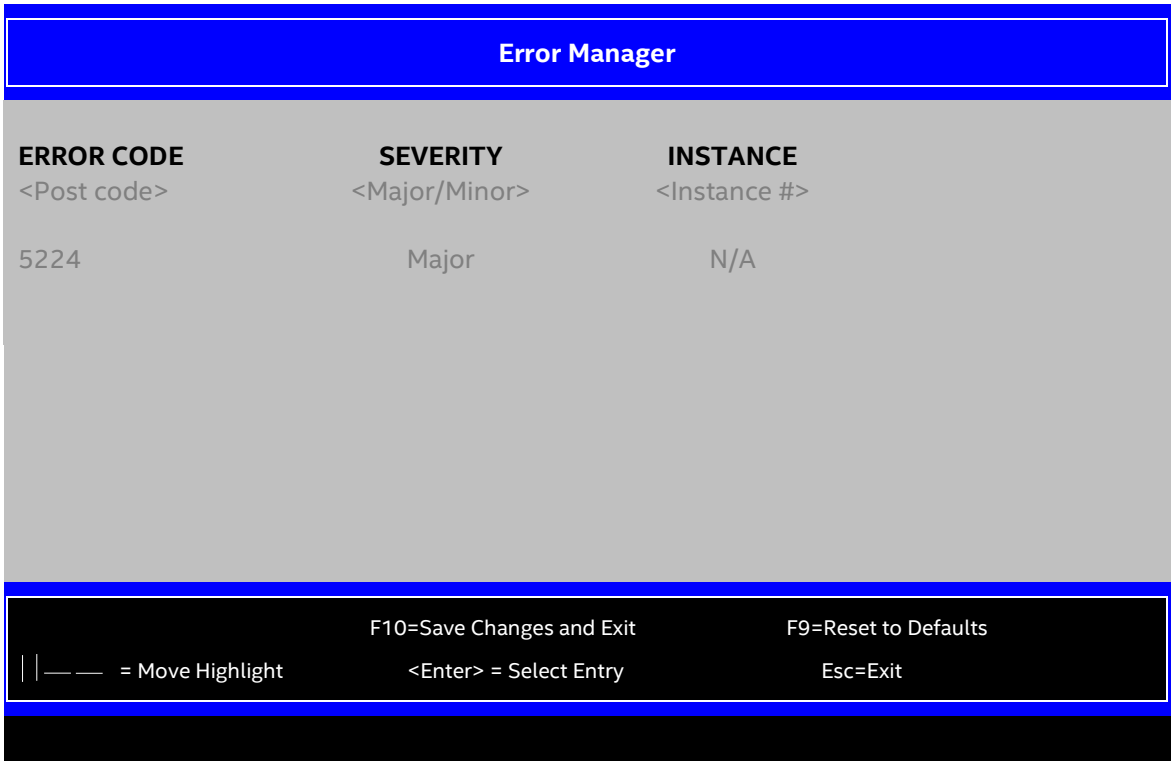


Figure 60. Error Manager Screen

1. **ERROR CODE**

   Value: <POST error code>

   Help text: Not applicable.

   Comments: The POST error code is a BIOS-originated error that occurred during the POST initialization. For more information on POST error codes, refer to the *BIOS EPS for Intel® Server Boards D50TNP, M50CYP, and D40AMP*, Section 10.5.4.1.3.

   Back to: Error Manager Screen – Screen Map

2. **SEVERITY**

   Value: Minor/Major/Fatal

   Help text: Not applicable.

   Comments: Each POST error code has a severity associated with it. For more information on POST error codes, refer to the *BIOS EPS for Intel® Server Boards D50TNP, M50CYP, and D40AMP*, Section 10.5.4.3.4.

   Back to: Error Manager Screen – Screen Map

3. INSTANCE

Value: <Depends on error code>

Help text: Not applicable.

Comments: Where applicable, this field shows a value indicating which one of a group of components is responsible for generating the POST error code 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: A legal disclaimer footnote appears at the bottom of the Save & Exit screen:

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

This disclaimer refers 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.

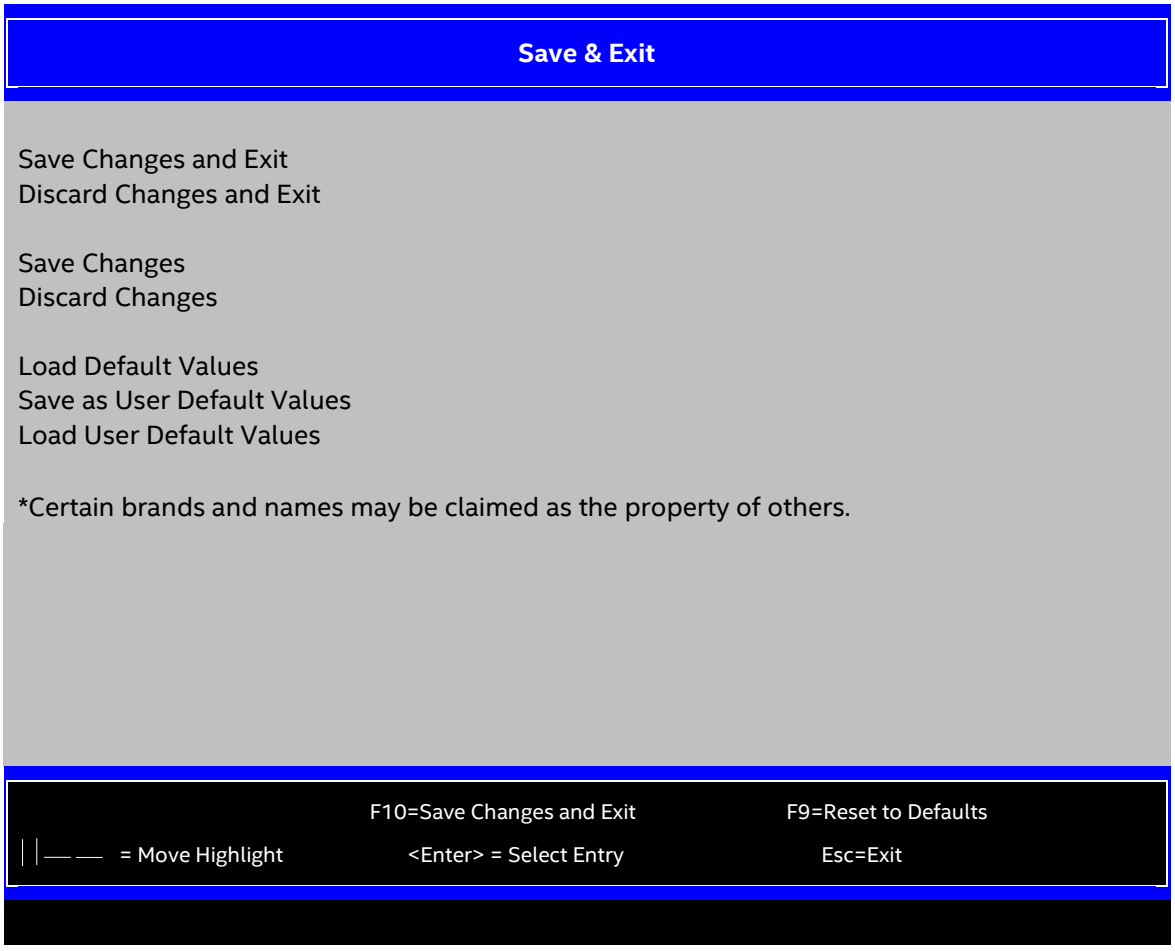


Figure 61. Save & Exit Screen

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 are no changes made in the settings, the BIOS resumes executing the POST.

   If changes are made in BIOS settings, a confirmation popup 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. Then, if necessary (which is normally the case), the system reboots.

   If the Save Changes and Exit action is not confirmed, the BIOS resumes executing setup.

   The **<F10>** function key can 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 are no changes made in the settings, the BIOS resumes executing the POST.

   If changes are made in BIOS settings, a confirmation popup appears.

   If the Discard Changes and Exit action is positively confirmed, all the pending changes are discarded and the BIOS resumes executing the 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 are no changes made in the settings, the BIOS resumes executing the POST.

   The user must be aware that most changes require a reboot to become active. If changes are made and saved without exiting setup, the system must 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 are no changes made in the settings, the BIOS resumes executing the POST.

   If changes are made in BIOS settings and not yet saved, a confirmation popup appears.

   If the Discard Changes action is positively confirmed, all the pending changes are discarded and the BIOS resumes executing the 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 Default Values for all the setup options.`

   Comments: *Selection only*. Select this line and press the **<Enter>** key to load default values for all BIOS settings. Such values are the initial factory settings (“failsafe” settings) for all BIOS parameters.

   A confirmation popup asks the users if they really intend to perform this action.

   After initializing all BIOS settings to default values, the BIOS resumes executing setup. Resuming setup allows the user to make additional changes in the BIOS settings if necessary (for example, a boot order).

   A Save Changes and Exit action with a reboot makes the default settings take effect, including any changes made after loading the defaults.

   The **<F9>** function key can be used also 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 user-determined sets of BIOS default settings can be used as an alternative, instead of using 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.

A confirmation popup asks the users if they really intend to perform this action.

Loading the factory default values does not affect the user default values. They remain set to whatever values that they were last saved as.

Note: Due to a setup limitation, BIOS variables in type `VARSTORE` do not need to support Save As/Load User Default. For example, BMC owned options are within this scope, such as Power Restore Policy, thermal related options, and all settings under BMC LAN Configuration.

Back to: Save & Exit Screen – Screen Map

7. Load User Default Values

Value: None.

Help text: `Load the User Default Values to all the setup options.`

Comments: *Selection only*. Select this line and press the **<Enter>** key to load user default values for all BIOS settings.

These are user-customized BIOS default settings for all the BIOS parameters previously established by doing a Save User Defaults action.

A confirmation popup asks the users if they really intend to perform 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 within this scope, such as Power Restore Policy, thermal related options, and all settings under BMC LAN Configuration.

Back to: Save & Exit Screen – Screen Map

3.10 Intel® Optane™ PMem Setup

The information in this section applies to the Intel® Server Systems M50CYP, D50TNP, and D40AMP.

Note: Only Intel® Optane™ PMem 200 series modules are supported. Previous generations of Intel® Optane™ PMem modules are not supported.

3.10.1 Configure Modes for Intel® Optane™ PMem Using BIOS for Intel® Server Boards

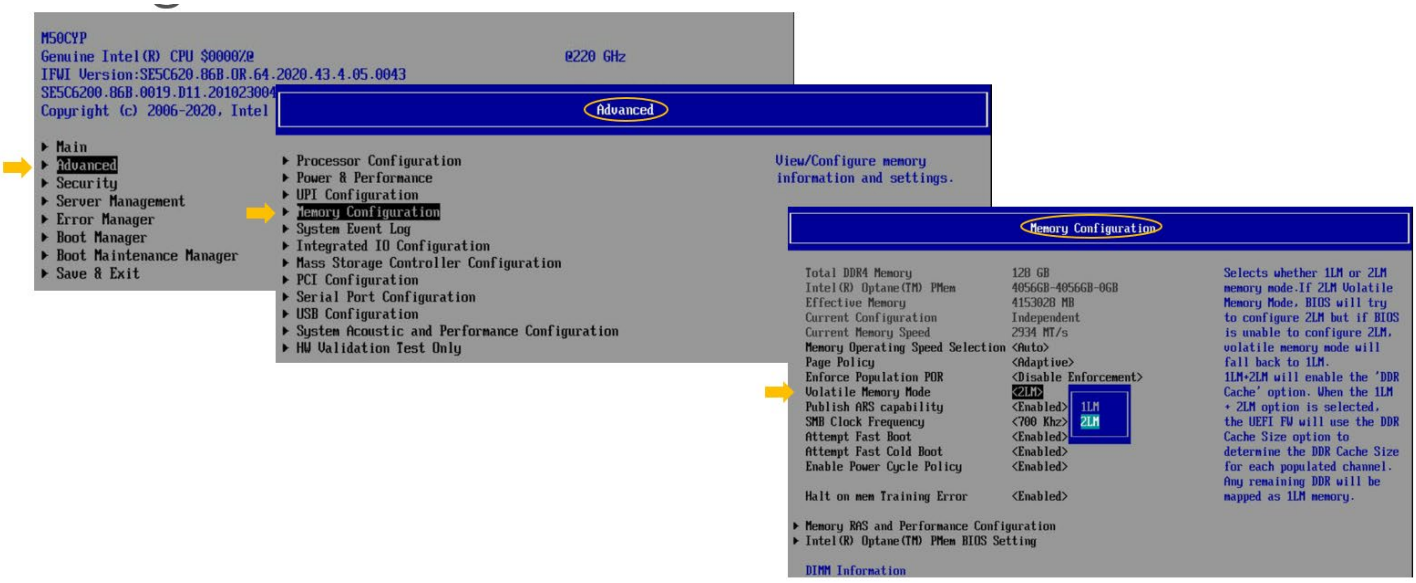


Figure 62. Configure PMem Mode

From the opening BIOS screen, click **Advanced** > **Memory Configuration** > **Volatile Memory Mode**. Select **1LM** to configure Intel® Optane™ PMem in App Direct mode, **2LM** for Memory Mode.

3.10.2 View Memory Information

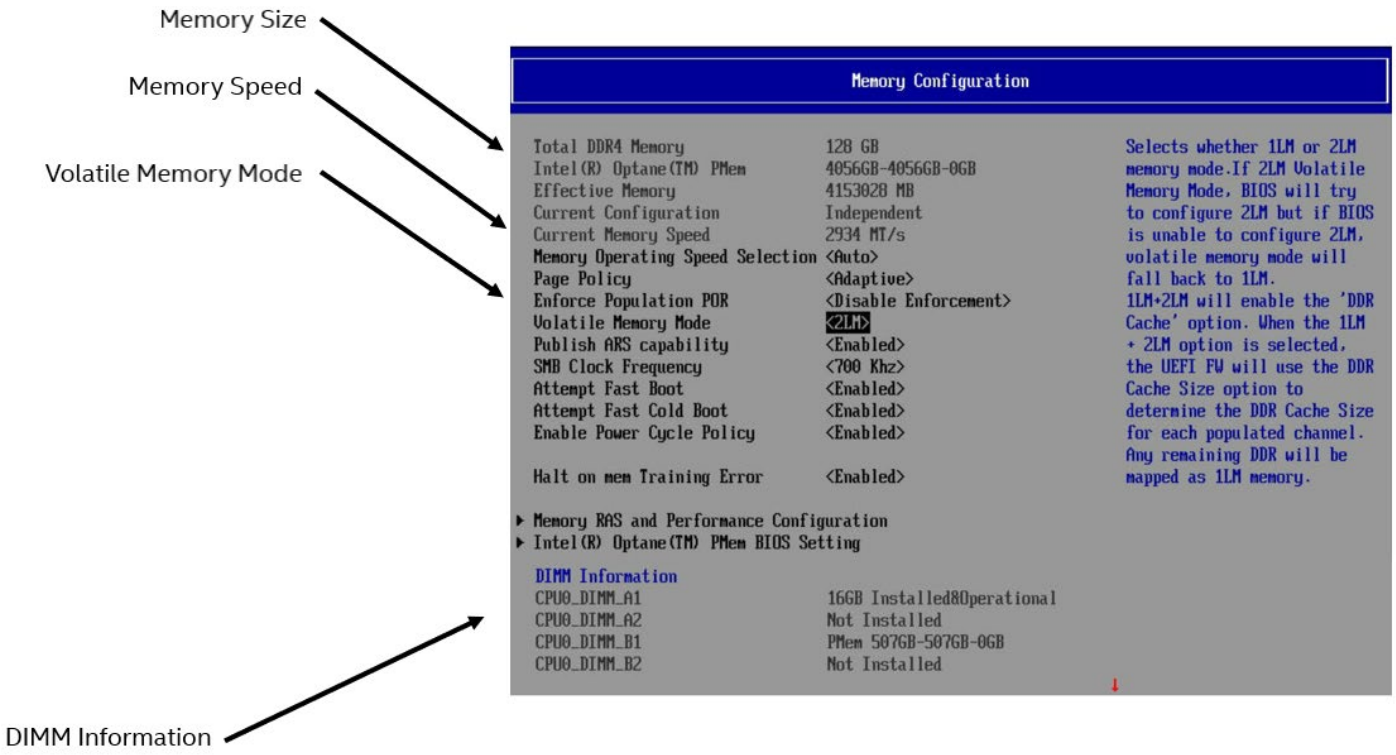


Figure 63. Memory Configuration

Figure 63 shows the **Memory Configuration** screen. Information and settings on the screen include memory size, memory speed, volatile memory mode, and DIMM.

Intel(R) Optane(TM) PMem BIOS Setting is one of the options included in this screen. For more details, see Section 3.10.3.

3.10.3 Configure Intel® Optane™ PMem BIOS Setting

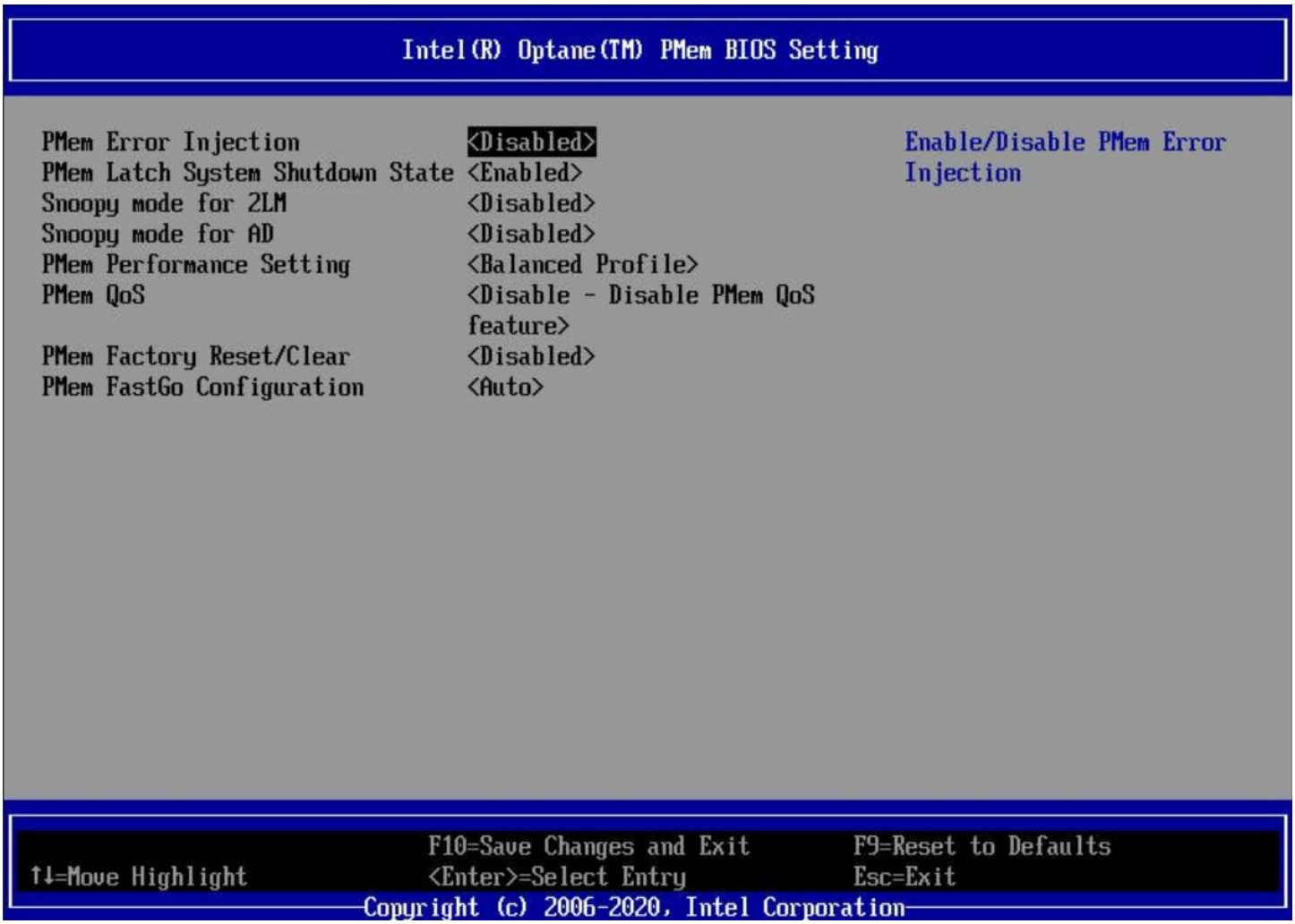


Figure 64. Intel® Optane™ PMem BIOS Setting

Figure 64 shows the **Intel(R) Optane(TM) PMem BIOS Setting** screen. This screen includes all the PMem related BIOS settings.

3.10.4 Navigate to the Main Intel® Optane™ PMem Setup Screens

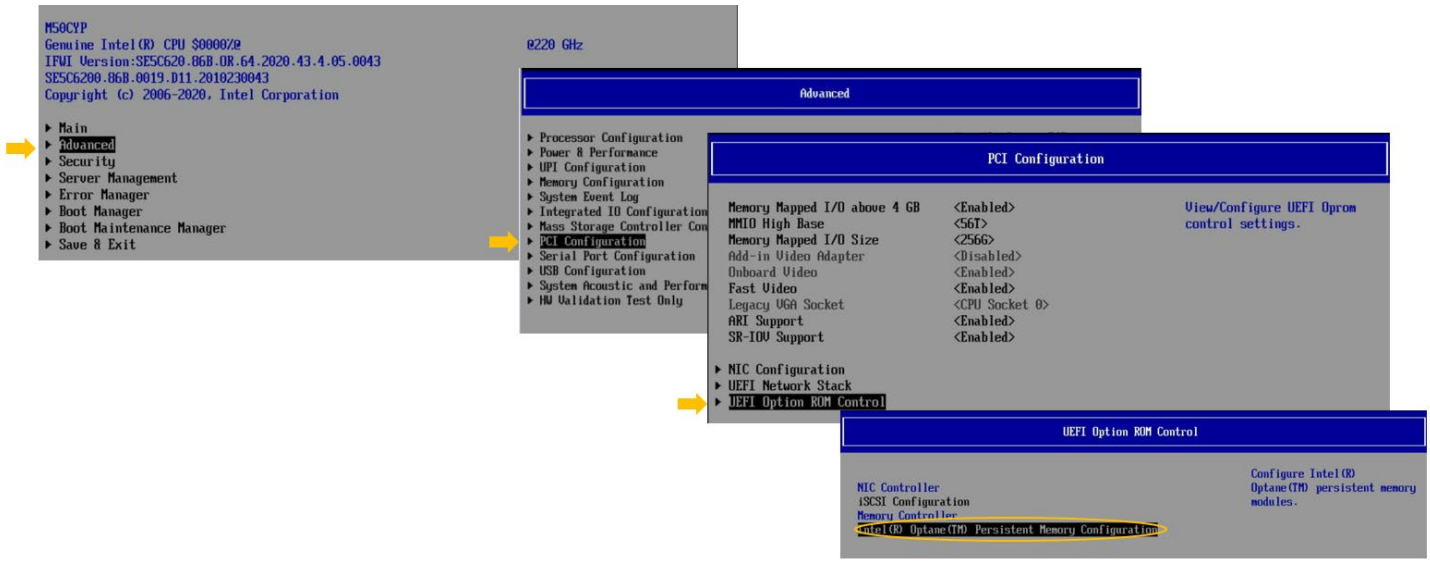


Figure 65. Intel® Optane™ PMem Setup Screens

Most setup options for Intel® Optane™ PMem are in the **Intel(R) Optane(TM) Persistent Memory Configuration** screen.

To get to this screen from the opening BIOS screen, select **Advanced** > **PCI Configuration** > **UEFI option ROM Control** > **Intel(R) Optane(TM) Persistent Memory Configuration.**

Refer to Section 3.10.5 to see this screen's options.

3.10.5 Intel® Optane™ Persistent Memory Configuration

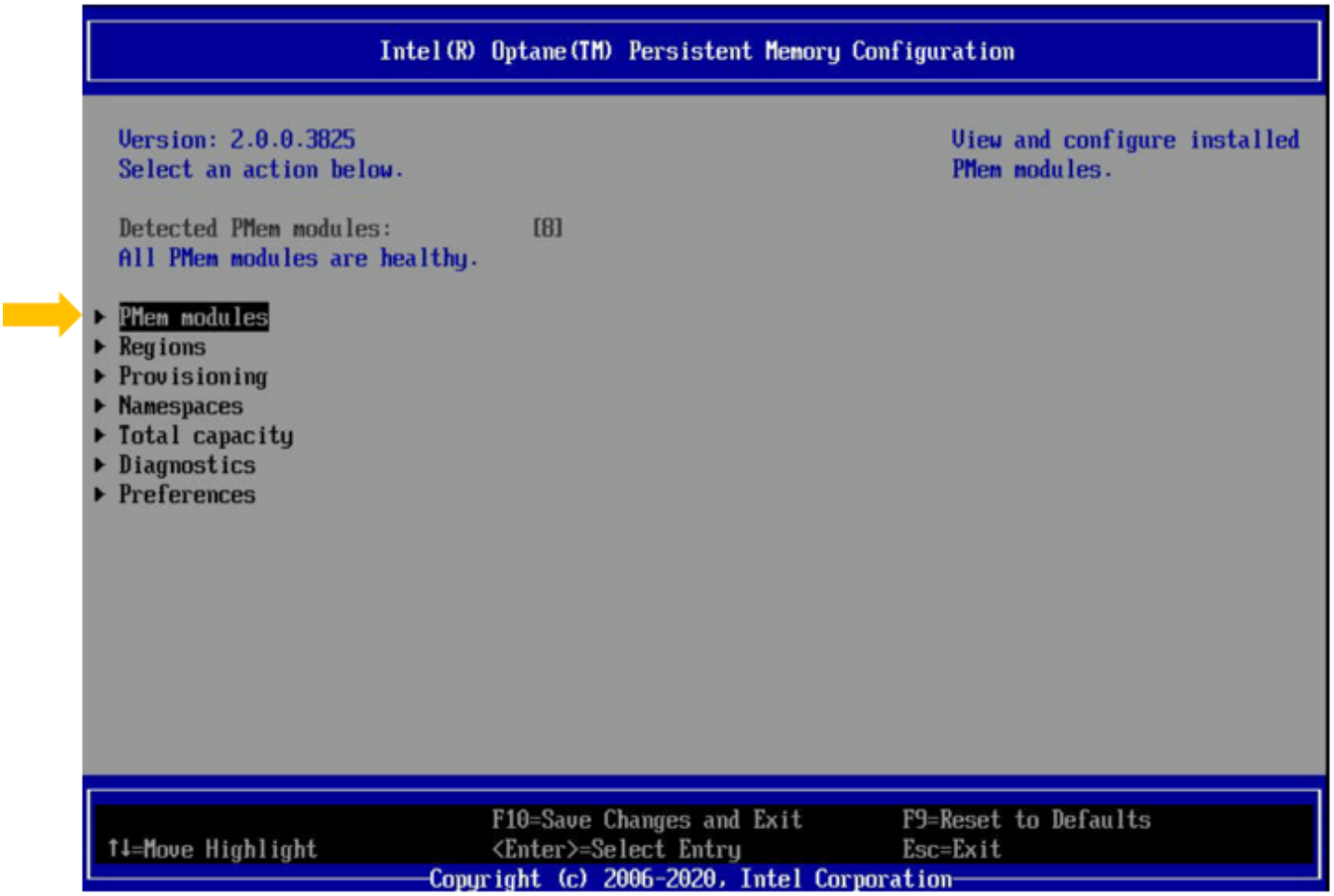


Figure 66. Intel® Optane™ PMem Configuration

Figure 66 shows the main **Intel(R) Optane(TM) Persistent Memory Configuration** screen. This screen shows the count of detected DIMMS, and a quick check of their health.

From this screen, DIMM-specific information can be accessed, including regions, namespaces, capacity readings, diagnostics, and preferences.

Section 3.10.8 discusses the available options when clicking the PMem modules link.

3.10.6 View More DIMM Information

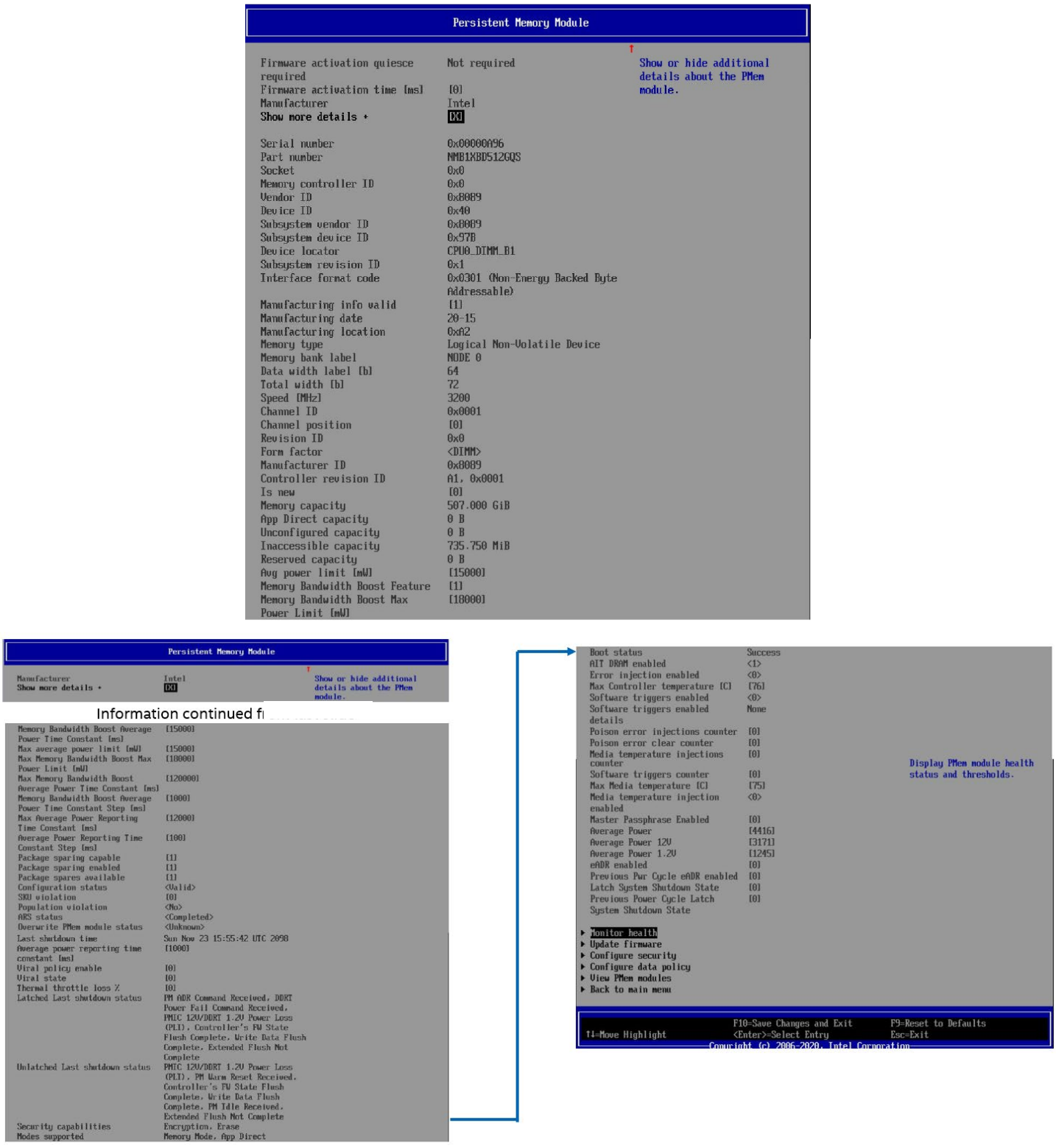


Figure 67. Show More Details

In the Persistent Memory Module screen, when Show More Details is selected, the user accesses to the screen shown in Figure 67.

Plenty of information about the DIMM is displayed, including the serial number, manufacturing date, channel position, and controller revision.

3.10.7 Monitor Intel® Optane™ PMem Health

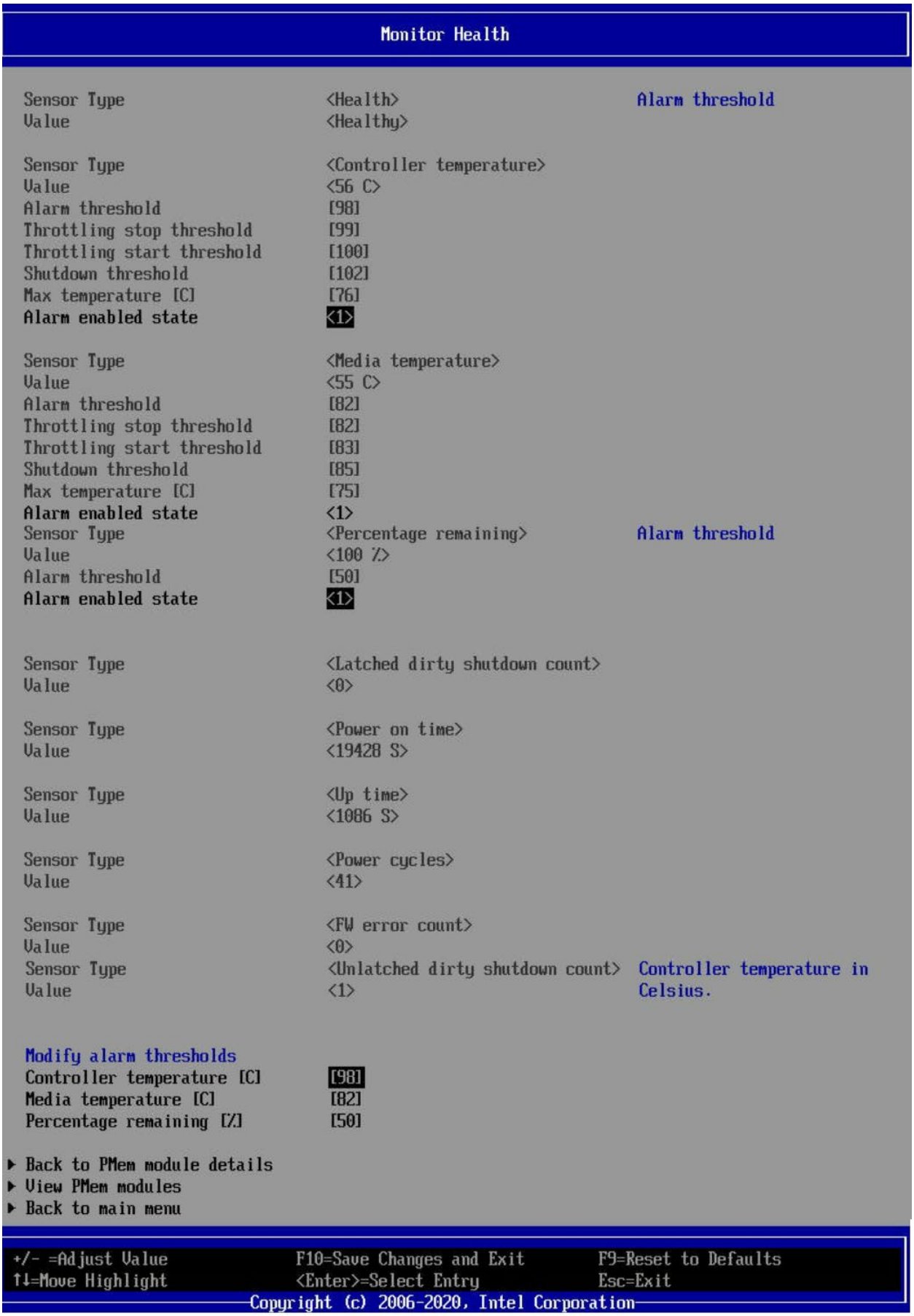


Figure 68. Monitor Health

In Persistent Memory Module screen (see Figure 69), when Monitor Health is selected, the screen in Figure 68 is presented. This screen shows the values for various sensors and how many times the thresholds have been exceeded or not met on items like the temperature of the Media on the DIMM or the controller temperature.

The user can get a reading of how much “life” is left in the DIMM, expressed as a percentage. In addition, there is information on the power on time, up time, power cycles, and firmware error counts. At the bottom of Monitor Health screen, non-critical thresholds can be set.

The user must click **Apply Changes** if any settings are updated.

3.10.8 View Individual Intel® Optane™ PMem DIMM Information

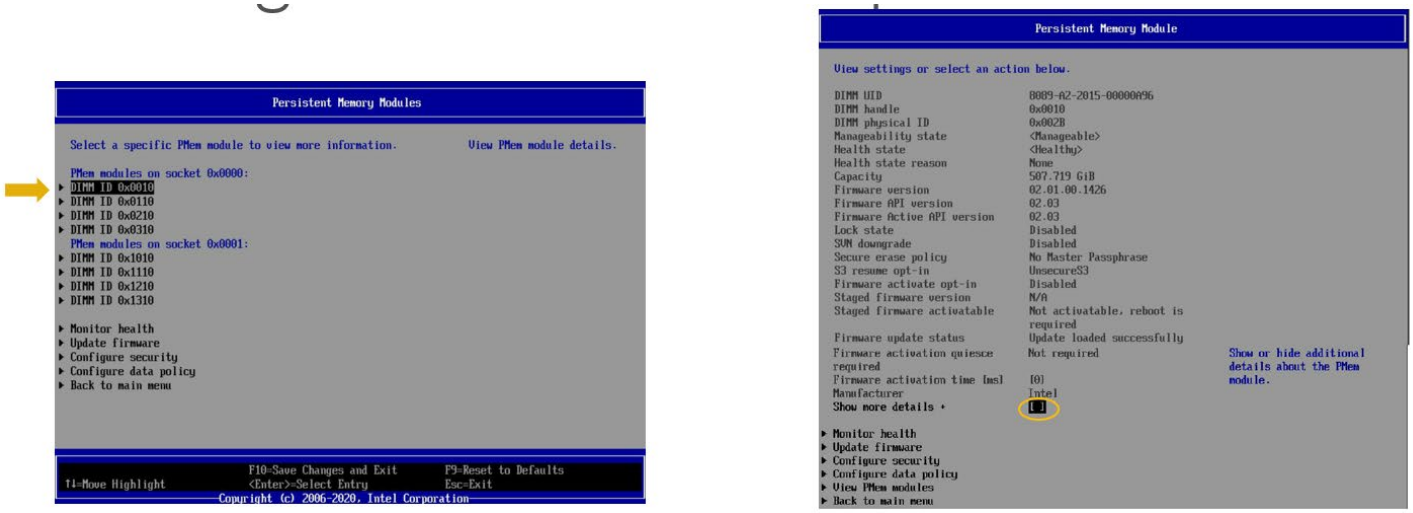


Figure 69. Persistent Memory Modules

When PMem modules are selected (see Figure 66), the screen on the left in Figure 69 is presented.

Click a specific DIMM to get information about that DIMM. The right image in Figure 69 is an example of the DIMM-specific information shown.

This DIMM-specific screen provides information about the DIMM, like handle number, health, capacity, and the firmware version.

In addition, the user can probe deeper into the health of the DIMM, update the firmware, and configure security and data policy on the DIMM.

Click **Show More Details** to get more information about the DIMM, as is discussed in Section 3.10.6.

3.10.9 Update Intel® Optane™ PMem Firmware

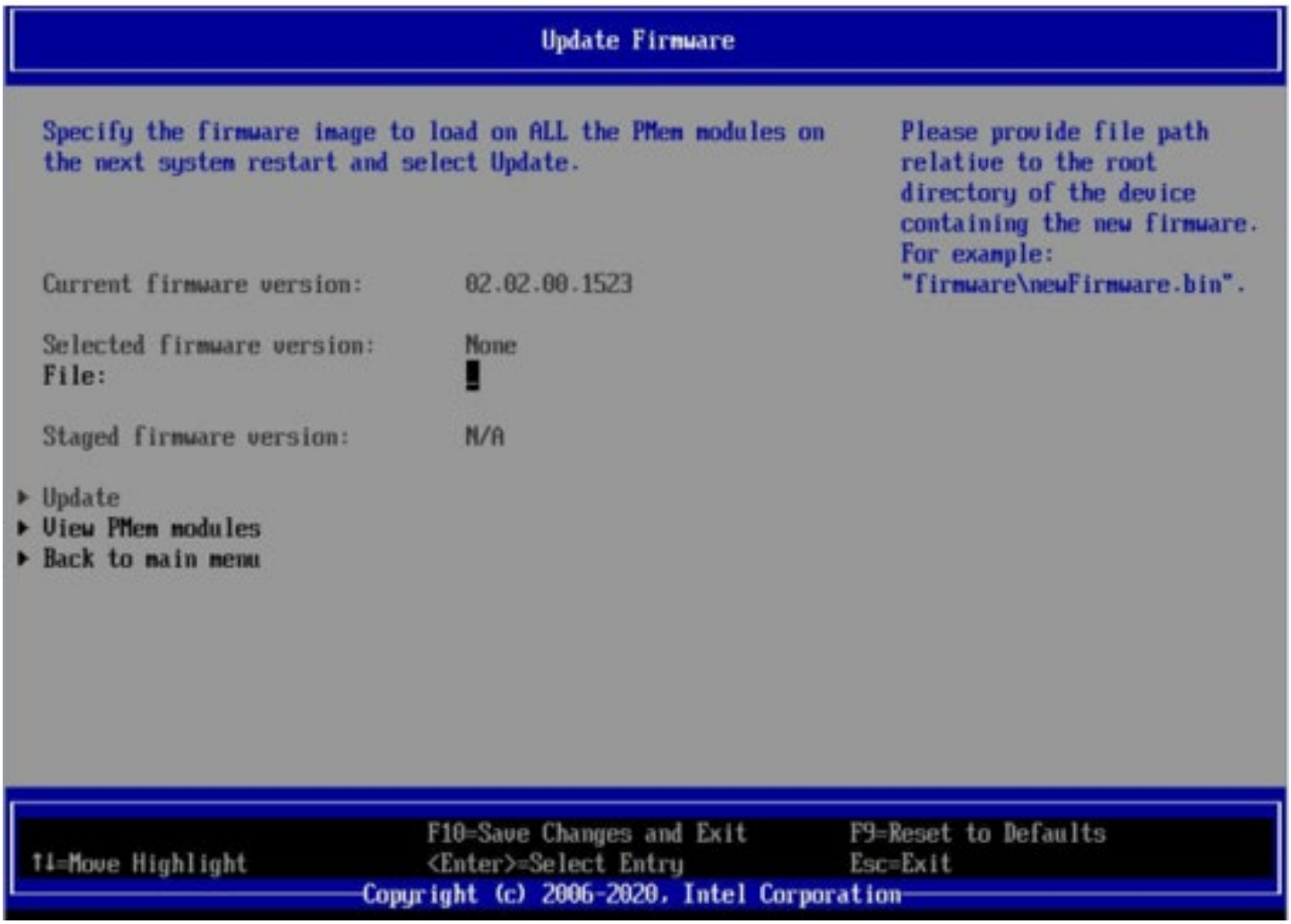


Figure 70. Update Firmware

In the **Persistent Memory Module** screen (see Figure 69), when Update Firmware is selected, the screen in Figure 70 is presented.

The user can specify a file containing the new firmware code and then select **Update**.

3.10.10 Configure Intel® Optane™ PMem Security

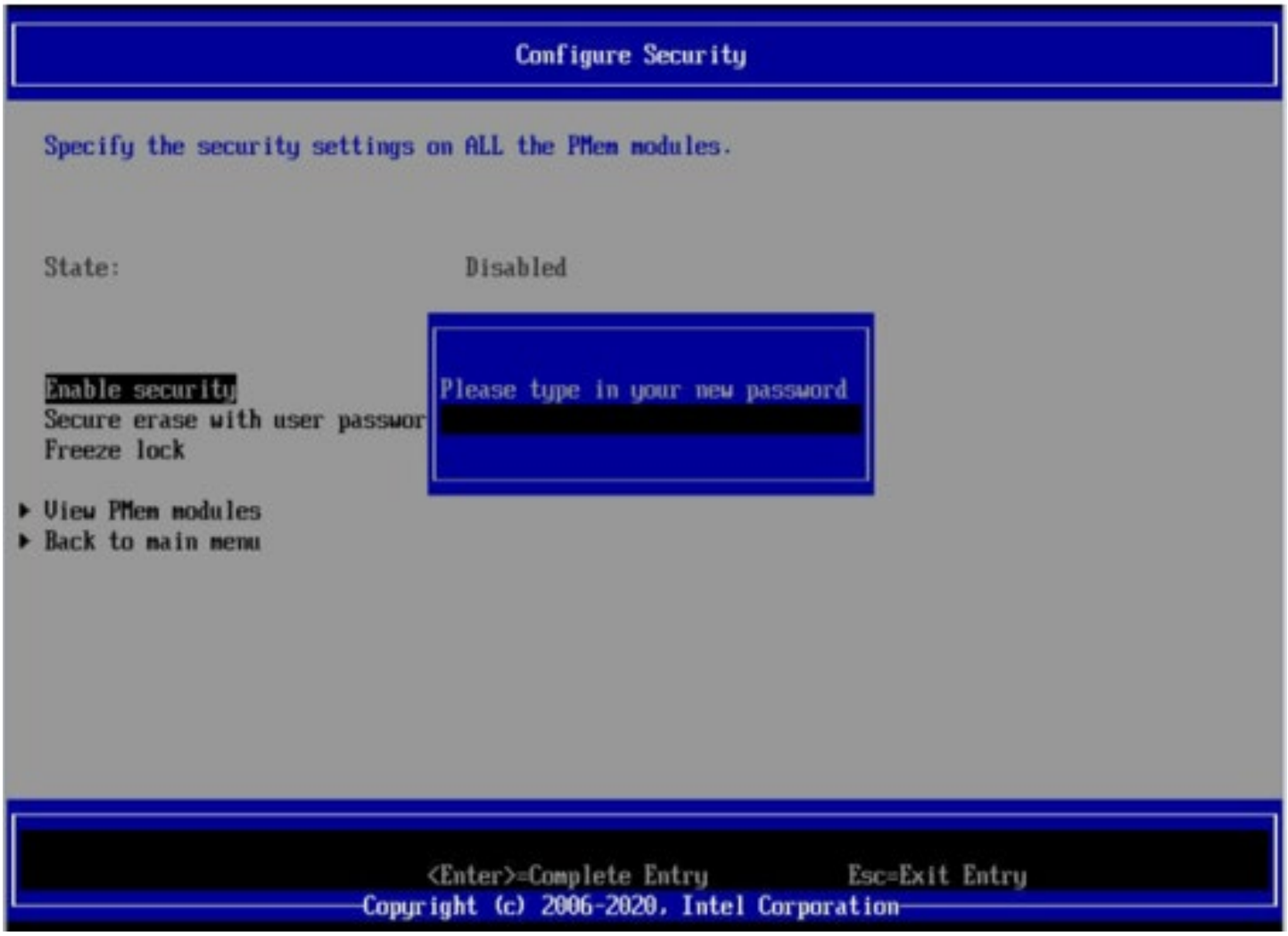


Figure 71. Configure Security

In the Persistent Memory Module screen (see Figure 69), when Configure Security is selected, the screen presented in Figure 71 is shown.

If the user selects to set a password, it is stored and automatically applied to unlock Intel® Optane™ PMem before the operating system starts running.

The secure erase action still requires the passphrase. Secure erase is used to erase the encrypted data on the DIMM. Freeze lock is used to lock the security settings of the DIMM.

3.10.11 Settings in BIOS for App Direct

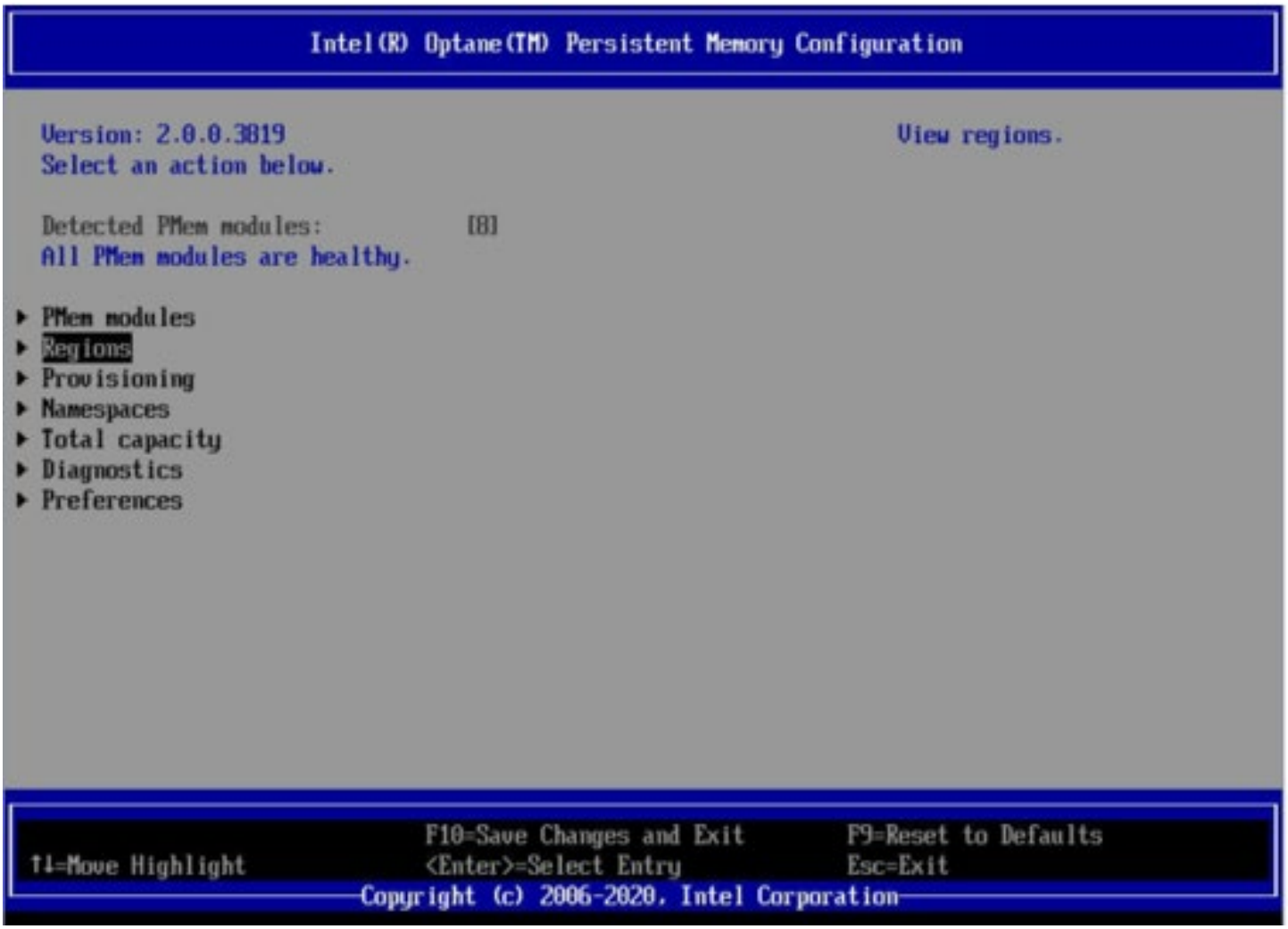


Figure 72. Intel® Optane™ PMem configuration – Regions

To use Intel® Optane™ PMem in App Direct mode, these steps need to be performed:

- Create a **goal** that identifies how much memory to use.
- Create **regions** (a group of one or more Intel® Optane™ PMem).
- Create **namespaces** that define a contiguously addressed range of non-volatile memory conceptually similar to a hard disk drive partition.

From the **Intel(R) Optane(TM) Persistent Memory Configuration BIOS** screen, all these steps can be done.

Creating a goal is part of the creating namespaces process.

Also in this screen, there is an option for running diagnostics on the Intel® Optane™ PMem. For more details, see Section 3.10.15.

3.10.12 Create Intel® Optane™ PMem Goals in BIOS

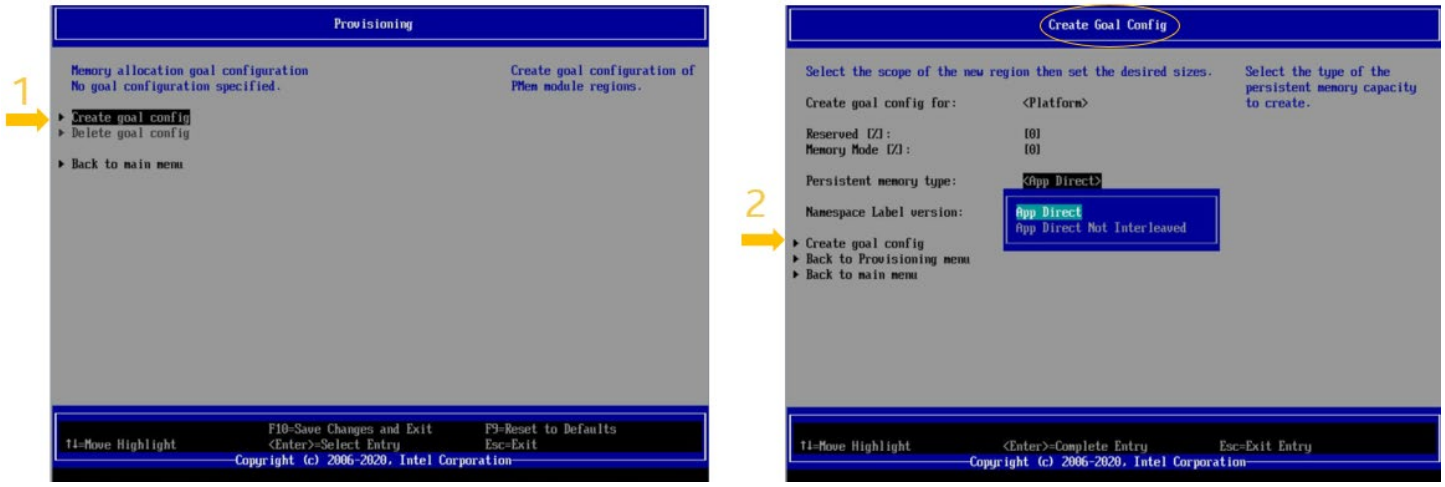


Figure 73. Create Goal Steps

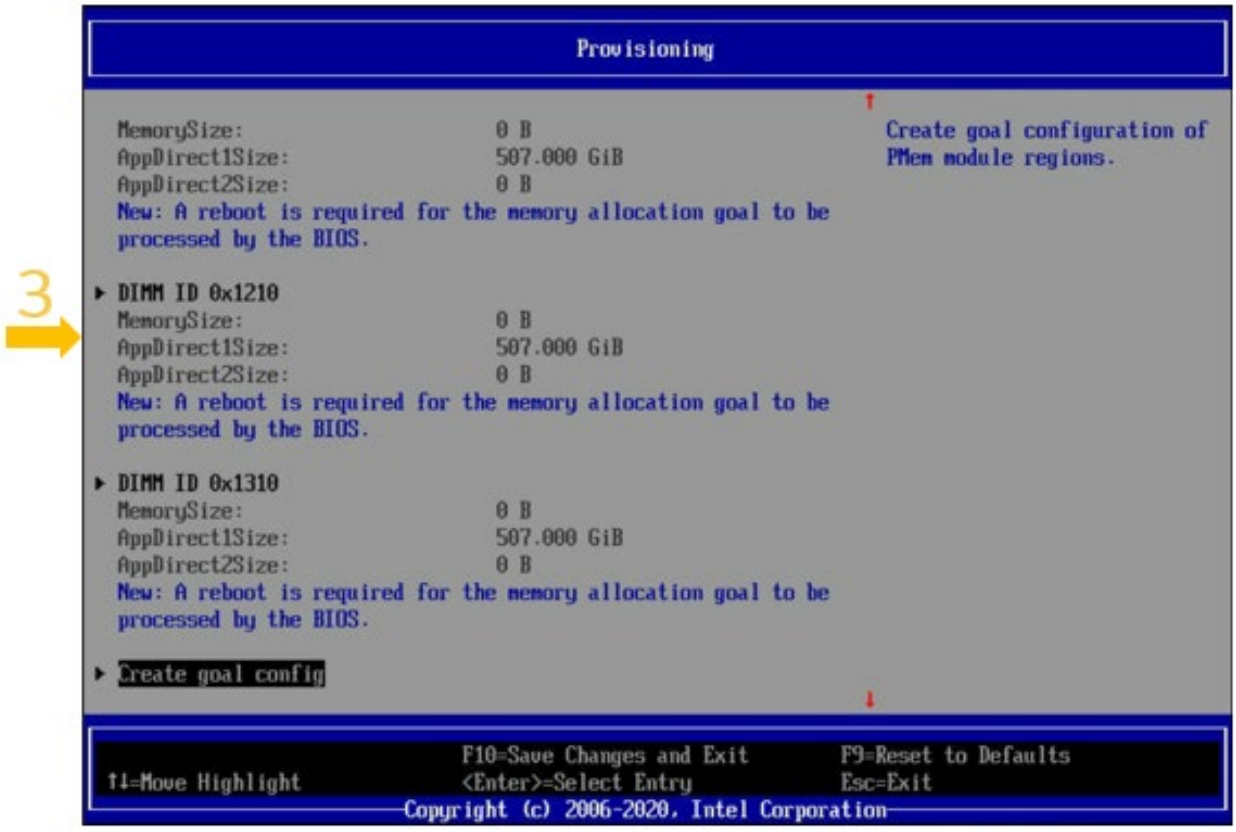


Figure 74. Create Goal Steps 1

Creating a goal is a two-step process. The first step is to select **Create Goal Config** from the **Provisioning** screen (shown in the left in Figure 73). Once this step is done, the screen on the right side of Figure 73 is presented. When creating a goal, there are several options.

One option is to select if the goal is for the entire platform (which is the default) or for one socket on the platform. Another option is determining if the memory is standard App Direct (interleaved) or if the memory is App Direct (non-interleaved).

Once the selections are done, the second and last step is to click **Create Goal Config** (shown in Figure 74).

A **reboot** is required.

3.10.13 View Intel® Optane™ PMem Region Setting in BIOS

Figure 75. Region Settings

To view region settings, select a region from the **Regions** screen. When Enter is pressed, a screen similar to the one on the right side of Figure 75 is presented.

This screen shows region ID, the DIMMs that are part of that region, persistent memory type (standard interleaved or non-interleaved), capacity, health, and the socket the region is tied to.

3.10.14 Create Intel® Optane™ PMem namespace Setting in BIOS

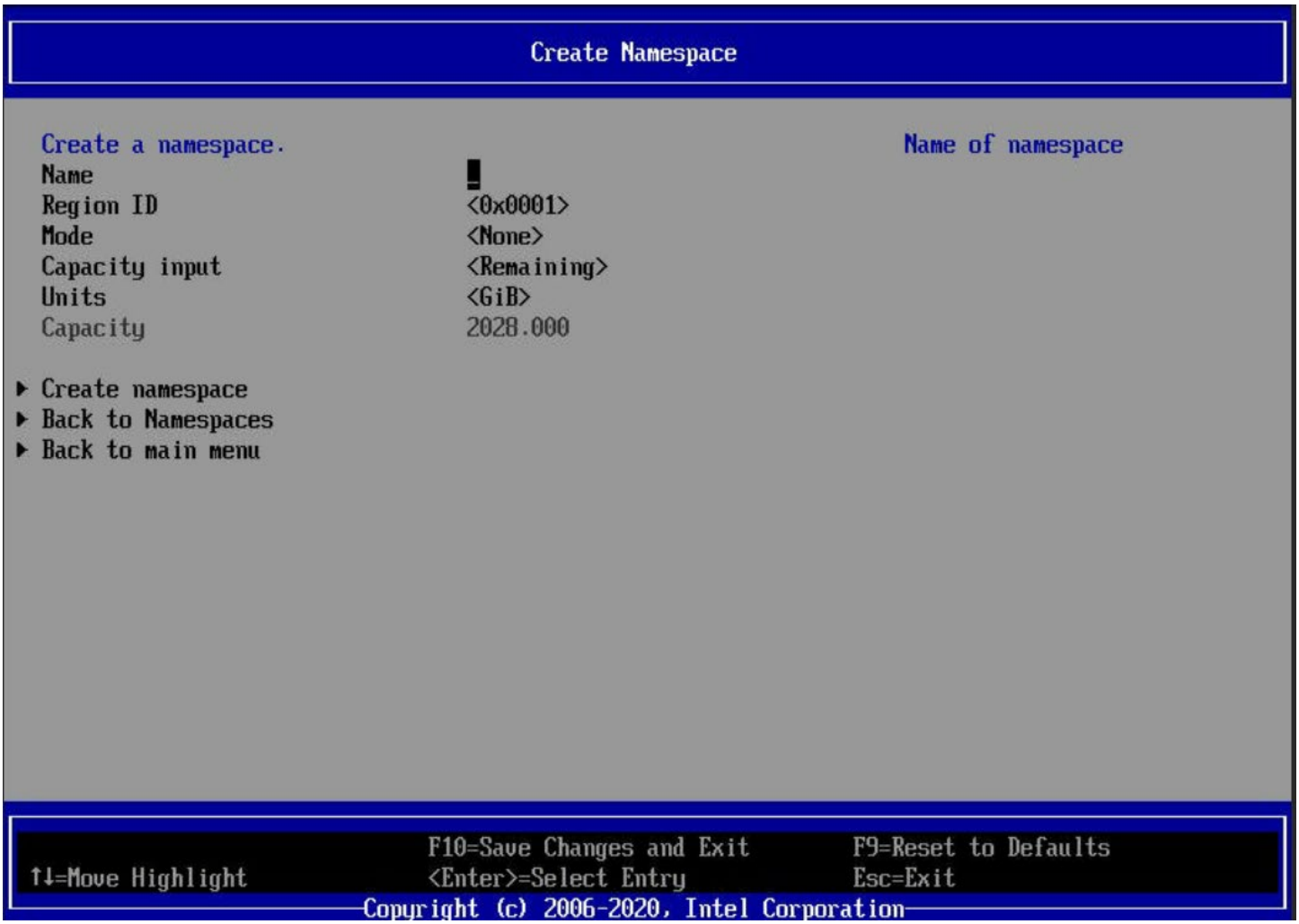


Figure 76. Create Namespace

From the **Intel(R) Optane(TM) Persistent Memory Configuration BIOS** screen, creating a namespace can be selected.

The screen presented in Figure 76 displays and allows options to give the namespace a name or label, associate it with a region, and assign a size to the namespace.

3.10.15 Run Diagnostics on Intel® Optane™ PMem

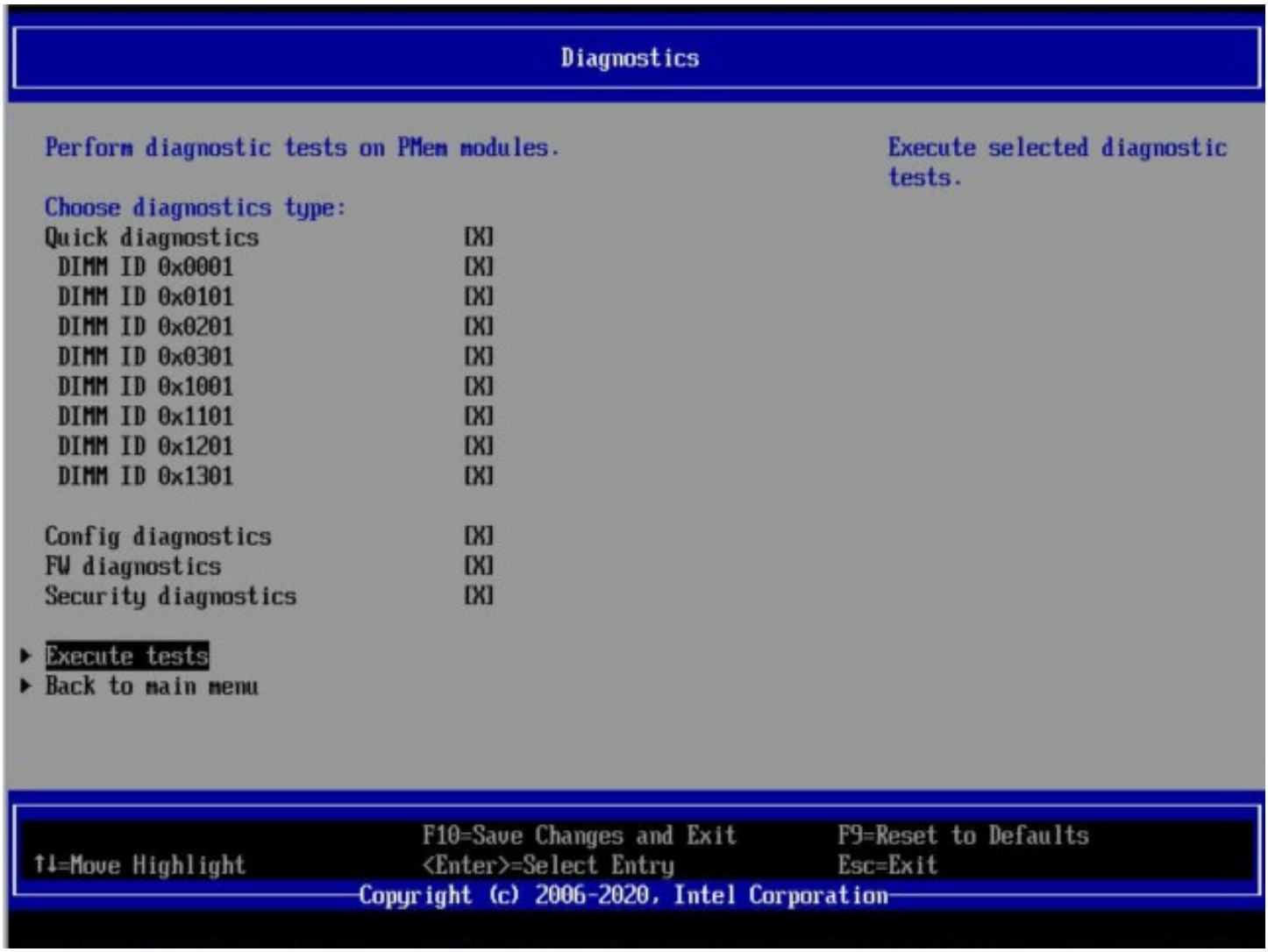


Figure 77. Diagnostics

From the **Intel(R) Optane(TM) PMem Memory Configuration BIOS** screen, Diagnostics can be selected.

The Diagnostics screen allows diagnostics to be run on individual DIMMs or on all of them. This screen allows the user to validate the configuration parameters and check the firmware and security settings.

3.11 Intel® VROC Setup

This chapter use an example to show how to install the Windows*OS on an Intel® Virtual RAID on CPU (Intel® VROC) Virtual drive(VD), also, it shows how to create and configure both, Intel® VROC for SATA VD and Intel® VROC for NVMe VD.

The information in this section applies to the Intel® Server Systems M50CYP, D50TNP, and D40AMP

3.11.1 Configuration for Intel® Server Boards

Hardware configuration used for the example:

- 1 Intel® Server System M50CYP
- 2 x Intel® SSD S4610 for SATA drives
- 8 x Intel® SSD P5510 for NVMe* drives.

Storage configuration:

2 x SATA SSD drives in a RAID 1 VD for the OS, connected to the onboard SATA controller.

4 x NVMe drives in a RAID 5 VD for Data 1.

4 x NVMe drives in a RAID 5 VD for Data 2.

All 8 drives connected to the onboard PCIe* ports.

3.11.2 Verify the Installed Storage

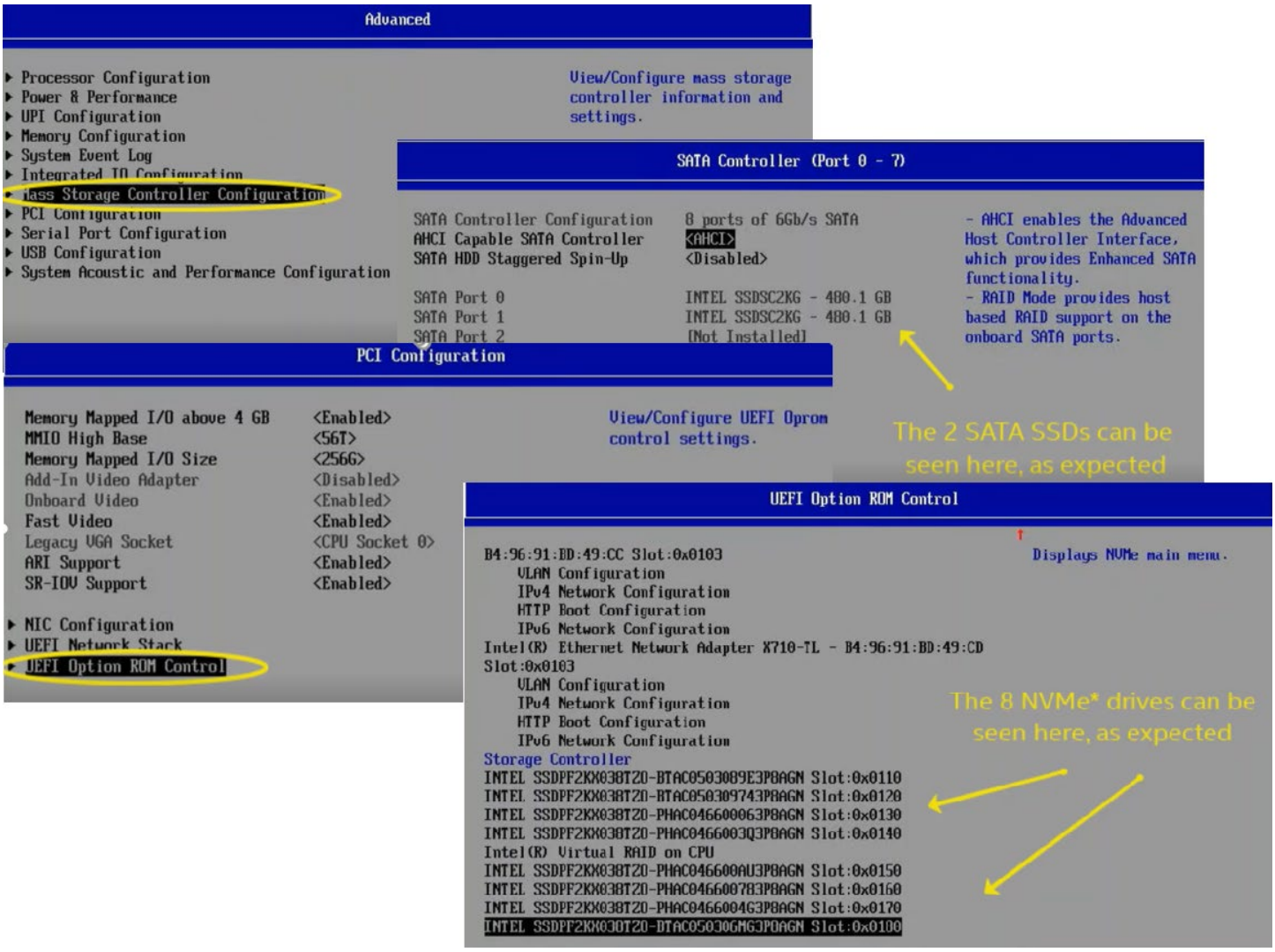


Figure 78. Verify the Installed Storage

From the opening BIOS screen, click **Advanced** > **Mass Storage Controller Configuration** > **SATA Controller (Port 0 - 7)** check the 2 SATA SSD information.

From the opening BIOS screen, click **Advanced** > **PCI Configuration** > **UEFI Option ROM Control** check the 8 NVMe* drives information.

3.11.3 Enable the Controllers for RAID Mode

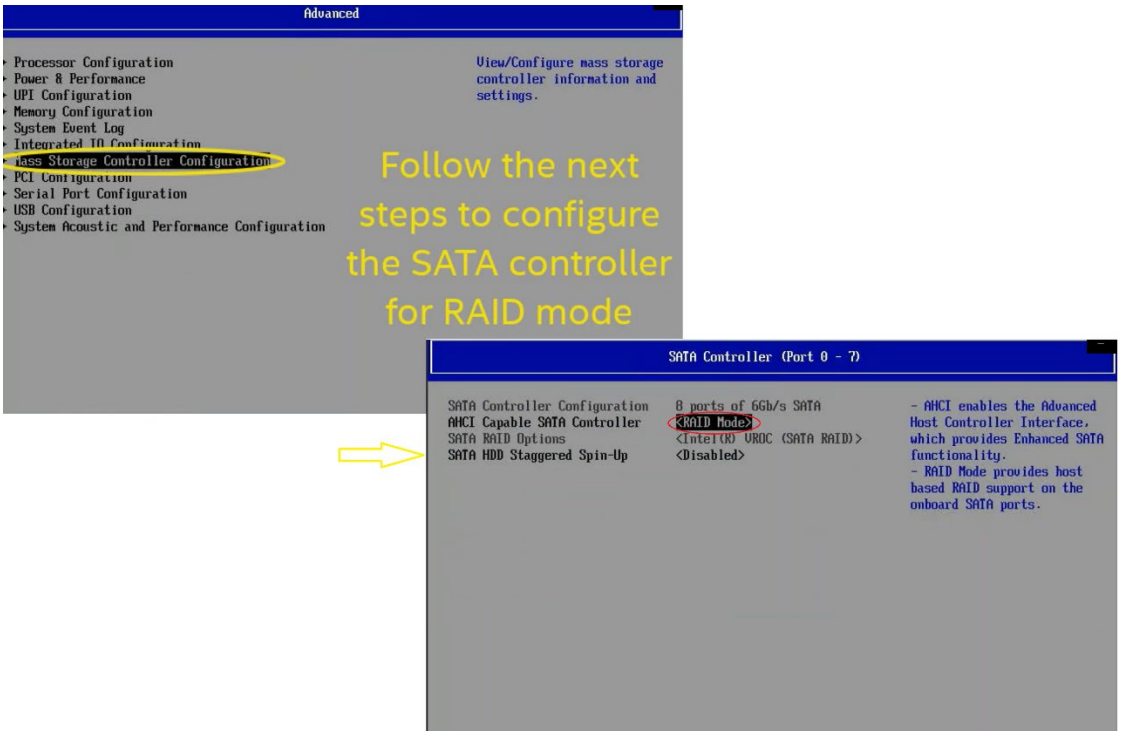


Figure 79. Enable RAID mode for SATA Controller

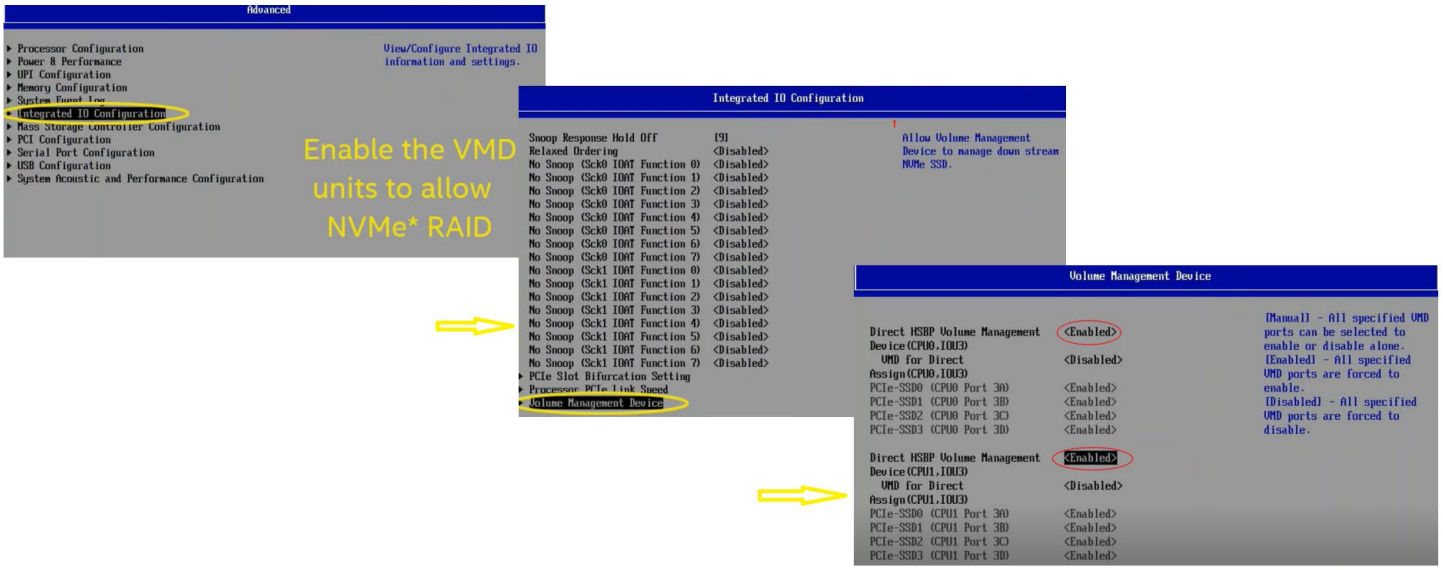


Figure 80. Enable the VMD to allow NVMe* RAID

Pressing F10 Save and reboot system to make changes take effect.

3.11.4 Create the RAID VDs

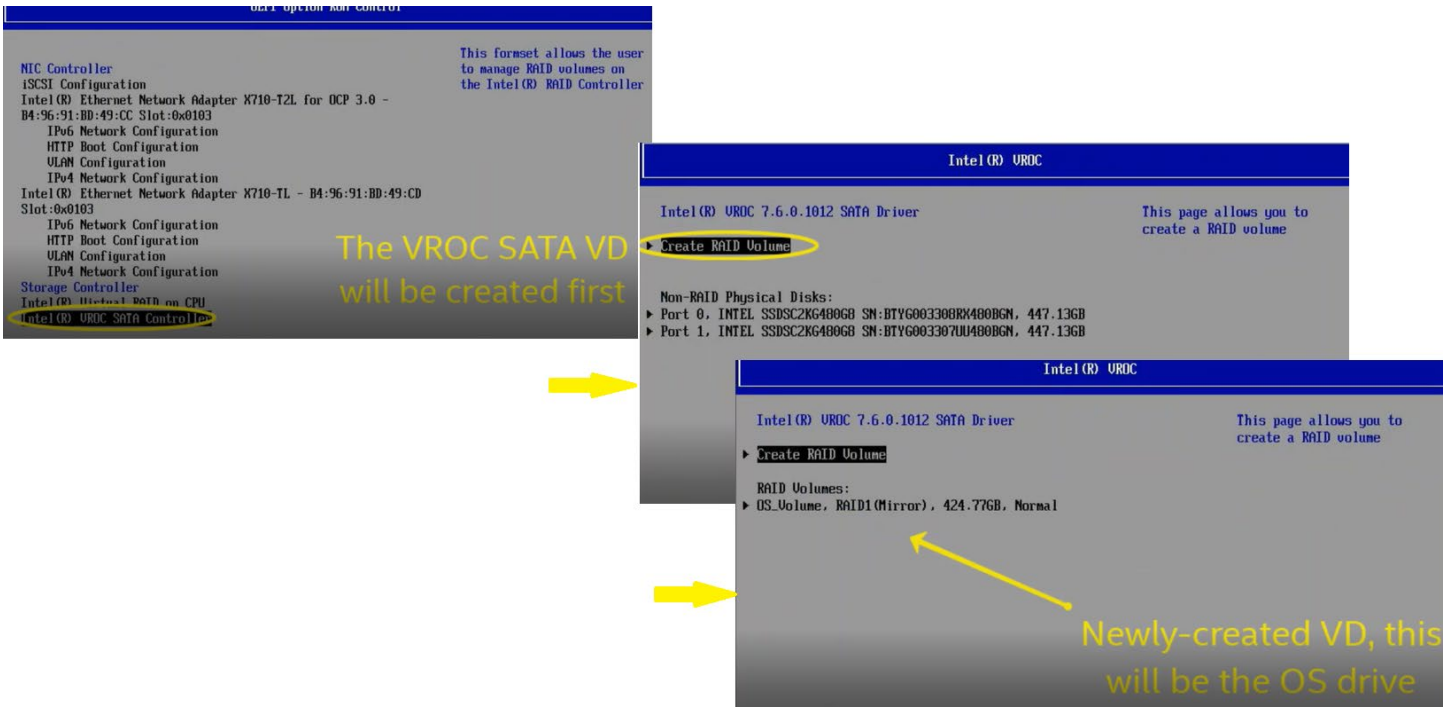
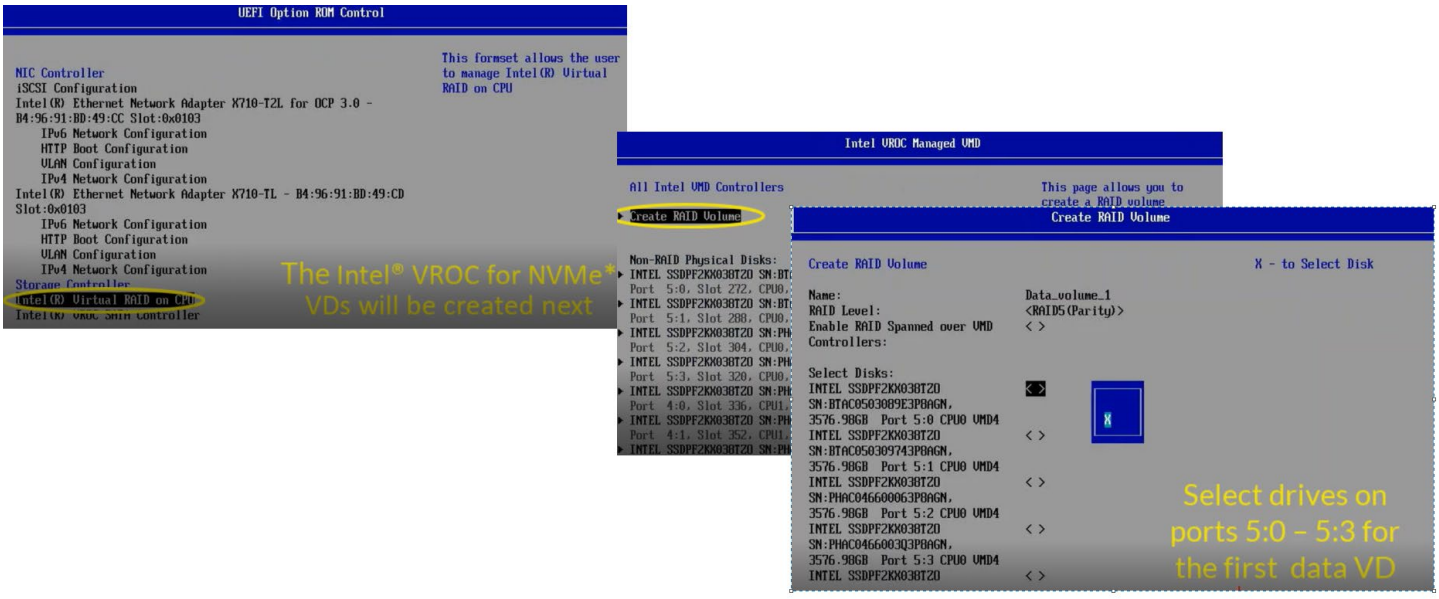


Figure 81. Create the RAID VDs-1



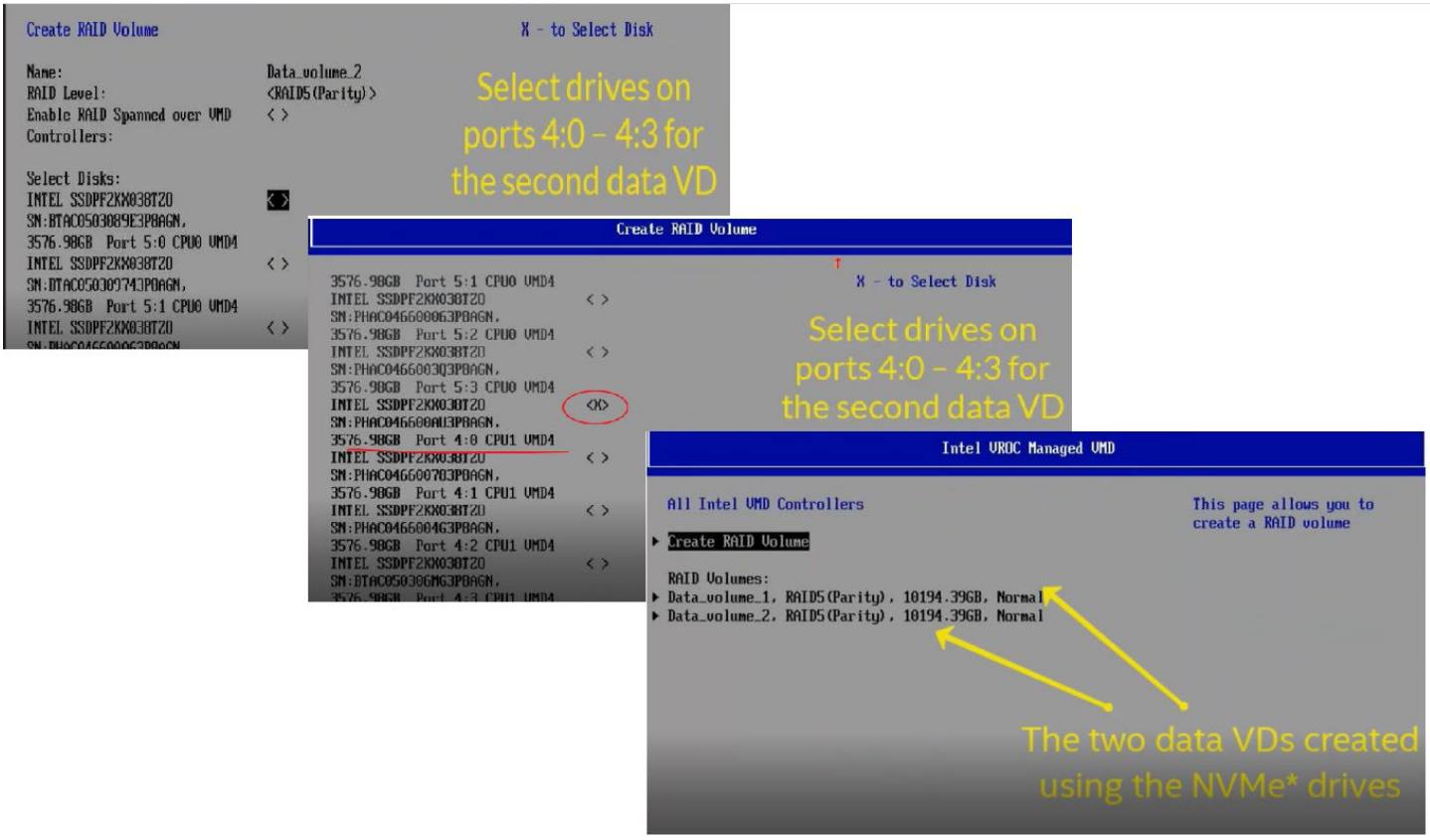


Figure 82. Create the RAID VDs-2

Pressing F10 Save and reboot system to make changes take effect.

3.11.5 Install the Windows* OS on the Intel® VROC VD

Boot the installation media, Install Windows OS.

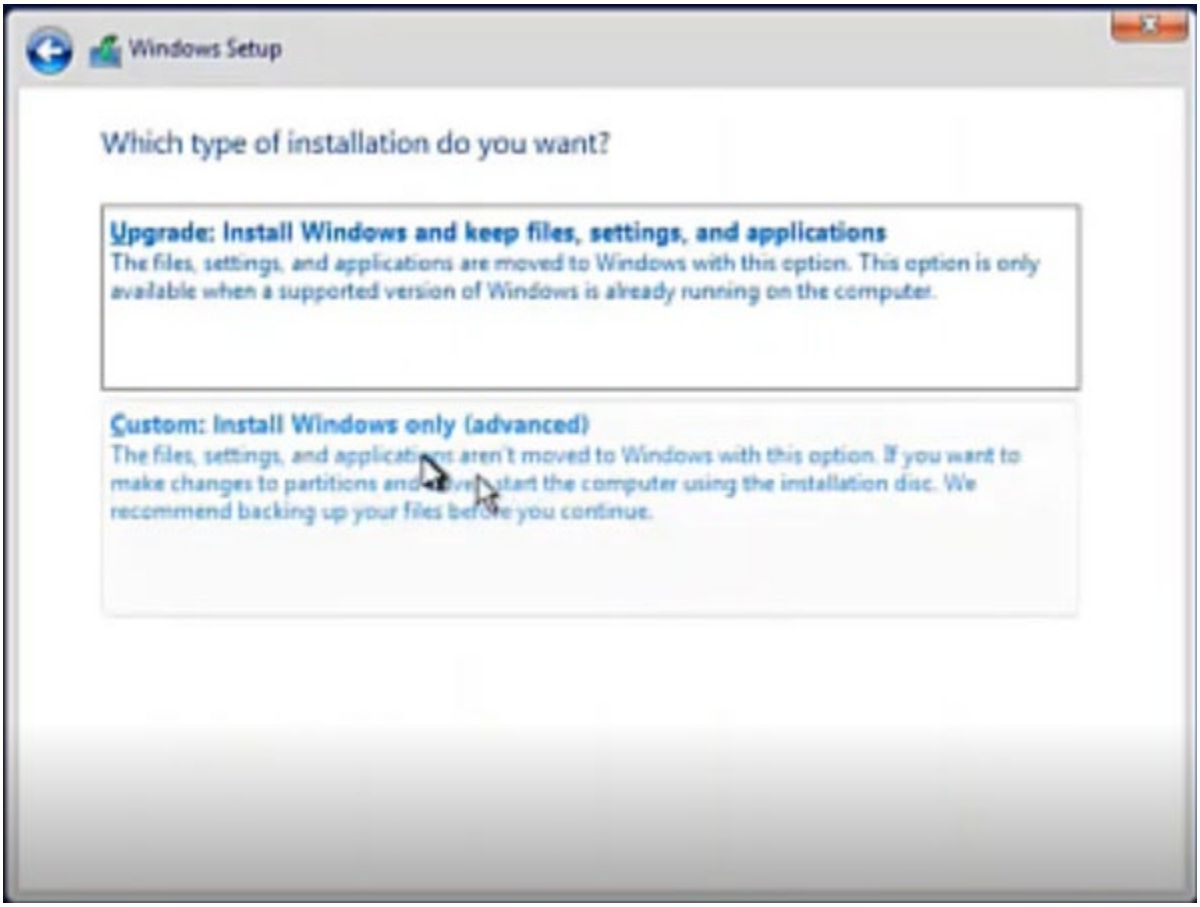


Figure 83. Install Windows OS

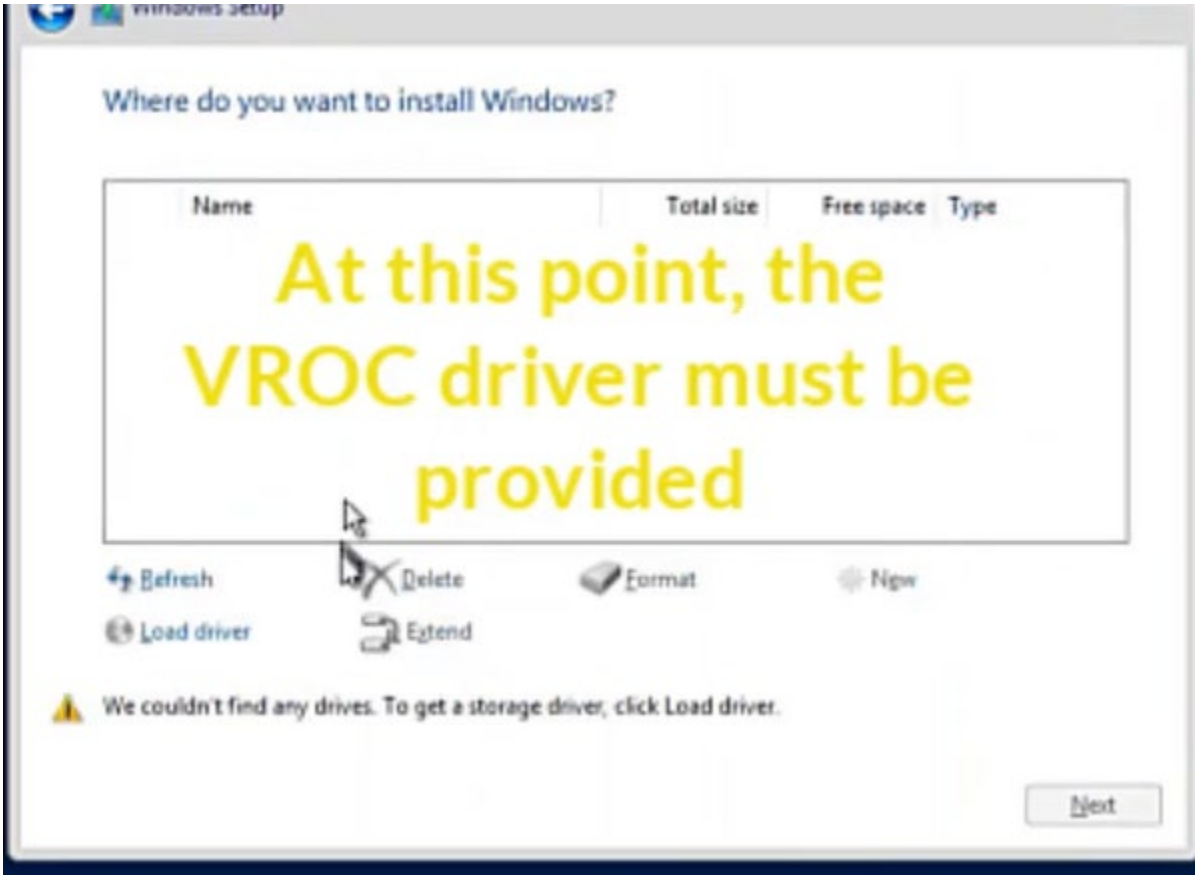


Figure 84. Provide VROC Driver during the OS installation

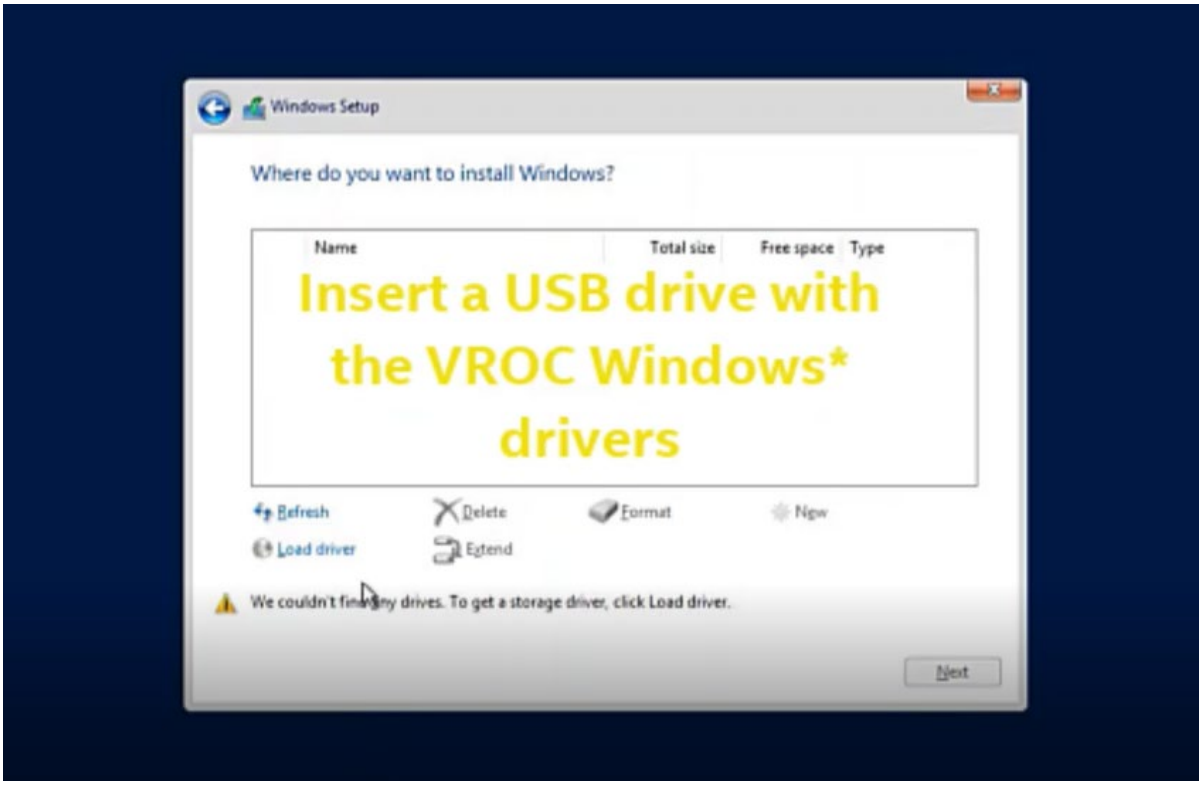


Figure 85. Install VROC Driver

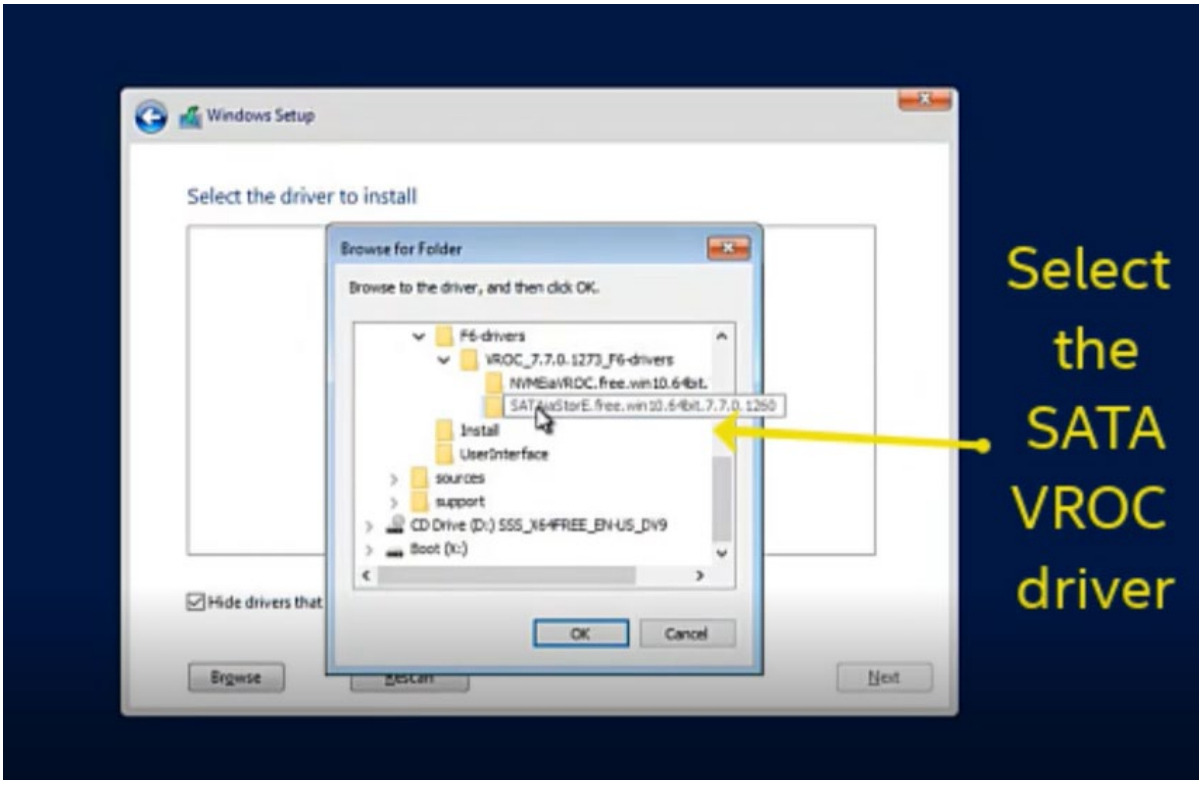


Figure 86. Select SATA VROC driver

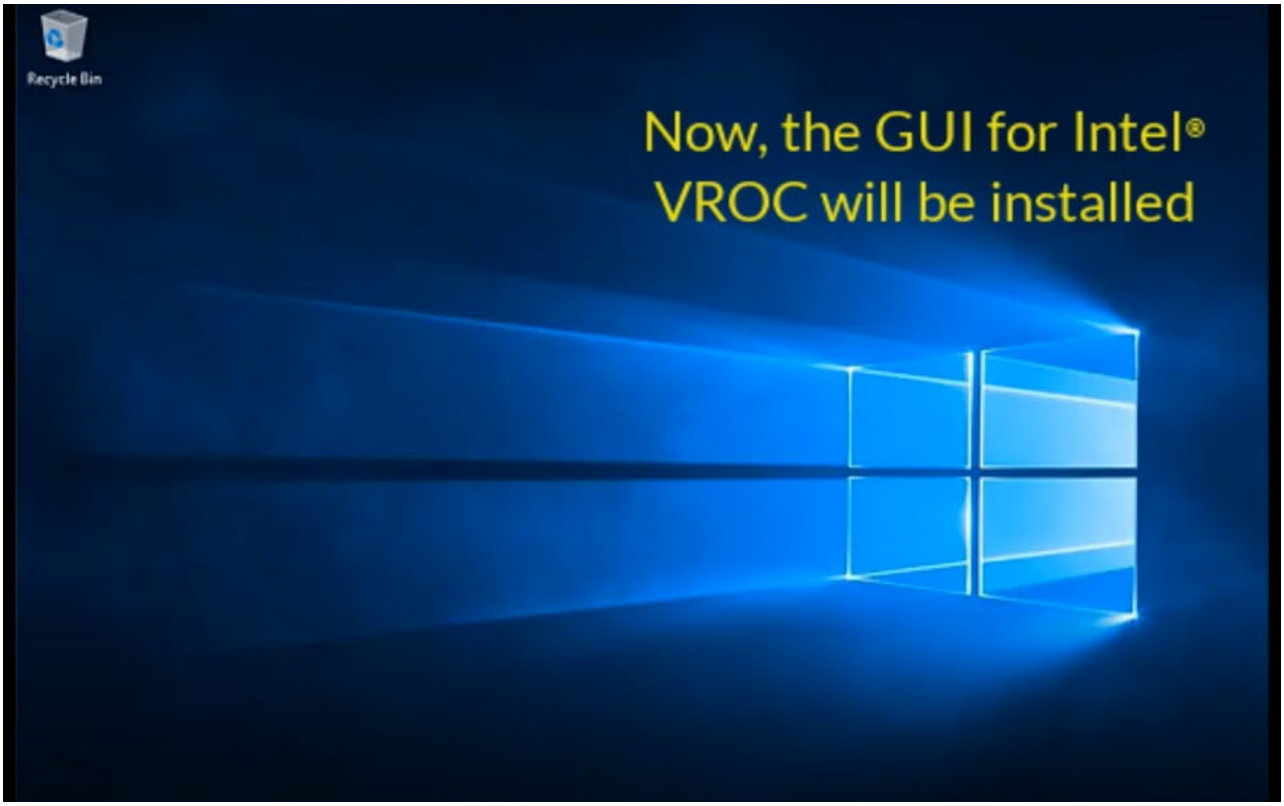


Figure 87. OS GUI

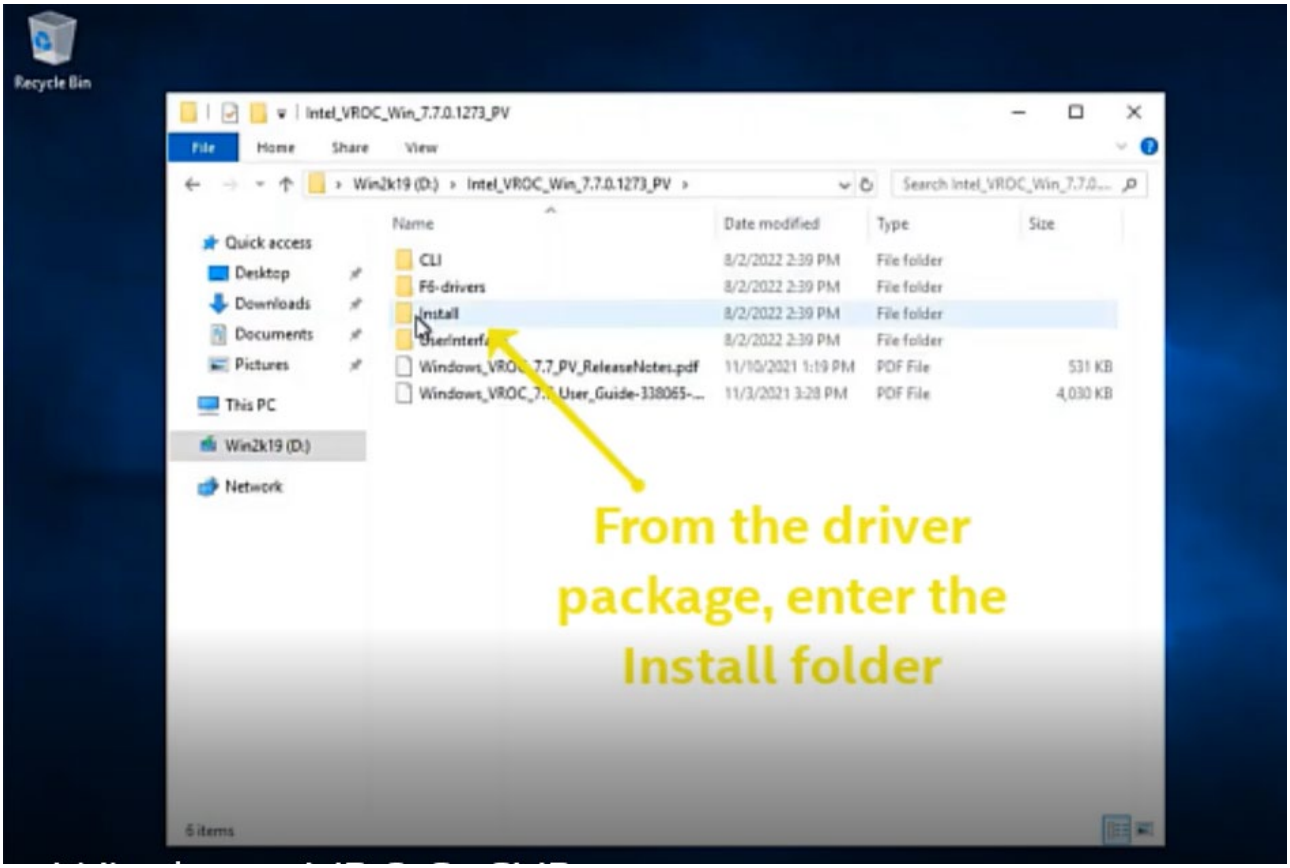


Figure 88. Install VROC Driver on Windows

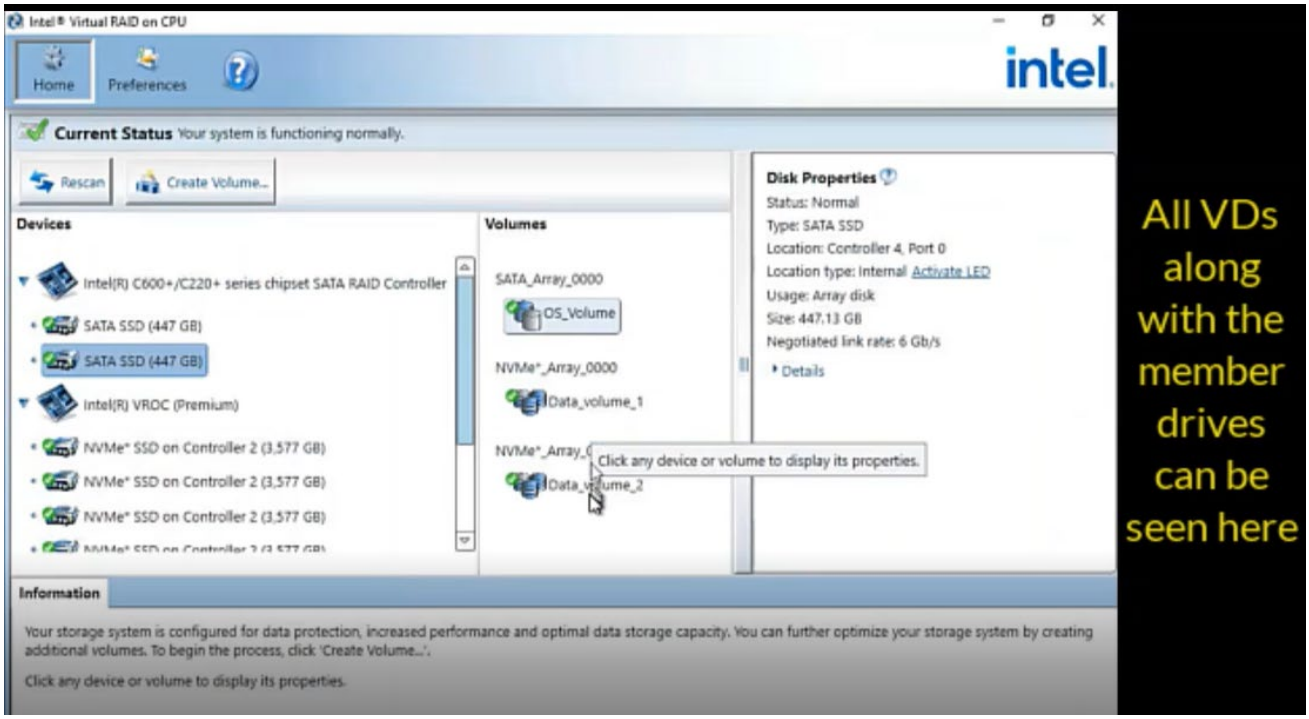


Figure 89. Virtual RAID Status

Figure 90. Install the Windows* OS on the VROC RAID

Now, the Windows* OS is installed on the Intel® VROC RAID 1 VD, and the two Intel® VROC RAID 5 data VDs are ready for use.

Appendix A. Intel's Tool Support

Intel has developed tools that allow the user to customize BIOS settings, meaning that these tools support actions like saving and setting selected configurations for the system firmware and the BIOS. Such tools include Firmware Customization, Intel® Server Configuration Utility, and Intel® Server Information Retrieval Utility. The following table summarizes these tools' support status for the BIOS setup utility options.

The table includes these symbols:

- "×" means that the corresponding tool is not supported.
- "√" means that the corresponding tool is supported.

Note: Some options are supported by the BIOS, while some may need Intel® Server Configuration Utility or Intel® Server Information Retrieval Utility to get values from the BMC via IPMI. Said values cannot be obtained from the BIOS variable via `/bcs`, especially for the BMC-controlled setup options.

For BMC-controlled options, the BIOS does not support neither Intel® Server Configuration Utility nor Intel® Server Information Retrieval Utility via `/bcs` command. For information-only items, if Intel® Server Configuration Utility is marked as √, the items are read-only for this tool.

Setup Option	Firmware Customization	Intel® Server Configuration Utility	Intel® Server Information Retrieval Utility	Comments
Main				
Logged in as	×	√	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
Platform ID	×	√	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
BIOS Boot From	×	√	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
BIOS Version in Active Region	×	√	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
Active BIOS Build Date	×	√	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
SPS FW Version in Active Region	×	√	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
BIOS Version in Recovery Region	×	√	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
SPS FW Version in Recovery Region	×	√	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
Total DDR4 Memory	×	√	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
PMem	×	√	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
Quiet Boot	√	√	√	
POST Error Pause	√	√	√	
System Date	×	√	×	For Intel® Server Configuration Utility, support `/dt`, but not `/bcs`.
System Weekday	×	×	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
System Time	×	√	×	For Intel® Server Configuration Utility, support `/dt`, but not `/bcs`.

Setup Option	Firmware Customization	Intel® Server Configuration Utility	Intel® Server Information Retrieval Utility	Comments
PFR				
PFR Lock	×	×	√	Information-only. By default, is enabled in production phase and provides no way to unlock the function.
PFR Provision	×	×	√	Since PFR is locked and must provision, the function is not supported via ITK to change the setting.
PFR UnProvision	×	×	√	Since PFR is locked and must provision, the function is not supported via ITK to change the setting.
PFR Status	×	×	×	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
PFR Locked Status	×	×	×	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
PFR Provision Status	×	×	×	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
CPLD Common Code version	×	×	×	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
CPLD RoT Release Version	×	×	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
CPLD RoT SVN	×	×	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
PCH PFR Active SVN	×	×	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
BMC PFR Active SVN	×	×	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
BMC PFM Active Major Version	×	×	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
BMC PFM Active Minor Version	×	×	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
PCH PFR Recovery SVN	×	×	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
BMC PFR Recovery SVN	×	×	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
BMC PFM Recovery Major Version	×	×	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
BMC PFM Recovery Minor Version	×	×	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
PCH SVN Bypass Jumper Status	×	×	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
BMC SVN Bypass Jumper Status	×	×	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
Advanced: Processor Configuration				
Processor Socket	×	×	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
Processor ID	×	×	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
Processor Frequency	×	×	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
Microcode Revision	×	×	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.

Setup Option	Firmware Customization	Intel® Server Configuration Utility	Intel® Server Information Retrieval Utility	Comments
L1 Cache RAM	×	×	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
L2 Cache RAM	×	×	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
L3 Cache RAM	×	×	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
Processor 0 Version	×	√	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
Processor 1 Version	×	√	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
Intel(R) HT Technology	√	√	√	
Current Active Processor Cores	×	×	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
Active Processor Cores	√	×	√	
Intel(R) Virtualization Technology	√	√	√	
Intel(R) TXT	√	√	√	
MLC Streamer	√	√	√	
MLC Spatial Prefetcher	√	√	√	
DCU Data Prefetcher	√	√	√	
DCU Instruction Prefetcher	√	√	√	
X2APIC	√	√	√	
Limit CPU PA to 46 bits	√	√	√	
PPIN Control	√	×	×	
DBP-F	√	√	√	
LLC Prefetch	√	√	√	
Total Memory Encryption (TME)	√	√	√	
Total Memory Encryption Multi-Tenant (TME-MT)	√	√	√	
Max MKTME Keys	×	×	×	Depends on MK-TME capability and maximum supported keys.
SGX Factory Reset	√	×	√	Callback function to complete the function, Does not support `/bcs` command for Intel® Server Configuration Utility.
SW Guard Extensions (Intel SGX)	√	√	√	
Intel SGX Package Info In-Band Access	√	√	√	
PRMRR Size	√	√	√	
SGX QoS	√	√	√	
Select Owner EPOCH input type	√	√	√	
Software Guard Extensions Epoch 0	×	√	√	
Software Guard Extensions Epoch 1	×	√	√	

Setup Option	Firmware Customization	Intel® Server Configuration Utility	Intel® Server Information Retrieval Utility	Comments
SGXLEPUBKEYHASHx Write Enable	√	√	√	
SGXLEPUBKEYHASH0	√	√	√	
SGXLEPUBKEYHASH1	√	√	√	
SGXLEPUBKEYHASH2	√	√	√	
SGXLEPUBKEYHASH3	√	√	√	
Enable/Disable Intel SGX Auto MP Registration Agent	√	√	√	
Advanced: Power & Performance				
CPU Power and Performance Policy	√	√	√	
Workload Configuration	√	√	√	
Advanced: Power & Performance: Uncore Power Management				
Performance P-Limit	√	√	√	This option can support ITK customization, but the value may be overwritten by changing special options after entering BIOS Setup.
Uncore Freq Scaling	√	√	√	
Uncore Freq	√	√	√	
Uncore Freq RAPL	√	√	√	
Advanced: Power & Performance: CPU P State Control				
AVX License Pre-Grant Override	√	√	√	
AVX ICCP Pre-Grant Level	√	√	√	
Enhanced Intel(R) SpeedStep(R) Technology	√	√	√	
Intel(R) Turbo Boost Technology	√	√	√	
Energy Efficient Turbo	√	√	√	
AVX P1	√	√	√	
Dynamic SST-PP	√	×	√	
Intel SST-PP	√	×	√	
Intel Speed Select Base | Config 3 | Config 4	×	×	×	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
Core Count	×	×	×	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
Current P1 Ratio [4]	×	×	×	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
Package TDP (W)	×	×	×	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
Tjmax	×	×	×	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
Activate SST-BF	√	√	√	
Configure SST-BF	√	√	√	
EIST PSD Function	√	√	√	
Advanced: Power & Performance: Hardware P States				

Setup Option	Firmware Customization	Intel® Server Configuration Utility	Intel® Server Information Retrieval Utility	Comments
Hardware P-States	√	√	√	
HardwarePM Interrupt	√	√	√	
EPP Enable	√	√	√	
APS Rocketing	√	√	√	
Scalability	√	√	√	
RAPL Prioritization	√	√	√	
Advanced: Power & Performance: CPU C State Control				
Package C-State	√	√	√	
C1E	√	√	√	This option can support Firmware customization, but the value may be overwritten by changing special options after entering BIOS Setup.
Processor C6	√	√	√	
Advanced: UPI Configuration				
Current Intel(R) UPI Link Speed	×	×	×	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
Intel(R) UPI Link Frequency	×	×	×	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
Intel(R) UPI Frequency Select	√	√	√	
XPT Prefetch	√	√	√	
IO Directory Cache (IODC)	√	√	√	
KTI Prefetch	√	√	√	
Stale AtoS	√	√	√	
LLC Dead Line Alloc	√	√	√	
Advanced: Memory Configuration				
Total DDR4 Memory	×	√	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
PMem	×	√	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
Effective Memory	×	√	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
Current Configuration	×	√	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
Current Memory Speed	×	√	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
Memory Operating Speed Selection	√	√	√	
Page Policy	√	√	√	
Enforce Population POR	√	√	√	
Volatile Memory Mode	√	√	√	
Publish ARS Capability	√	√	√	
SMB Clock Frequency	√	√	√	
PPR Type	√	√	√	
Attempt Fast Boot	√	√	√	
Attempt Fast Cold Boot	√	√	√	
Custom Refresh Enable	√	√	√	

Setup Option	Firmware Customization	Intel® Server Configuration Utility	Intel® Server Information Retrieval Utility	Comments
Custom Refresh Rate	√	√	√	
Enable Power Cycle Policy	√	√	√	
Promote Warnings	√	√	√	
Halt on Mem Training Error	√	√	√	
MemTest	√	√	√	
MemTestLoops	√	√	√	
Adv MemTest Options	√	√	√	
Adv MemTest PPR Flow	√	√	√	
Adv MemTest Retry After Repair	√	√	√	
Adv MemTest Reset Failure Tracking List	√	√	√	
Adv MemTest Conditions	√	√	√	
Adv MemTest VDD Level	√	√	√	
Adv MemTest tWR	√	√	√	
Adv MemTest tREFI	√	√	√	
Adv MemTest Pause	√	√	√	
CPU0_DIMM_A1	×	√	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
...	×	√	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
CPU1_DIMM_H2	×	√	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
Advanced: Memory Configuration: Memory RAS and Performance Configuration				
Memory Mirroring Possible	×	√	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
Memory ADDDC Possible	×	√	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
Mirror Mode	√	√	√	Must disable ADDDC Sparing first in Setup UI for x4 DIMM. For ITK support, the ITK GUI shows three options for Mirror Mode, the user should choose which option to change based on their real configuration.
Partial Mirror 1 Size (GB)	√	√	√	Must set Mirror Mode to Partial Mirror Mode at first.
Partial Mirror 2 Size (GB)	√	√	√	Must set Mirror Mode to Partial Mirror Mode and set Partial Mirror 1 Size to non-zero at first.
Partial Mirror 3 Size (GB)	√	√	√	Must set Mirror Mode to Partial Mirror Mode and set Partial Mirror 2 Size to non-zero at first.
Partial Mirror 4 Size (GB)	√	√	√	Must set Mirror Mode to Partial Mirror Mode and set Partial Mirror 3 Size to non-zero at first.

Setup Option	Firmware Customization	Intel® Server Configuration Utility	Intel® Server Information Retrieval Utility	Comments
Mirror TAD0	√	√	√	Must disable ADDDC Sparing first in Setup UI for x4 DIMM. For ITK support, the ITK GUI shows two options for Mirror TAD0, the user should choose which option to change based on their real configuration
ADDDC Sparing	√	√	√	
NUMA Optimized	√	√	√	
SNC(Sub NUMA)	√	√	√	
UMA-Based Clustering	√	√	√	
Patrol Scrub	√	√	√	
Correctable Error Threshold	√	√	√	For ITK support, the user should know the configuration and choose the proper value to update, or it may cause potential issues for RAS Error handling.
Trigger SW Error Threshold	√	√	√	
SW Per Bank Threshold	√	√	√	
SW Correctable Error Time Window	√	√	√	
Memory Corrected Error	√	√	√	
Memory Error	√	√	√	
Cloaking	√	√	√	
Partial Cache Line Sparing PCLS	√	√	√	
Advanced: Memory Configuration: Intel(R) Optane(TM) PMem Setting				
PMem Error Injection	√	√	√	
PMem Factory Reset/Clear	√	×	×	
Snoopy Mode for 2LM	√	√	√	
Snoopy Mode for AD	√	√	√	
PMem Performance Setting	√	√	√	
PMem FastGo Configuration	√	√	√	
PMem Latch System Shutdown State	√	√	√	
PMem QoS	√	√	√	
Advanced: System Event Log				
System Errors	√	√	√	
System Poison	√	√	√	
Viral Status	√	√	×	
IIO/PCH Global Error Support	√	√	√	
WHEA Support	√	√	√	
IERR Shutdown Policy	√	√	√	
OS Native AER Support	√	√	√	
IIO Error Registers Clear	√	√	√	

Setup Option	Firmware Customization	Intel® Server Configuration Utility	Intel® Server Information Retrieval Utility	Comments
PCIE Correctable Errors	√	√	√	
PCIE Correctable Error Threshold	√	√	√	
Assert NMI on SERR	√	√	√	
Assert NMI on PERR	√	√	√	
Advanced: Integrated I/O Configuration				
Intel(R) VT for Directed I/O	√	√	√	
ACS Control	√	√	√	Need to enable Intel® VT for Directed I/O first.
DMA Control Opt-In Flag	√	√	√	Need to enable Intel® VT for Directed I/O first.
Pre-Boot DMA Protection	√	√	√	Need to enable Intel® VT for Directed I/O first.
PCIe Pll SSC	√	√	√	
DMI-PCIe Port MPSWorkaround	√	√	√	
Snoop Response Hold Off	√	√	√	
Relaxed Ordering	√	√	√	
No Snoop (Sck0 IOAT Function 0)	√	√	√	
No Snoop (Sck0 IOAT Function 1)	√	√	√	
No Snoop (Sck0 IOAT Function 2)	√	√	√	
No Snoop (Sck0 IOAT Function 3)	√	√	√	
No Snoop (Sck0 IOAT Function 4)	√	√	√	
No Snoop (Sck0 IOAT Function 5)	√	√	√	
No Snoop (Sck0 IOAT Function 6)	√	√	√	
No Snoop (Sck0 IOAT Function 7)	√	√	√	
No Snoop (Sck1 IOAT Function 0)	√	√	√	
No Snoop (Sck1 IOAT Function 1)	√	√	√	
No Snoop (Sck1 IOAT Function 2)	√	√	√	
No Snoop (Sck1 IOAT Function 3)	√	√	√	
No Snoop (Sck1 IOAT Function 4)	√	√	√	
No Snoop (Sck1 IOAT Function 5)	√	√	√	
No Snoop (Sck1 IOAT Function 6)	√	√	√	
No Snoop (Sck1 IOAT Function 7)	√	√	√	

Setup Option	Firmware Customization	Intel® Server Configuration Utility	Intel® Server Information Retrieval Utility	Comments
Integrated I/O Configuration: PCIe* Slot Bifurcation Setting				
Riserx_Slot_x Bifurcation	√	√	√	
Integrated I/O Configuration: Processor PCIe* Link Speed				
Integrated I/O Configuration: Processor PCIe* Link Speed: Socket x PCIe* Link Speed				
Socket x, DMI	√	√	×	
Socket x, PCIe Port 0a	√	√	√	
Socket x, PCIe Port 0b	√	√	√	
Socket x, PCIe Port 0c	√	√	√	
Socket x, PCIe Port 0d	√	√	√	
Socket x, PCIe Port 1a	√	√	√	
Socket x, PCIe Port 1b	√	√	√	
Socket x, PCIe Port 1c	√	√	√	
Socket x, PCIe Port 1d	√	√	√	
Socket x, PCIe Port 2a	√	√	√	
Socket x, PCIe Port 2b	√	√	√	
Socket x, PCIe Port 2c	√	√	√	
Socket x, PCIe Port 2d	√	√	√	
Socket x, PCIe Port 3a	√	√	√	
Socket x, PCIe Port 3b	√	√	√	
Socket x, PCIe Port 3c	√	√	√	
Socket x, PCIe Port 3d	√	√	√	

Setup Option	Firmware Customization	Intel® Server Configuration Utility	Intel® Server Information Retrieval Utility	Comments
Integrated I/O Configuration: PCIe Misc. Configuration				
PCIe ASPM Support (Global)	√	√	√	Intel® Server Configuration Utility can only support the first port variable change since the sting is the same in other port.
ECRC Generation	√	√	√	Intel® Server Configuration Utility can only support the first port variable change since the sting is the same in other port.
ECRC Check	√	√	√	Intel® Server Configuration Utility can only support the first port variable change since the sting is the same in other port.
PCIe ASPM Support	√	√	√	Intel® Server Configuration Utility can only support the first port variable change since the sting is the same in other port.
Data Link Feature Exchange	√	√	√	Intel® Server Configuration Utility can only support the first port variable change since the sting is the same in other port.
Gen3 Override mode	√	√	√	Intel® Server Configuration Utility can only support the first port variable change since the sting is the same in other port.
Ph3 TxEq Precursor	√	√	√	Intel® Server Configuration Utility can only support the first port variable change since the sting is the same in other port.
Ph3 TxEq Postcursor	√	√	√	Intel® Server Configuration Utility can only support the first port variable change since the sting is the same in other port.
Gen4 Override mode	√	√	√	Intel® Server Configuration Utility can only support the first port variable change since the sting is the same in other port.
Integrated I/O Configuration: Volume Management Device				
Riser1 Volume Management Device (CPU0, IOU2)	√	√	√	Intel® Server Board M50CYP, Riser 1 with Retimer.
VMD for Direct Assign (CPU0, IOU2)	√	√	√	
PCIe-SSD0 (CPU0 Port 2A)	√	√	√	Intel® Server Board M50CYP.
PCIe-SSD1 (CPU0 Port 2B)	√	√	√	Intel® Server Board M50CYP.
PCIe-SSD2 (CPU0 Port 2C)	√	√	√	Intel® Server Board M50CYP.
PCIe-SSD3 (CPU0 Port 2D)	√	√	√	Intel® Server Board M50CYP.
Riser3, NVMe Volume Management Device (CPU1, IOU0)	√	√	√	Intel® Server Board M50CYP, Riser 3 with NVMe* card.
VMD for Direct Assign (CPU1, IOU0)	√	√	√	
PCIe-SSD0 (CPU1 Port 0A)	√	√	√	Intel® Server Board M50CYP.
PCIe-SSD1 (CPU1 Port 0B)	√	√	√	Intel® Server Board M50CYP.

Setup Option	Firmware Customization	Intel® Server Configuration Utility	Intel® Server Information Retrieval Utility	Comments
PCIe-SSD2 (CPU1 Port 0C)	√	√	√	Intel® Server Board M50CYP.
PCIe-SSD3 (CPU1 Port 0D)	√	√	√	Intel® Server Board M50CYP.
Mid-Plane 1 Volume Management Device (CPU0, IOU3)	√	√	√	Intel® Server Board M50CYP, Riser with Mid-Plane 1.
VMD for Direct Assign(CPU0, IOU3)	√	√	√	
PCIe-SSD0 (CPU0 Port 3A)	√	√	√	Intel® Server Board M50CYP.
PCIe-SSD1 (CPU0 Port 3B)	√	√	√	Intel® Server Board M50CYP.
PCIe-SSD2 (CPU0 Port 3C)	√	√	√	Intel® Server Board M50CYP.
PCIe-SSD3 (CPU0 Port 3D)	√	√	√	Intel® Server Board M50CYP.
Mid-Plane 2 Volume Management Device (CPU1, IOU3)	√	√	√	Intel® Server Board M50CYP, Riser with Mid-Plane 2.
VMD for Direct Assign (CPU1, IOU3)	√	√	√	
PCIe-SSD0 (CPU1 Port 3A)	√	√	√	Intel® Server Board M50CYP.
PCIe-SSD1 (CPU1 Port 3B)	√	√	√	
PCIe-SSD2 (CPU1 Port 3C)	√	√	√	Intel® Server Board M50CYP.
PCIe-SSD3 (CPU1 Port 3D)	√	√	√	Intel® Server Board M50CYP.
Direct HSBP Volume Management Device (CPU0, IOU3)	√	√	√	Intel® Server Board M50CYP, HSBP Direct connection.
VMD for Direct Assign (CPU0, IOU3)	√	√	√	
PCIe-SSD0 (CPU0 Port 3A)	√	√	√	Intel® Server Board M50CYP.
PCIe-SSD1 (CPU0 Port 3B)	√	√	√	Intel® Server Board M50CYP.
PCIe-SSD2 (CPU0 Port 3C)	√	√	√	Intel® Server Board M50CYP.
PCIe-SSD3 (CPU0 Port 3D)	√	√	√	Intel® Server Board M50CYP.
Direct HSBP Volume Management Device (CPU1, IOU3)	√	√	√	Intel® Server Board M50CYP, HSBP Direct connection.
VMD for Direct Assign (CPU1, IOU3)	√	√	√	
PCIe-SSD0 (CPU1 Port 3A)	√	√	√	Intel® Server Board M50CYP.

Setup Option	Firmware Customization	Intel® Server Configuration Utility	Intel® Server Information Retrieval Utility	Comments
PCIe-SSD1 (CPU1 Port 3B)	√	√	√	Intel® Server Board M50CYP.
PCIe-SSD2 (CPU1 Port 3C)	√	√	√	Intel® Server Board M50CYP.
PCIe-SSD3 (CPU1 Port 3D)	√	√	√	Intel® Server Board M50CYP.
PCIe M.2 Volume Management Device (CPU0 PCH)	√	√	√	Intel® Server Board M50CYP.
VMD for Direct Assign (PCH ports)	√	√	√	
M.2 x4 PCIE _1	√	√	√	Intel® Server Board M50CYP.
M.2 x4 PCIE _2	√	√	√	Intel® Server Board M50CYP.
Ruler SSD Volume Management Device	√	√	√	Intel® Server Board D50TNP, Ruler SSD.
VMD for Direct Assign(CPU0, IOU0)	√	√	√	
VMD for Direct Assign(CPU0, IOU1)	√	√	√	
VMD for Direct Assign(CPU1, IOU0)	√	√	√	
VMD for Direct Assign(CPU1, IOU3)	√	√	√	
RSSD #0 (CPU0 Port 0A)	√	√	√	Intel® Server Board D50TNP.
RSSD #1 (CPU0 Port 0B)	√	√	√	Intel® Server Board D50TNP.
RSSD #2 (CPU0 Port 0C)	√	√	√	Intel® Server Board D50TNP.
RSSD #3 (CPU0 Port 0D)	√	√	√	Intel® Server Board D50TNP.
RSSD #4 (CPU0 Port 1A)	√	√	√	Intel® Server Board D50TNP.
RSSD #5 (CPU0 Port 1B)	√	√	√	Intel® Server Board D50TNP.
RSSD #6 (CPU0 Port 1C)	√	√	√	Intel® Server Board D50TNP.
RSSD #7 (CPU0 Port 1D)	√	√	√	Intel® Server Board D50TNP.
RSSD #8 (CPU1 Port 0A)	√	√	√	Intel® Server Board D50TNP.
RSSD #9 (CPU1 Port 0B)	√	√	√	Intel® Server Board D50TNP.
RSSD #10 (CPU1 Port 0C)	√	√	√	Intel® Server Board D50TNP.
RSSD #11 (CPU1 Port 0D)	√	√	√	Intel® Server Board D50TNP.
RSSD #12 (CPU1 Port 3A)	√	√	√	Intel® Server Board D50TNP.
RSSD #13 (CPU1 Port 3B)	√	√	√	Intel® Server Board D50TNP.
RSSD #14 (CPU1 Port 3C)	√	√	√	Intel® Server Board D50TNP.
RSSD #15 (CPU1 Port 3D)	√	√	√	Intel® Server Board D50TNP.
2U Riser Volume Management Device	√	√	√	Intel® Server Board D50TNP, 2U Riser.
PCIe-SSD0 (CPU0 Port 3C)	√	√	√	Intel® Server Board D50TNP.

Setup Option	Firmware Customization	Intel® Server Configuration Utility	Intel® Server Information Retrieval Utility	Comments
PCIe-SSD1 (CPU0 Port 3D)	√	√	√	Intel® Server Board D50TNP.
PCIe M.2 Volume Management Device (CPU0 PCH)	√	√	√	Intel® Server Board D50TNP.
M.2 x4 PCIE _1	√	√	√	Intel® Server Board D50TNP.
M.2 x4 PCIE _2	√	√	√	Intel® Server Board D50TNP.
Integrated I/O Configuration: NTB Configuration				
NTB PCIe Port 0a on CPU socket 0/1	√	√	√	
Enable NTB Bars	√	√	√	
Enable SPLIT BARs	√	√	√	
Imbar1 Size	√	√	√	
Imbar2_0 Size	√	√	√	
Imbar2_1 Size	√	√	√	
Imbar2 Size	√	√	√	
Embar1 Size	√	√	√	
Embar2_0 Size	√	√	√	
Embar2_1 Size	√	√	√	
Embar2 Size	√	√	√	
Crosslink Control Override	√	√	√	
NTB PCIe Port 1a on CPU socket 0/1	√	√	√	
Enable NTB Bars	√	√	√	
Enable SPLIT BARs	√	√	√	
mbar1 Size	√	√	√	
Imbar2_0 Size	√	√	√	
Imbar2_1 Size	√	√	√	
Imbar2 Size	√	√	√	
Embar1 Size	√	√	√	
Embar2_0 Size	√	√	√	
Embar2_1 Size	√	√	√	
Embar2 Size	√	√	√	
Crosslink Control Override	√	√	√	
NTB PCIe Port 2a on CPU socket 0/1	√	√	√	
Enable NTB Bars	√	√	√	
Enable SPLIT BARs	√	√	√	
mbar1 Size	√	√	√	
Imbar2_0 Size	√	√	√	
Imbar2_1 Size	√	√	√	
Imbar2 Size	√	√	√	
Embar1 Size	√	√	√	
Embar2_0 Size	√	√	√	
Embar2_1 Size	√	√	√	

Setup Option	Firmware Customization	Intel® Server Configuration Utility	Intel® Server Information Retrieval Utility	Comments
Embar2 Size	√	√	√	
Crosslink Control Override	√	√	√	
NTB PCIe Port 3a on CPU socket 0/1	√	√	√	
Enable NTB Bars	√	√	√	
Enable SPLIT BARs	√	√	√	
mbar1 Size	√	√	√	
Imbar2_0 Size	√	√	√	
Imbar2_1 Size	√	√	√	
Embar1 Size	√	√	√	
Embar2_0 Size	√	√	√	
Embar2_1 Size	√	√	√	
Embar2 Size	√	√	√	
Crosslink Control Override	√	√	√	
NTB Link Train by BIOS	√	√	√	
Advanced: Mass Storage Controller Configuration				
Intel(R) Storage Module	×	×	x	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
Advanced: Mass Storage Controller Configuration: sSATA Controller (Port 0–5)\ SATA Controller (Port 0–7)				
(s)SATA Controller Configuration	×	√	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
AHCI Capable (s)SATA Controller	√	√	√	
(s)SATA RAID Options	×	√	×	
(s)SATA HDD Staggered Spin-Up	√	√	√	
SATA Port 0...7	×	√	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
Advanced: PCI Configuration				
Memory Mapped I/O above 4 GB	√	√	√	
MMIO High Base	√	√	√	
Memory Mapped I/O Size	√	√	√	
Add-In Video Adapter	√	√	√	
Onboard Video	√	√	√	
Fast Video	√	√	√	
Legacy VGA Socket	√	√	√	
ARI Support	√	√	√	
SR-IOV Support	√	√	√	
Reset PCI Rebalance Data	√	×	×	
Advanced: PCI Configuration: NIC Configuration				
Onboard NIC1 Type	×	×	×	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.

Setup Option	Firmware Customization	Intel® Server Configuration Utility	Intel® Server Information Retrieval Utility	Comments
NIC1 Controller	×	×	×	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
NIC1 Port1	×	×	×	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
NIC1 Port2	×	×	×	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
NIC1 Port3	×	×	×	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
NIC1 Port4	×	×	×	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
NIC1 Port1 MAC Address	×	×	×	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
NIC1 Port2 MAC Address	×	×	×	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
NIC1 Port3 MAC Address	×	×	×	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
NIC1 Port4 MAC Address	×	×	×	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
Onboard NIC2 Type	×	×	×	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
NIC2 Controller	×	×	×	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
NIC2 Port1	×	×	×	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
NIC2 Port2	×	×	×	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
NIC2 Port3	×	×	×	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
NIC2 Port4	×	×	×	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
NIC2 Port1 MAC Address	×	×	×	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
NIC2 Port2 MAC Address	×	×	×	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
NIC2 Port3 MAC Address	×	×	×	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
NIC2 Port4 MAC Address	×	×	×	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
Advanced: PCI Configuration: UEFI Network Stack				
UEFI Network Stack	√	√	√	
IPv4 PXE Support	√	√	√	
IPv6 PXE Support	√	√	√	
Advanced: PCI Configuration: UEFI Option ROM Control				
NIC Controller	×	×	×	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
NIC Card 1 Port1 OPROM Slot:	×	×	×	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
NIC Card 1 Port2 OPROM Slot:	×	×	×	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.

Setup Option	Firmware Customization	Intel® Server Configuration Utility	Intel® Server Information Retrieval Utility	Comments
Fiber Channel	×	×	×	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
FC Adapter Slot	×	×	×	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
FC Adapter Slot	×	×	×	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
Storage Controller	×	×	×	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
Storage Card 1 OPROM Slot:	×	×	×	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
Storage Card 2 OPROM Slot:	×	×	×	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
Others	×	×	×	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
OPROM Name Slot:	×	×	×	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
Advanced: Serial Port Configuration				
Serial A Enable	√	√	√	
Serial A Address	√	√	√	
Serial A IRQ	×	×	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
Serial B Enable	√	√	√	
Serial B Address	√	√	√	
Serial B IRQ	×	×	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
Advanced: USB Configuration				
USB Front Ports Enable	√	√	√	
USB Rear Ports Enable	√	√	√	
USB Internal Ports Enable	√	√	√	
Advanced: System Acoustic and Performance Configuration				
Set Fan Profile	√	√	√	BMC-controlled option. The BIOS does not support Intel® Server Configuration Utility/Intel® Server Information Retrieval Utility via `/bcs` command.
Fan PWM Offset	×	×	×	BMC-controlled option. The BIOS does not support Intel® Server Configuration Utility/Intel® Server Information Retrieval Utility via `/bcs` command.
Air Flow Limit	×	×	×	BMC-controlled option. The BIOS does not support Intel® Server Configuration Utility/Intel® Server Information Retrieval Utility via `/bcs` command.
Exit Air Temp	×	×	×	BMC-controlled option. The BIOS does not support Intel® Server Configuration Utility/Intel® Server Information Retrieval Utility via `/bcs` command.
Fan UCC	×	×	×	BMC-controlled option. The BIOS does not support Intel® Server Configuration Utility/Intel® Server Information Retrieval Utility via `/bcs` command.

Setup Option	Firmware Customization	Intel® Server Configuration Utility	Intel® Server Information Retrieval Utility	Comments
Security				
Administrator Password Status	×	√	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
User Password Status	×	√	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
Set Administrator Password	×	√	×	Intel® Server Configuration Utility does not support `/bcs` command, but supports `/bap`.
Set User Password	×	√	×	Intel® Server Configuration Utility does not support `/bcs` command, but supports `/bup`.
Power On Password	√	√	√	
Front Panel Lockout	√	√	√	
Current TPM Device	×	×	×	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
TPM2 Operation	×	×	×	Purpose to clear TPM state.
PCR Bank: SHA1	×	×	×	Use the checkbox to select the **TPM Active PRC Bank**.
PCR Bank: SHA256	×	×	×	Use the checkbox to select the **TPM Active PRC Bank**.
TPM FW Update	√	√	√	The BIOS does not support Intel® Server Configuration Utility via `/d` command. But the user can add a “hidden” parameter to support it.
TPM FW Version	×	×	×	Information-only.
Server Management				
Reset on CATERR	√	√	√	
Reset on ERR2	√	√	√	
Enforced Password Support	√	√	√	
Resume on AC Power Loss	×	√	√	For Intel® Server Configuration Utility, supports `/prp, which` is equal to IPMI command. For ITK, due to the limitation, this setting does not take effect and should not modify the default value, which is always IpmiPowerOff.
Power Restore Delay	√	√	√	BMC-controlled option. The BIOS does not support Intel® Server Configuration Utility/Intel® Server Information Retrieval Utility via `/bcs` command.
Power Restore Delay Value	√	√	√	BMC-controlled option. The BIOS does not support Intel® Server Configuration Utility/Intel® Server Information Retrieval Utility via `/bcs` command.
Clear System Event Log	×	√	×	Intel® Server Configuration Utility does not support `/bcs` command but supports `/csel`.
FRB-2 Enable	√	√	√	
FRB-2 Timeout Value	√	√	√	
OS Boot Watchdog Timer	√	√	√	
OS Boot Watchdog Timer Policy	√	√	√	
OS Boot Watchdog Timer Timeout	√	√	√	

Setup Option	Firmware Customization	Intel® Server Configuration Utility	Intel® Server Information Retrieval Utility	Comments
Plug & Play BMC Detection	√	√	√	
Shutdown Policy	×	√	×	For Intel® Server Configuration Utility/Intel® Server Information Retrieval Utility, this setting should be gotten from the BMC via IPMI but not from the BIOS variable via `/bcs`.
Server Management: Console Redirection				
SOL for Baseboard Mgmt	×	√	√	BMC-controlled option. The BIOS does not support Intel® Server Configuration Utility/Intel® Server Information Retrieval Utility via `/bcs` command.
SOL for Baseboard Mgmt2	×	√	√	BMC-controlled option. The BIOS does not support Intel® Server Configuration Utility/Intel® Server Information Retrieval Utility via `/bcs` command.
SOL for Dedicated Mgmt NIC	×	√	√	BMC-controlled option. The BIOS does not support Intel® Server Configuration Utility/Intel® Server Information Retrieval Utility via `/bcs` command.
Console Redirection	√	√	√	
Flow Control	√	√	√	
Baud Rate	√	√	√	
Terminal Type	√	√	√	
Terminal Resolution	√	√	√	
Diagnostic Messages	√	×	×	
Server Management: System Information				
Board Part Number	×	×	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
Board Serial Number	×	×	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
System Part Number	×	×	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
System Serial Number	×	×	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
Chassis Part Number	×	×	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
Chassis Serial Number	×	×	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
Asset Tag	×	×	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
BMC Status	×	×	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
BMC Firmware Revision	×	×	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
ME Status	×	×	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
ME Firmware Revision	×	×	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
SDR Revision	×	×	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.

Setup Option	Firmware Customization	Intel® Server Configuration Utility	Intel® Server Information Retrieval Utility	Comments
UUID	×	×	√	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
Server Management: BMC LAN Configuration **Note:** For Intel® Server Configuration Utility/Intel® Server Information Retrieval Utility, if support is needed, all settings under BMC LAN Configuration should be gotten from BMC via IPMI but not from the BIOS variable via `/bcs`. This screen field does not support Firmware Customization.				
Baseboard LAN configuration	×	×	×	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
IP Source	×	√	√	Does not support `/bcs` command for Intel® Server Configuration Utility.
IP Address	×	√	√	Does not support `/bcs` command for Intel® Server Configuration Utility.
Subnet Mask	×	√	√	Does not support `/bcs` command for Intel® Server Configuration Utility.
Gateway IP	×	√	√	Does not support `/bcs` command for Intel® Server Configuration Utility.
Baseboard LAN IPv6 configuration	×	×	×	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
IPv6	×	√	√	Does not support `/bcs` command for Intel® Server Configuration Utility.
IPv6 Source	×	√	√	Does not support `/bcs` command for Intel® Server Configuration Utility.
IPv6 Address	×	√	√	Does not support `/bcs` command for Intel® Server Configuration Utility.
Gateway IPv6	×	√	√	Does not support `/bcs` command for Intel® Server Configuration Utility.
IPv6 Prefix Length	×	√	√	Does not support `/bcs` command for Intel® Server Configuration Utility.
Dedicated Management LAN Configuration	×	×	×	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
Remote Management Module	×	×	×	Does not support `/bcs` command for Intel® Server Configuration Utility.
IP Source	×	√	√	Does not support `/bcs` command for Intel® Server Configuration Utility.
IP Address	×	√	√	Does not support `/bcs` command for Intel® Server Configuration Utility.
Subnet Mask	×	√	√	Does not support `/bcs` command for Intel® Server Configuration Utility.
Gateway IP	×	√	√	Does not support `/bcs` command for Intel® Server Configuration Utility.
Dedicated Management LAN IPv6 Configuration	×	×	×	Information-only. Does not support `/bcs` command for Intel® Server Configuration Utility.
IPv6 Source	×	√	√	Does not support `/bcs` command for Intel® Server Configuration Utility.
IPv6 Address	×	√	√	Does not support `/bcs` command for Intel® Server Configuration Utility.
Gateway IPv6	×	√	√	Does not support `/bcs` command for Intel® Server Configuration Utility.
IPv6 Prefix Length	×	√	√	Does not support `/bcs` command for Intel® Server Configuration Utility.

Setup Option	Firmware Customization	Intel® Server Configuration Utility	Intel® Server Information Retrieval Utility	Comments
BMC DHCP Host Name	×	√	√	Does not support `/bcs` command for Intel® Server Configuration Utility.
Server Management: BMC LAN Configuration: User Configuration				
Enable Complex Password	×	×	×	Does not support `/bcs` command for Intel® Server Configuration Utility.
User ID	×	√	√	These five user IDs are fixed and cannot be changed. Does not support `/bcs` command for Intel® Server Configuration Utility.
Privilege	×	×	×	It is assigned for a user ID. Does not support `/bcs` command for Intel® Server Configuration Utility.
User Status	×	√	√	Does not support `/bcs` command for Intel® Server Configuration Utility.
User Name	×	√	√	Does not support `/bcs` command for Intel® Server Configuration Utility.
User Password	×	√	√	Does not support `/bcs` command for Intel® Server Configuration Utility.
Boot Maintenance Manager				
Boot Maintenance Manager: Advanced Boot Options				
System Boot Timeout	√	√	√	
Early System Boot Timeout	√	√	√	
USB Boot Priority	√	√	√	
Boot Maintenance Manager: Advanced Boot Options: Secure Boot Configuration				
Current Secure Boot State	×	√	×	ITK support through the Secure Boot Enable option. To enable the secure boot feature by ITK, the user must follow EPS instructions to set: Secure Boot Enable=enable and Boot Mode=UEFI. For Intel® Server Configuration Utility-related support, Secure Boot just supports the proprietary solution defined in the Intel® Server Configuration Utility User Guide, but does not support other general commands for general setup options, such as `/s` or `/bcs` commands.
Attempt Secure Boot	√	√	×	
Boot Maintenance Manager: Add EFI Boot Option				
EFI Boot Option to be selected	×	×	×	For Intel® Server Configuration Utility, this screen field does not support Intel® Server Configuration Utility change via `/bcs` command. However, the user can use Intel® Server Configuration Utility `/bbo` or `/bbosys` commands to set boot order.
Boot Maintenance Manager: Delete EFI Boot Option				
EFI Boot Option to be deleted	×	×	×	For Intel® Server Configuration Utility, this screen field does not support Intel® Server Configuration Utility change via `/bcs` command. However, the user can use Intel® Server Configuration Utility `/bbo` or `/bbosys` commands to set boot order.
Boot Maintenance Manager: Change Boot Order				

Setup Option	Firmware Customization	Intel® Server Configuration Utility	Intel® Server Information Retrieval Utility	Comments
Change the order	√	×	×	1. For Intel® Server Configuration Utility, this screen field does not support Intel® Server Configuration Utility change via `/bcs` command. However, the user can use Intel® Server Configuration Utility `/bbo` or `/bbosys` commands to set boot order. 2. ITK can only support Add Boot order option by customized ITK GUI.
Boot Manager Screen				
UEFI Internal Shell	×	×	×	Boot order list. Does not support `/bcs` command, but support `/bbo` or `/bbosys` for Intel® Server Configuration Utility.
UEFI Floppy Driver	×	×	×	Boot order list. Does not support `/bcs` command, but support `/bbo` or `/bbosys` for Intel® Server Configuration Utility.
UEFI Hard Disk Driver	×	×	×	Boot order list. Does not support `/bcs` command, but support `/bbo` or `/bbosys` for Intel® Server Configuration Utility.
UEFI CD-ROM Driver	×	×	×	Boot order list. Does not support `/bcs` command, but support `/bbo` or `/bbosys` for Intel® Server Configuration Utility.
UEFI NET Driver	×	×	×	Boot order list. Does not support `/bcs` command, but support `/bbo` or `/bbosys` for Intel® Server Configuration Utility.
UEFI HTTPS boot	×	×	×	Boot order list. Does not support `/bcs` command, but support `/bbo` or `/bbosys` for Intel® Server Configuration Utility.
Error Manager				
Save & Exit				
Save Changes and Exit	×	×	×	Selection only.
Discard Changes and Exit	×	×	×	Selection only.
Save Changes	×	×	×	Selection only.
Discard Changes	×	×	×	Selection only.
Load Default Values	×	×	×	Selection only.
Save as User Default Values	×	×	×	Selection only.
Load User Default Values	×	×	×	Selection only.

Appendix B. Glossary

Term	Definition
16-bit legacy	The traditional personal computer environment. Includes legacy Option ROMs and legacy 16-bit code.
ACM	Authenticated Code Mode.
ACPI	Advanced Configuration and Power Interface. ACPI is an open industry specification proposed by Intel, Microsoft* and Toshiba*. ACPI enables and supports reliable power management through improved hardware and OS coordination.
AES	Advanced Encryption Standard. An 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.
BOM	Bill of materials.
BOT	Boot Order Table.
BSP	Bootstrap processor. In a multi-processor system, the processor selected at boot time to be the primary processor.
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.
EAN	International article number (barcode).
FRU	Field-replaceable unit.
iPC	Intel product code. This code is used to identify an orderable Intel product.
iPN	Intel part number. An internal part number issued to a component within a product BOM. Individual Intel part numbers are not orderable unless it is included within an orderable iPC.

Term	Definition
Intel® Optane™ PMem	Intel® Optane™ persistent memory module.
DDR3	Double Data Rate 3 is a high bandwidth memory technology.
DMA	Direct Memory Access.
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).
DMN	Dedicated management NIC
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 operating system. The DSDT contains the Differentiating Definition Block, which supplies the implementation and configuration information about the base system.
DWORD	Double Word, a 32-bit quantity.
DXE	Driver Execution Environment. Component of Intel® Platform Innovation Framework for EFI architecture.
ECC	Error Correction Code. A memory system that has extra bit(s) to support limited detection/correction of memory errors.
EEPROM	Electrically Erasable Programmable Read Only Memory, also 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 is the 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.

Term	Definition
IPMI	Intelligent Platform Management Interface. An industry standard that defines standardized, abstracted interfaces to platform management hardware.
IRQ	Interrupt Request.
ITK	Firmware Customization.
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	Main 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.
MM#	Main material order number, used to identify an orderable Intel product.
MMIO	Memory Mapped I/O.
MOQ	Minimum order quantity.
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.

Term	Definition
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. RAID 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 diverse 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 Set up Engine – the Setup screen display and options choosing utility.
TSS	TCG Software Stack.
Intel® TXT	Intel® Trusted Execution Technology.

Term	Definition
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 malware to execute code.