Basic Input/Output System Setup Utility

User Guide

For the Intel® Server Board M70KLP family.

Rev. 1.3

November 2021

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

<This page intentionally left blank>

Document Revision History

Date	Revision	Changes
February 2021	1.0	Initial release.
February 2021	1.1	• Updated Mass Storage Controller Configuration page, PCH sSATA Configuration page, and Memory RAS Configuration page.
April 2021	1.2	• Updated Uncore General Configuration page, Processor Configuration page, Memory Configuration page, and Memory RAS Configuration page.
November 2021	1.3	• Updated Root page, PFR page, and Processor page. • Edits throughout the document to improve clarity and format.

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.

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, Intel Xeon, Intel Server BIOS Toolkit, Intel Node Manager, Intel Management Engine, Intel Optane, Intel VT for Directed I/O, Intel Volume Management Device, Intel Hyper-Threading Technology, Intel Virtualization Technology, Intel Trusted Execution Technology, Intel Virtualization Technology for Directed I/O, Intel AES New Instructions, Intel Platform Innovation Framework for EFI, Intel Intelligent Power Node Manager, and the Intel logo are trademarks of Intel Corporation or its subsidiaries in the U.S. and/or other countries.

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

© Intel Corporation

Table of Contents

List of Figures

List of Tables

1. Introduction

This document provides an overview of the features and functions supported by the embedded basic input/output system (BIOS) setup utility for Intel® Server Board M70KLP family based on the 3rd Generation Intel® Xeon® Scalable processor family.

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.

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 interface consists of multiple pages or screens. Each screen contains information and links to other screens. The Advanced tab in the Setup screen displays a list of general categories and links. These links take the user to screens that contain configuration options for specific categories.

The BIOS setup utility has the following characteristics:

- **Localization:** The Intel® Server BIOS Toolkit is only available in English.
- **Console redirection:** The BIOS setup utility is functional via console redirection over various terminal emulation standards.

  Note: When the console redirection feature is enabled, the power on self-test (POST) display is in text mode because of redirection data transfer in a serial port data terminal emulation mode. This display may limit some functionality due to compatibility. For example, the usage of colors, 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 to work with console redirection. However, this screen layout should display correctly on any format with longer lines or more lines on the screen.

2. BIOS Setup Operation

2.1 Setup Screen Layout

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

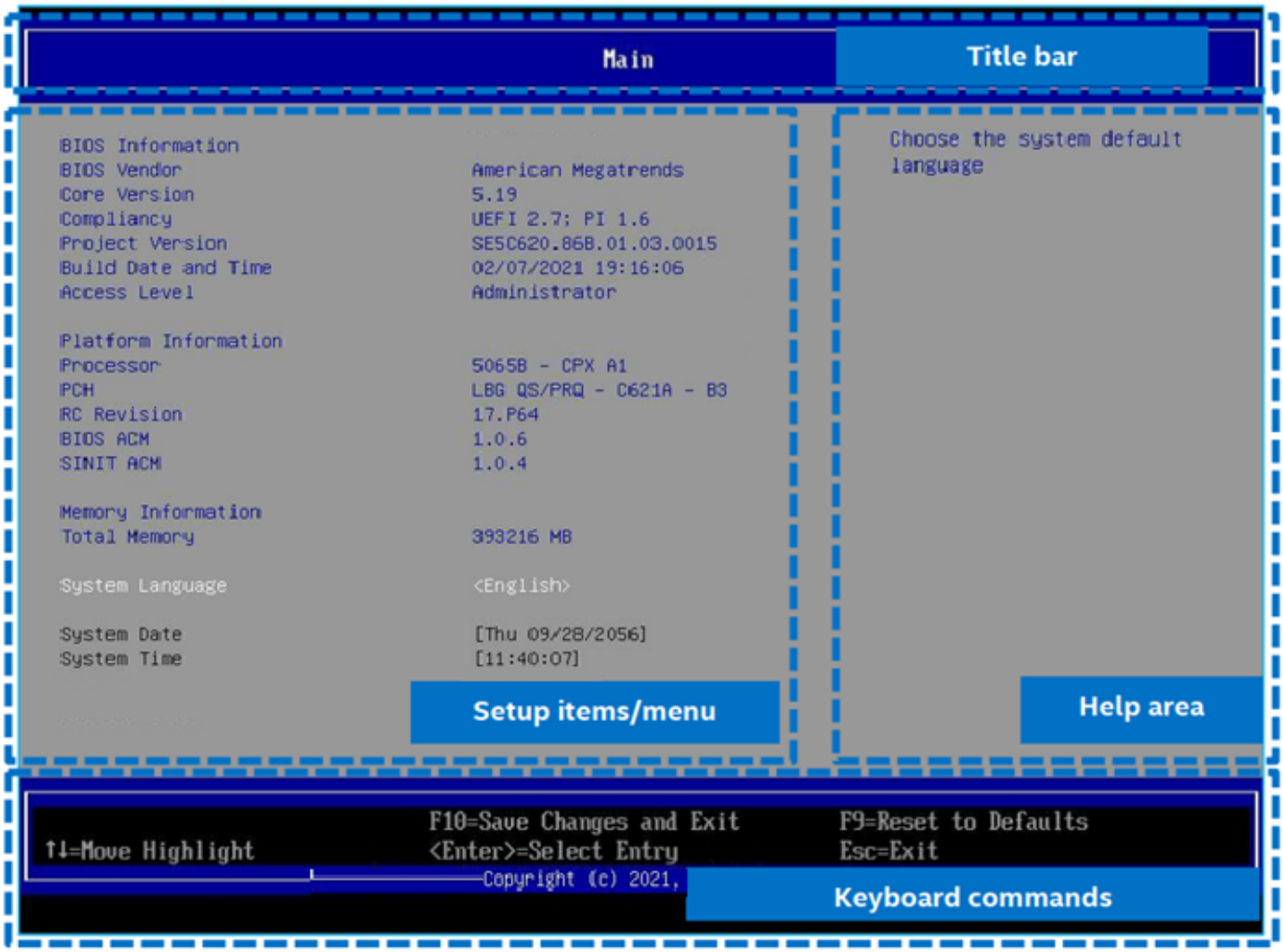

Figure 1. BIOS Setup Screen Layout

Table 1. BIOS Setup Page Layout

Functional Area	Description
Title bar	The title bar 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 arrow) 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, the page title identifying the specific page that the user is viewing is in the upper left corner of the page. Use the **<ESC>** key to return to a higher level in the hierarchy. By repeatedly pressing this key, the user can reach the top-level page.
Setup items/menu	The setup item list is a set of control entries and informational items. The list is displayed in two columns. For each item in the list: • The operator navigates up and down the right 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, navigate to the desired selection and presses **<Enter>** to go to the new screen.
Help area	The item-specific help area is in 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 others.
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 Screen

To enter the BIOS Setup screen using a keyboard (or emulated keyboard), press the **<F2>** function key during boot time while one of these screens is being displayed: original equipment manufacturer (OEM) logo, Intel logo, power oneself-test (POST) diagnostic.

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

```
Press <F2> to enter setup
```

Note: With a USB keyboard, it is important to wait until the basic input/output system (BIOS) discovers the keyboard and beeps. Key pressing is read by the system only after the USB controller has been initialized and the USB keyboard is activated.

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

The user can also cause a boot directly to setup using the IPMI 2.0 command `Get/Set System Boot Options`. For details on that capability, see the explanation in the Intelligent Platform Management Interface (IPMI)description.

2.3 Exit BIOS Setup Screen

The user can exit the BIOS Setup screen through one of these three methods:

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 performs a cold reset after any of the above methods is applied. For more information on the Save & Exit screen, see Section 11.

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

Table 2. BIOS Setup Keyboard Command Bar

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

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

<F10>	Save changes and exit	Pressing the **<F10>** key causes the following message to display:
		`Save configuration changes and exit?`
		`Press 'Y' to confirm, 'N' / 'ESC' to ignore.`
		If **<Y>** is pressed, all changes are saved and the setup is exited. If **<N>** 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 Menu

3.1 Front Page and Setup Menu

The front page is the first screen that appears when the basic input/output (BIOS) setup utility is entered and it contains the entry to the BIOS Setup menu.

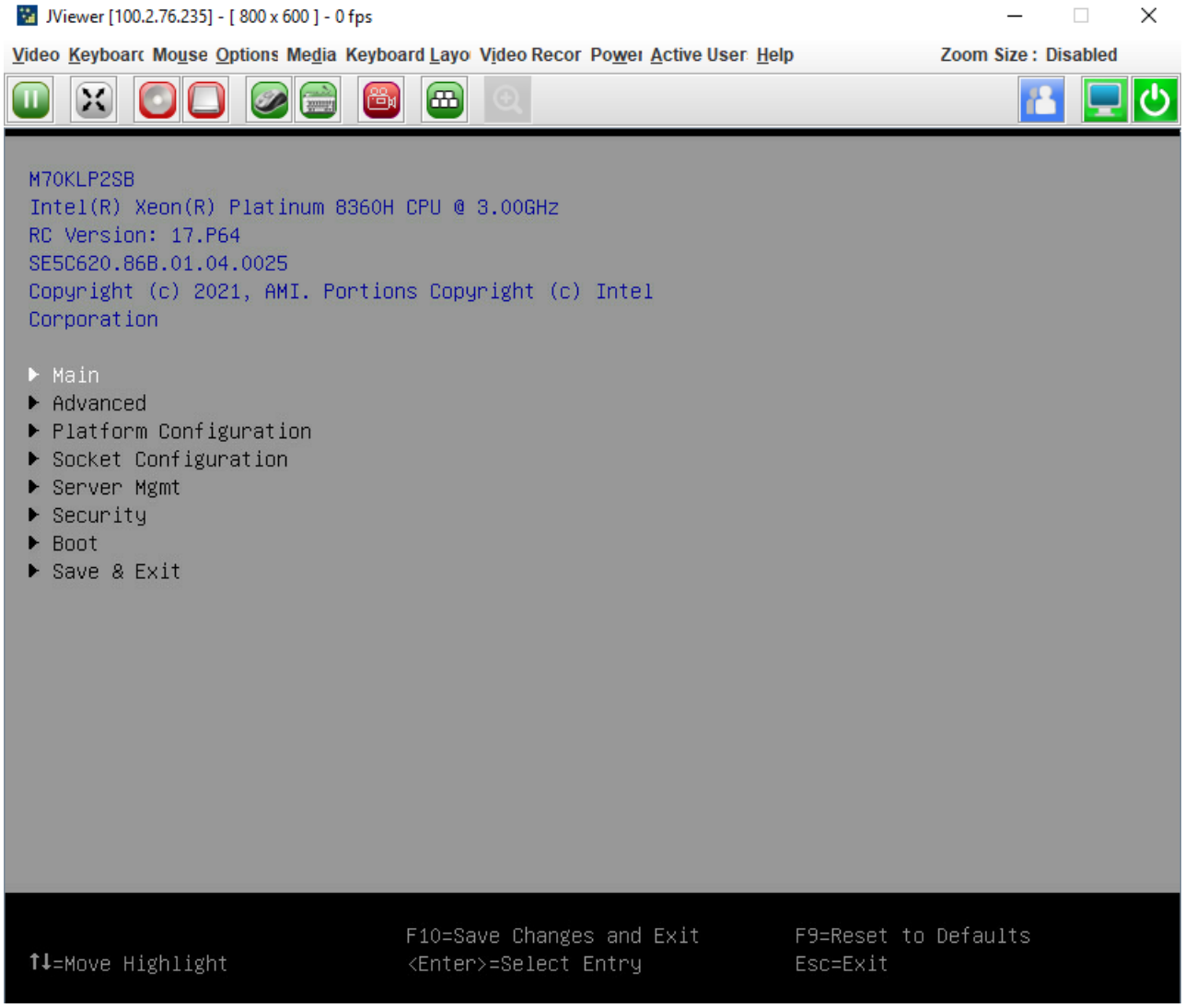

Figure 2. Front Page and Setup Menu

The setup menu contains the entire BIOS setup collection and organizes the options into major categories. Each category has a hierarchy with a top-level screen from which lower-level screens may be selected. Each top-level screen appears as a tab entry, arranged across the top of all top-level screens.

To access a top-level screen from the front page or other top-level screen, press the **<↑>** (up arrow) or **<↓>** (down arrow) keys to go across the tabs. Repeat until the desired screen is selected.

The categories and the screens included in each category are listed in Table 3, with links to each of the screens named.

Table 3. Screen Map

Top-Level Categories	Second Level Screens	Third Level Screens
Main	-	-
Advanced	Redfish Host Interface Settings	-
	AST2500 Super IO Configuration	Serial Port 1 Configuration
		Serial Port 2 Configuration
	Serial Port Console Redirection	Console Redirection Settings (COM0)
		Console Redirection Settings (COM1)
	PCI Configuration	Network Stack Configuration
	USB Configuration	-
	NVMe Configuration	PCIe SSD
	Tls Auth Configuration	Server CA Configuration
	All Cpu Information	-
	RAM Disk Configuration	Create raw
		Create from file
	iSCSI Configuration	Host iSCSI Configuration
	VLAN Configuration	Enter Configuration Menu
	IPv4 Network Configuration	-
	HTTP Boot Configuration	-
	IPv6 Network Configuration	Enter Configuration Menu
	Power & Performance	CPU P State Control
		Hardware PM State Control
		CPU C State Control
		Package C State Control
Platform Configuration	PCH Configuration	Mass Storage Controller Configuration
		PCH sSATA Configuration
	PFR	-
	Server ME Configuration	-
Socket Configuration	Processor Configuration	-
	Uncore Configuration	Uncore General Configuration
	Memory Configuration	Memory RAS Configuration
		Intel(R) Optane(TM) PMem Configuration
	IIO Configuration	Intel® VT for Directed I/O (VT-d)
		Intel® VMD technology
		Intel® AIC Retimer/AIC SSD Technology (non-VMD)

Top-Level Categories	Second Level Screens	Third Level Screens
Server Mgmt	System Event Log	-
	Bmc self test log	-
	BMC network configuration	-
	BMC User Settings	Add User
		Delete User
		Change User Settings
Security	Trusted Computing	-
	Secure Boot	Key Management
	TCG Storage device Security Configuration	-
Boot	-	-
Save & Exit	-	-

4. Main

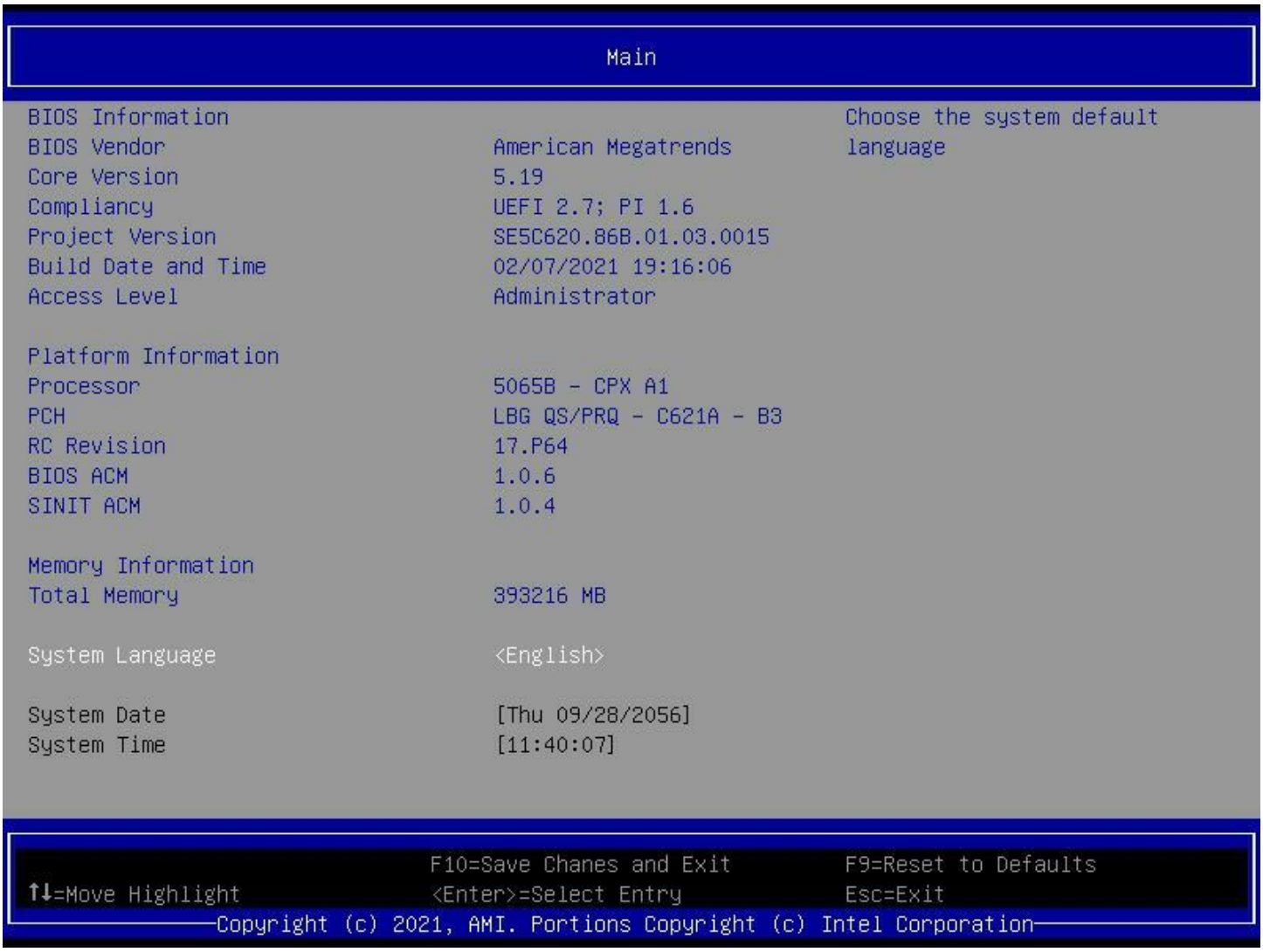

Figure 3. Main Screen

1. **BIOS Vendor**

   Value: American Megatrends

   Help text: None.

   Comments: *Information only.*

   Back to: **Main** – **Screen Map**

2. **Core Version**

   Value: 5.19

   Help text: None.

   Comments: *Information only.*

   Back to: **Main** – **Screen Map**

3. **Compliancy**

   Value: UEFI 2.7; PI 1.6

   Help text: None.

   Comments: *Information only.*

   Back to: **Main** – **Screen Map**

4. **Project Version**

   Value: <BoardFamilyID&BoardRev.86B.xx.yy.zzzz>

   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 – Defines the level of debug output built into and enabled by the BIOS.
   - 86B – Identifies this BIOS as being an Intel® server BIOS.
   - xx – Major revision level of the BIOS.
   - yy – Minor revision of the BIOS.
   - zzzz – Release number of the BIOS.

   Back to: **Main** – **Screen Map**

5. **Build Date and Time**

   Value: <MM/DD/YYYY hh:mm:ss>

   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).

   Back to: **Main** – **Screen Map**

6. **Access Level**

   Value: **Administrator** / User

   Help text: None.

   Comments: *Information only*. Displays the password level in which the setup is running: Administrator or user. With no passwords set, administrator is the default mode.

   Back to: **Main** – **Screen Map**

7. **Processor**

   Value: <Processor Info>

   Help text: None.

   Comments: *Information only.*

   Back to: **Main** – **Screen Map**

8. **PCH**

   Value: <PCH Info>

   Help text: None.

   Comments: *Information only.*

   Back to: **Main** – **Screen Map**

9. **RC Revision**

   Value: <RC Revision>

   Help text: None.

   Comments: *Information only.*

   Back to: **Main** – **Screen Map**

10. **BIOS ACM**

    Value: <BIOS ACM>

    Help text: None.

    Comments: *Information only.*

    Back to: **Main** – **Screen Map**

11. **SINIT ACM**

    Value: <SINIT ACM>

    Help text: None.

    Comments: *Information only.*

    Back to: **Main** – **Screen Map**

12. **Total Memory**

    Value: <Total Memory>

    Help text: None.

    Comments: *Information only.* Displays the amount of memory available in the system. The total memory is expressed in MB of installed DDR4 DIMMs.

    Back to: **Main** – **Screen Map**

13. **System Language**

    Value: English

    Help text: `Choose the System default language.`

    Comments: None.

    Back to: **Main** – **Screen Map**

14. System Date

Value: <W MM/DD/YYYY>

Help text:
```
Set the Date. Use Tab to switch between Date elements.

Default Ranges:
    Year: 2020-2099
    Months: 1-12
    Days: Dependent on month

Range of Years may vary.
```

Comments: This field initially displays the current system date. It may be edited to change the system date. When the system date is reset by the BIOS defaults jumper, BIOS recovery flash update, or other method, the date is the earliest date in the allowed range: 01/01/2020.

Back to: **Main** – **Screen Map**

15. System Time

Value: <hh:mm:ss>

Help text:
```
Set the Time. Use Tab to switch between time elements.
```

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

Back to: **Main** – **Screen Map**

5. Advanced

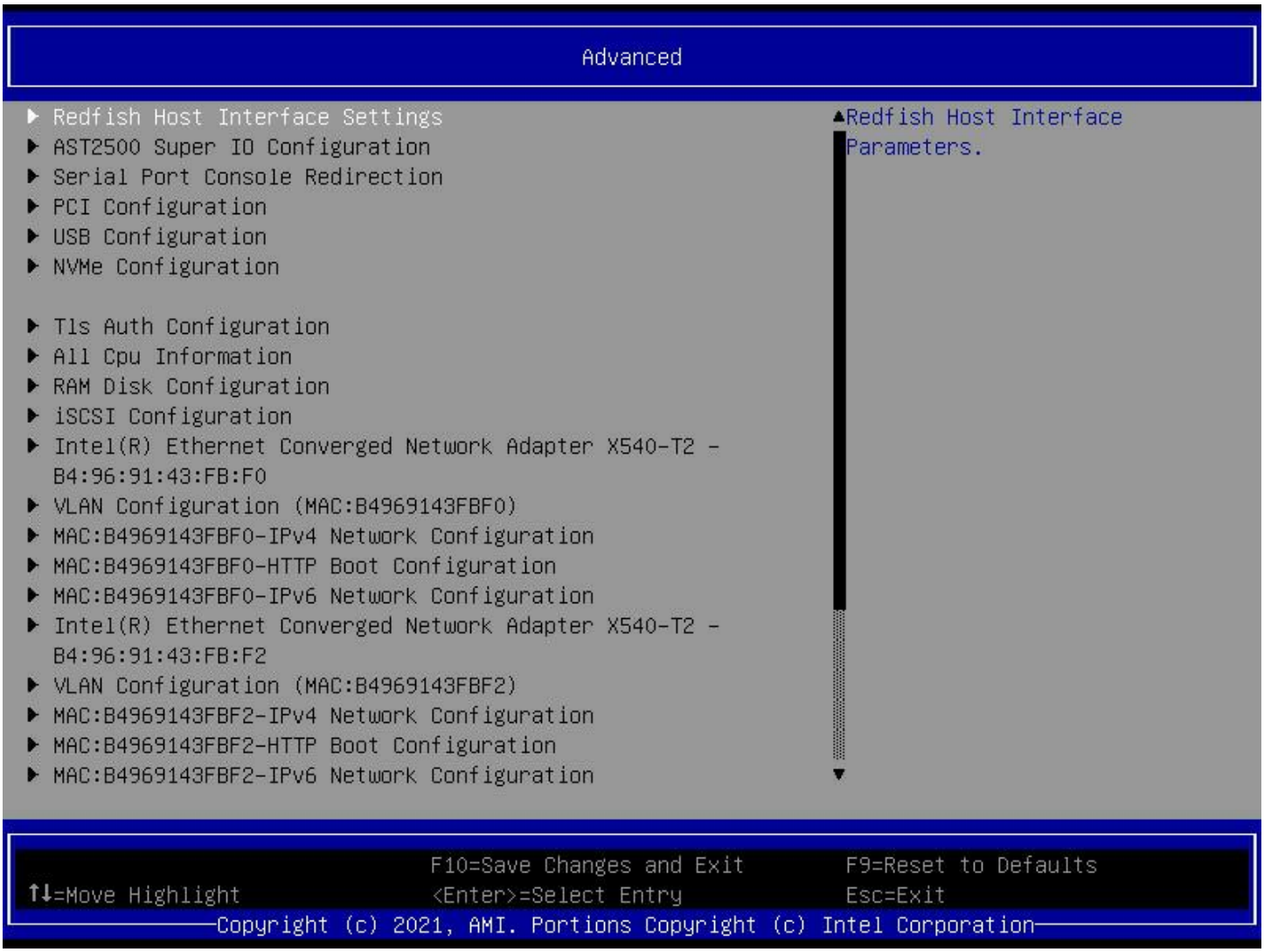

Figure 4. Advanced Screen (1)

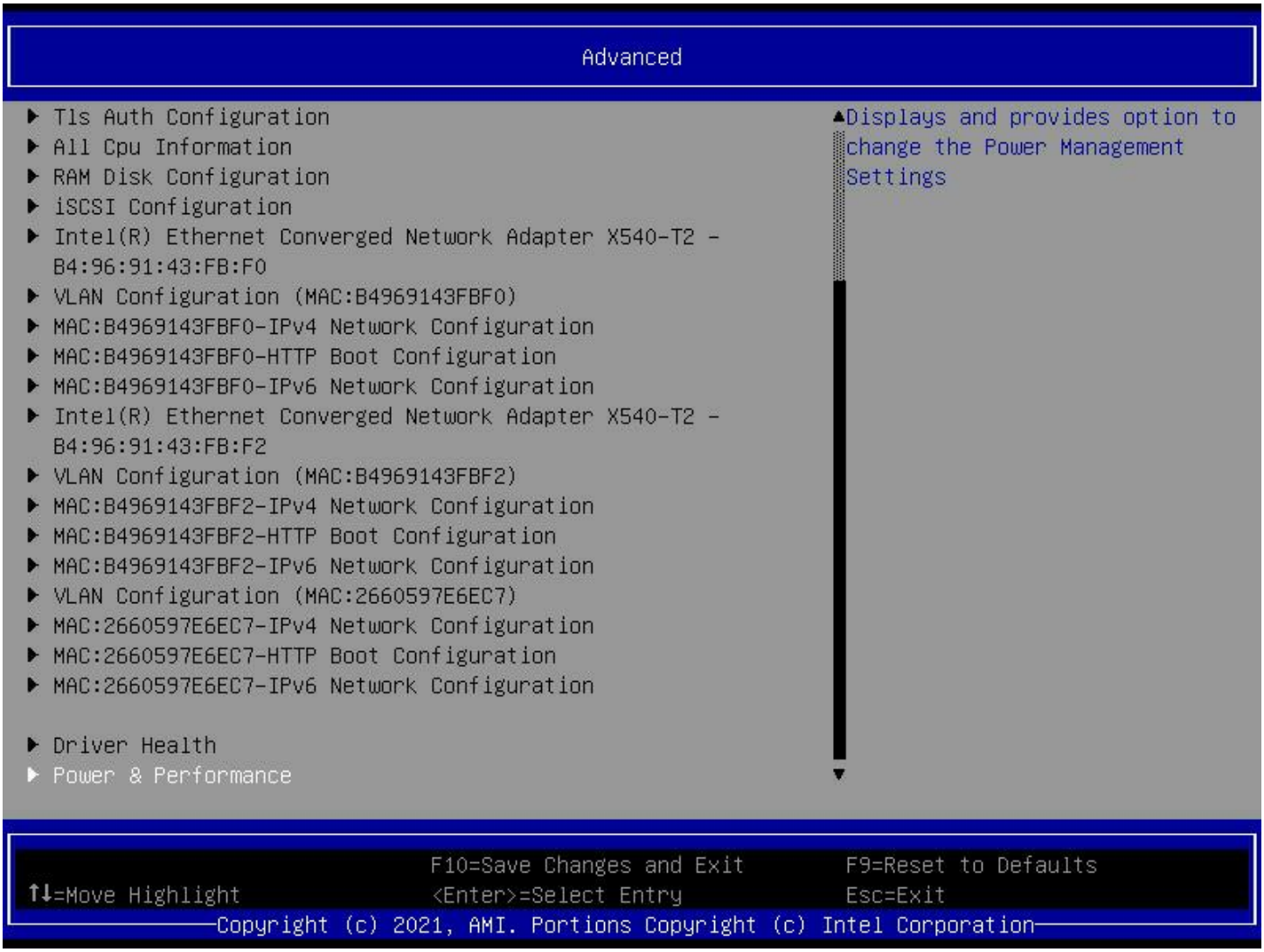

Figure 5. Advanced Screen (2)

1. Redfish Host Interface Settings

Value: None.

Help text: `Redfish Host Interface Parameters.`

Comments: *Selection only.*

Back to: **Advanced** – **Screen Map**

2. AST2500 Super IO Configuration

Value: None.

Help text: `System Super IO Chip Parameters.`

Comments: *Selection only.*

Back to: **Advanced** – **Screen Map**

3. Serial Port Console Redirection

Value: None.

Help text: `Console Redirection Settings.`

Comments: *Selection only.*

Back to: **Advanced** – **Screen Map**

4. PCI Configuration

Value: None.

Help text: `PCI Configuration Parameters.`

Comments: *Selection only.*

Back to: **Advanced** – **Screen Map**

5. USB Configuration

Value: None.

Help text: `USB Configuration Parameters.`

Comments: *Selection only.*

Back to: **Advanced** – **Screen Map**

6. NVMe Configuration

Value: None.

Help text: `NVMe Configuration Parameters.`

Comments: *Selection only.*

Back to: **Advanced** – **Screen Map**

7. Tls Auth Configuration

Value: None.

Help text: `Press <Enter> to select Tls Auth Configuration.`

Comments: *Selection only.*

Back to: **Advanced** – **Screen Map**

8. All Cpu Information

Value: None.

Help text: `Display all CPU information.`

Comments: *Selection only.*

Back to: **Advanced** – **Screen Map**

9. RAM Disk Configuration

Value: None.

Help text: `Press <Enter> to add/remove RAM disks.`

Comments: *Selection only.*

Back to: **Advanced** – **Screen Map**

10. iSCSI Configuration

Value: None.

Help text: `Configure the iSCSI parameters.`

Comments: *Selection only.*

Back to: **Advanced** – **Screen Map**

11. VLAN Configuration

Value: None.

Help text: `VLAN configuration for this network device.`

Comments: *Selection only.*

Back to: **Advanced** – **Screen Map**

12. MAC: xxxxxxxxxxxx Configuration

Value: None.

Help text: None.

Comments: *Selection only.* This option is only visible if a network interface card (NIC) of that media access control (MAC) connected to the system.

Back to: **Advanced** – **Screen Map**

13. Driver Health

Value: None.

Help text: `Provides Health Status for the Drivers/Controllers.`

Comments: *Selection only.* This option is only visible if there are additional devices connected to the system.

Back to: **Advanced** – **Screen Map**

14. Power & Performance

Value: None.

Help text: `Displays and provides option to change the Power Management Settings.`

Comments: *Selection only.*

Back to: **Advanced** – **Screen Map**

5.1 Redfish Host Interface Settings

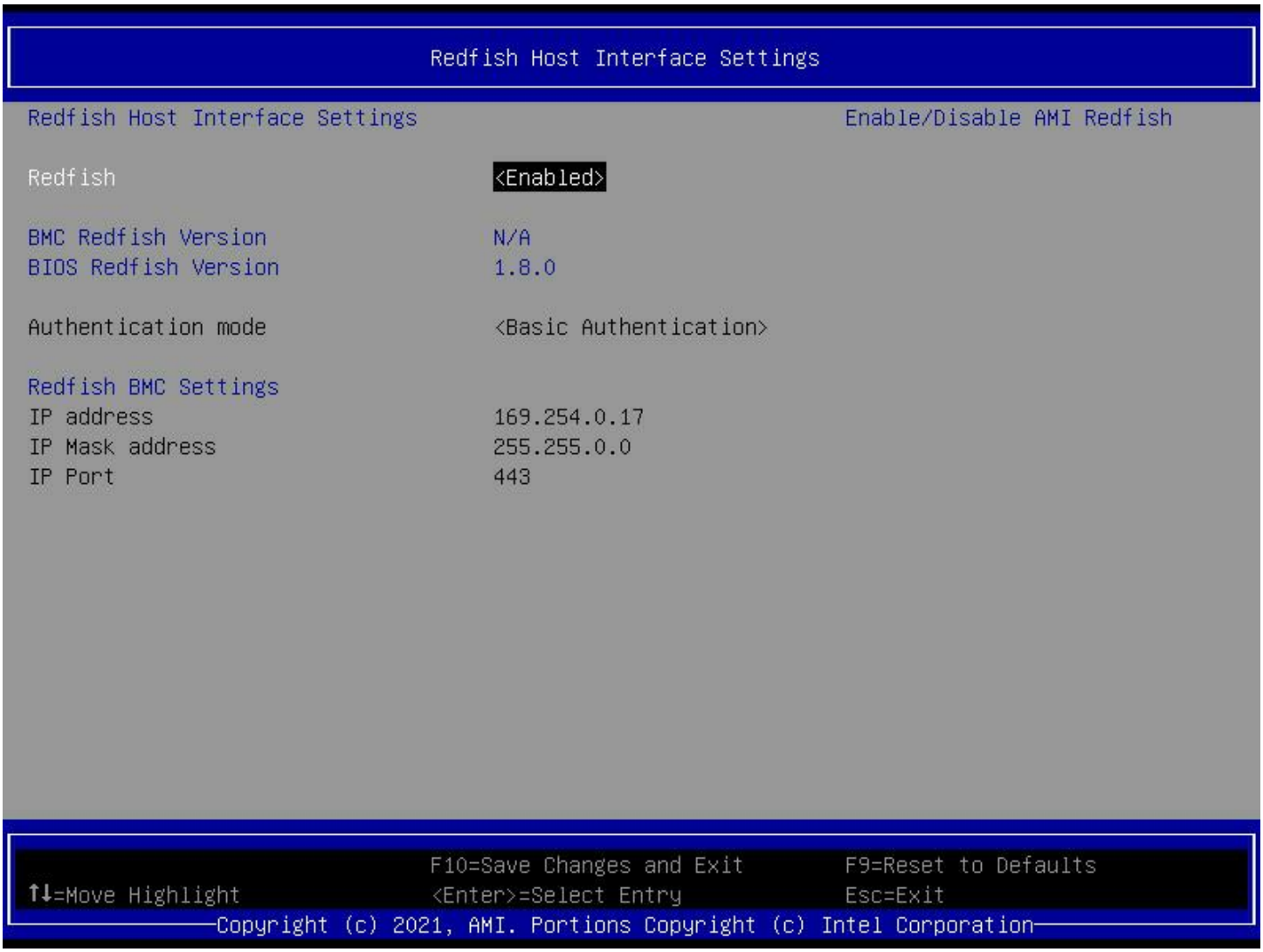

Figure 6. Redfish* Host Interface Settings Screen

1. **Redfish**

Value: **Enable** / Disable

Help text: `Enable/Disable AMI Redfish.`

Comments: None.

Back to: **Redfish Host Interface Settings** – **Advanced** – **Screen Map**

2. **BMC Redfish Version**

Value: <BMC Redfish Version>

Help text: `Redfish version supported by BMC.`

Comments: Dynamically updated.

Back to: **Redfish Host Interface Settings** – **Advanced** – **Screen Map**

3. BIOS Redfish Version

Value: <BIOS Redfish Version>

Help text: `Redfish version supported by BIOS.`

Comments: Dynamically updated.

Back to: **Redfish Host Interface Settings** – **Advanced** – **Screen Map**

4. Authentication mode

Value: **Basic Authentication** / Session Authentication / OEM Authentication

Help text: `Select authentication mode.`

Comments: None.

Back to: **Redfish Host Interface Settings** – **Advanced** – **Screen Map**

5. IP address

Value: <IP address>

Help text: `Enter IP address.`

Comments: None.

Back to: **Redfish Host Interface Settings** – **Advanced** – **Screen Map**

6. IP Mask address

Value: <IP mask address>

Help text: `Enter IP mask address.`

Comments: None.

Back to: **Redfish Host Interface Settings** – **Advanced** – **Screen Map**

7. IP Port

Value: <IP port>

Help text: `Enter IP port.`

Comments: None.

Back to: **Redfish Host Interface Settings** – **Advanced** – **Screen Map**

5.2 AST2500 Super IO Configuration

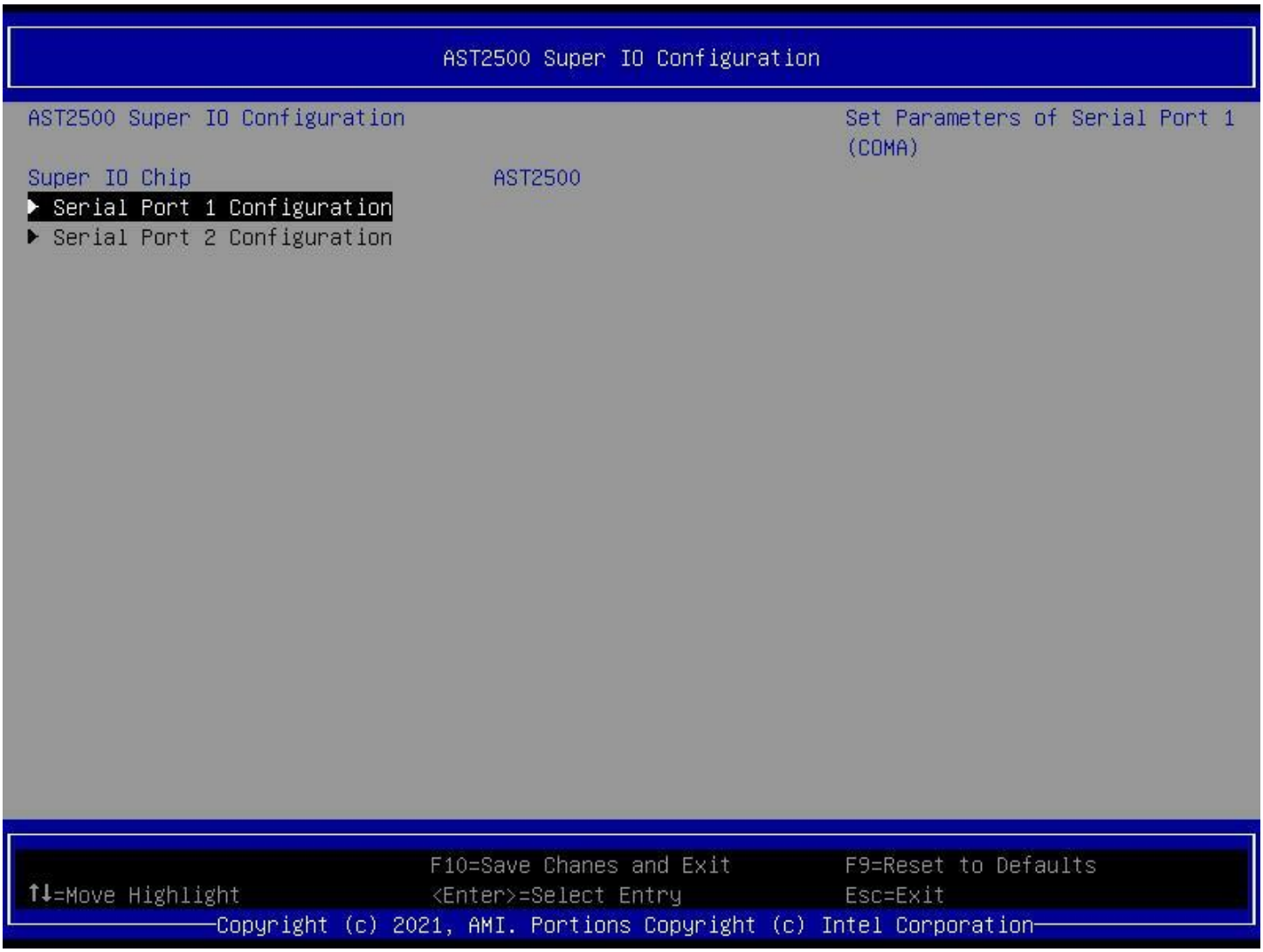

Figure 7. AST2500* Super IO Configuration Screen

1. Serial Port 1 Configuration

Value: None.

Help text: `Set Parameters of Serial Port 1 (COMA).`

Comments: *Selection only.*

Back to: **AST2500 Super IO Configuration** – **Advanced** – **Screen Map**

2. Serial Port 2 Configuration

Value: None.

Help text: `Set Parameters of Serial Port 2 (COMB).`

Comments: *Selection only.*

Back to: **AST2500 Super IO Configuration** – **Advanced** – **Screen Map**

5.2.1 Serial Port 1 Configuration

Figure 8. Serial Port 1 Configuration Screen

1. Serial Port

Value: **Enabled** / Disabled

Help text: `Enable or Disable Serial Port (COM).`

Comments: None.

Back to: **Serial Port 1 Configuration** – **AST2500 Super IO Configuration** – **Advanced** – **Screen Map**

2. Current Limit Override

Value: **IO=3F8h; IRQ=4;** / IO=2F8h; IRQ=3; / IO=3E8h; IRQ=7; / IO=2E8h; IRQ=7; / IO=220h; IRQ=10; / IO=228h; IRQ=10;

Help text: `0 - Default, do nothing; 1 - Manual, override Current limitation in 1/8 A increments.`

Comments: None.

Back to: **Serial Port 1 Configuration** – **AST2500 Super IO Configuration** – **Advanced** – **Screen Map**

3. Change Settings

Value: **Auto**

Help text: `Select an optimal setting for Super IO Device.`

Comments: None.

Back to: **Serial Port 1 Configuration** – **AST2500 Super IO Configuration** – **Advanced** – **Screen Map**

5.2.2 Serial Port 2 Configuration

Figure 9. Serial Port 2 Configuration Screen

1. Serial Port

Value: **Enabled** / Disabled

Help text: `Enable or Disable Serial Port (COM).`

Comments: None.

Back to: **Serial Port 2 Configuration** – **AST2500 Super IO Configuration** – **Advanced** – **Screen Map**

2. Current Limit Override

Value: IO=3F8h; IRQ=4; / **IO=2F8h; IRQ=3;** / IO=3E8h; IRQ=7; / IO=2E8h; IRQ=7; / IO=220h; IRQ=10; / IO=228h; IRQ=10;

Help text: `0 - Default, do nothing; 1 - Manual, override Current limitation in 1/8 A increments.`

Comments: None.

Back to: **Serial Port 2 Configuration** – **AST2500 Super IO Configuration** – **Advanced** – **Screen Map**

3. Change Settings

Value: **Auto**

Help text: `Select an optimal setting for Super IO Device.`

Comments: None.

Back to: **Serial Port 2 Configuration** – **AST2500 Super IO Configuration** – **Advanced** – **Screen Map**

5.3 Serial Port Console Redirection

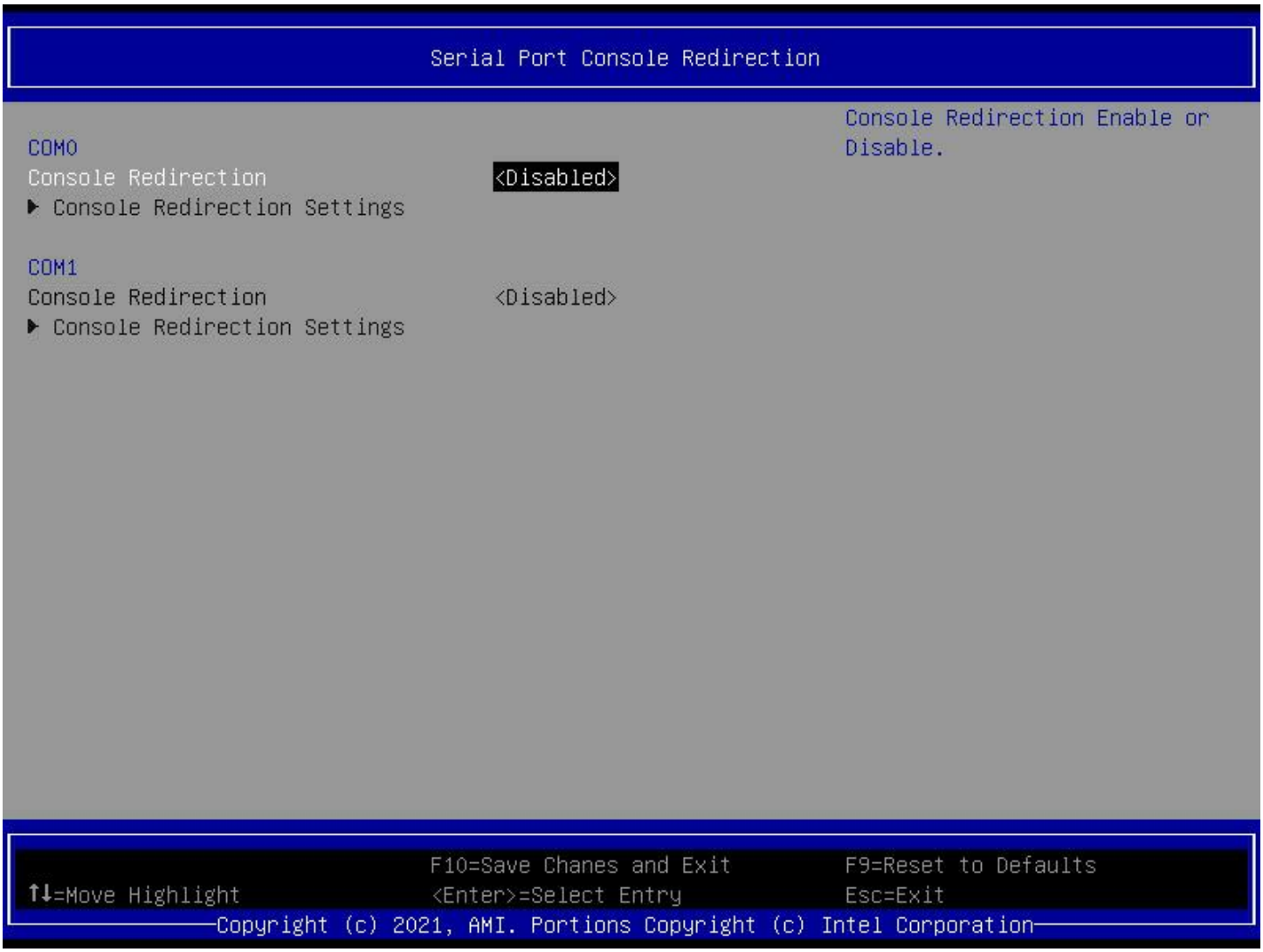

Figure 10. Serial Port Console Redirection Screen

1. **Console Redirection (COM0)**

Value: Enabled / **Disabled**

Help text: `Console Redirection Enable or Disable.`

Comments: Console Redirection Settings is selectable only when this option is enabled.

Back to: **Serial Port Console Redirection** – **Advanced** – **Screen Map**

2. **Console Redirection (COM1)**

Value: Enabled / **Disabled**

Help text: `Console Redirection Enable or Disable.`

Comments: Console Redirection Settings is selectable only when this option is enabled.

Back to: **Serial Port Console Redirection** – **Advanced** – **Screen Map**

5.3.1 Console Redirection Settings (COM0)

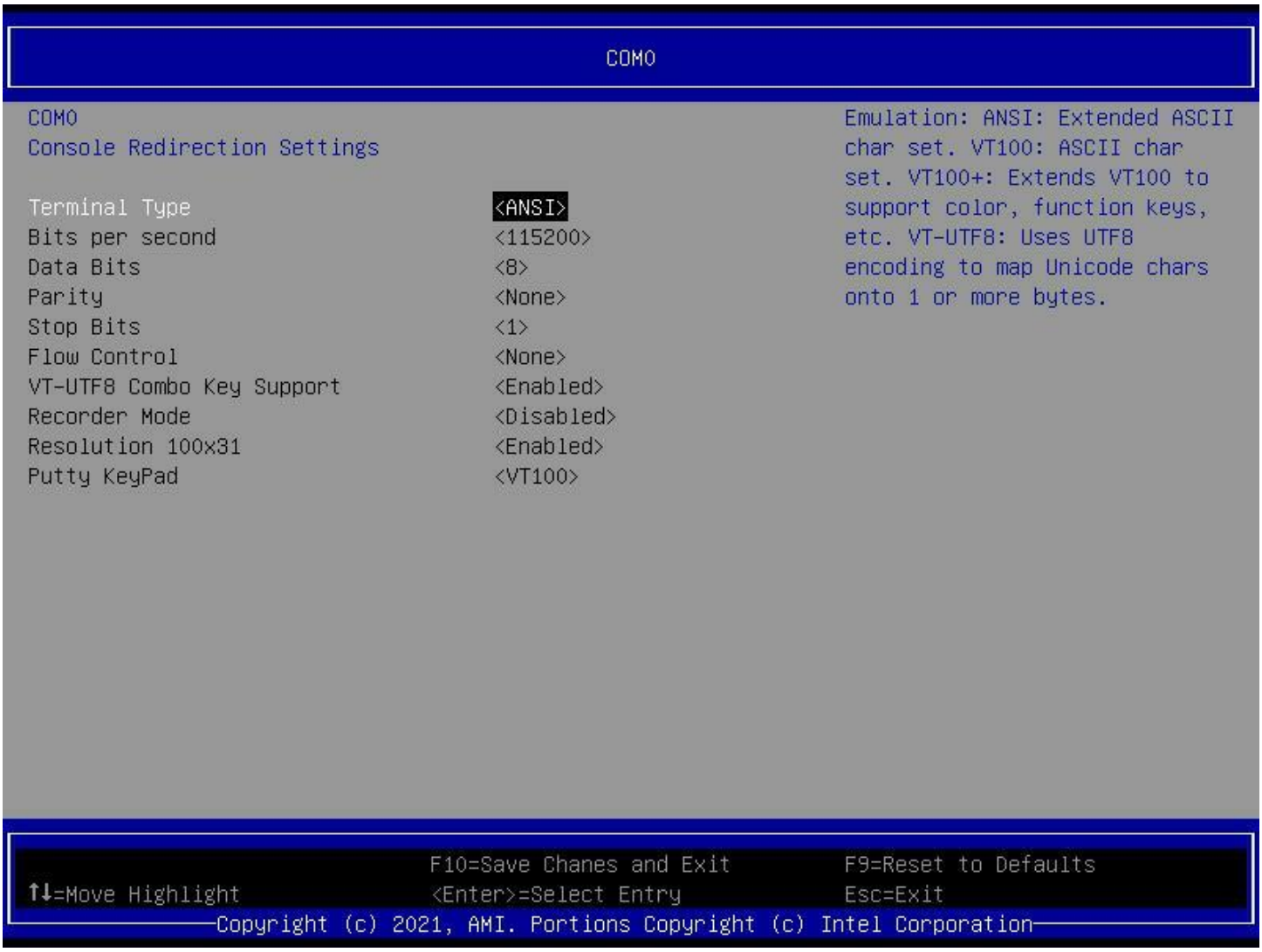

Figure 11. COM0 Screen

1. Thermal Type

Value: **ANSI** / VT100 / VT100+ / VT-UTF8

Help text:

```
Emulation:
    ANSI: Extended ASCII char set.
    VT100: ASCII char set.
    VT100+: Extends VT100 to support color, function keys, etc.
    VT-UTF8: Uses UTF8 encoding to map Unicode chars onto 1 or more
             bytes.
```

Comments: None.

Back to: Console Redirection Settings (COM0) – Serial Port Console Redirection – Advanced – Screen Map

2. Bit per second

Value: 9600 / 19200 / 57600 / 38400 / **115200**

Help text: `Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.`

Comments: None.

Back to: **Console Redirection Settings (COM0)** – **Serial Port Console Redirection** – **Advanced** – **Screen Map**

3. Data Bits

Value: 7 / **8**

Help text: `Data Bits.`

Comments: None.

Back to: **Console Redirection Settings (COM0)** – **Serial Port Console Redirection** – **Advanced** – **Screen Map**

4. Parity

Value: **None** / Even / Odd / Mark / Space

Help text: `A parity bit can be sent with the data bits to detect some transmission errors.`

```
Even: parity bit is 0 if the num of 1's in the data bits is even.
Odd: parity bit is 0 if num of 1's in the data bits is odd.
Mark: parity bit is always 1. Space: Parity bit is always 0.
```

`Mark and Space Parity do not allow for error detection. They can be used as an additional data bit.`

Comments: None.

Back to: **Console Redirection Settings (COM0)** – **Serial Port Console Redirection** – **Advanced** – **Screen Map**

5. Stop Bits

Value: **1** / 2

Help text: `Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stop bit.`

Comments: None.

Back to: **Console Redirection Settings (COM0)** – **Serial Port Console Redirection** – **Advanced** – **Screen Map**

6. Flow Control

Value: <**None**> / <Hardware RTS/CTS>

Help text: `Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals.`

Comments: None.

Back to: **Console Redirection Settings (COM0)** – **Serial Port Console Redirection** – **Advanced** – **Screen Map**

7. VT-UTF8 Combo Key Support

Value: **Enabled** / Disabled

Help text: `Enable VT-UTF8 Combination Key Support for ANSI/VT100 terminals.`

Comments: None.

Back to: **Console Redirection Settings (COM0)** – **Serial Port Console Redirection** – **Advanced** – **Screen Map**

8. Recorder Mode

Value: Enabled / **Disabled**

Help text: `With this mode enabled only text will be sent. This is to capture Terminal data.`

Comments: None.

Back to: **Console Redirection Settings (COM0)** – **Serial Port Console Redirection** – **Advanced** – **Screen Map**

9. Resolution 100X31

Value: **Enabled** / Disabled

Help text: `Enables or disables extended terminal resolution.`

Comments: None.

Back to: **Console Redirection Settings (COM0)** – **Serial Port Console Redirection** – **Advanced** – **Screen Map**

10. Putty KeyPad

Value: **VT100** / Linux / XTERMR6 / SCO / ESCN / VT400

Help text: `Select FunctionKey and KeyPad on Putty.`

Comments: None.

Back to: **Console Redirection Settings (COM0)** – **Serial Port Console Redirection** – **Advanced** – **Screen Map**

5.3.2 Console Redirection Settings (COM1)

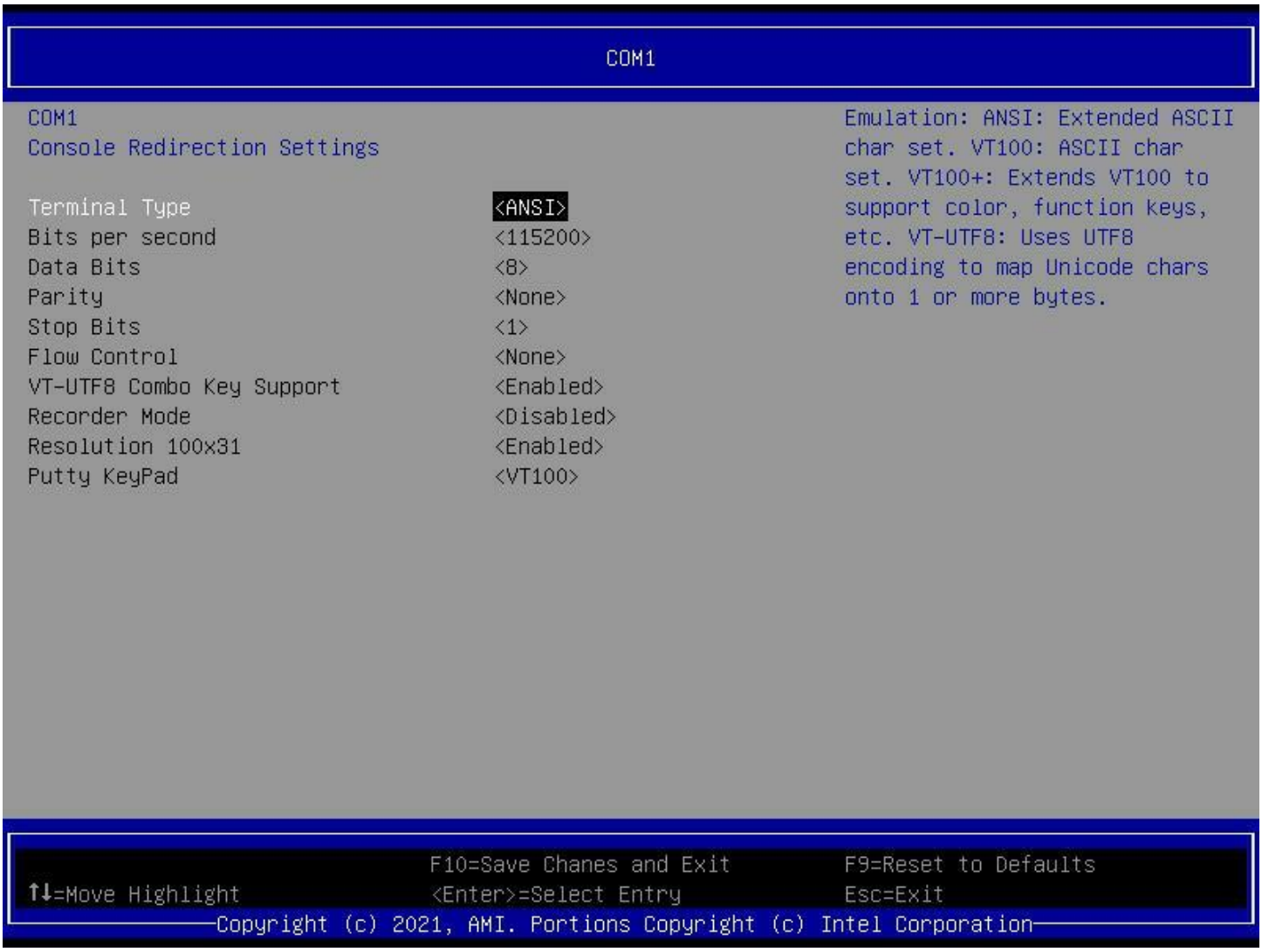

Figure 12. COM1 Screen

1. Thermal Type

Value: **ANSI** / VT100 / VT100+ / VT-UTF8

Help text:

```
Emulation:
    ANSI: Extended ASCII char set.
    VT100: ASCII char set.
    VT100+: Extends VT100 to support color, function keys, etc.
    VT-UTF8: Uses UTF8 encoding to map Unicode chars onto 1 or more
             bytes.
```

Comments: None.

Back to: Console Redirection Settings (COM1) – Serial Port Console Redirection – Advanced – Screen Map

2. Bit per second

Value: 9600 / 19200 / 57600 / 38400 / **115200**

Help text: `Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.`

Comments: None.

Back to: **Console Redirection Settings (COM1)** – **Serial Port Console Redirection** – **Advanced** – **Screen Map**

3. Data Bits

Value: 7 / **8**

Help text: `Data Bits.`

Comments: None.

Back to: **Console Redirection Settings (COM1)** – **Serial Port Console Redirection** – **Advanced** – **Screen Map**

4. Parity

Value: **None** / Even / Odd / Mark / Space

Help text: `A parity bit can be sent with the data bits to detect some transmission errors.`

```
Even: parity bit is 0 if the num of 1's in the data bits is even.
Odd: parity bit is 0 if num of 1's in the data bits is odd.
Mark: parity bit is always 1. Space: Parity bit is always 0.
```

`Mark and Space Parity do not allow for error detection. They can be used as an additional data bit.`

Comments: None.

Back to: **Console Redirection Settings (COM1)** – **Serial Port Console Redirection** – **Advanced** – **Screen Map**

5. Stop Bits

Value: **1** / 2

Help text: `Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stop bit.`

Comments: None.

Back to: **Console Redirection Settings (COM1)** – **Serial Port Console Redirection** – **Advanced** – **Screen Map**

6. Flow Control

Value: <**None**> / <Hardware RTS / CTS>

Help text: `Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals.`

Comments: None.

Back to: **Console Redirection Settings (COM1)** – **Serial Port Console Redirection** – **Advanced** – **Screen Map**

7. VT-UTF8 Combo Key Support

Value: **Enabled** / Disabled

Help text: `Enable VT-UTF8 Combination Key Support for ANSI/VT100 terminals.`

Comments: None.

Back to: **Console Redirection Settings (COM1)** – **Serial Port Console Redirection** – **Advanced** – **Screen Map**

8. Recorder Mode

Value: **Enabled** / Disabled

Help text: `Enables or disables extended terminal resolution.`

Comments: None.

Back to: **Console Redirection Settings (COM1)** – **Serial Port Console Redirection** – **Advanced** – **Screen Map**

9. Resolution 100X31

Value: **Enabled** / Disabled

Help text: `Enables or disables extended terminal resolution.`

Comments: None.

Back to: **Console Redirection Settings (COM1)** – **Serial Port Console Redirection** – **Advanced** – **Screen Map**

10. Putty KeyPad

Value: **VT100** / Linux / XTERMR6 / SCO / ESCN / VT400

Help text: `Select FunctionKey and KeyPad on Putty.`

Comments: None.

Back to: **Console Redirection Settings (COM1)** – **Serial Port Console Redirection** – **Advanced** – **Screen Map**

5.4 PCI Configuration

Figure 13. PCI Configuration Screen

1. PCI Bus Driver Version

Value: <PCI Bus Driver Version>

Help text: None.

Comments: *Information only.*

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

2. Network Stack Configuration

Value: None

Help text: `Network Stack Settings.`

Comments: *Selection only.*

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

3. Above 4G Decoding

Value: **Enabled** / Disabled

Help text: `Enables or Disables 64bit capable Devices to be Decoded in Above 4G Address Space (Only if System Supports 64-bit PCI Decoding).`

Comments: None.

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

4. SR-IOV Support

Value: **Enabled** / Disabled

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

Comments: None.

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

5. BME DMA Mitigation

Value: Enabled / **Disabled**

Help text: `Re-enable Bus Master Attribute disabled during PCI enumeration for PCI Bridges after SMM Locked.`

Comments: None.

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

5.4.1 Network Stack Configuration

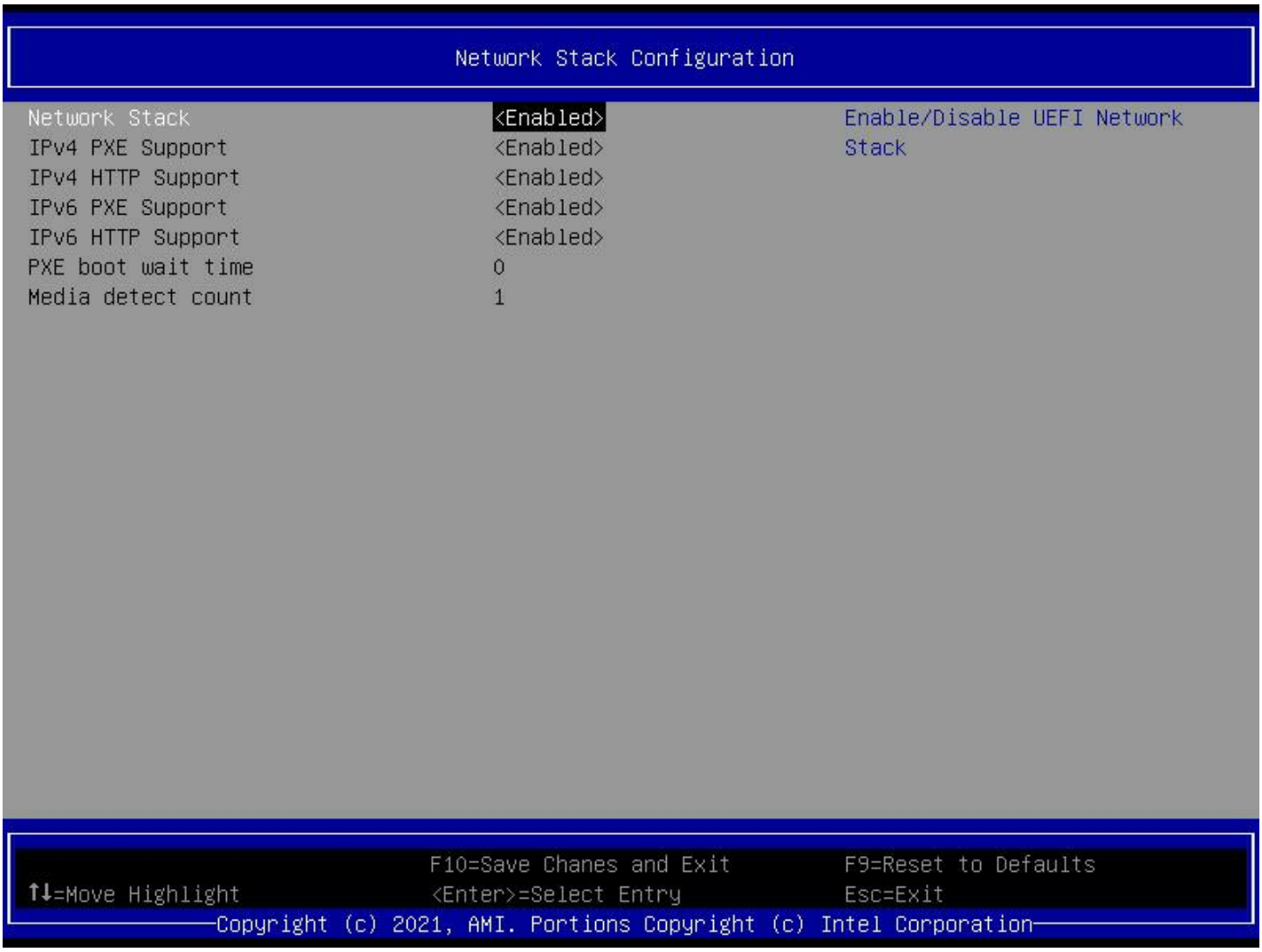

Figure 14. Network Stack Configuration Screen

1. Network Stack

Value: **Enabled** / Disabled

Help text: `Enable/Disable UEFI Network Stack.`

Comments: None.

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

2. IPv4 PXE Support

Value: **Enabled** / Disabled

Help text: `Enable/Disable IPv4 PXE boot support. If disabled, IPv4 PXE boot support will not be available.`

Comments: None.

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

3. IPv4 HTTP Support

Value: **Enabled** / Disabled

Help text: `Enable/Disable IPv4 HTTP boot support. If disabled, IPv4 HTTP boot support will not be available.`

Comments: None.

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

4. IPv6 PXE Support

Value: **Enabled** / Disabled

Help text: `Enable/Disable IPv6 PXE boot support. If disabled, IPv6 PXE boot support will not be available.`

Comments: None.

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

5. IPv6 HTTP Support

Value: **Enabled** / Disabled

Help text: `Enable/Disable IPv6 HTTP boot support. If disabled, IPv6 HTTP boot support will not be available.`

Comments: None.

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

6. PXE boot wait time

Value: 0

Help text: `Wait time in seconds to press ESC key to abort the PXE boot. Use either +/- or numeric keys to set the value.`

Comments: None.

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

7. Media detect count

Value: 1

Help text: `Number of times the presence of media will be checked. Use either +/- or numeric keys to set the value.`

Comments: None.

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

5.5 USB Configuration

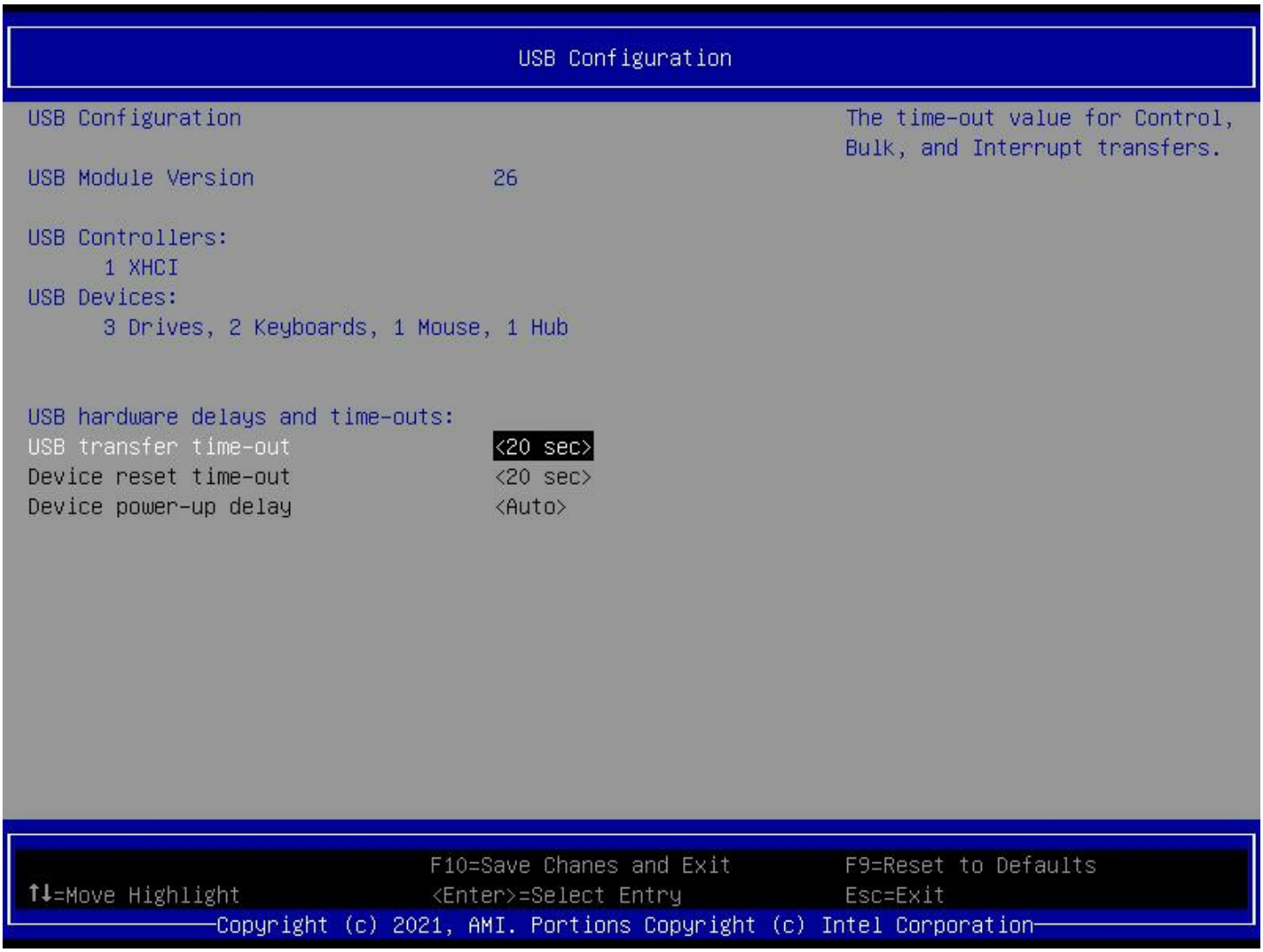

Figure 15. USB Configuration Screen

1. USB Module Version

Value: <USB Module Version>

Help text: None.

Comments: *Information only.*

Back to: **USB Configuration** – **Advanced** – **Screen Map**

2. USB Controllers

Value: <USB Controllers>

Help text: None.

Comments: *Information only.*

Back to: **USB Configuration** – **Advanced** – **Screen Map**

3. USB Devices

Value: <USB Devices>

Help text: None.

Comments: *Information only.*

Back to: **USB Configuration – Advanced – Screen Map**

4. USB transfer time-out

Value: 1 / 5 / 10 / **20** sec

Help text: `The time-out value for Control, Bulk, and Interrupt transfers.`

Comments: None.

Back to: **USB Configuration – Advanced – Screen Map**

5. Device reset time-out

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

Help text: `USB mass storage device Start Unit command time-out.`

Comments: None.

Back to: **USB Configuration – Advanced – Screen Map**

6. Device power-up delay

Value: Auto / <custom>

Help text: `Maximum time the device will take before it properly reports itself to the Host Controller.`

`'Auto' uses default value: for a Root port it is 100 ms, for a Hub port the delay is taken from Hub descriptor.`

Comments: None.

Back to: **USB Configuration – Advanced – Screen Map**

5.6 NVMe Configuration

Figure 16. NVMe* Controller and Drive Information Screen

1. PCIe SSD

Value: <Name of SSD>

Help text: None.

Comments: *Selection only.* This page lists all Non-Volatile Memory Express* (NVMe*) solid state drives (SSDs) connected.

Back to: **NVMe Configuration** – **Advanced** – **Screen Map**

5.7 Tls Auth Configuration

Figure 17. Tls Auth Configuration Screen

1. **Server CA Configuration**

Value: None.

Help text: `Press <Enter> to configure Server CA.`

Comments: *Selection only.*

Back to: **Tls Auth Configuration** – **Advanced** – **Screen Map**

5.7.1 Server CA Configuration

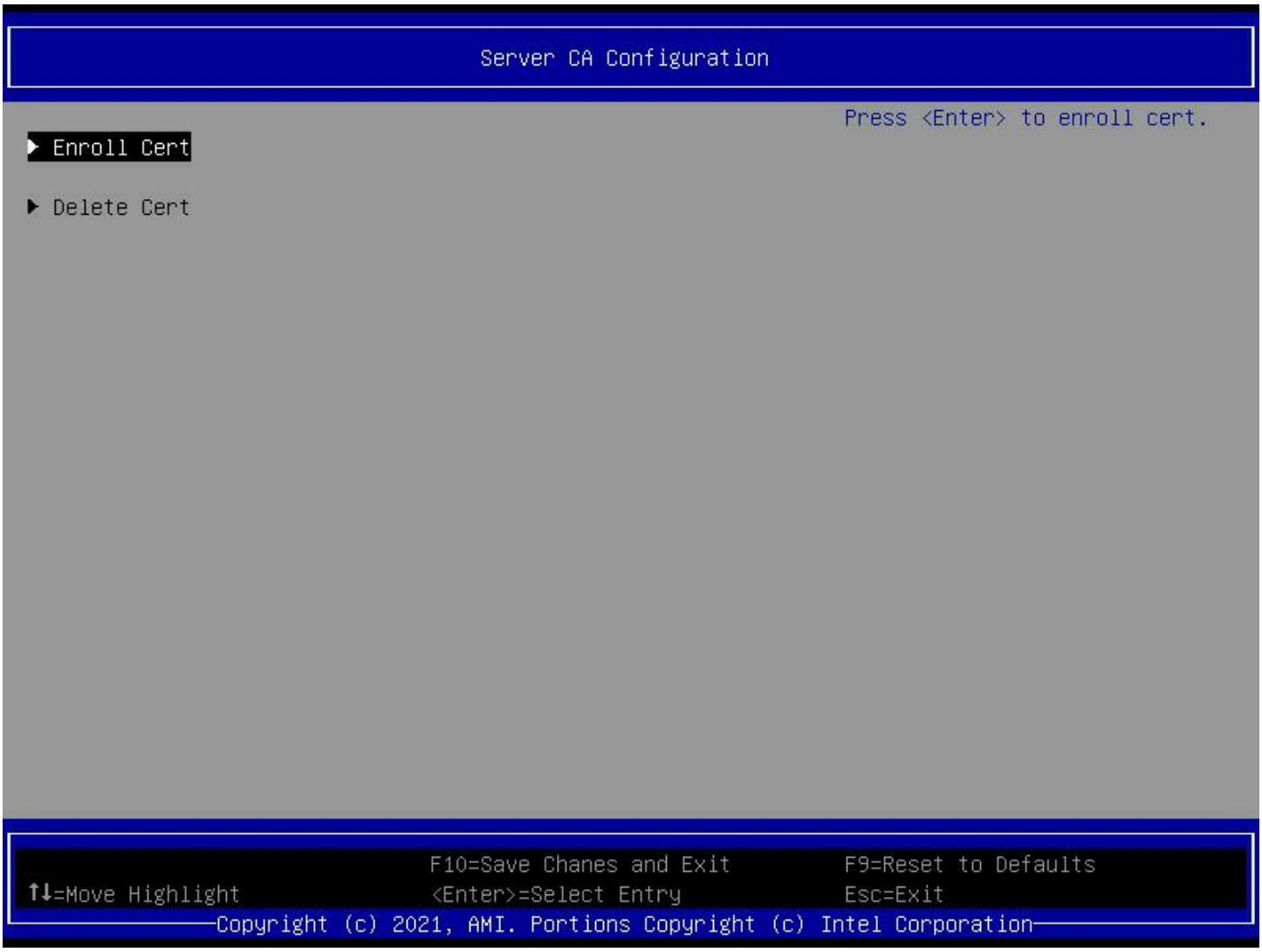

Figure 18. Server CA Configuration Screen

1. **Enroll Cert**

Value: None.

Help text: `Press <Enter> to enroll cert.`

Comments: *Selection only.*

Back to: **Server CA Configuration** – **Tls Auth Configuration** – **Advanced** – **Screen Map**

2. **Delete Cert**

Value: None.

Help text: `Press <Enter> to delete cert.`

Comments: *Selection only.*

Back to: **Server CA Configuration** – **Tls Auth Configuration** – **Advanced** – **Screen Map**

5.7.1.1 Enroll Cert

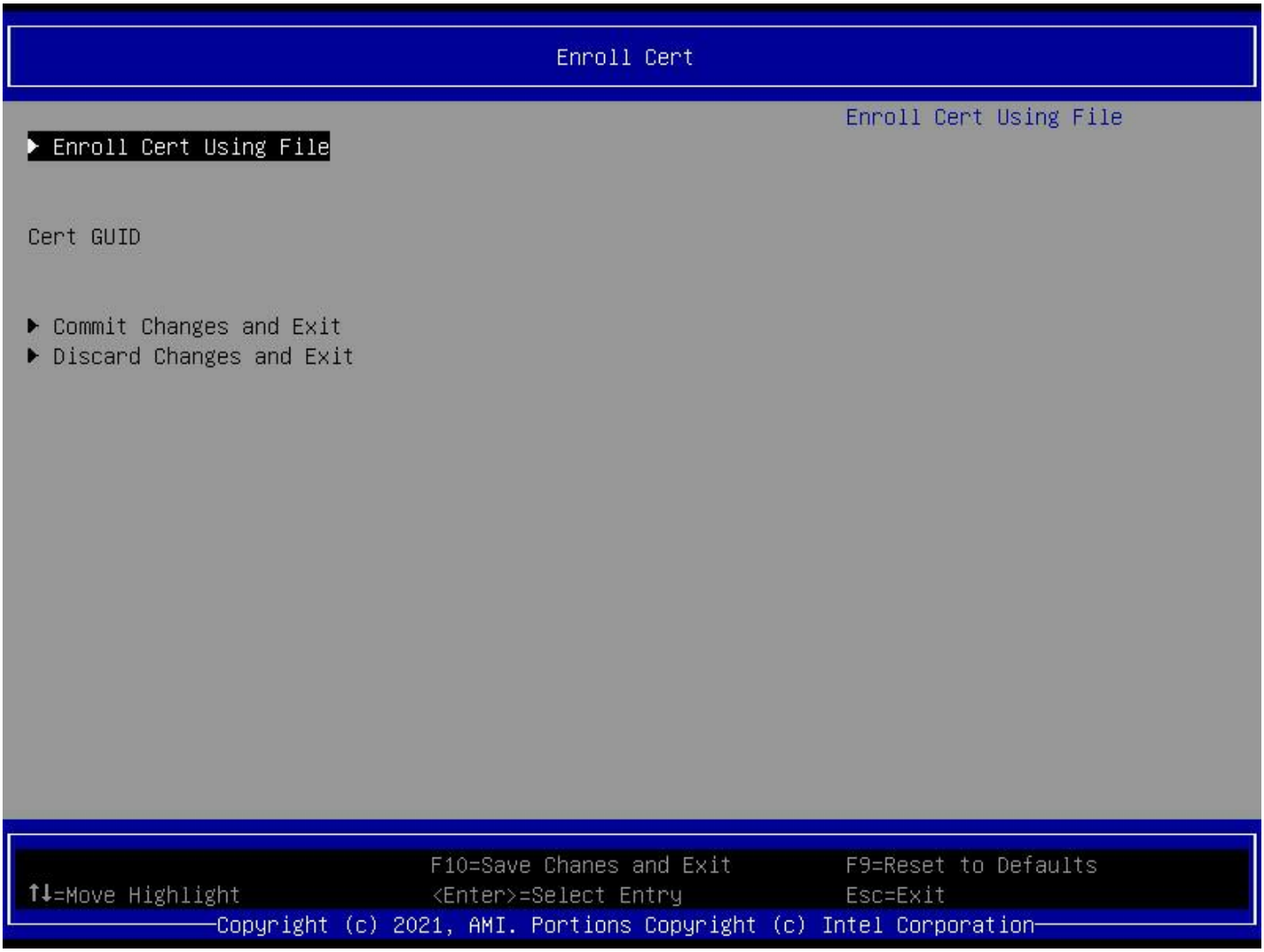

Figure 19. Enroll Cert Screen

1. **Enroll Cert Using File**

Value: None.

Help text: `Enroll Cert Using File.`

Comments: *Selection only.*

Back to: **Enroll Cert** – **Server CA Configuration** – **Tls Auth Configuration** – **Advanced** – **Screen Map**

2. **Commit Changes and Exit**

Value: None.

Help text: `Commit Changes and Exit.`

Comments: *Selection only.*

Back to: **Enroll Cert** – **Server CA Configuration** – **Tls Auth Configuration** – **Advanced** – **Screen Map**

3. Discard Changes and Exit

Value: None.

Help text: `Discard Changes and Exit.`

Comments: *Selection only.*

Back to: **Enroll Cert – Server CA Configuration – Tls Auth Configuration – Advanced – Screen Map**

5.7.1.2 Delete Cert

Figure 20. Delete Cert Screen

1. **Cert GUID**

Value: Enabled / **Disabled**

Help text: `GUID for CERT.`

Comments: Set the globally unique identifier (GUID) as enabled to delete it.

Back to: **Delete Cert** – **Server CA Configuration** – **Tls Auth Configuration** – **Advanced** – **Screen Map**

5.8 All Cpu Information

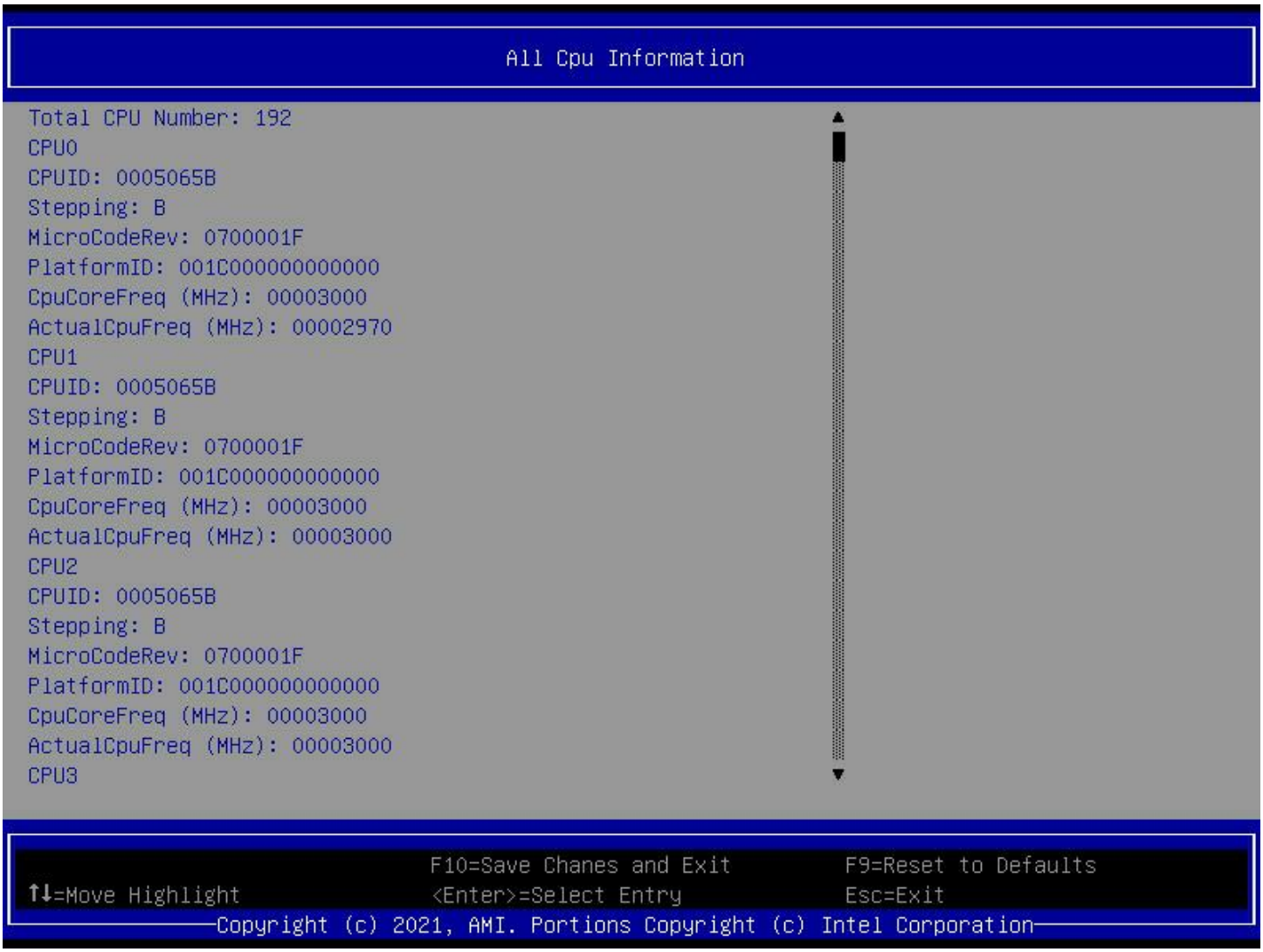

Figure 21. All CPU Information Screen

1. Total CPU Number

Value: <Total CPU Number>

Help text: None.

Comments: *Information only.* Indicates Total CPU cores number.

Back to: **All Cpu Information** – **Advanced** – **Screen Map**

2. CPUID

Value: <CPUID>

Help text: None.

Comments: *Information only.*

Back to: **All Cpu Information** – **Advanced** – **Screen Map**

3. Stepping

Value: <CPU Stepping>

Help text: None.

Comments: *Information only.*

Back to: **All Cpu Information – Advanced – Screen Map**

4. MicroCodeRev

Value: <Micro Code Revision>

Help text: None.

Comments: *Information only.*

Back to: **All Cpu Information – Advanced – Screen Map**

5. PlatformID

Value: <Platform ID>

Help text: None.

Comments: *Information only.*

Back to: **All Cpu Information – Advanced – Screen Map**

6. CpuCoreFreq(MHz)

Value: <CPU Core Frequency in MHz>

Help text: None.

Comments: *Information only.*

Back to: **All Cpu Information – Advanced – Screen Map**

7. ActualCoreFreq(MHz)

Value: <Actual Core Frequency in MHz>

Help text: None.

Comments: *Information only.*

Back to: **All Cpu Information – Advanced – Screen Map**

5.9 RAM Disk Configuration

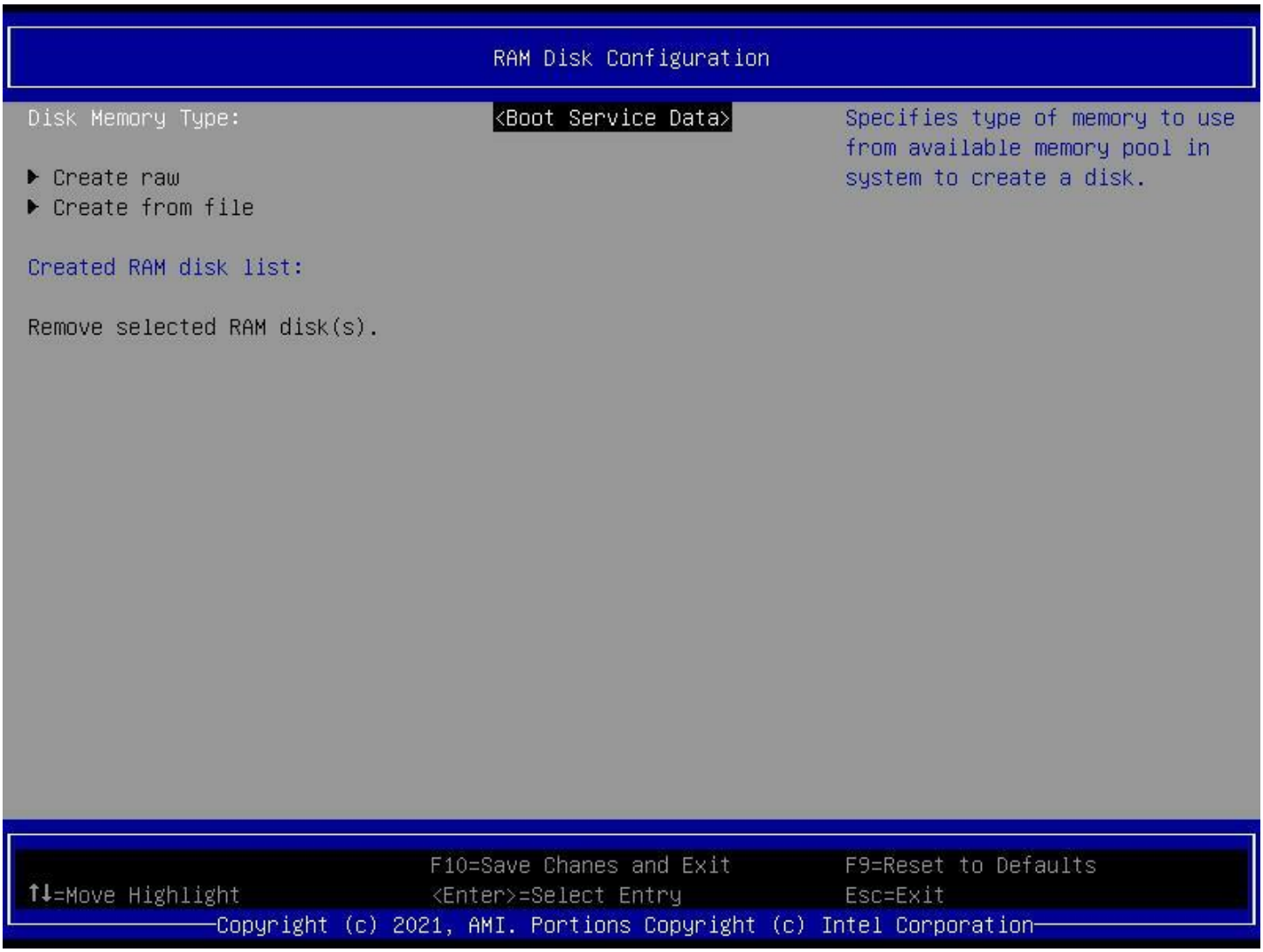

Figure 22. RAM Disk Configuration Screen

1. **Disk Memory Type:**

Value: <**Boot Service Data**> / <Reserved>

Help text: `Specifies type of memory to use from available memory pool in system to create a disk.`

Comments: None.

Back to: **RAM Disk Configuration – Advanced – Screen Map**

2. **Create raw**

Value: None.

Help text: `Create a raw RAM disk.`

Comments: *Selection only.*

Back to: **RAM Disk Configuration – Advanced – Screen Map**

3. Create from file

Value: None.

Help text: `Create a RAM disk from a given file.`

Comments: *Selection only.*

Back to: **RAM Disk Configuration** – **Advanced** – **Screen Map**

4. Created RAM disk list

Value: None.

Help text: None.

Comments: This option offers a list of all the RAM disks created. Select for removal.

Back to: **RAM Disk Configuration** – **Advanced** – **Screen Map**

5.9.1 Create raw

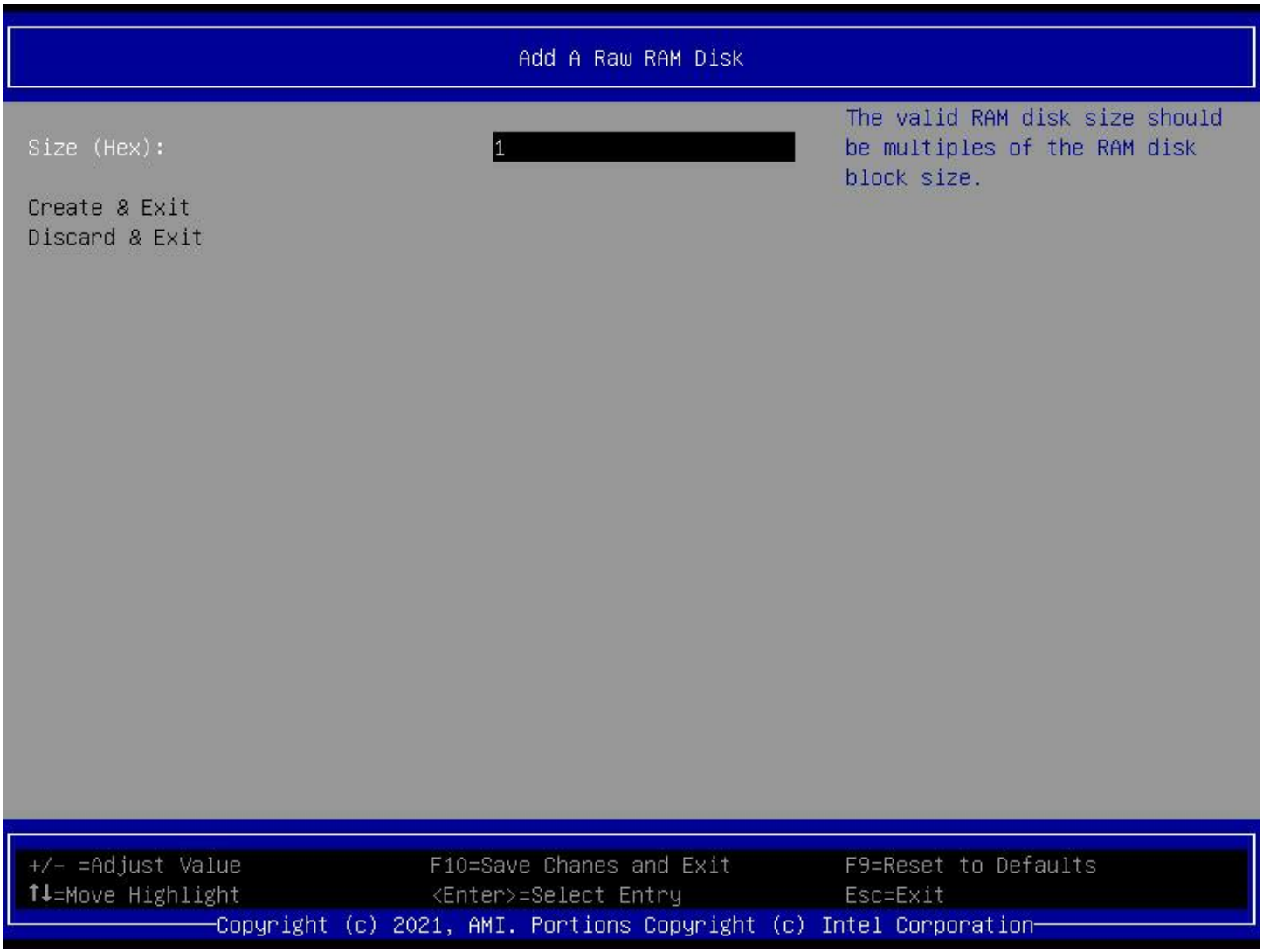

Figure 23. Add a Raw RAM Screen

1. **Size (Hex):**

Value: <Size in hex>

Help text: `The valid RAM disk size should be multiples of the RAM disk block size.`

Comments: None.

Back to: **Create raw** – **RAM Disk Configuration** – **Advanced** – **Screen Map**

5.10 iSCSI Configuration

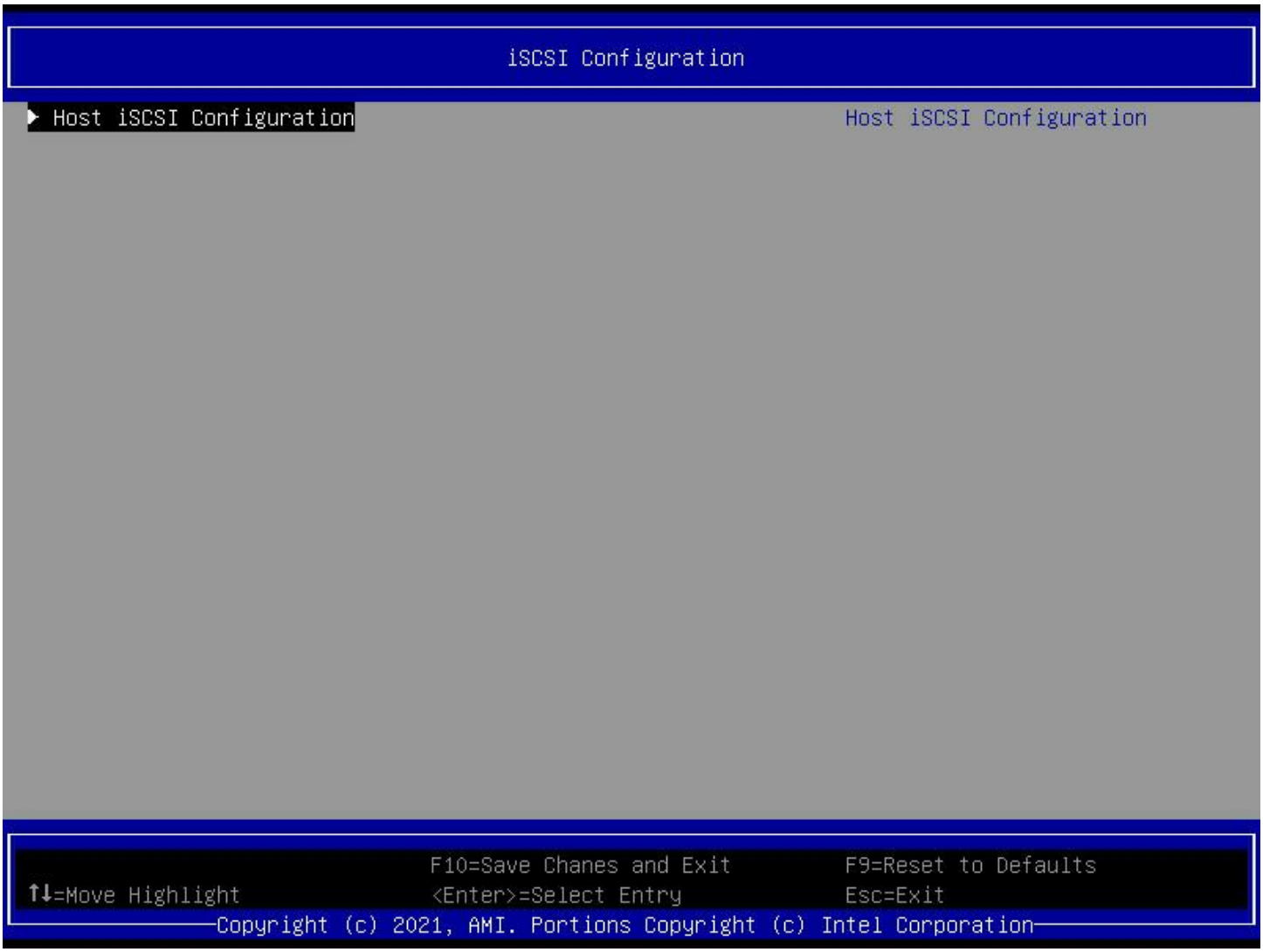

Figure 24. iSCSI Configuration Screen

1. Host iSCSI Configuration

Value: None.

Help text: `Host iSCSI Configuration.`

Comments: *Selection only.*

Back to: **iSCSI Configuration – Advanced – Screen Map**

5.10.1 Host iSCSI Configuration

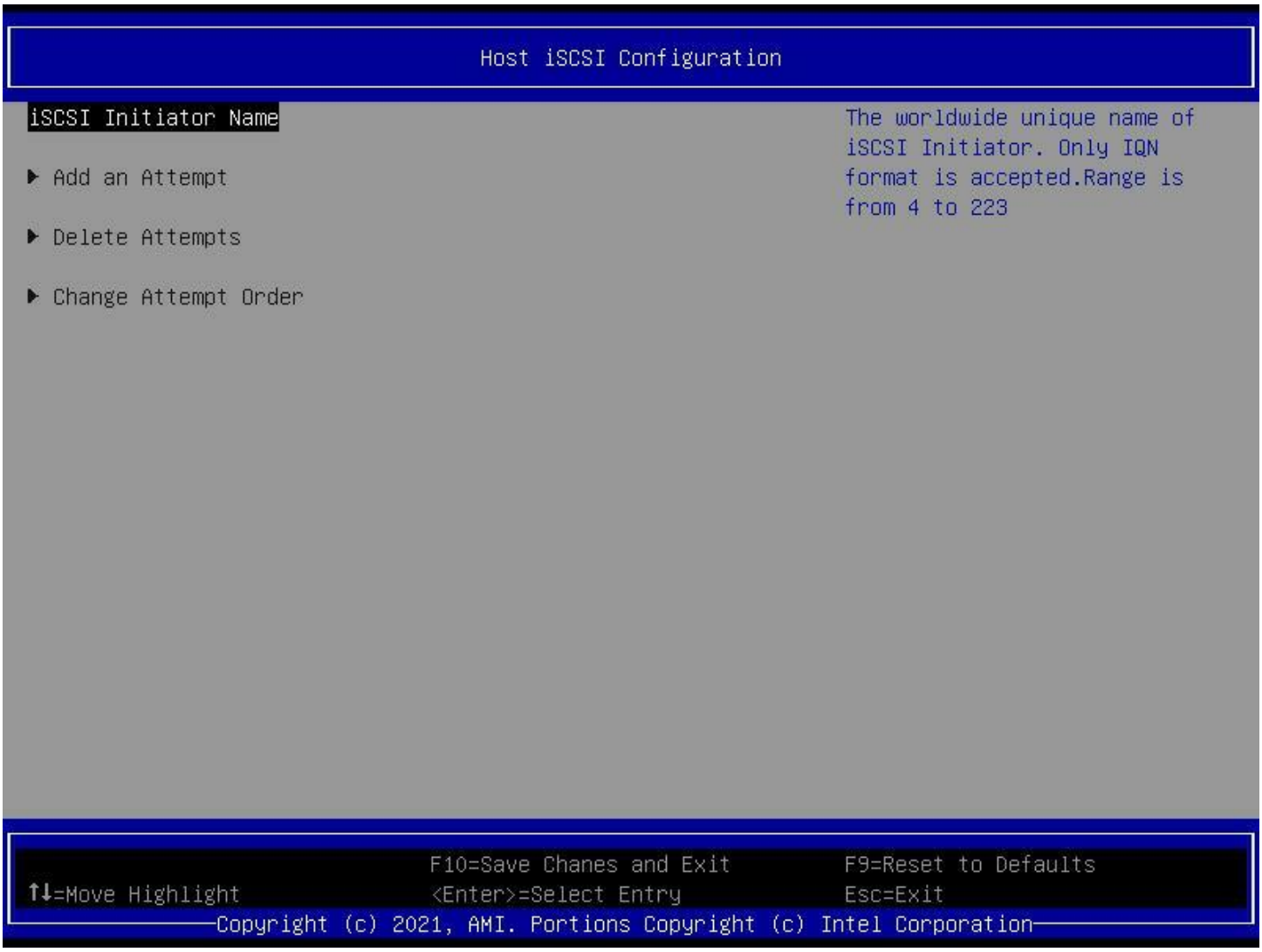

Figure 25. Host iSCSI Configuration Screen

1. Add an Attempt

Value: None.

Help text: `Add an Attempt.`

Comments: *Selection only.*

Back to: **Host iSCSI Configuration** – **iSCSI Configuration** – **Advanced** – **Screen Map**

2. Delete an Attempt

Value: None.

Help text: `Delete one or more attempts.`

Comments: *Selection only.*

Back to: **Host iSCSI Configuration** – **iSCSI Configuration** – **Advanced** – **Screen Map**

3. Change Attempt Order

Value: None.

Help text: `Change Attempt Order.`

Comments: *Selection only.*

Back to: **Host iSCSI Configuration – iSCSI Configuration – Advanced – Screen Map**

5.11 VLAN Configuration

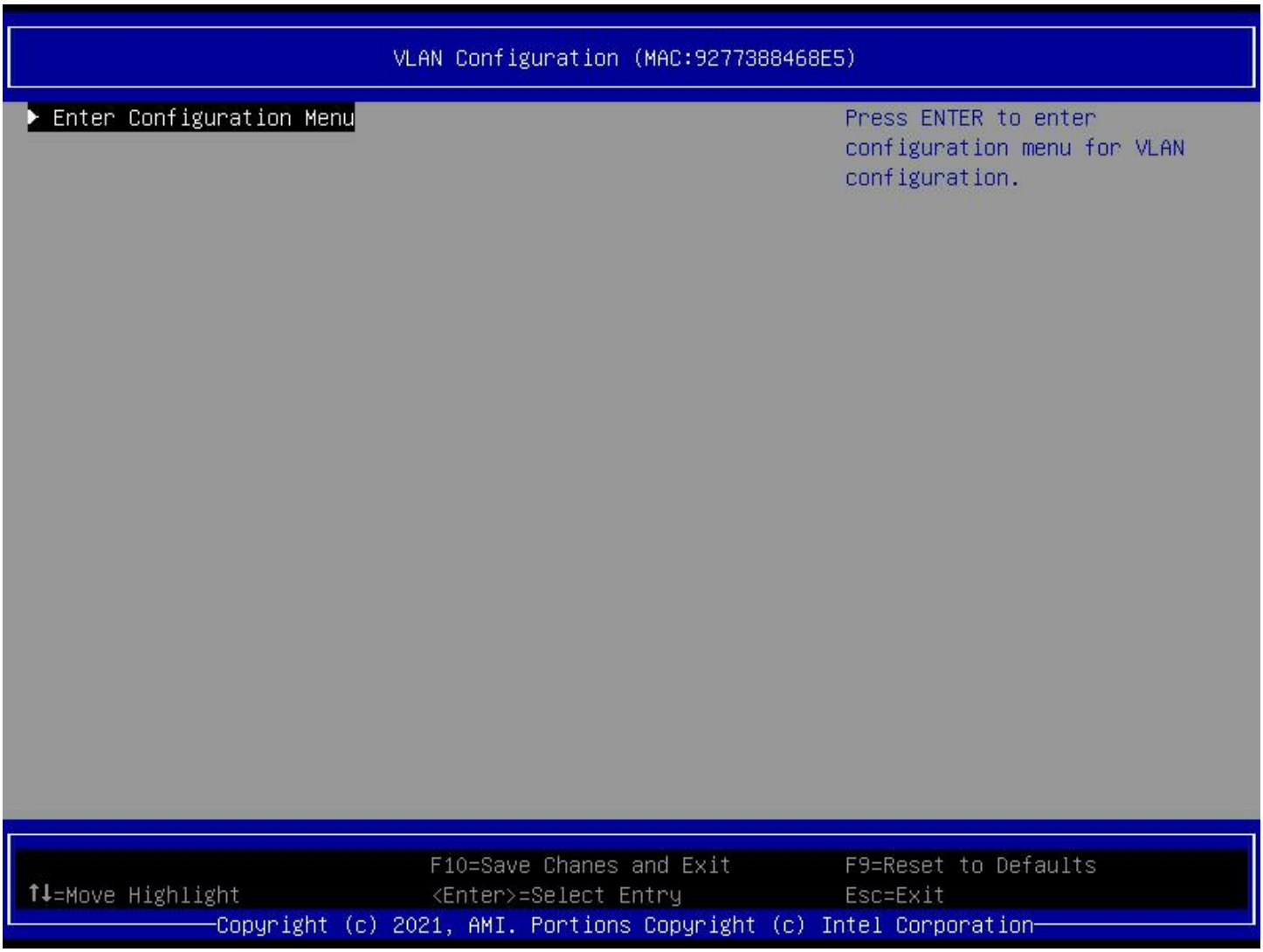

Figure 26. VLAN Configuration (MAC) Screen

1. Enter Configuration Menu

Value: None.

Help text: `Press ENTER to enter configuration menu for VLAN configuration.`

Comments: *Selection only.*

Back to: **VLAN Configuration** – **Advanced** – **Screen Map**

5.11.1 Enter Configuration Menu

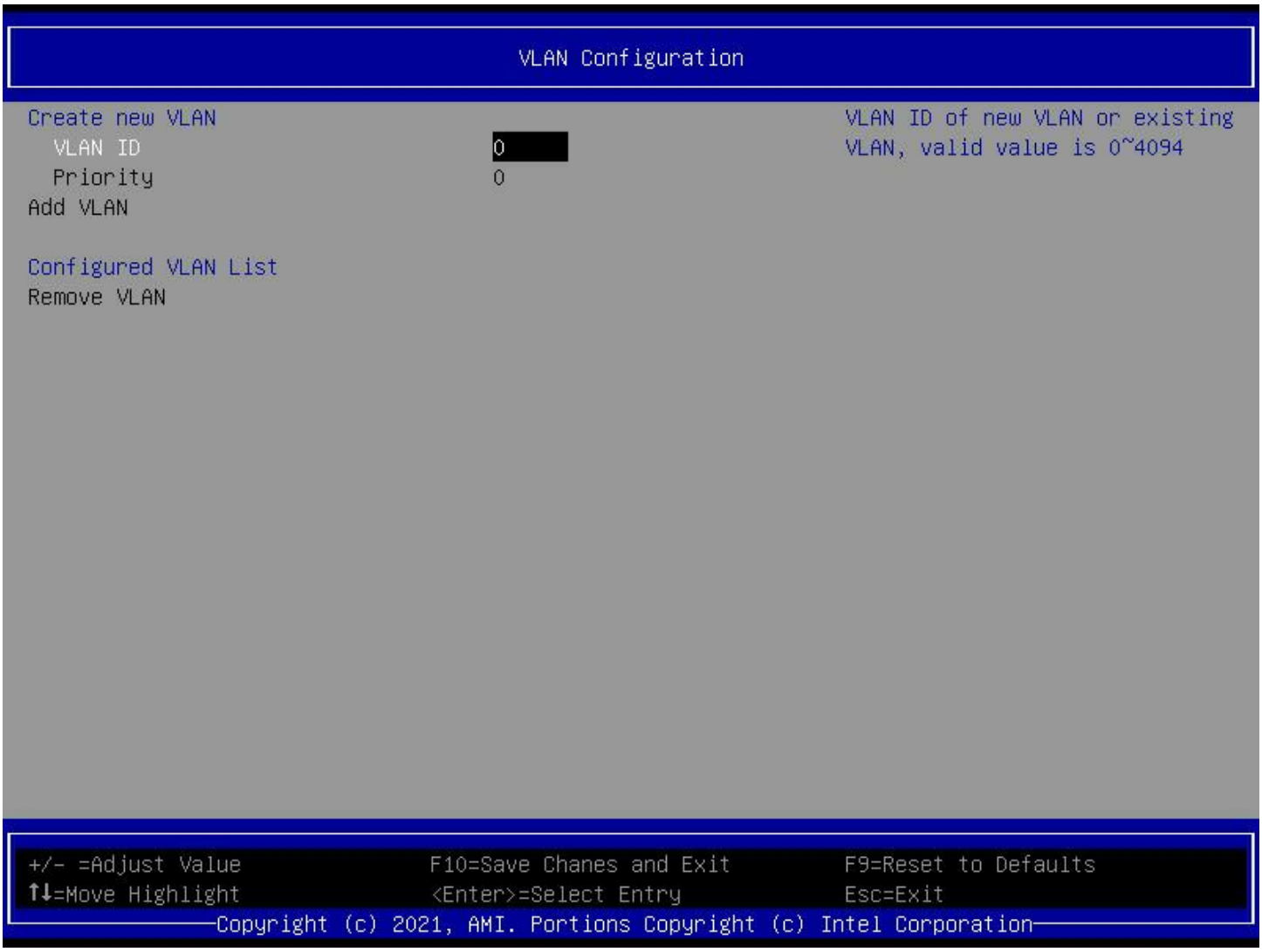

Figure 27. VLAN Configuration Screen

1. VLAN ID

Value: 0

Help text: `VLAN ID of new VLAN or existing VLAN, valid value is 0~4094.`

Comments: None.

Back to: **Enter Configuration Menu – VLAN Configuration – Advanced – Screen Map**

2. Priority

Value: 0

Help text: `802.1Q Priority, valid value is 0~7.`

Comments: None.

Back to: **Enter Configuration Menu – VLAN Configuration – Advanced – Screen Map**

3. Add VLAN

Value: None.

Help text: `Create a new VLAN or update existing VLAN.`

Comments: *Selection only.*

Back to: **Enter Configuration Menu – VLAN Configuration – Advanced – Screen Map**

4. Remove VLAN

Value: None.

Help text: `Remove selected VLANs.`

Comments: *Selection only.*

Back to: **Enter Configuration Menu – VLAN Configuration – Advanced – Screen Map**

5.12 IPv4 Network Configuration

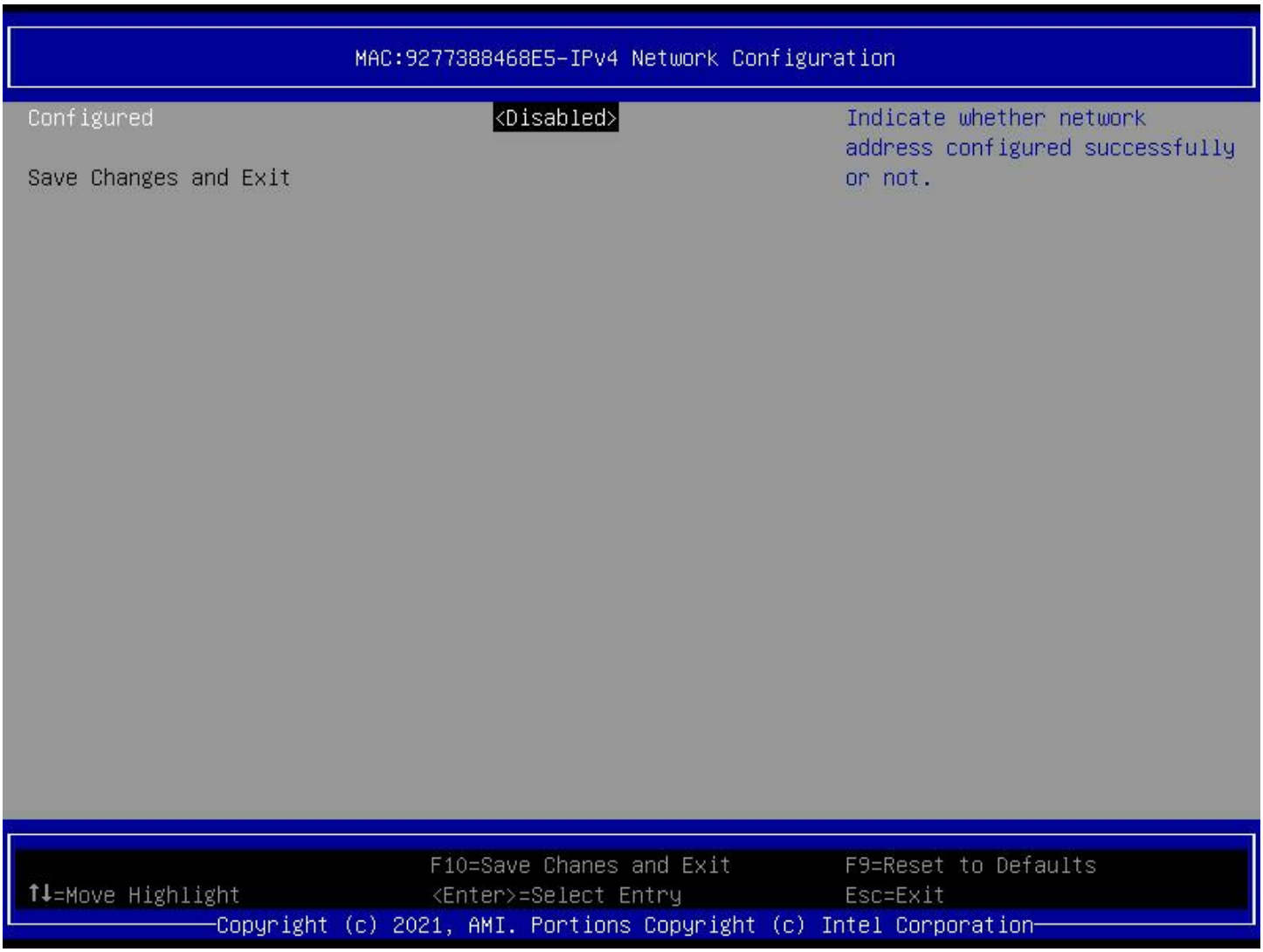

Figure 28. MAC: IPv4 Network Configuration Screen

1. **Configured**

Value: Enabled / **Disabled**

Help text: `Indicate whether network address configured successfully or not.`

Comments: None.

Back to: **IPv4 Network Configuration – Advanced – Screen Map**

5.13 HTTP Boot Configuration

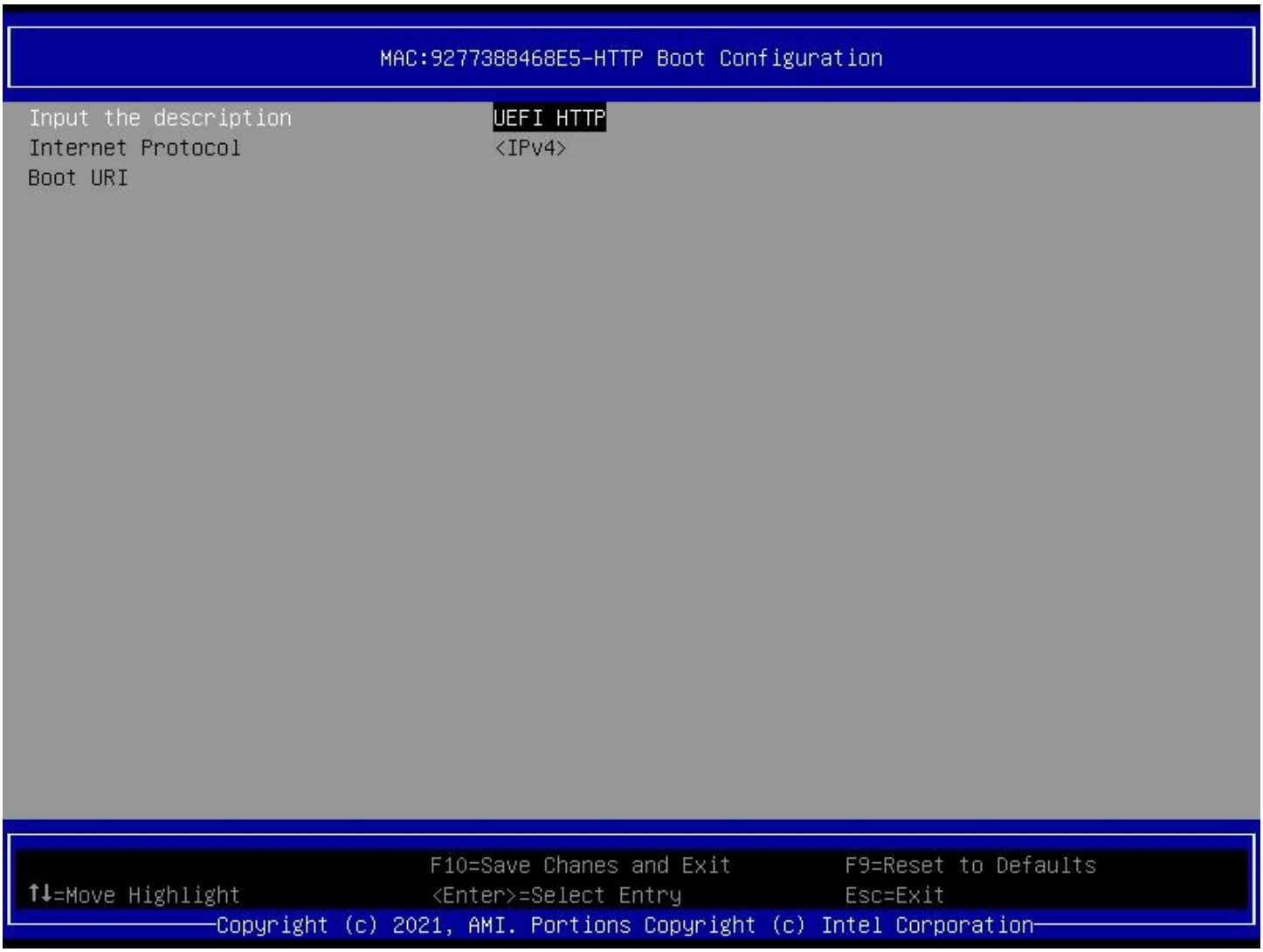

Figure 29. MAC: HTTP Boot Configuration Screen

1. Input the description

Value: UEFI HTTP

Help text: None.

Comments: None.

Back to: HTTP Boot Configuration – Advanced – Screen Map

2. Internet Protocol

Value: **IPv4** / IPv6

Help text: `Select the version of Internet Protocol.`

Comments: None.

Back to: HTTP Boot Configuration – Advanced – Screen Map

3. Boot URI

Value: None.

Help text: `A new Boot Option will be created according to this Boot URI.`

Comments: None.

Back to: **HTTP Boot Configuration – Advanced – Screen Map**

5.14 IPv6 Network Configuration

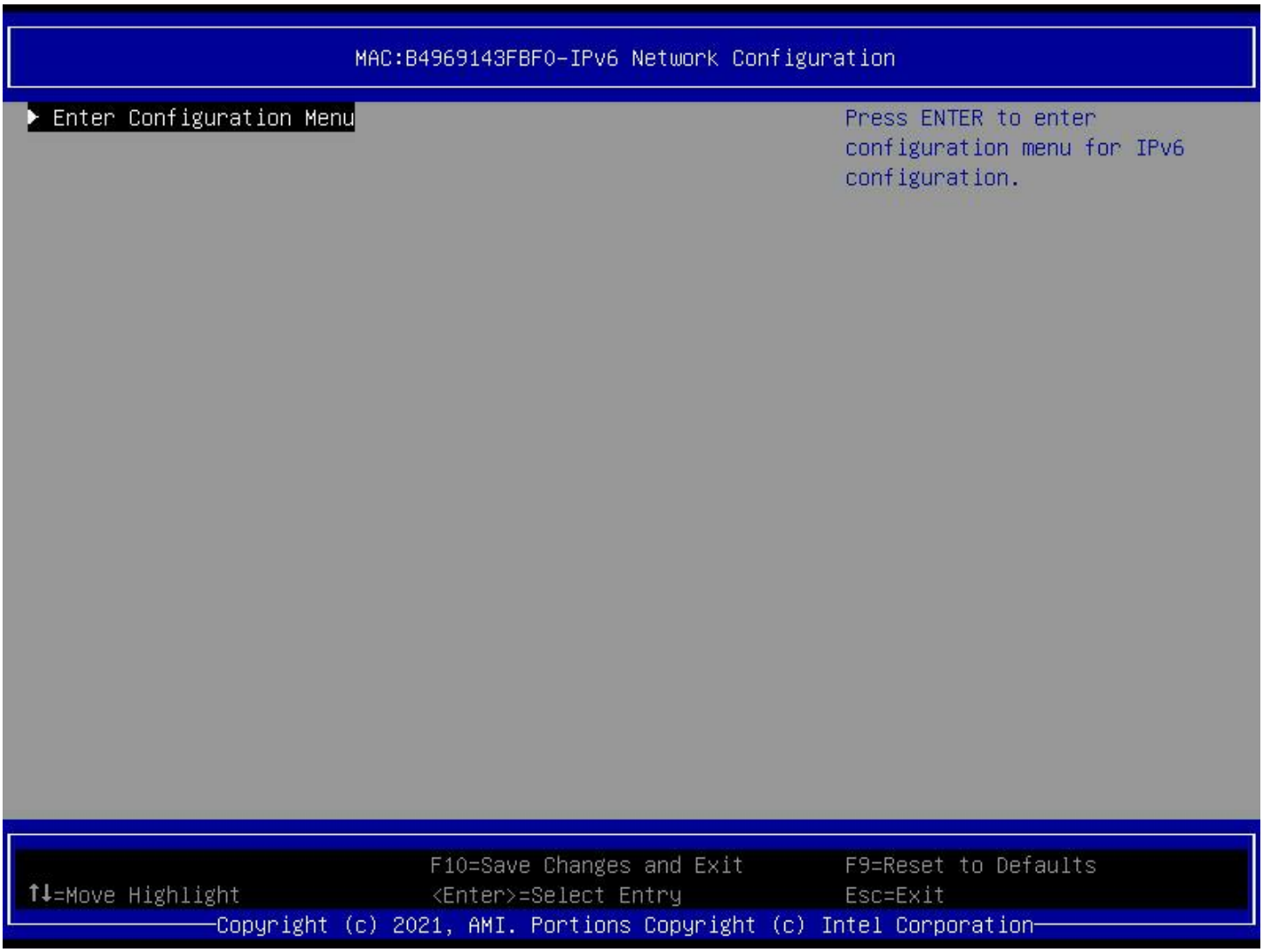

Figure 30. MAC: IPv6 Network Configuration Screen

1. Enter Configuration Menu

Value: None.

Help text: `Press ENTER to enter configuration menu for IPv6 configuration.`

Comments: *Selection only.*

Back to: **IPv6 Network Configuration – Advanced – Screen Map**

5.14.1 Enter Configuration Menu

Figure 31. IPv6 Current Setting Screen

1. **Interface Name**

Value: <Interface Name>

Help text: None.

Comments: *Information only.*

Back to: **Enter Configuration Menu** – **IPv6 Network Configuration** – **Advanced** – **Screen Map**

2. **Interface Type**

Value: <Interface type>

Help text: None.

Comments: *Information only.*

Back to: **Enter Configuration Menu** – **IPv6 Network Configuration** – **Advanced** – **Screen Map**

3. MAC address

Value: <MAC address>

Help text: None.

Comments: *Information only.*

Back to: **Enter Configuration Menu – IPv6 Network Configuration – Advanced – Screen Map**

4. Host address

Value: <Host address>

Help text: None.

Comments: *Information only.*

Back to: **Enter Configuration Menu – IPv6 Network Configuration – Advanced – Screen Map**

5. Route Table

Value: <Route Table>

Help text: None.

Comments: *Information only.*

Back to: **Enter Configuration Menu – IPv6 Network Configuration – Advanced – Screen Map**

6. Gateway addresses

Value: <Gateway addresses>

Help text: None.

Comments: *Information only.*

Back to: **Enter Configuration Menu – IPv6 Network Configuration – Advanced – Screen Map**

7. DNS addresses

Value: <DNS addresses>

Help text: None.

Comments: *Information only.*

Back to: **Enter Configuration Menu – IPv6 Network Configuration – Advanced – Screen Map**

8. Interface ID

Value: <Interface ID>

Help text: `The 64 bit alternative interface ID for the device. The string is colon separated. e.g. ff:dd:88:66:cc:1:2:3.`

Comments: None.

Back to: **Enter Configuration Menu – IPv6 Network Configuration – Advanced – Screen Map**

9. DAD Transmit Count Policy

Value: 1

Help text: `The number of consecutive Neighbor Solicitation messages sent while performing Duplicate Address Detection on a tentative address. A value of zero indicates that Duplicate Address Detection is not performed.`

Comments: None.

Back to: **Enter Configuration Menu** – **IPv6 Network Configuration** – **Advanced** – **Screen Map**

5.15 Power & Performance

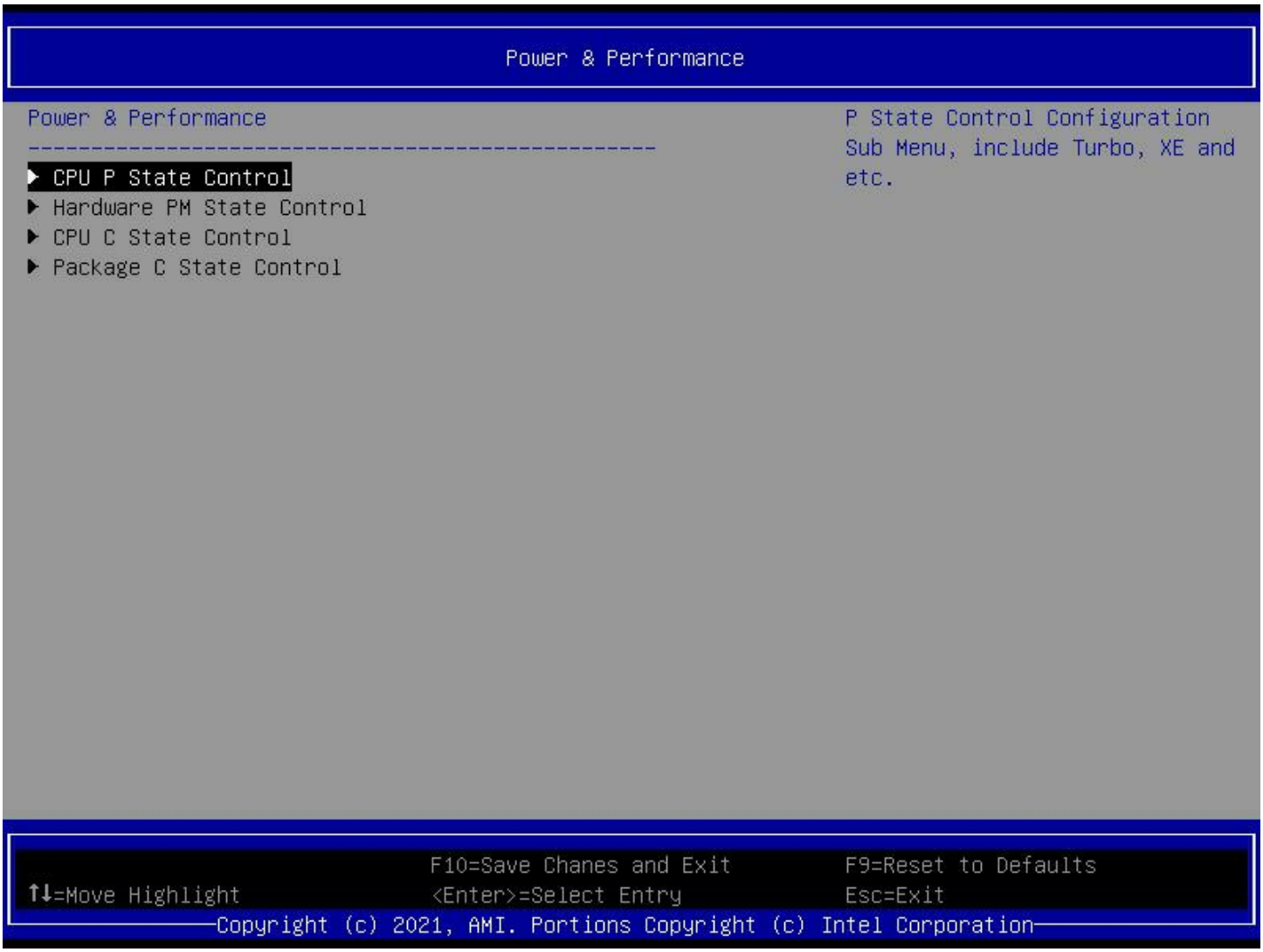

Figure 32. Power & Performance Screen

1. CPU P State Control

Value: None.

Help text: `P State Control Configuration Sub Menu, include Turbo, XE and etc.`

Comments: *Selection only.*

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

2. Hardware PM State Control

Value: None.

Help text: `Hardware P-State setting.`

Comments: *Selection only.*

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

3. CPU C State Control

Value: None.

Help text: `CPU C State setting.`

Comments: *Selection only.*

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

4. Package C State Control

Value: None.

Help text: `Package C State setting.`

Comments: *Selection only.*

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

5.15.1 CPU P State Control

Figure 33. CPU P State Control Screen

1. **SpeedStep (Pstates)**

Value: **Enable** / Disable

Help text: `Enable/Disable EIST (P-States).`

Comments: None.

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

2. **Config TDP Lock**

Value: **Enable** / Disable

Help text: `Config TDP CONTROL Lock Bit.`

Comments: None.

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

3. Boot performance mode

Value: <**Max Performance**> / <Max Efficient> / <Set by Intel Node Manager>

Help text: `Select the performance state that the BIOS will set before OS hand off.`

Comments: None.

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

4. Energy Efficient Turbo

Value: **Enable** / Disable

Help text: `Energy Efficient Turbo Disable, MSR 0x1FC [19].`

Comments: None.

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

5. Turbo Mode

Value: **Enable** / Disable

Help text: `Enable/Disable processor Turbo Mode (requires EMTTM enabled too).`

Comments: None.

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

6. Perf P-Limit

Value: None.

Help text: `Program PERF_P_LIMIT 1:30:2:0xe4 Sub Menu.`

Comments: *Selection only.*

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

5.15.1.1 Perf P-Limit

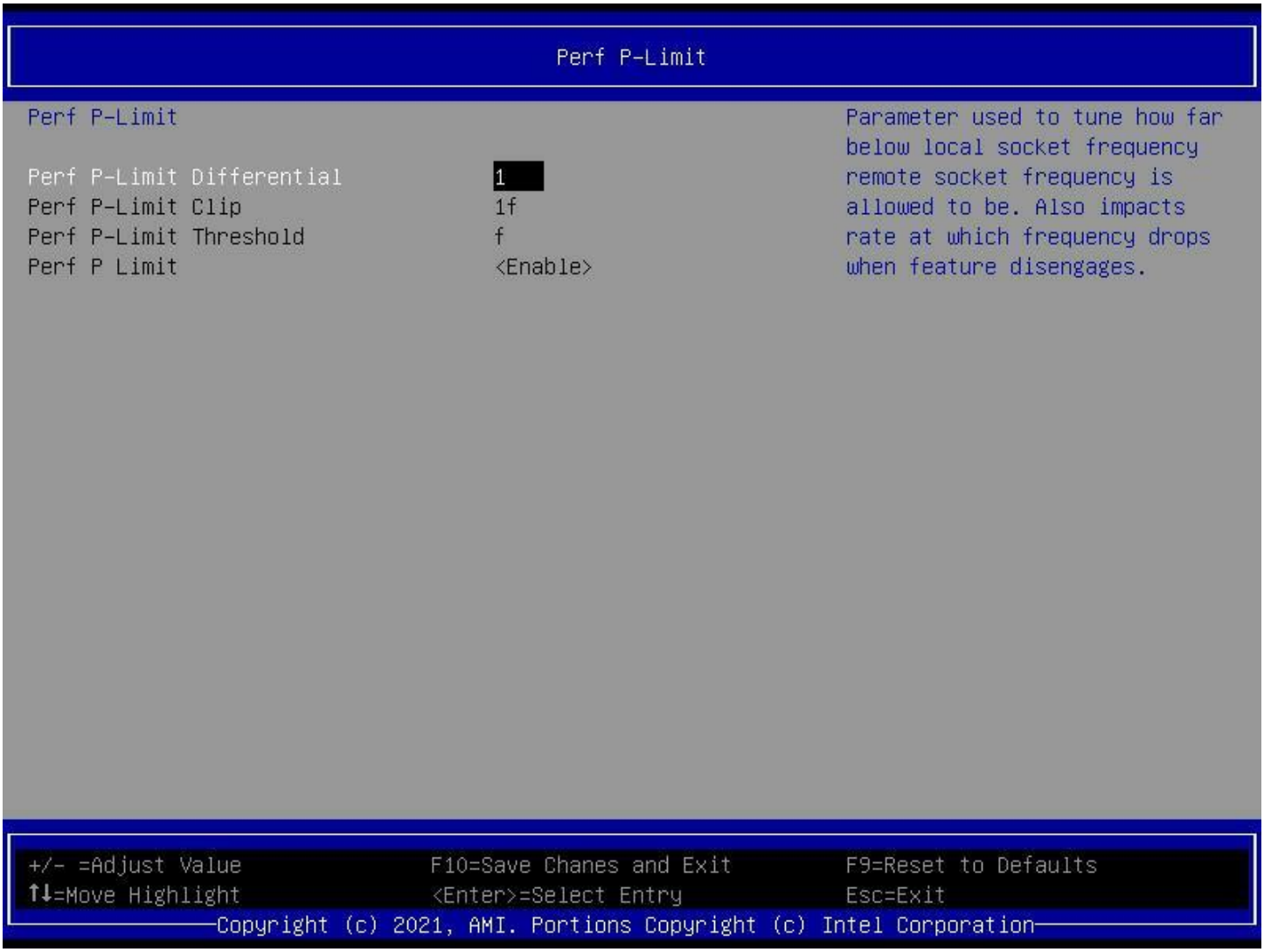

Figure 34. Perf P-Limit Screen

1. Perf P-Limit Differential

Value: 1

Help text: `Parameter used to tune how far below local socket frequency remote socket frequency is allowed to be. Also impacts rate at which frequency drops when feature disengages.`

Comments: None.

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

2. Perf P-Limit Clip

Value: 1f

Help text: `Maximum value the floor is allowed to be set to for perf P-limit.`

Comments: Ranges from 0 to 0x1f.

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

3. Perf P-Limit Threshold

Value: f

Help text: `Uncore frequency threshold above which this socket will trigger the feature and start trying to raise frequency of other sockets.`

Comments: Ranges from 0 to 0x1f.

Back to: **Perf P-Limit** – **CPU P State Control** – **Power & Performance** – **Advanced** – **Screen Map**

4. Perf P-Limit

Value: **Enable** / Disable

Help text: `Enable/Disable Performance P-Limit.`

Comments: None.

Back to: **Perf P-Limit** – **CPU P State Control** – **Power & Performance** – **Advanced** – **Screen Map**

5.15.2 Hardware PM State Control

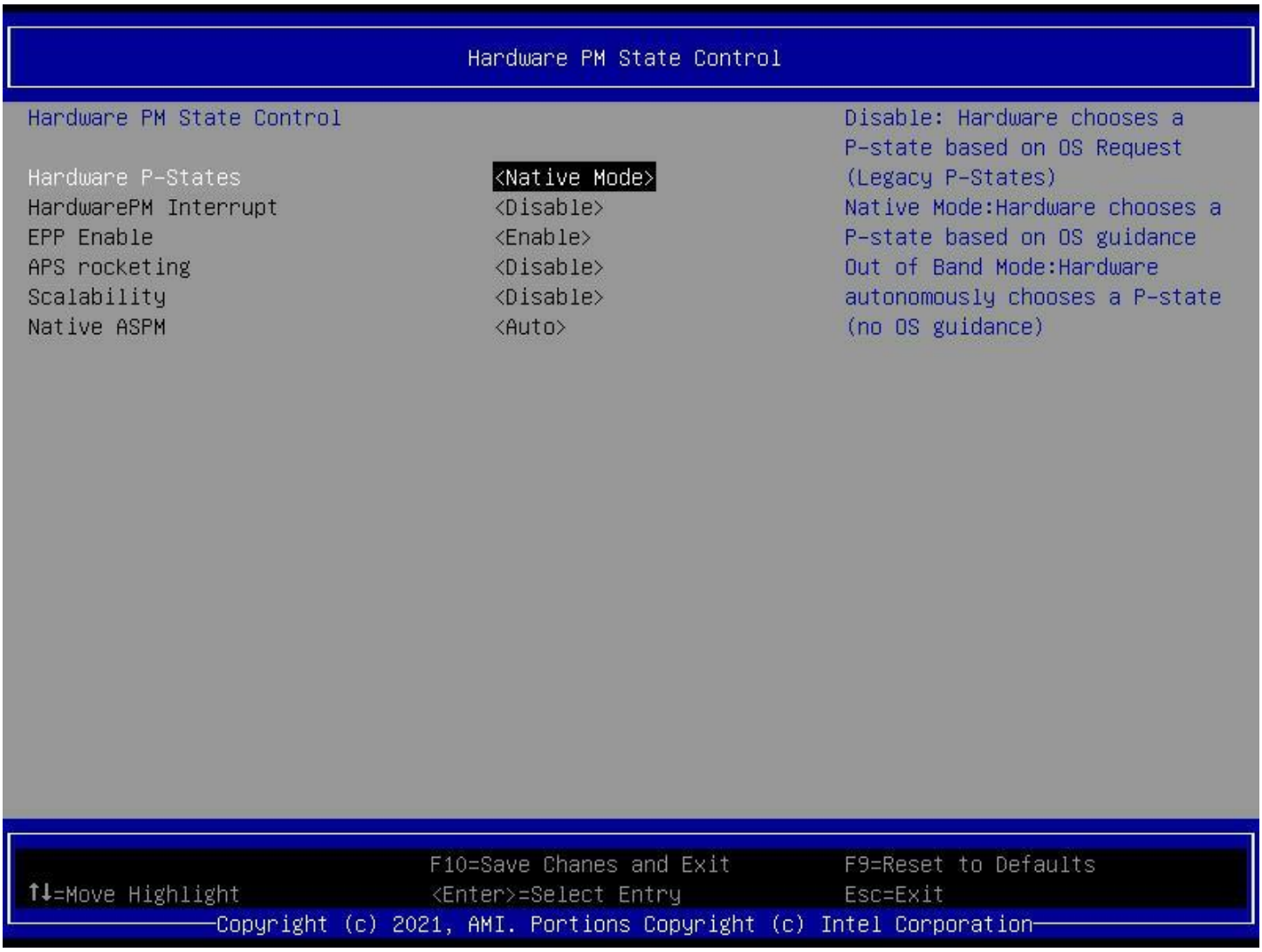

Figure 35. Hardware PM-State Control Screen

1. Hardware P-States

Value: **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 PM State Control – Power & Performance – Advanced – Screen Map

2. HardwarePM Interrupt

Value: Enable / **Disable**

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

Comments: None.

Back to: Hardware PM State Control – Power & Performance – Advanced – Screen Map

3. EPP Enable

Value: **Enable** / Disable

Help text: `When disabled, HW masks EPP in CPUID[6].10 and uses EPB for EPP.`

Comments: None.

Back to: **Hardware PM State Control** – **Power & Performance** – **Advanced** – **Screen Map**

4. APS rocketing

Value: Enable / **Disable**

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

Comments: None.

Back to: **Hardware PM State Control** – **Power & Performance** – **Advanced** – **Screen Map**

5. Scalability

Value: Enable / **Disable**

Help text: `Enable/Disable Core Performance to Frequency Scalability Based Optimizations in the CPU.`

Comments: None.

Back to: **Hardware PM State Control** – **Power & Performance** – **Advanced** – **Screen Map**

6. Native ASPM

Value: **Auto** / Enable / Disable

Help text: `Enabled – OS Controlled ASPM, Disabled – ASPM Off, AUTO – BIOS Controlled ASPM.`

Comments: None.

Back to: **Hardware PM State Control** – **Power & Performance** – **Advanced** – **Screen Map**

5.15.3 CPU C State Control

Figure 36. CPU C-State Control Screen

1. CPU C6 report

Value: **Auto** / Enable / Disable

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

Comments: None.

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

2. Enhanced Halt State (C1E)

Value: **Enable** / Disable

Help text: `Core C1E auto promotion Control. Takes effect after reboot.`

Comments: None.

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

3. OS ACPI Cx

Value: **ACPI C2** / ACPI C3

Help text: `Report CC3/CC6 to OS ACPI C2 or ACPI C3.`

Comments: None.

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

5.15.4 Package C State Control

Figure 37. Package C-State Control Screen

1. **Package C State**

Value: <**Auto**> / <C0/C1 state> / <C2 state> / <C6 (non-Retention) state> / <C6 (Retention) state> / <No limit>

Help text: `Package C State limit.`

Comments: <No limit> is invisible with ICXSP or ICXD CPUs.

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

6. Platform Configuration

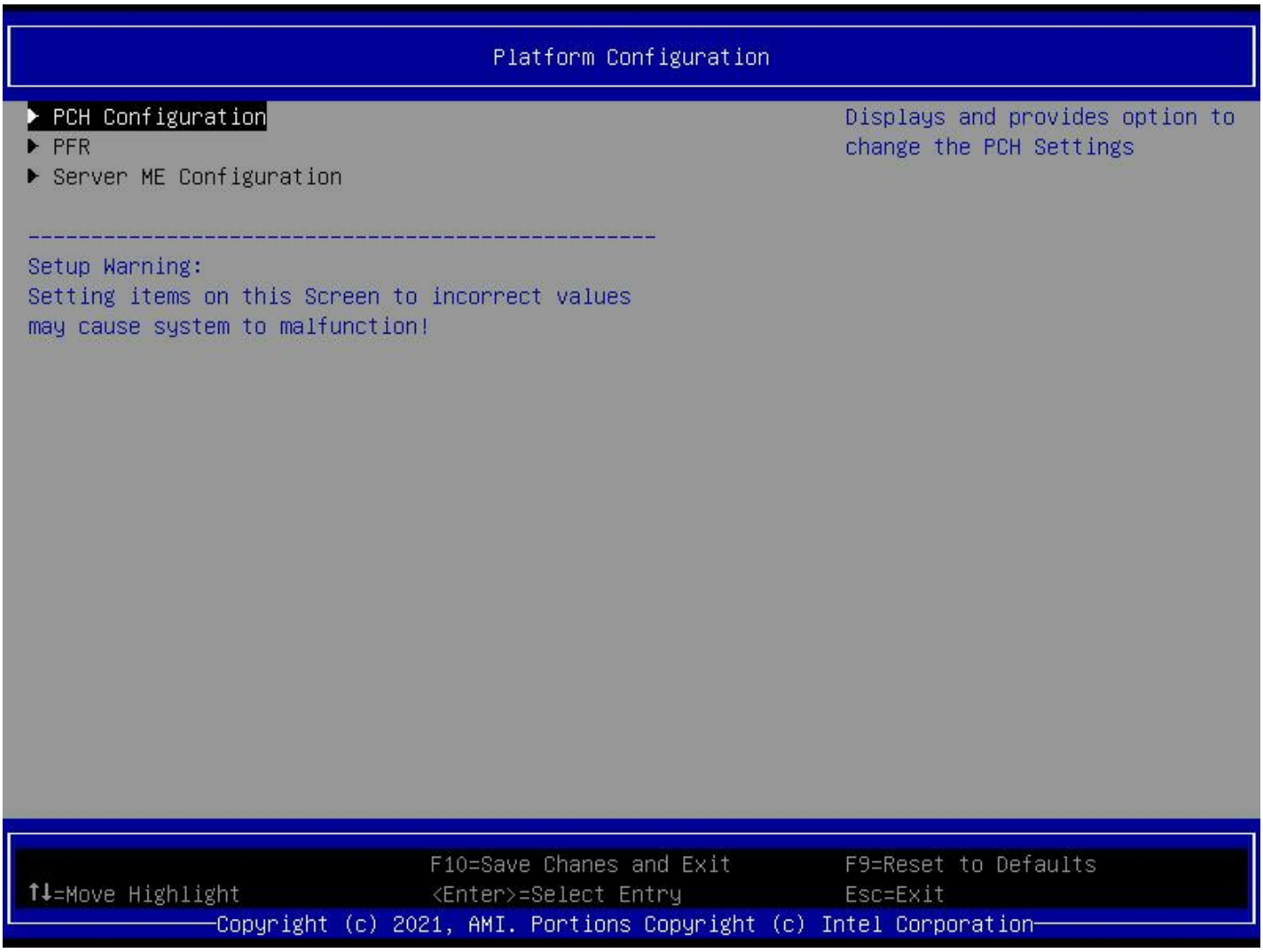

Figure 38. Platform Configuration Screen

1. Platform Configuration

Value: None.

Help text: `Displays and provides option to change the PCH Settings.`

Comments: *Selection only.*

Back to: **Platform Configuration** – **Screen Map**

2. PFR

Value: None.

Help text: None.

Comments: *Selection only.*

Back to: **Platform Configuration** – **Screen Map**

3. Server ME Configuration

Value: None.

Help text: `Configure Server ME Technology Parameters.`

Comments: *Selection only.*

Back to: **Platform Configuration** – **Screen Map**

6.1 PCH Configuration

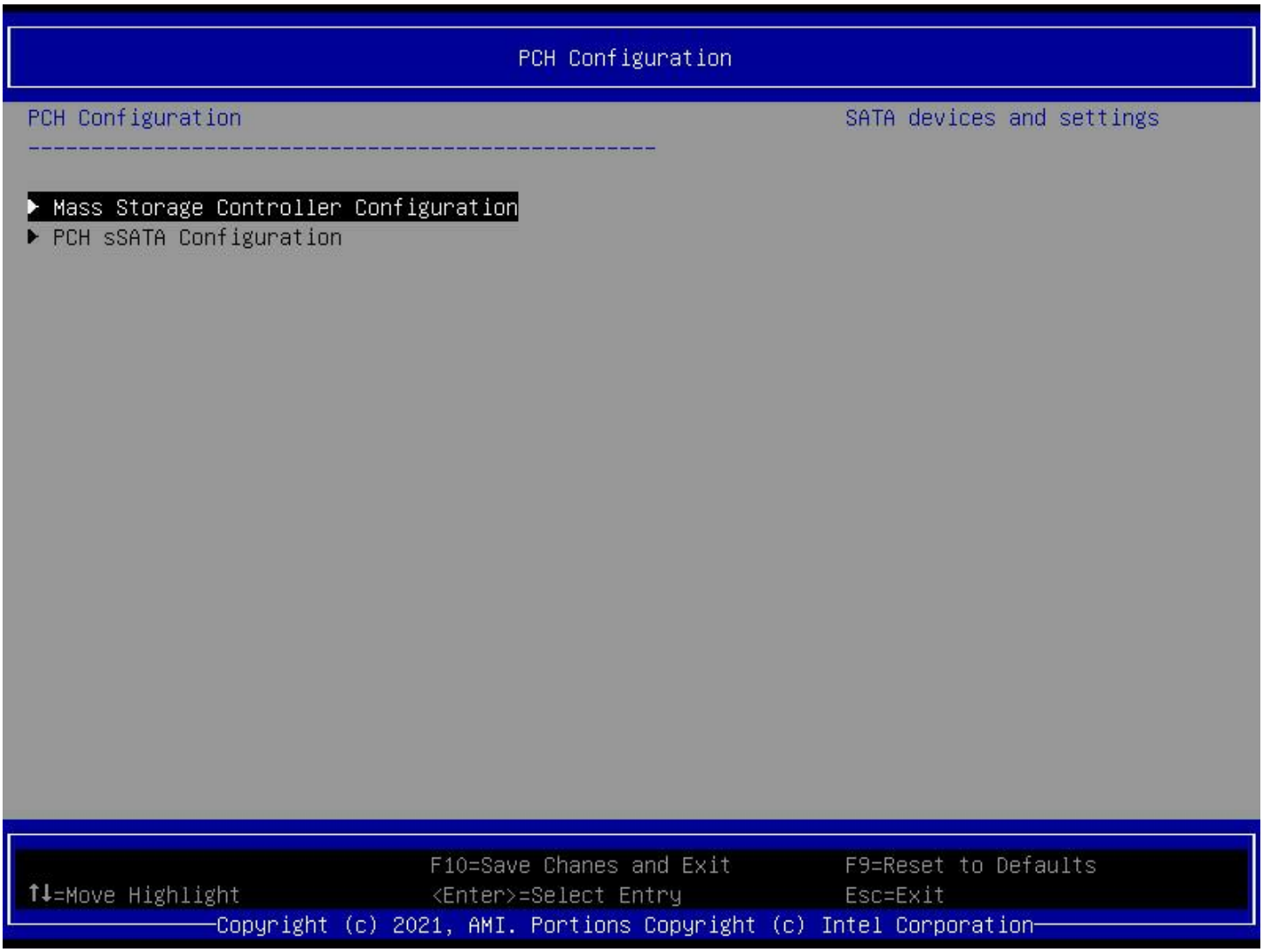

Figure 39. PCH Configuration Screen

1. Mass Storage Controller Configuration

Value: None.

Help text: `SATA devices and settings.`

Comments: *Selection only.*

Back to: PCH Configuration – Platform Configuration – Screen Map

2. PCH sSATA Configuration

Value: None.

Help text: `sSATA devices and settings.`

Comments: *Selection only.*

Back to: PCH Configuration – Platform Configuration – Screen Map

6.1.1 Mass Storage Controller Configuration

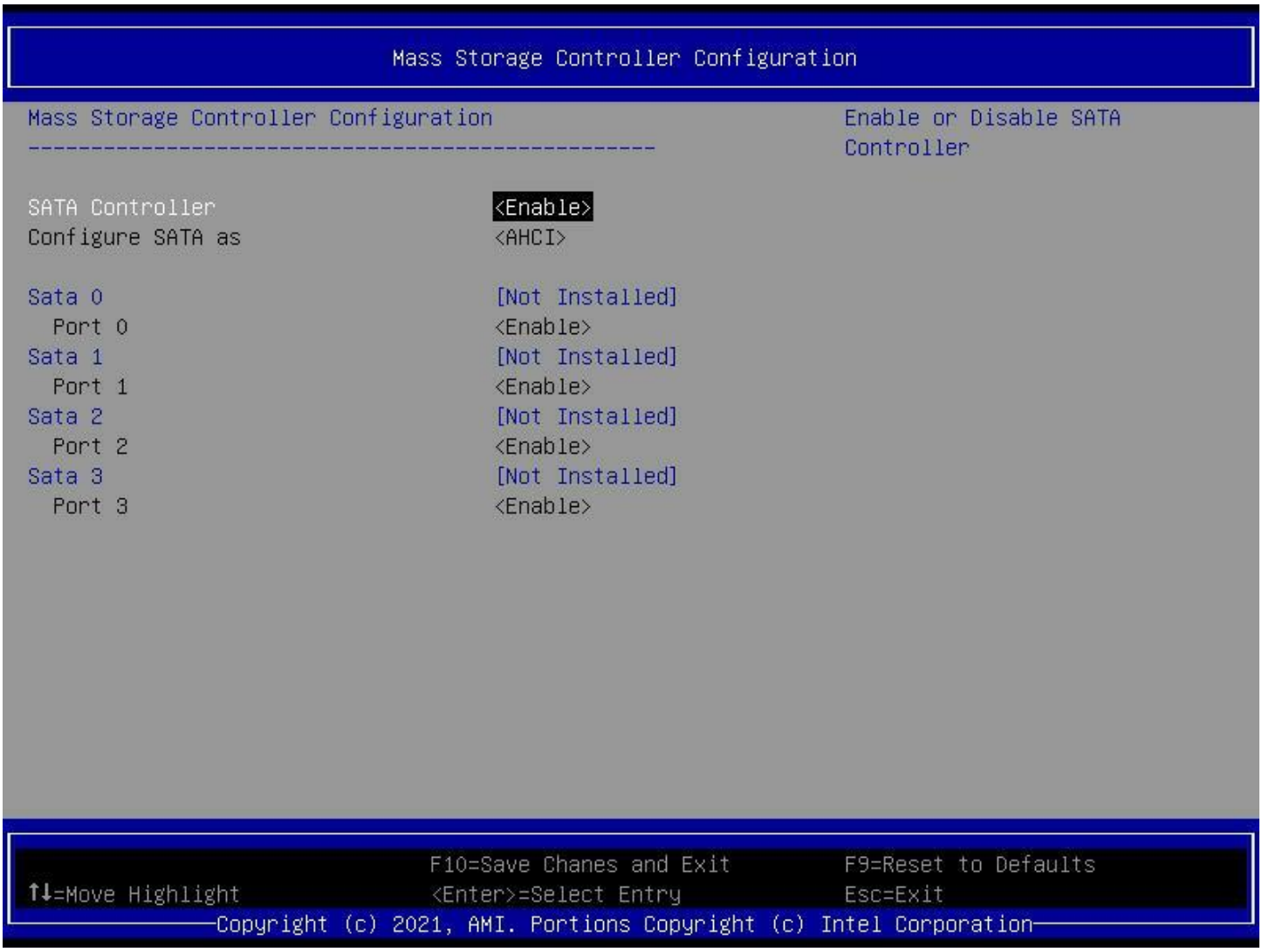

Figure 40. Mass Storage Controller Configuration Screen

1. SATA Controller

Value: **Enable** / Disable

Help text: `Enable or Disable SATA Controller.`

Comments: None.

Back to: **Mass Storage Controller Configuration** – **PCH Configuration** – **Platform Configuration** – **Screen Map**

2. Configure SATA as

Value: **AHCI** / RAID

Help text: `This will configure SATA as IDE, RAID or AHCI.`

Comments: This option is visible only when SATA Controller is enabled.

Back to: **Mass Storage Controller Configuration** – **PCH Configuration** – **Platform Configuration** – **Screen Map**

6.1.2 PCH sSATA Configuration

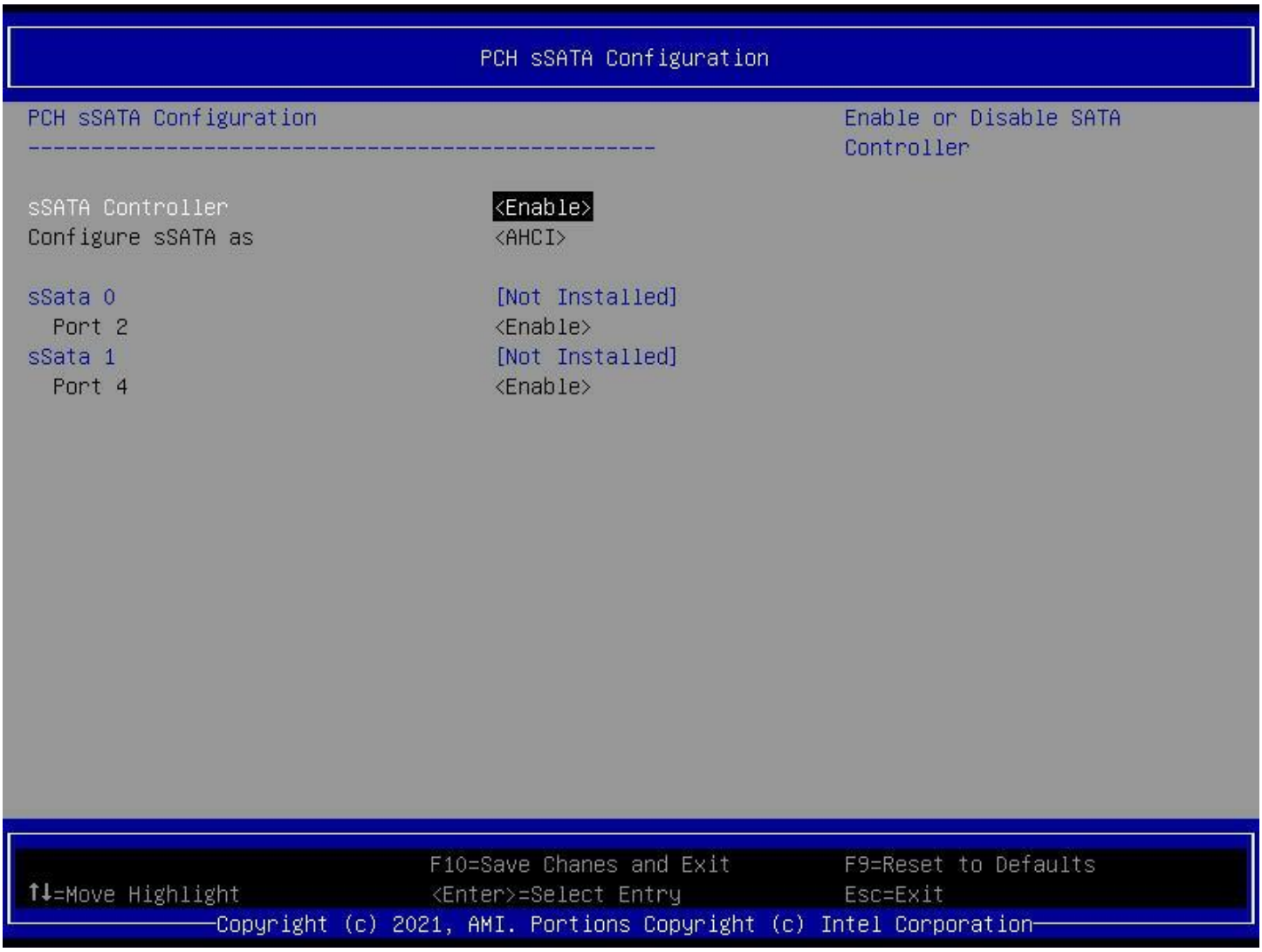

Figure 41. PCH sSATA Configuration Screen

1. sSATA Controller

Value: **Enable** / Disable

Help text: `Enable or Disable SATA Controller.`

Comments: None.

Back to: PCH sSATA Configuration – PCH Configuration – Platform Configuration – Screen Map

2. Configure sSATA as

Value: **AHCI** / RAID

Help text: `This will configure sSATA as IDE, RAID or AHCI.`

Comments: This option is visible only when sSATA Controller is enabled.

Back to: PCH sSATA Configuration – PCH Configuration – Platform Configuration – Screen Map

6.2 PFR

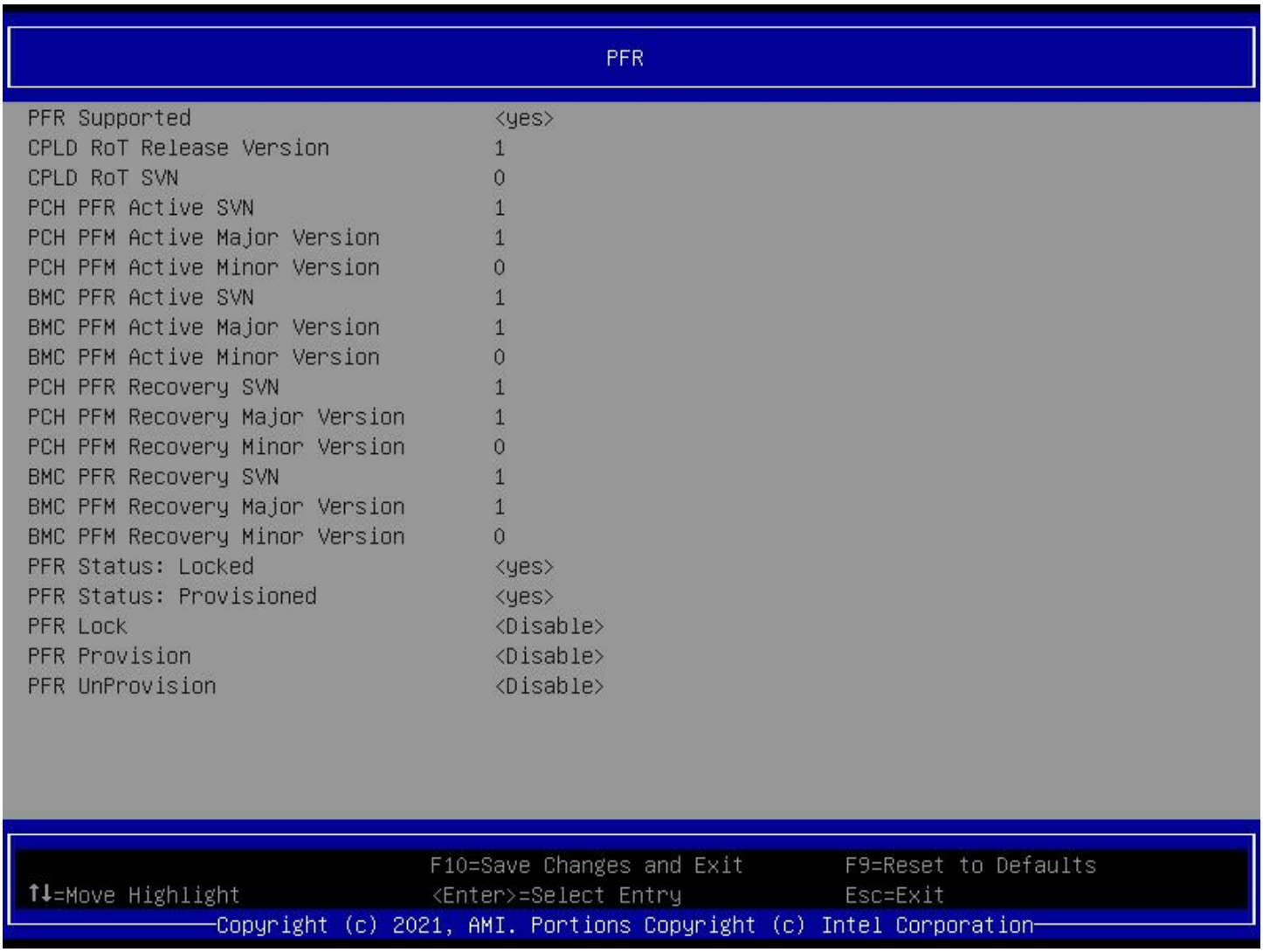

Figure 42. PFR Screen

1. PFR Supported

Value: **yes** / no

Help text: None.

Comments: *Information only.*

Back to: **PFR – Platform Configuration – Screen Map**

2. **CPLD RoT Released Version**
   CPLD RoT SVN
   PCH PFR Active SVN
   PCH PFR Active Major Version
   PCH PFR Active Minor Version
   BMC PFR Active SVN
   BMC PFR Active Major Version
   BMC PFR Active Minor Version
   PCH PFR Recovery SVN
   PCH PFR Recovery Major Version
   PCH PFR Recovery Minor Version
   BMC PFR Recovery SVN
   BMC PFR Recovery Major Version
   BMC PFR Recovery Minor Version

Value: <FW PFM versions>

Help text: None.

Comments: *Information only.* Note that the firmware of a higher SVN cannot be updated to one of a lower SVN.

Back to: **PFR – Platform Configuration – Screen Map**

3. **PFR Status: Locked**

Value: **yes** / no

Help text: None.

Comments: *Information only.* This item indicates whether the platform is PFR locked.

Back to: **PFR – Platform Configuration – Screen Map**

4. **PFR Status: Provisioned**

Value: **yes** / no

Help text: None.

Comments: *Information only.* This item indicates whether PFR provisioning is enabled.

Back to: **PFR – Platform Configuration – Screen Map**

5. **PFR Lock**

Value: Enable / **Disable**

Help text: `When locked, PFR cannot be unlocked unless CPLD is reprogrammed. Selectable if PFR is provisioned.`

Comments: To enable PFR lock, enable this option, save, and reset. After the reset, this option changes back to disabled automatically.

To see whether PFR lock is enabled, check the option PFR Status: Locked.

Back to: **PFR – Platform Configuration – Screen Map**

6. PFR Provision

Value: Enable / **Disable**

Help text: `Selectable if PFR is not locked.`

Comments: To enable PFR provision, enable this option, save, and reset. After the reset, this option changes back to disabled automatically.

To see whether PFR provision is enabled, check the option PFR Status: Provisioned.

Back to: **PFR – Platform Configuration – Screen Map**

7. PFR UnProvisioned

Value: Enable / **Disable**

Help text: `Enable to Erase PFR Provision Information, including PIT Level-1 and Level-2 information. Selectable only if PFR is provisioned AND not locked.`

Comments: To disable PFR provision, enable this option, save, and reset. After the reset, this option changes back to disabled automatically.

To see whether PFR provision is disabled, check the option PFR Status: Provisioned.

Back to: **PFR – Platform Configuration – Screen Map**

6.3 Server ME Configuration

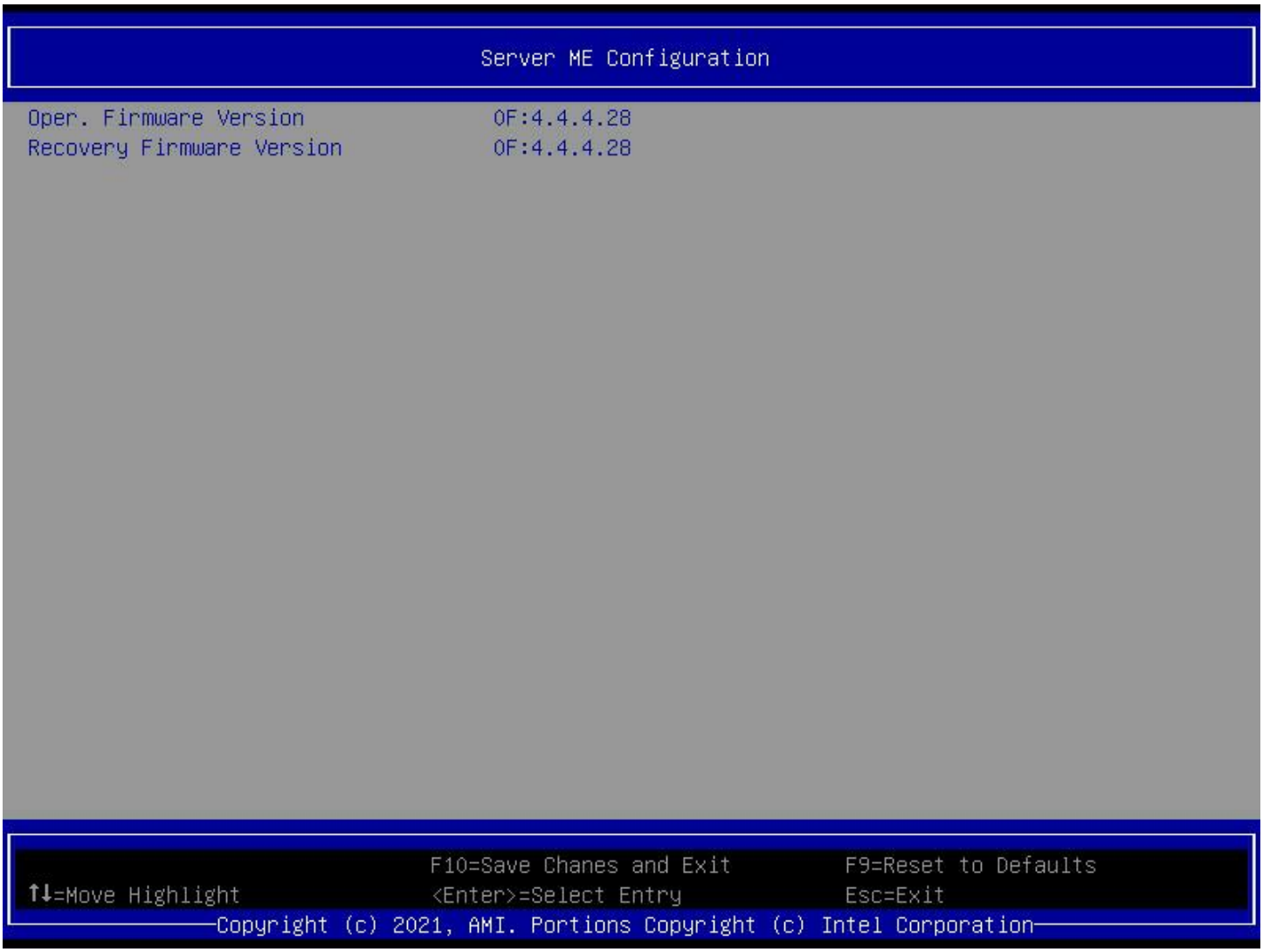

Figure 43. Server ME Configuration Screen

1. **Oper. Firmware Version**

Value: <Operational ME version>

Help text: None.

Comments: *Information only.*

Back to: **Server ME Configuration** – **Platform Configuration** – **Screen Map**

2. **Recovery Firmware Version**

Value: <Recovery ME version>

Help text: None.

Comments: *Information only.*

Back to: **Server ME Configuration** – **Platform Configuration** – **Screen Map**

7. Socket Configuration

Figure 44. Socket Configuration Screen

1. Processor Configuration

Value: None.

Help text: `Displays and provides option to change the Processor Settings.`

Comments: *Selection only.*

Back to: **Socket Configuration** – **Screen Map**

2. Uncore Configuration

Value: None.

Help text: `Displays and provides option to change the Uncore Settings.`

Comments: *Selection only.*

Back to: **Socket Configuration** – **Screen Map**

3. Memory Configuration

Value: None.

Help text: `Displays and provides option to change the Memory Settings.`

Comments: *Selection only.*

Back to: **Socket Configuration** – **Screen Map**

4. IIO Configuration

Value: None.

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

Comments: *Selection only.*

Back to: **Socket Configuration** – **Screen Map**

7.1 Processor Configuration

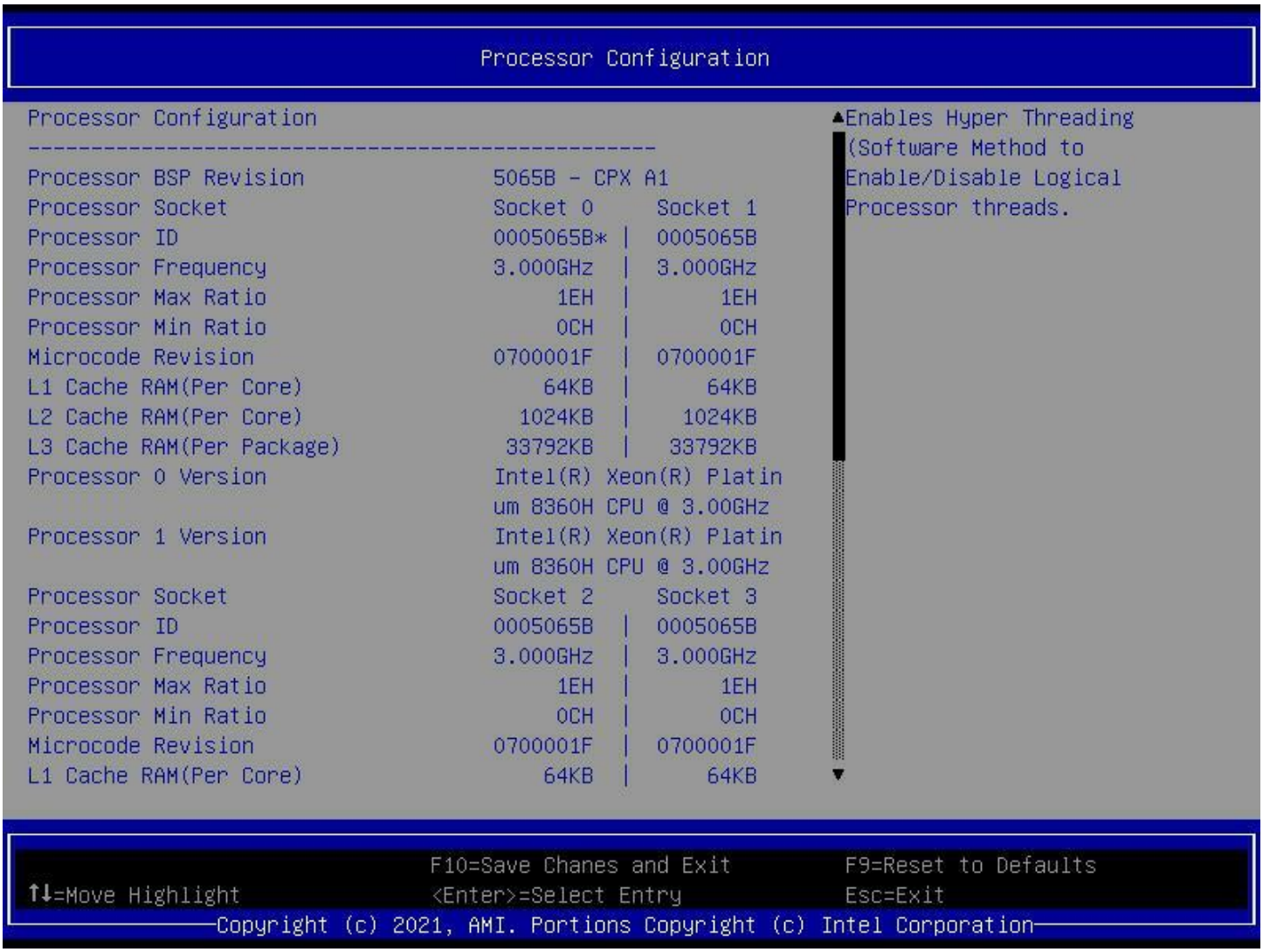

Figure 45. Processor Configuration Screen (1)

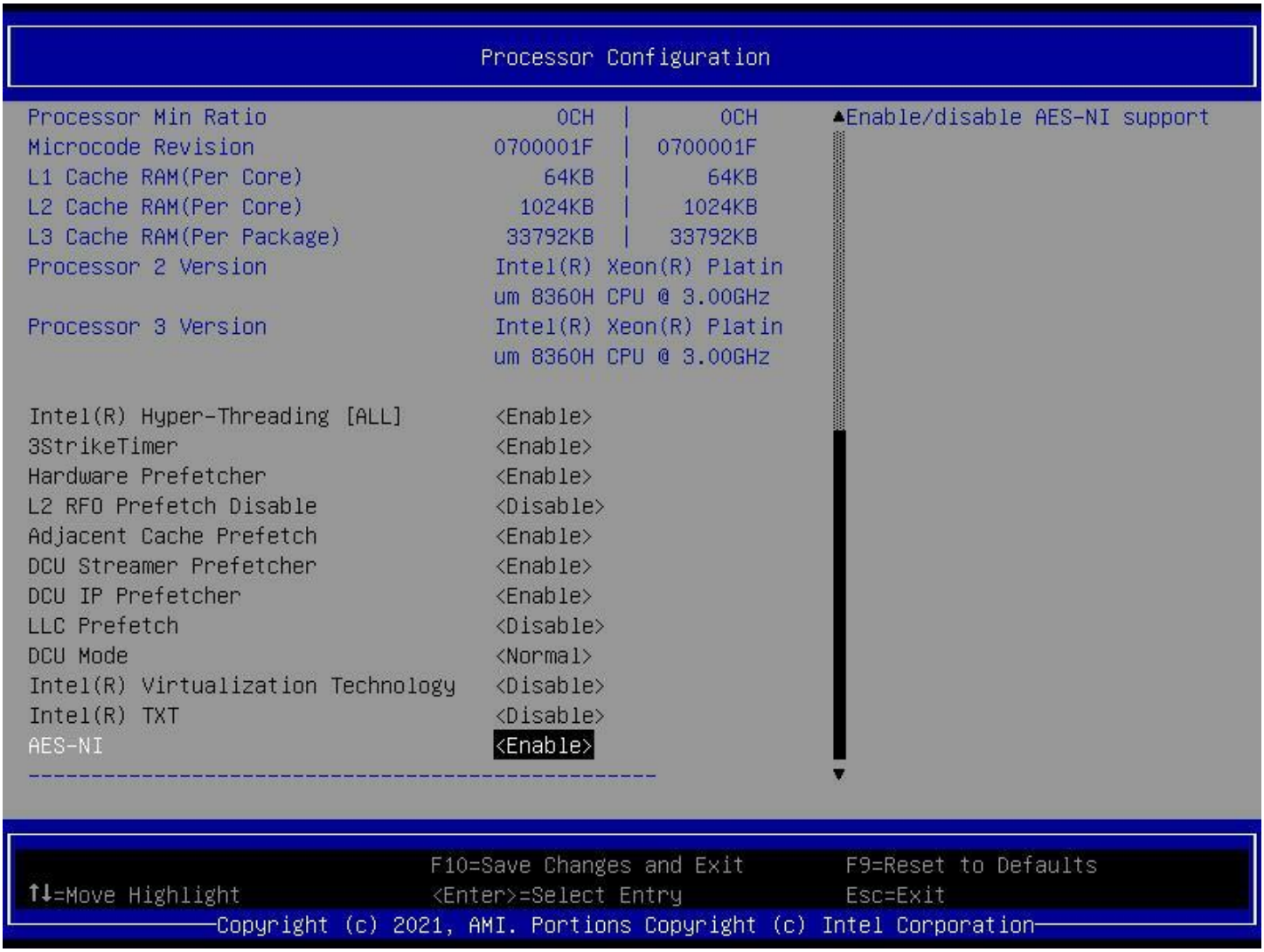

Figure 46. Processor Configuration Screen (2)

1. Processor BPS Revision

Value: <Processor BPS Revision>

Help text: None.

Comments: *Information only.*

Back to: **Processor Configuration** – **Socket Configuration** – **Screen Map**

2. Processor Socket

Value: <Processor Socket>

Help text: None.

Comments: *Information only.*

Back to: **Processor Configuration** – **Socket Configuration** – **Screen Map**

3. Processor ID

Value: <CPUID>

Help text: None.

Comments: *Information only.* Displays the processor signature value (from the CPUID instruction), which identifies the processor type and the stepping.

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

Back to: **Processor Configuration – Socket Configuration – Screen Map**

4. Processor Frequency

Value: <Current processor frequency>

Help text: None.

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

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

Back to: **Processor Configuration – Socket Configuration – Screen Map**

5. Processor Max Ratio

Value: <Processor Max Ratio>

Help text: None.

Comments: *Information only.*

Back to: **Processor Configuration – Socket Configuration – Screen Map**

6. Processor Min Ratio

Value: <Processor Min Ratio>

Help text: None.

Comments: *Information only.*

Back to: **Processor Configuration – Socket Configuration – Screen Map**

7. Microcode Revision

Value: <Microcode Revision>

Help text: None.

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

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

Back to: **Processor Configuration – Socket Configuration – Screen Map**

8. L1 Cache RAM(Per Core)

Value: <L1 Cache RAM (Per Core)>

Help text: None.

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

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

Back to: **Processor Configuration – Socket Configuration – Screen Map**

9. L2 Cache RAM(Per Core)

Value: <L2 Cache RAM (Per Core)>

Help text: None.

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

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

Back to: **Processor Configuration – Socket Configuration – Screen Map**

10. L3 Cache RAM(Per Package)

Value: <L3 Cache RAM (Per Package)>

Help text: None.

Comments: *Information only.* Displays the processor L3 cache's size in KB. Since L3 cache is shared between cores, this value is shown as the amount of L3 cache per package.

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

Back to: **Processor Configuration – Socket Configuration – Screen Map**

11. Processor 0 Version
Processor 1 Version

Value: <Processor 0/1 Version>

Help text: None.

Comments: *Information only.* Displays the brand ID string, read from the processor via CPUID instruction.

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

Back to: **Processor Configuration – Socket Configuration – Screen Map**

12. Intel(R) Hyper-Threading [All]

Value: **Enable** / Disable

Help text: `Enables Hyper Threading (Software Method to Enable/Disable Logical Processor threads).`

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

Back to: **Processor Configuration – Socket Configuration – Screen Map**

13. 3StrikeTimer

Value: **Enable** / Disable

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

Comments: None.

Back to: **Processor Configuration – Socket Configuration – Screen Map**

14. Hardware Prefetcher

Value: **Enable** / Disable

Help text: `= MLC Streamer Prefetcher (MSR 1A4h Bit [0]).`

Comments: None.

Back to: **Processor Configuration – Socket Configuration – Screen Map**

15. L2 RF0 Prefetch Disable

Value: Enable / **Disable**

Help text: `= L2 RF0 Prefetch (MSR 972h Bit [3]).`

Comments: None.

Back to: **Processor Configuration – Socket Configuration – Screen Map**

16. Adjacent Cache Prefetch

Value: **Enable** / Disable

Help text: `= MLC Spatial Prefetcher (MSR 1A4h Bit [1]).`

Comments: None.

Back to: **Processor Configuration – Socket Configuration – Screen Map**

17. DCU Streamer Prefetcher

Value: **Enable** / Disable

Help text: `DCU streamer prefetcher is an L1 data cache prefetcher (MSR 1A4h [2]).`

Comments: None.

Back to: **Processor Configuration – Socket Configuration – Screen Map**

18. DCU IP Prefetcher

Value: **Enable** / Disable

Help text: `DCU IP prefetcher is an L1 data cache prefetcher (MSR 1A4h [3]).`

Comments: None.

Back to: **Processor Configuration** – **Socket Configuration** – **Screen Map**

19. LCC Prefetch

Value: Enable / **Disable**

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

Comments: None.

Back to: **Processor Configuration** – **Socket Configuration** – **Screen Map**

20. DCU Mode

Value: **Normal** / Mirror-Mode

Help text: `Normal: The whole DCU used for caching;`
`Mirror-Mode: DCU organized as 2x16KB mirrored copies.`

Comments: None.

Back to: **Processor Configuration** – **Socket Configuration** – **Screen Map**

21. Intel(R) Virtualization Technology

Value: Enable / **Disable**

Help text: `Enables the Vanderpool Technology, takes effect after reboot.`

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

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

Back to: **Processor Configuration** – **Socket Configuration** – **Screen Map**

22. Intel(R) TXT

Value: Enable / **Disable**

Help text: `Enables Intel(R) TXT.`

Comments: Intel® TXT only appears 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 working on models equipped with a trusted platform module (TPM). The TPM must be active to support Intel® TXT.

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

Back to: **Processor Configuration** – **Socket Configuration** – **Screen Map**

23. AES-NI

Value: **Enable** / Disable

Help text: `Enable/disable AES-NI support.`

Comments: None.

Back to: **Processor Configuration** – **Socket Configuration** – **Screen Map**

7.2 Uncore Configuration

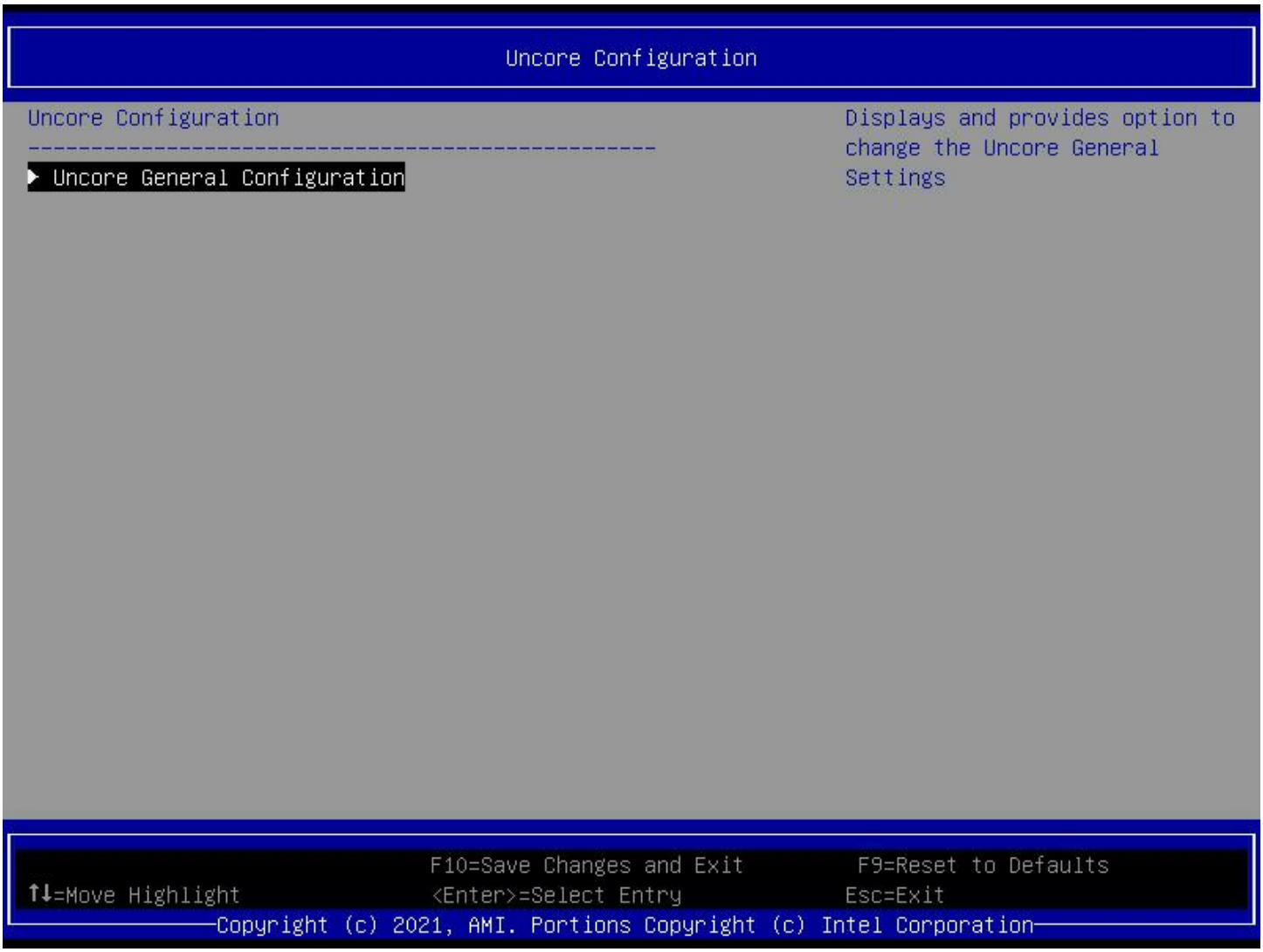

Figure 47. Uncore Configuration Screen

1. Uncore General Configuration

Value: None.

Help text: `Displays and provides option to change the Uncore Settings.`

Comments: *Selection only.*

Back to: **Uncore Configuration** – **Socket Configuration** – **Screen Map**

7.2.1 Uncore General Configuration

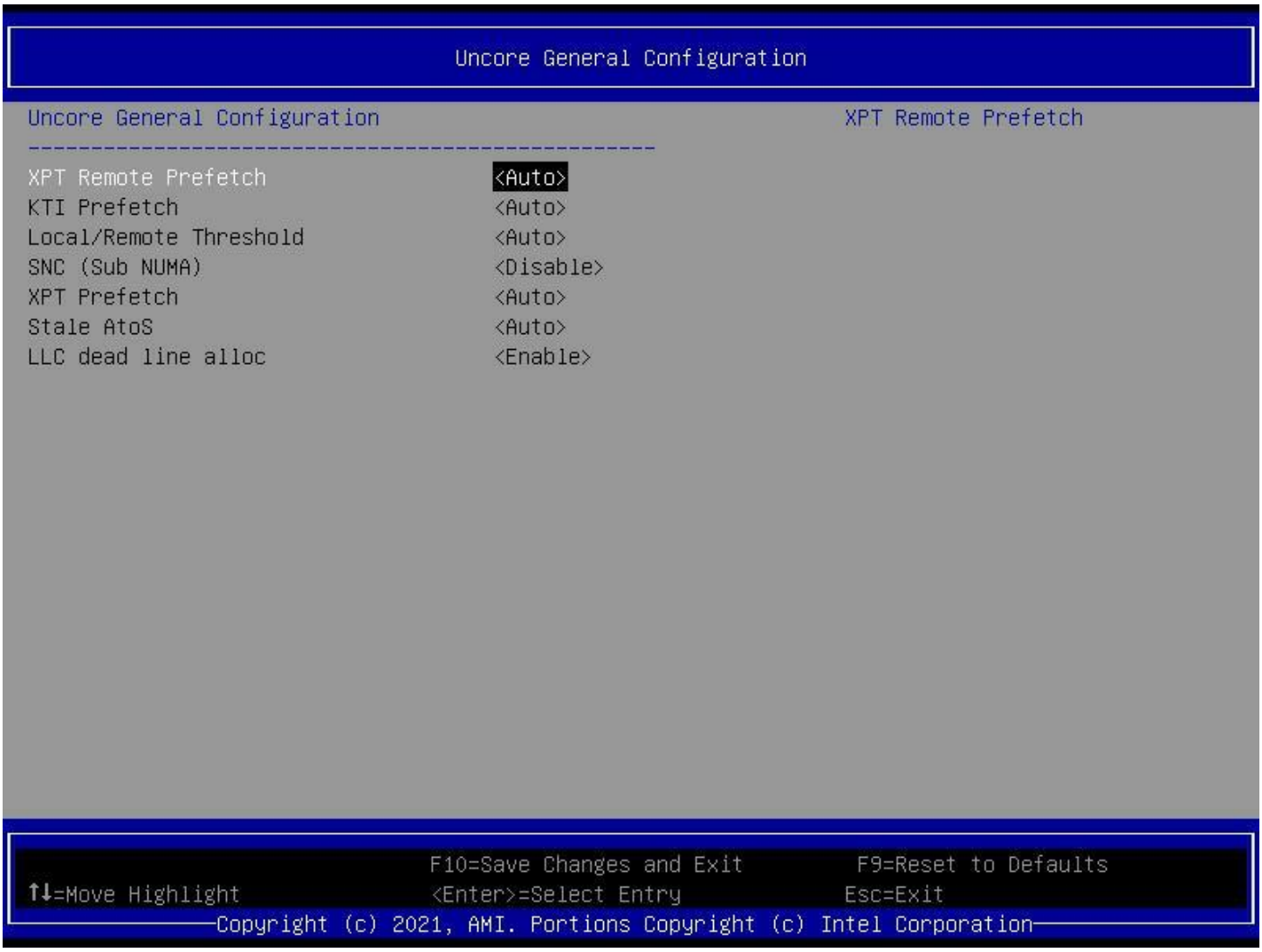

Figure 48. Uncore General Configuration Screen

1. XPT Remote Prefetch

Value: **Auto** / Enable / Disable

Help text: `XPT Remote Prefetch.`

Comments: None.

Back to: **Uncore General Configuration** – **Uncore Configuration** – **Socket Configuration** – **Screen Map**

2. KTI Prefetch

Value: **Auto** / Enable / Disable

Help text: `KTI Prefetch.`

Comments: None.

Back to: **Uncore General Configuration** – **Uncore Configuration** – **Socket Configuration** – **Screen Map**

3. Local / Remote Threshold

Value: **Auto** / Disable / Low / Medium / High

Help text: `Local/Remote Threshold setting.`

Comments: None.

Back to: **Uncore General Configuration** – **Uncore Configuration** – **Socket Configuration** – **Screen Map**

4. SNC (Sub NUMA)

Value: Enable / **Disable**

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. SNC4 Enable supports 4-clusters SNC and 1-way IMC interleave. Enable SNC2 or SNC4 will gray out iMC_Interleave knob and UmaBasedClustering knob.`

Comments: None.

Back to: **Uncore General Configuration** – **Uncore Configuration** – **Socket Configuration** – **Screen Map**

5. XPT Prefetch

Value: **Auto** / Enable / Disable

Help text: `XPT Prefetch.`

Comments: None.

Back to: **Uncore General Configuration** – **Uncore Configuration** – **Socket Configuration** – **Screen Map**

6. Stale AtoS

Value: **Auto** / Enable / Disable

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 the 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: **Uncore General Configuration** – **Uncore Configuration** – **Socket Configuration** – **Screen Map**

7. LLC dead line alloc

Value: **Enable** / Disable

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

`Disable - never fill dead lines in LLC.`

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

Back to: **Uncore General Configuration** – **Uncore Configuration** – **Socket Configuration** – **Screen Map**

7.3 Memory Configuration

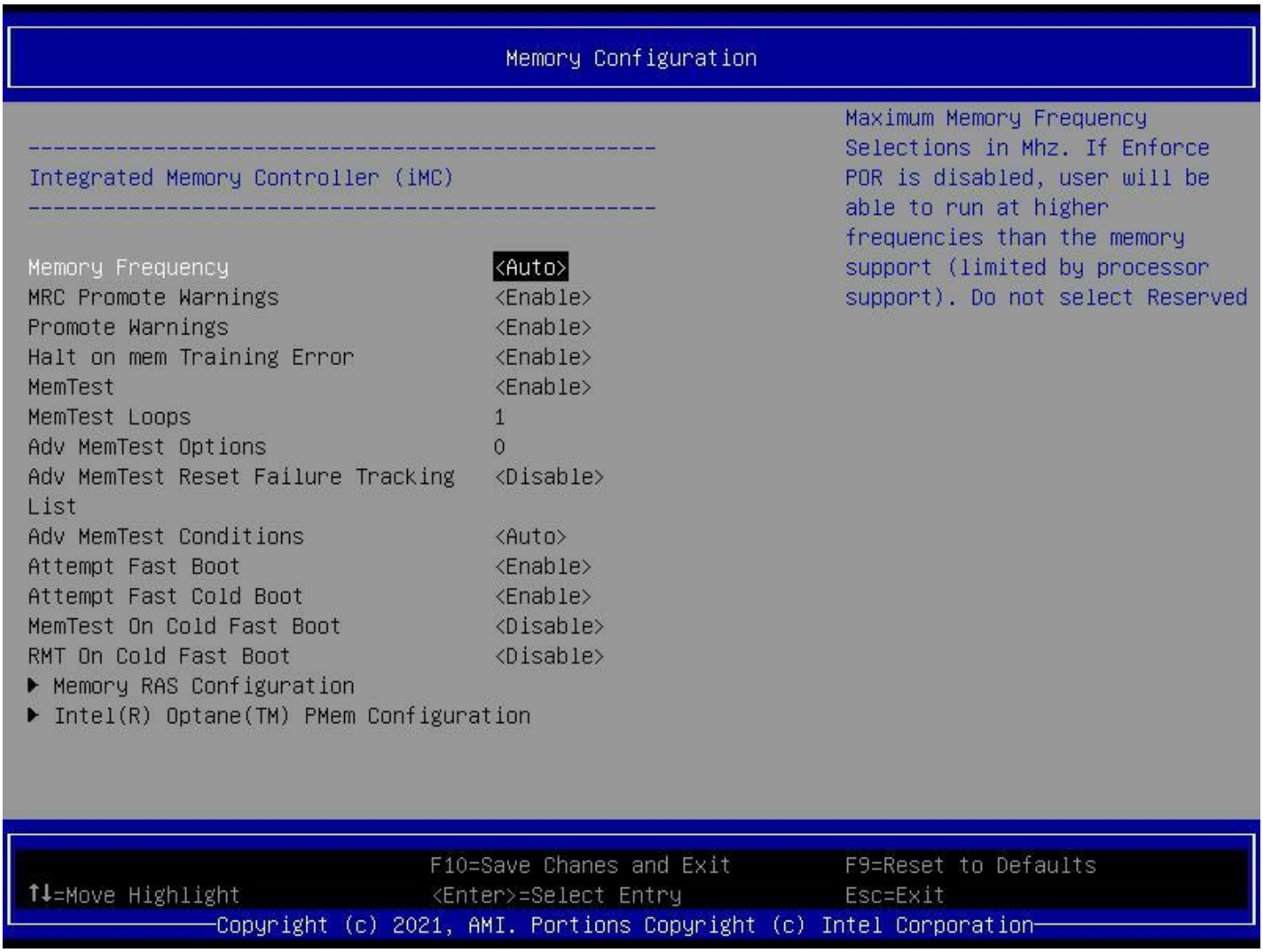

Figure 49. Memory Configuration Screen

1. Memory Frequency

Value: **Auto** / 1200 / 1333 / 1400 / 1600 / 1800 / 1866 / 2000 / 2133 / 2200 / 2400 / 2600 / 2666 / 2800 / 2933 / 3000 / 3200 / 3400-OvrClk / 3466-OvrClk / 3600-OvrClk / 3733-OvrClk / 3800-OvrClk / 4000-OvrClk / 4200-OvrClk / 4266-OvrClk / 4400-OvrClk

Help text: `Maximum Memory Frequency Selections in MHz. If Enforce POR is disabled, user will be able to run at higher frequencies than the memory support (limited by processor support). Do not select Reserved.`

Comments: None.

Back to: Memory Configuration – Socket Configuration – Screen Map

2. MRC Promote Warnings

Value: **Enable** / Disable

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

Comments: None.

Back to: **Memory Configuration – Socket Configuration – Screen Map**

3. Promote Warnings

Value: **Enable** / Disable

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

Comments: None.

Back to: **Memory Configuration – Socket Configuration – Screen Map**

4. Halt on mem Training Error

Value: **Enable** / Disable

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

Comments: None.

Back to: **Memory Configuration – Socket Configuration – Screen Map**

5. MemTest

Value: **Enable** / Disable

Help text: `Enable - Enables memory test during normal boot.`

`Disable - Disables this feature.`

Comments: None.

Back to: **Memory Configuration – Socket Configuration – Screen Map**

6. MemTest Loops

Value: <0~65535>

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

Comments: Default is 1.

Back to: **Memory Configuration – Socket Configuration – Screen Map**

7. Adv MemTest Options

Value: <0~65535>

Help text: `This option is a bit mask [15:0]: 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, bit-11=TWR, bit-12=DATARET, bit-13=MATS8TC1, bit-14=MATS8TC2, bit-15=MATS8TC3.`

Comments: None.

Back to: **Memory Configuration – Socket Configuration – Screen Map**

8. Adv MemTest Reset Failure Tracking List

Value: **Disable** / Enable

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 – Socket Configuration – Screen Map**

9. Adv MemTest Conditions

Value: **Auto** / Manual / Disable

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 – Socket Configuration – Screen Map**

10. Attempt Fast Boot

Value: **Enable** / Disable / Auto

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 Enable.

Comments: None.

Back to: **Memory Configuration – Socket Configuration – Screen Map**

11. Attempt Fast Cold Boot

Value: **Enable** / Disable / Auto

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 Disable.

Comments: None.

Back to: **Memory Configuration – Socket Configuration – Screen Map**

12. MemTest On Cold Fast Boot

Value: Enable / **Disable** / Auto

Help text: Enable - Enables memory test during cold fast boot.

Disable - Disables this feature.

Auto - Sets it to the MRC default setting; current default is Disable.

Comments: None.

Back to: **Memory Configuration – Socket Configuration – Screen Map**

13. RMT On Cold Fast Boot

Value: Enable / **Disable** / Auto

Help text: `Enable - Enables Rank Margin Tool on Cold Fast Boot.`

`Disable - Disables this feature.`

`Auto - Sets it to the MRC default setting; current default is Disable. Should be disabled in production releases.`

Comments: None.

Back to: **Memory Configuration** – **Socket Configuration** – **Screen Map**

14. Memory RAS Configuration

Value: None.

Help text: `Displays and provides option to change the Memory RAS Settings.`

Comments: *Selection only.*

Back to: **Memory Configuration** – **Socket Configuration** – **Screen Map**

15. Intel(R) Optane(TM) PMem Configuration

Value: None.

Help text: `Displays and provides option to change the PMem settings.`

Comments: *Selection only.*

Back to: **Memory Configuration** – **Socket Configuration** – **Screen Map**

7.3.1 Memory RAS Configuration

Figure 50. Memory Reliability, Availability, Serviceability Configuration Screen

1. Mirror Mode

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

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

Comments: None.

Back to: Memory RAS Configuration – Memory Configuration – Socket Configuration – Screen Map

2. Mirror TAD0

Value: Enabled / **Disabled**

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

Comments: None.

Back to: Memory RAS Configuration – Memory Configuration – Socket Configuration – Screen Map

3. UEFI ARM Mirror

Value: **Disabled** / Enabled

Help text: `Imitate behavior of UEFI based Address Range Mirror with setup option.`

Comments: None.

Back to: **Memory RAS Configuration** – **Memory Configuration** – **Socket Configuration** – **Screen Map**

4. Correctable Error Threshold

Value: <1~32767>

Help text: `Correctable Error Threshold (1 - 32767) used for sparing, and leaky bucket.`

Comments: None.

Back to: **Memory RAS Configuration** – **Memory Configuration** – **Socket Configuration** – **Screen Map**

5. Trigger SW Error Threshold

Value: **Disabled** / Enabled

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

Comments: None.

Back to: **Memory RAS Configuration** – **Memory Configuration** – **Socket Configuration** – **Screen Map**

6. Sparing SW Error Watch Threshold

Value: <0x0~0x7FFF>

Help text: `SW Correctable Error Threshold (1 - 32767) used for bank level information.`

Comments: Hexadecimal value, in which 14 means 0x14.

Back to: **Memory RAS Configuration** – **Memory Configuration** – **Socket Configuration** – **Screen Map**

7. Correctable Error Time Window

Value: <0x0~0x7FFF>

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

Comments: Hexadecimal value, in which 18 means 0x18.

Back to: **Memory RAS Configuration** – **Memory Configuration** – **Socket Configuration** – **Screen Map**

8. ADDDC Sparing

Value: **Disabled** / Enabled

Help text: `Enable/Disable ADDDC Sparing.`

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

Back to: **Memory RAS Configuration** – **Memory Configuration** – **Socket Configuration** – **Screen Map**

9. Patrol Scrub

Value: **Enable** / Disable

Help text: `Enable/Disable Patrol Scrub.`

Comments: None.

Back to: **Memory RAS Configuration** – **Memory Configuration** – **Socket Configuration** – **Screen Map**

7.3.2 Intel(R) Optane(TM) PMem Configuration

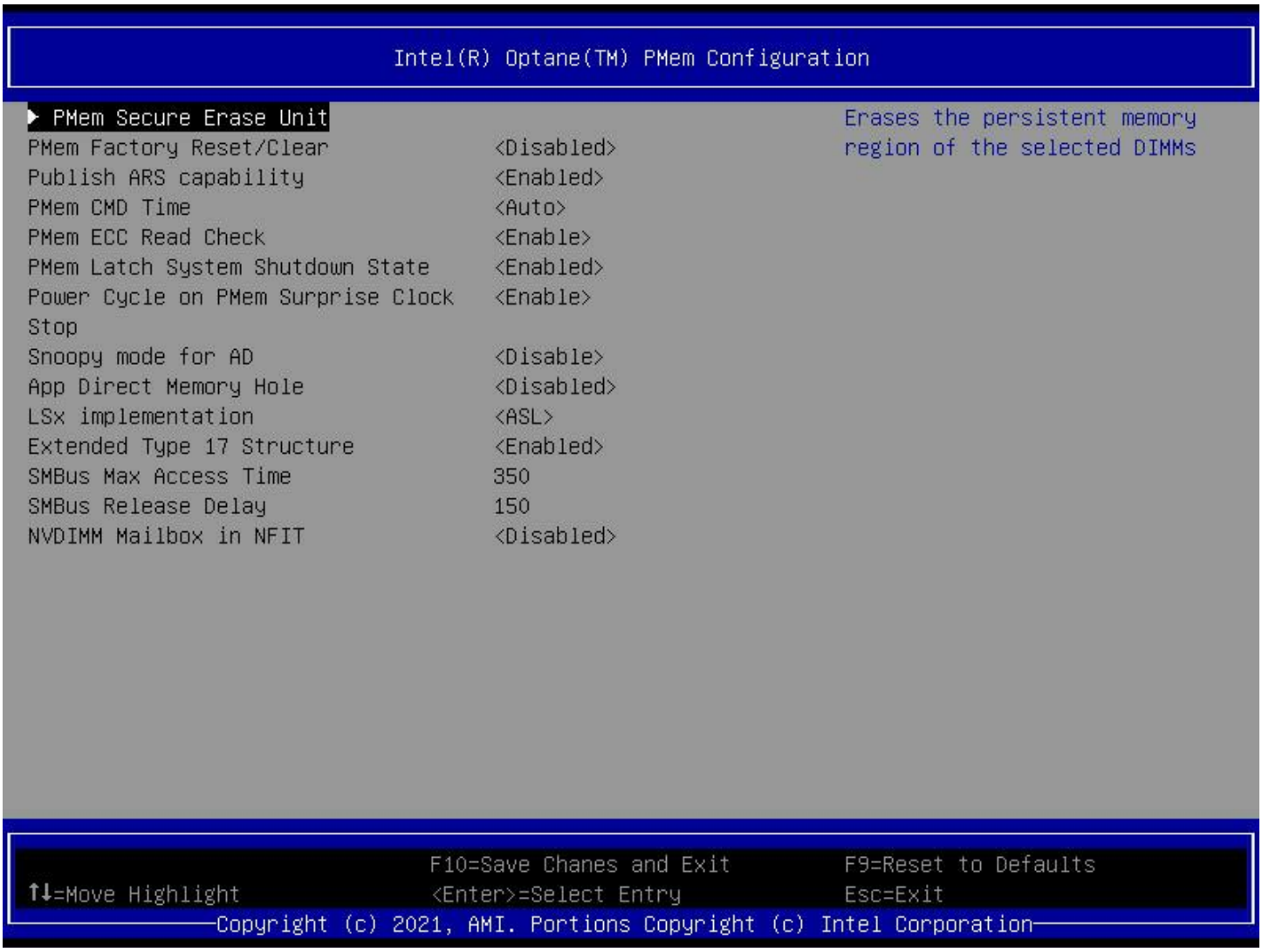

Figure 51. Intel® Optane™ PMem Configuration Screen

1. PMem Secure Erase Unit

Value: None.

Help text: `Erases the persistent memory region of the selected DIMMs.`

Comments: *Selection only.*

Back to: **Intel(R) Optane(TM) PMem Configuration – Memory Configuration – Socket Configuration – Screen Map**

2. PMem Factory Reset/Clear

Value: Enabled / **Disabled**

Help text: `Enable/Disable Factory Reset/Clear. 'Average Power Budget' setup question will override default Average Power Budget.`

Comments: None.

Back to: **Intel(R) Optane(TM) PMem Configuration – Memory Configuration – Socket Configuration – Screen Map**

3. Publish ARS capability

Value: **Enabled** / Disabled

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

Comments: None.

Back to: **Intel(R) Optane(TM) PMem Configuration – Memory Configuration – Socket Configuration – Screen Map**

4. PMem CMD Time

Value: **Auto** / 1N / 2N

Help text: `Select 1N/2N PMem Command time.`

Comments: None.

Back to: **Intel(R) Optane(TM) PMem Configuration – Memory Configuration – Socket Configuration – Screen Map**

5. PMem ECC Read Check

Value: **Enable** / Disable

Help text: `Enable/Disable PMem ECC Read Check.`

Comments: None.

Back to: **Intel(R) Optane(TM) PMem Configuration – Memory Configuration – Socket Configuration – Screen Map**

6. PMem Latch System Shutdown State

Value: **Enabled** / Disabled

Help text: `Latch System Shutdown State.`

Comments: None.

Back to: **Intel(R) Optane(TM) PMem Configuration – Memory Configuration – Socket Configuration – Screen Map**

7. Power Cycle on PMem Surprise Clock Stop

Value: **Enable** / Disable

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

Comments: None.

Back to: **Intel(R) Optane(TM) PMem Configuration – Memory Configuration – Socket Configuration – Screen Map**

8. Snoopy mode for AD

Value: **Disable** / Enable

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 Configuration – Memory Configuration – Socket Configuration – Screen Map**

9. App Direct Memory Hole

Value: **Disabled** / Enabled

Help text: `Enable/Disable the App Direct Memory Hole.`

Comments: None.

Back to: **Intel(R) Optane(TM) PMem Configuration – Memory Configuration – Socket Configuration – Screen Map**

10. LSx implementation

Value: SWSMI / **ASL**

Help text: `Select LSI/LSR/LSW ACPI method implementation.`

Comments: None.

Back to: **Intel(R) Optane(TM) PMem Configuration – Memory Configuration – Socket Configuration – Screen Map**

11. Extended Type 17 Structure

Value: Disabled / **Enabled**

Help text: `Use extended Type 17 SMBIOS Structures.`

Comments: None.

Back to: **Intel(R) Optane(TM) PMem Configuration – Memory Configuration – Socket Configuration – Screen Map**

12. SMBus Max Access Time

Value: <0x0~0xFFFFFFFF>

Help text: `Maximum amount of time (ms) UEFI mgmt driver is allowed to use the SMBus.`

Comments: Hexadecimal value.

Back to: **Intel(R) Optane(TM) PMem Configuration – Memory Configuration – Socket Configuration – Screen Map**

13. SMBus Release Delay

Value: <0x0~0xFFFFFFFF>

Help text: `Delay time (ms) before releasing after UEFI mgmt driver requests SMBus release.`

Comments: Hexadecimal value.

Back to: **Intel(R) Optane(TM) PMem Configuration – Memory Configuration – Socket Configuration – Screen Map**

14. NVDIMM Mailbox in NFIT

Value: **Disabled** / Enabled

Help text: `Enable/disable publishing NVDIMM mailbox registers in NFIT structures.`

Comments: None.

Back to: **Intel(R) Optane(TM) PMem Configuration – Memory Configuration – Socket Configuration – Screen Map**

7.3.2.1 PMem Secure Erase Unit

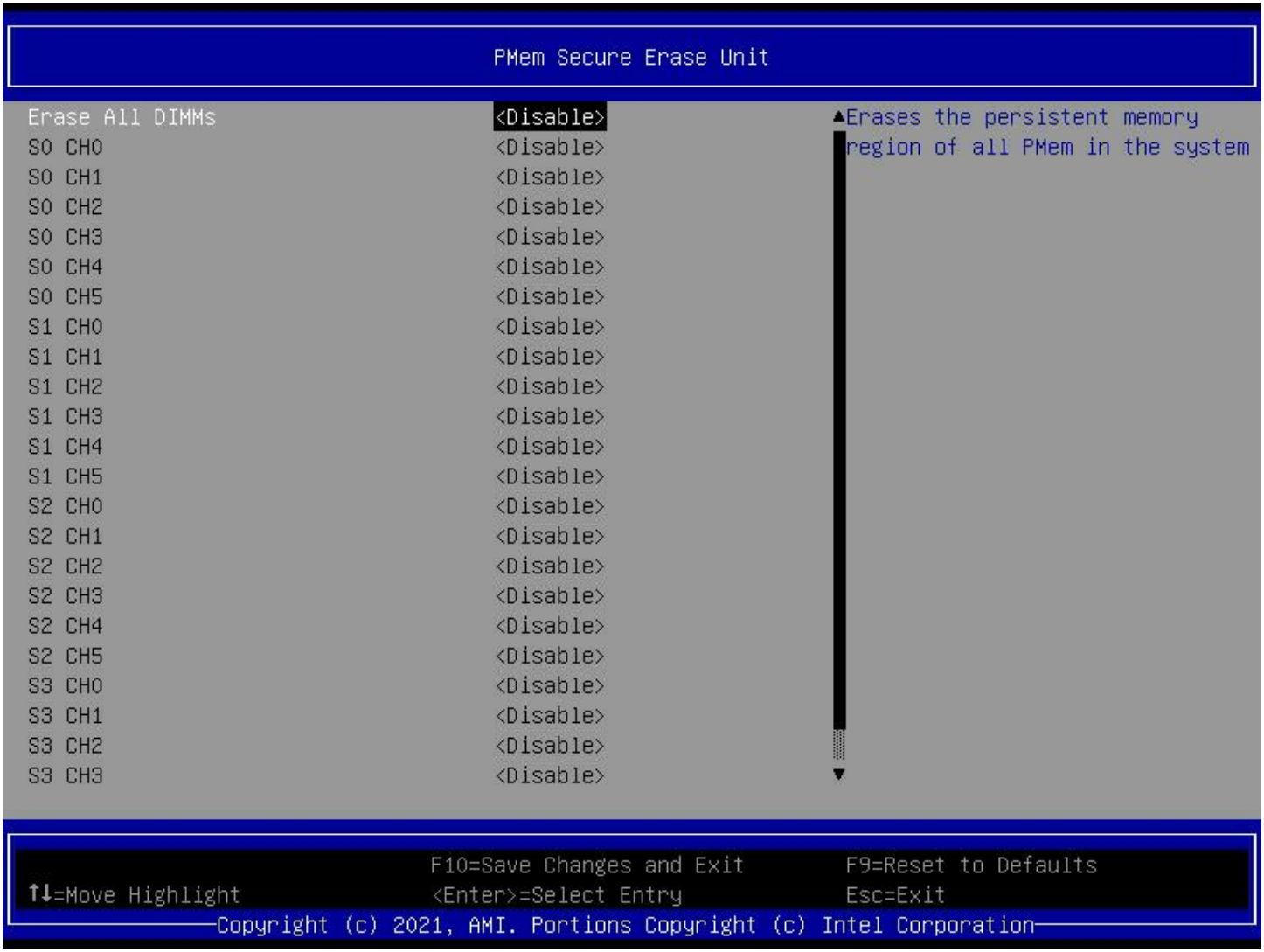

Figure 52. PMem Secure Erase Unit Screen (1)

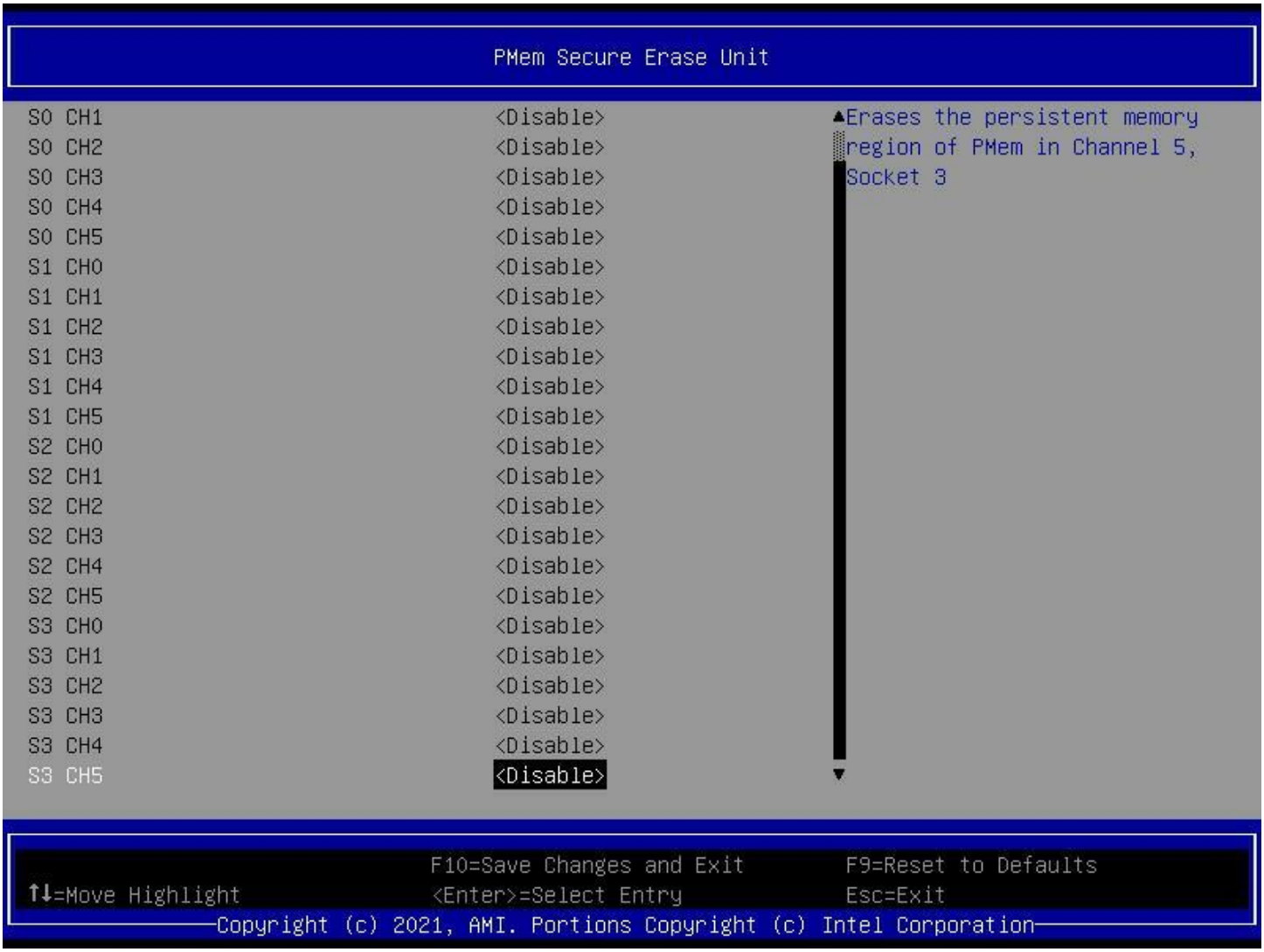

Figure 53. PMem Secure Erase Unit Screen (2)

1. Erase All DIMMs

Value: **Disable** / Enable

Help text: `Erases the persistent memory region of all PMem in the system.`

Comments: *Selection only.*

Back to: **PMem Secure Erase Unit** – **Intel(R) Optane(TM) PMem Configuration** – **Memory Configuration** – **Socket Configuration** – **Screen Map**

7.4 IIO Configuration

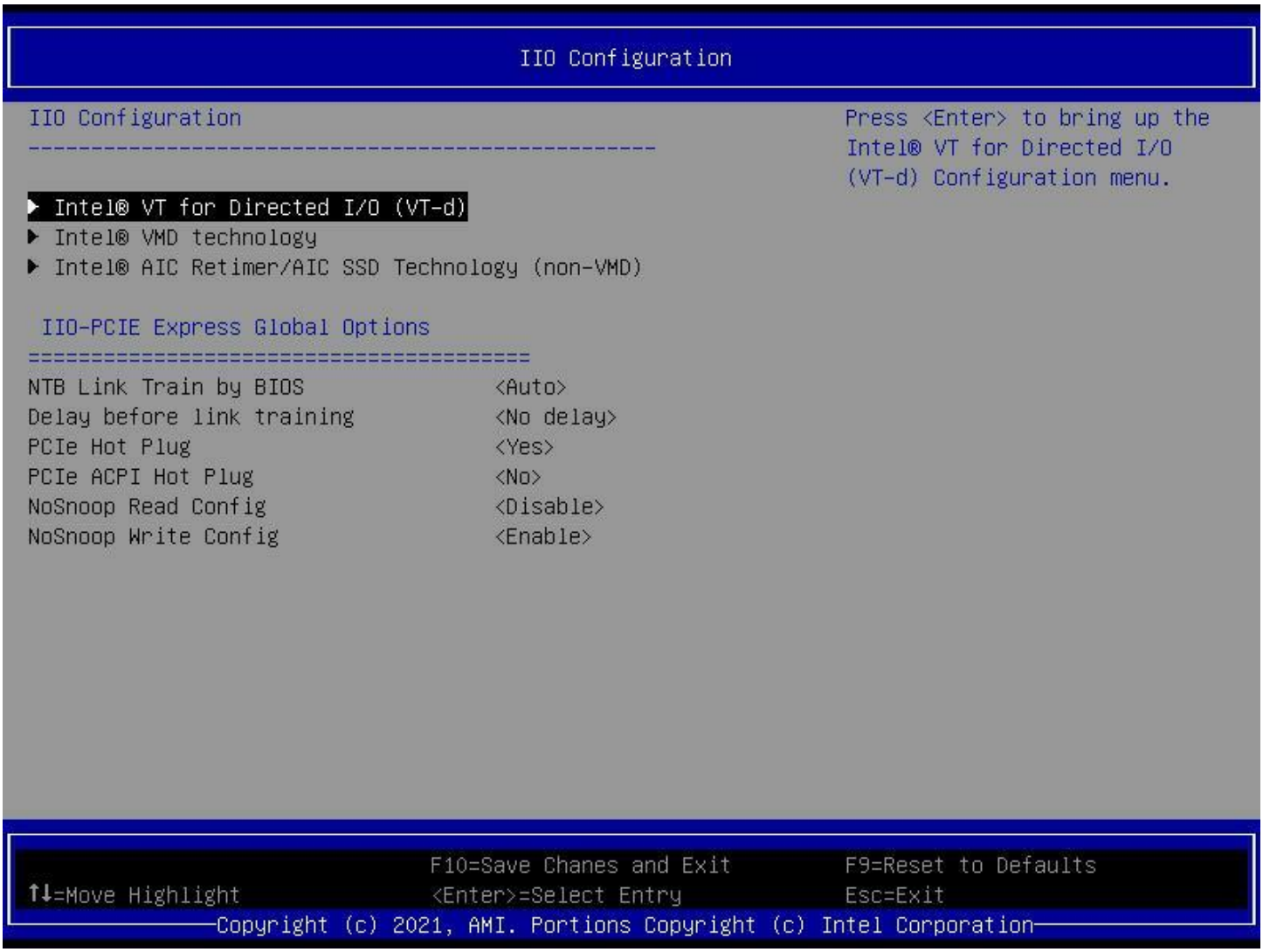

Figure 54. IIO Configuration Screen

1. Intel® VT for Direct I/O (VT-d)

Value: None.

Help text: `Press <Enter> to bring up the Intel® VT for Directed I/O (VT-d) Configuration menu.`

Comments: *Selection only.*

Back to: **IIO Configuration** – **Socket Configuration** – **Screen Map**

2. Intel® VMD technology

Value: None.

Help text: `Press <Enter> to bring up the Intel® VMD for Volume Management Device Configuration menu.`

Comments: *Selection only.*

Back to: **IIO Configuration** – **Socket Configuration** – **Screen Map**

3. Intel® AIC Retimer/AIC SSD Technology (non-VMD)

Value: None.

Help text: `Press <Enter> to bring up the Intel® AIC Retimer/AIC SSD Configuration menu.`

Comments: *Selection only.*

Back to: **IIO Configuration – Socket Configuration – Screen Map**

4. NTB Link Train by BIOS (IIO-PCIE Express Global Options)

Value: **Auto** / Yes / No

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

Comments: None.

Back to: **IIO Configuration – Socket Configuration – Screen Map**

5. Delay before link training (IIO-PCIE Express Global Options)

Value: **No delay** / 100ms / 300ms / 500ms / 1s / 2s

Help text: `Custom delay before PCIe link training on IIO ports.`

Comments: None.

Back to: **IIO Configuration – Socket Configuration – Screen Map**

6. PCIe Hot Plug (IIO-PCIE Express Global Options)

Value: **Yes** / No

Help text: `Enable/Disable PCIe Hot Plug globally.`

Comments: None.

Back to: **IIO Configuration – Socket Configuration – Screen Map**

7. PCIe ACPI Hot Plug (IIO-PCIE Express Global Options)

Value: Yes / **No**

Help text: `Enable/Disable PCIe ACPI Hot Plug globally or allow per-port control. When Disabled, MSI is generated on HP event. When enabled, _HPGPE message is generated.`

Comments: None.

Back to: **IIO Configuration – Socket Configuration – Screen Map**

8. NoSnoop Read Config (IIO-PCIE Express Global Options)

Value: Enable / **Disable**

Help text: `NoSnoop Read Configuration.`

Comments: None.

Back to: **IIO Configuration – Socket Configuration – Screen Map**

9. NoSnoop Write Config (IIO-PCIE Express Global Options)

Value: **Enable** / Disable

Help text: `NoSnoop Write Configuration.`

Comments: None.

Back to: **IIO Configuration – Socket Configuration – Screen Map**

7.4.1 Intel® VT for Directed I/O (VT-d)

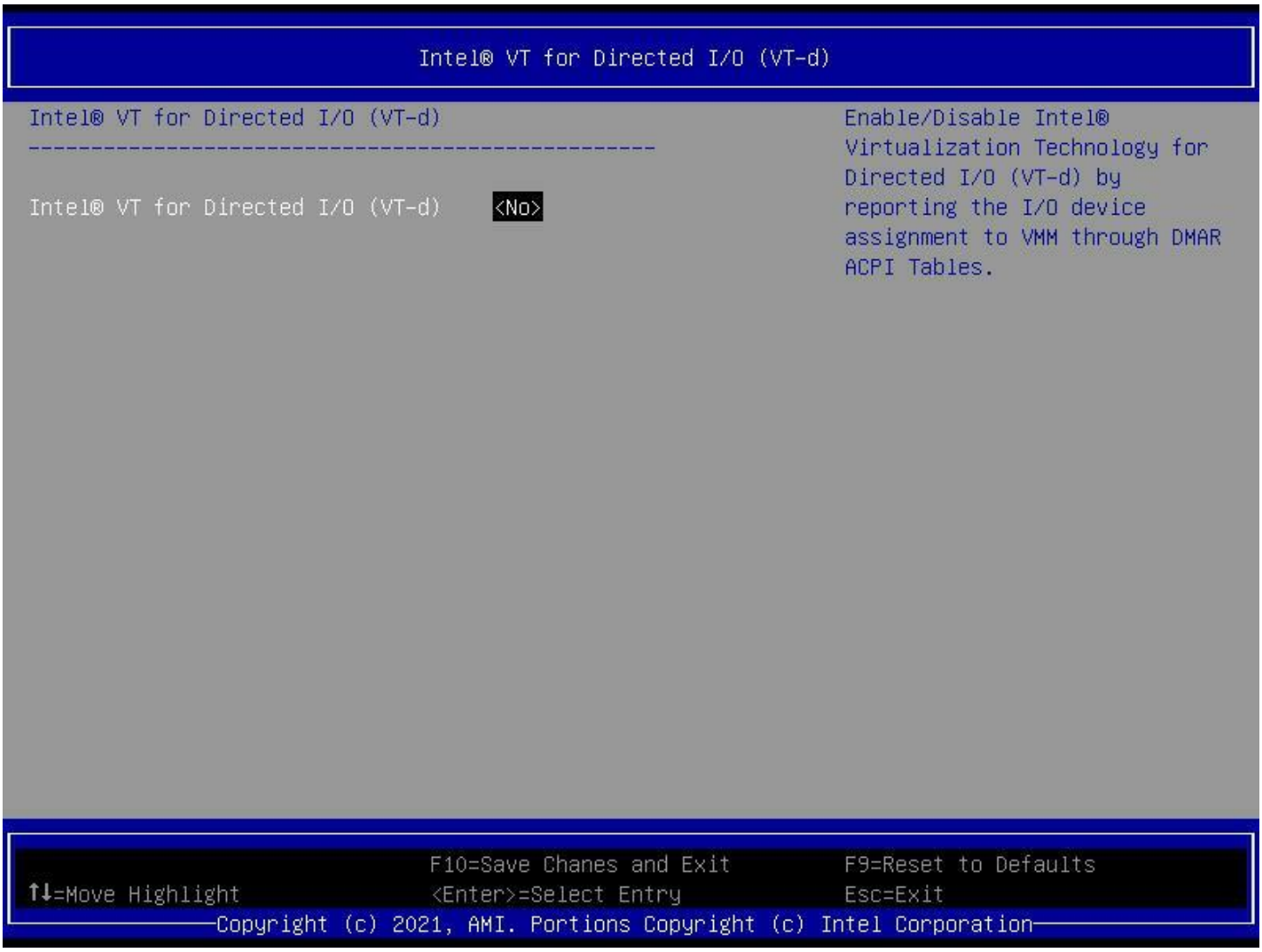

Figure 55. Intel® VT for Directed I/O (VT-d) Screen

1. **Intel® VT for Directed I/O (VT-d)**

Value: Yes / **No**

Help text: `Enable/Disable Intel® Virtualization Technology for Directed I/O (VT-d) by reporting the I/O device assignment to VMM through DMAR ACPI Tables.`

Comments: None.

Back to: Intel® VT for Directed I/O (VT-d) – IIO Configuration – Socket Configuration – Screen Map

7.4.2 Intel® VMD technology

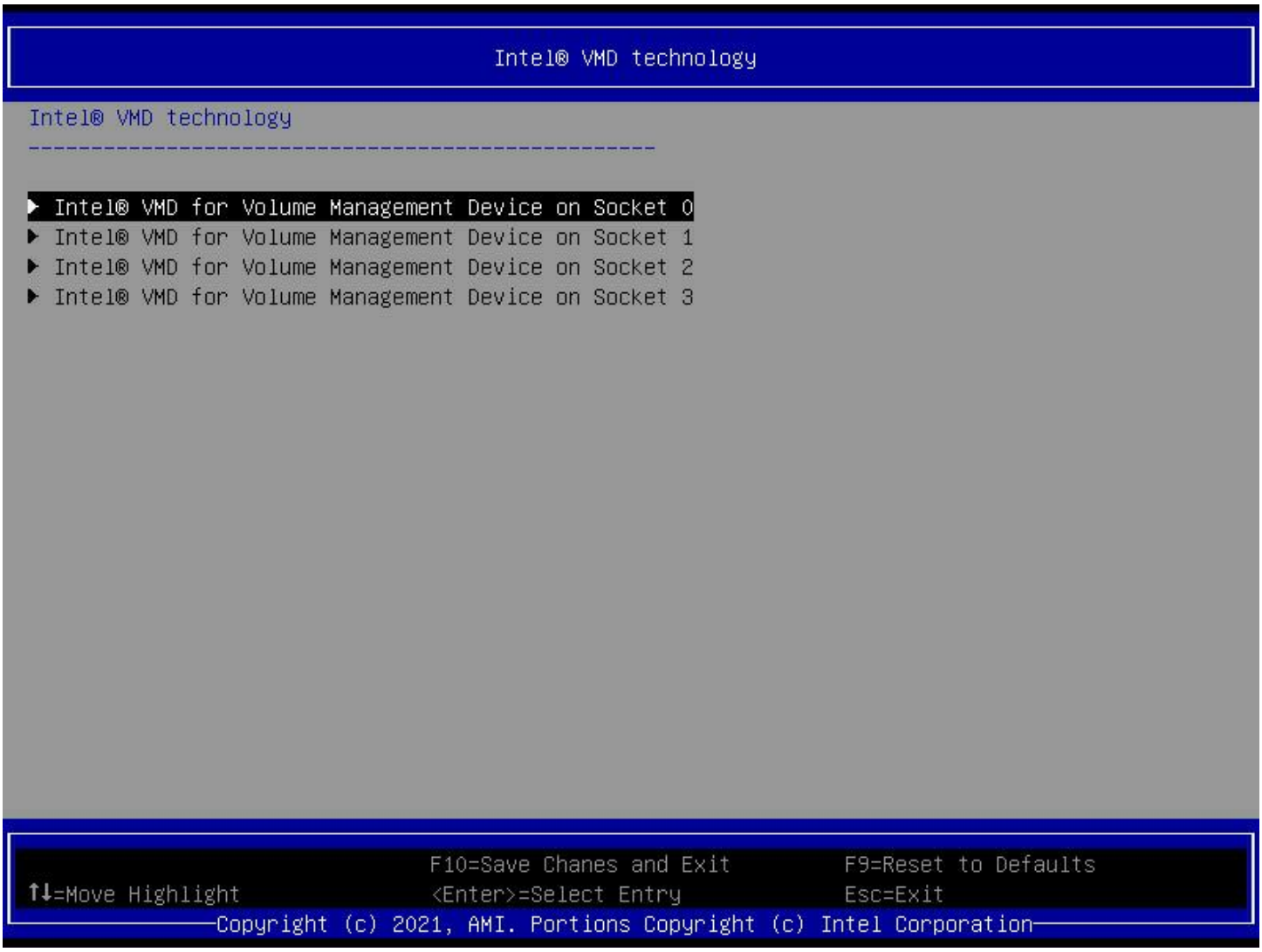

Figure 56. Intel® VMD Technology Screen

1. **Intel(R) VMD for Volume Management Device on Socket 0 / 1 / 2 / 3**

Value: None.

Help text: None.

Comments: *Selection only.*

Back to: Intel® VMD technology – IIO Configuration – Socket Configuration – Screen Map

7.4.2.1 Intel® VMD for Volume Management Device on Socket 0

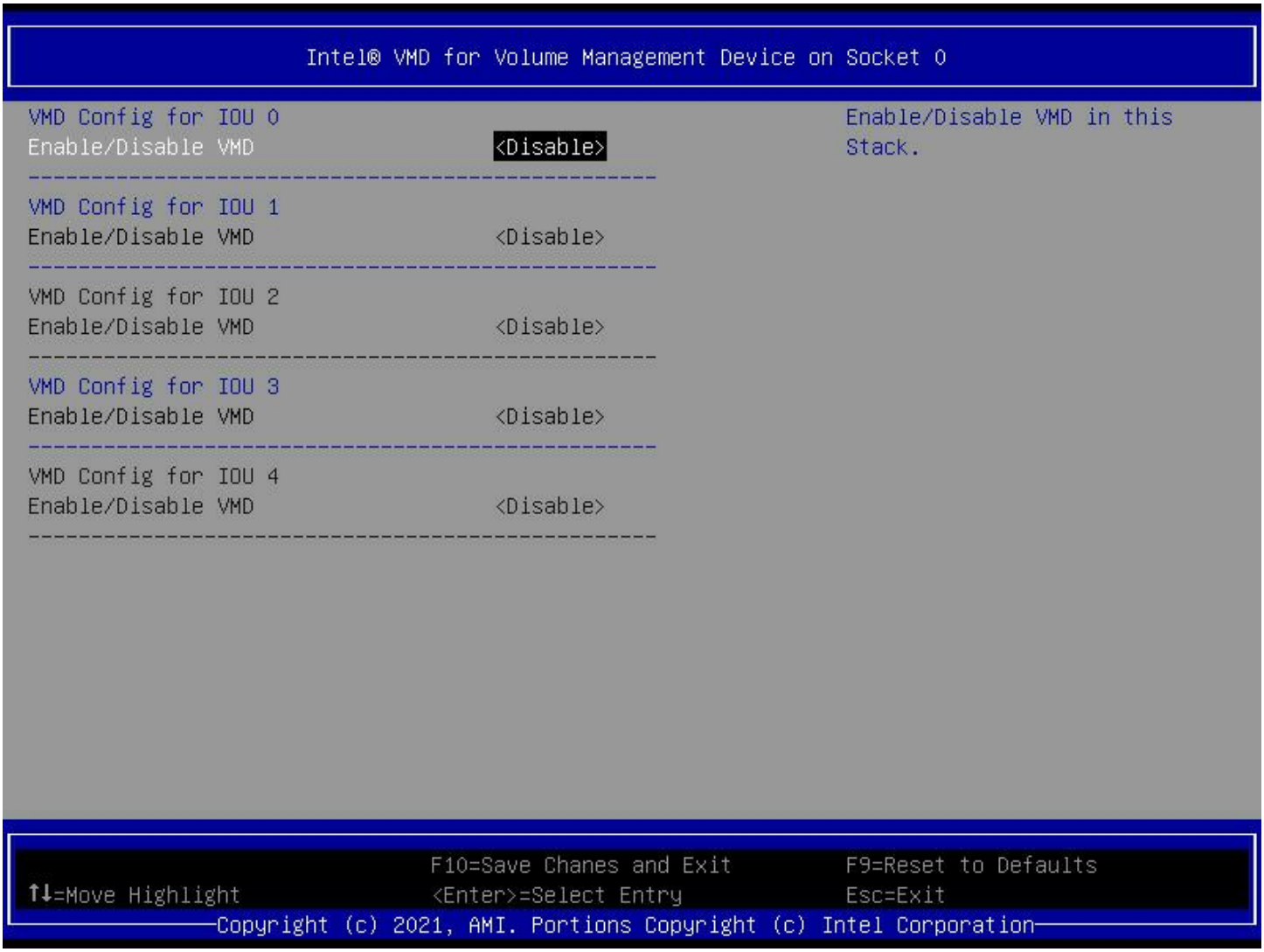

Figure 57. Intel® VMD for Volume Management Device on Socket 0 Screen

1. **VMD Config for IOU 0 / 1 / 2 / 3 / 4**

Value: Enable / **Disable**

Help text: `Enable/Disable VMD in this Stack.`

Comments: None.

Back to: **Intel® VMD for Volume Management Device on Socket 0 – Intel® VMD technology – IIO Configuration – Socket Configuration – Screen Map**

7.4.2.2 Intel® VMD for Volume Management Device on Socket 1

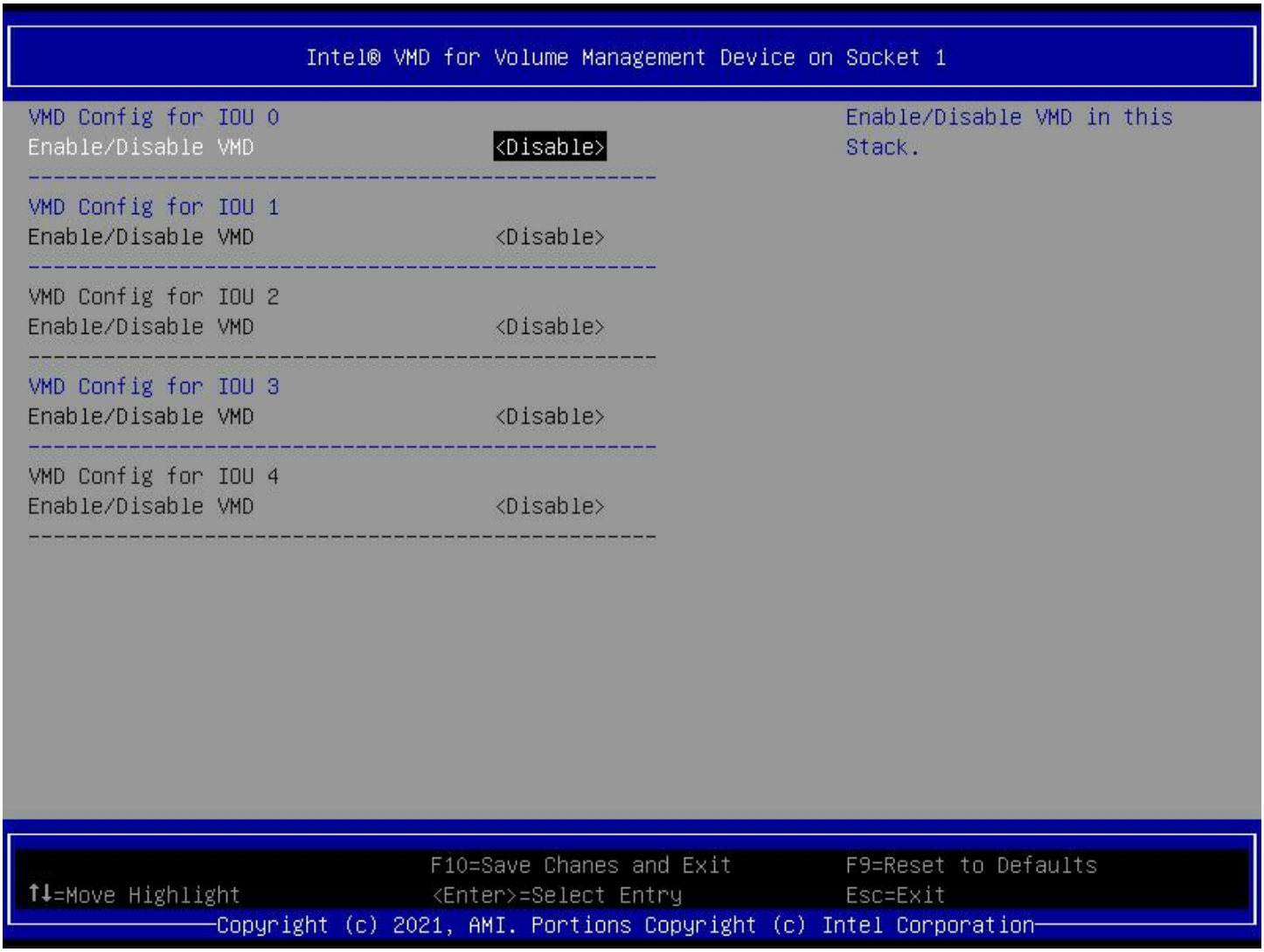

Figure 58. Intel® VMD for Volume Management Device on Socket 1 Screen

7.4.2.3 Intel® VMD for Volume Management Device on Socket 2

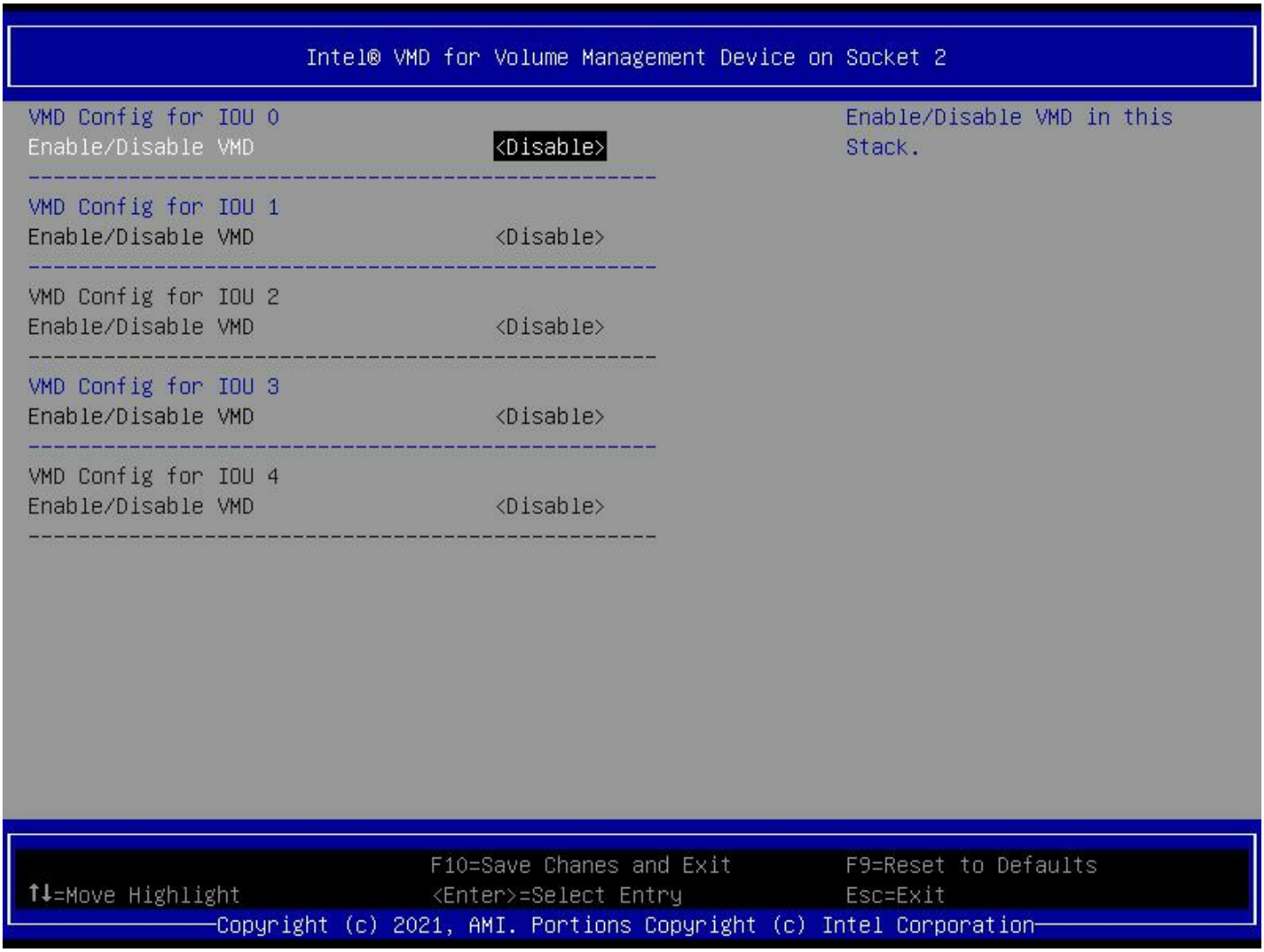

Figure 59. Intel® VMD for Volume Management Device on Socket 2 Screen

7.4.2.4 Intel® VMD for Volume Management Device on Socket 3

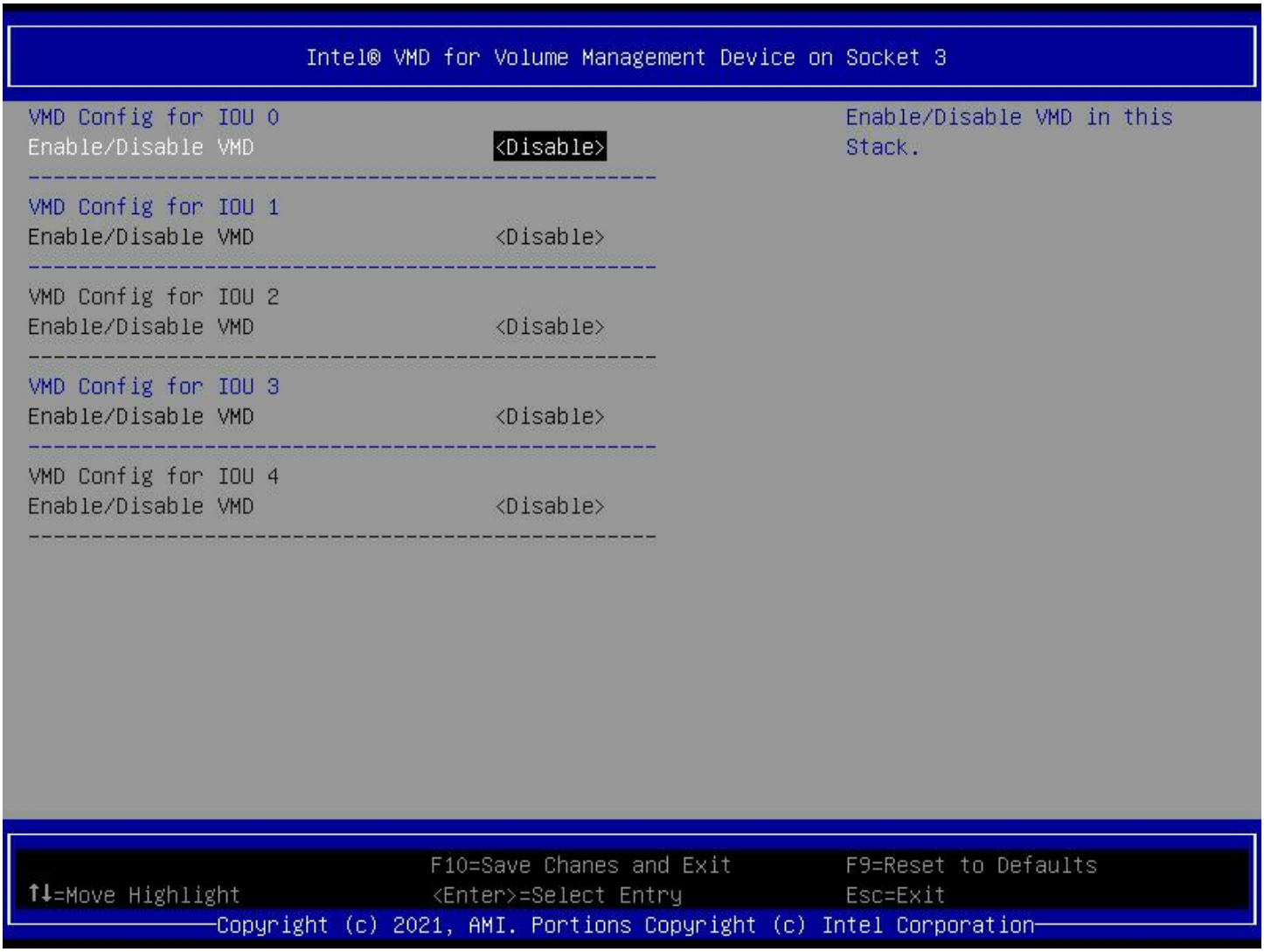

Figure 60. Intel® VMD for Volume Management Device on Socket 3 Screen

7.4.3 Intel® AIC Retimer/AIC SSD Technology (non-VMD)

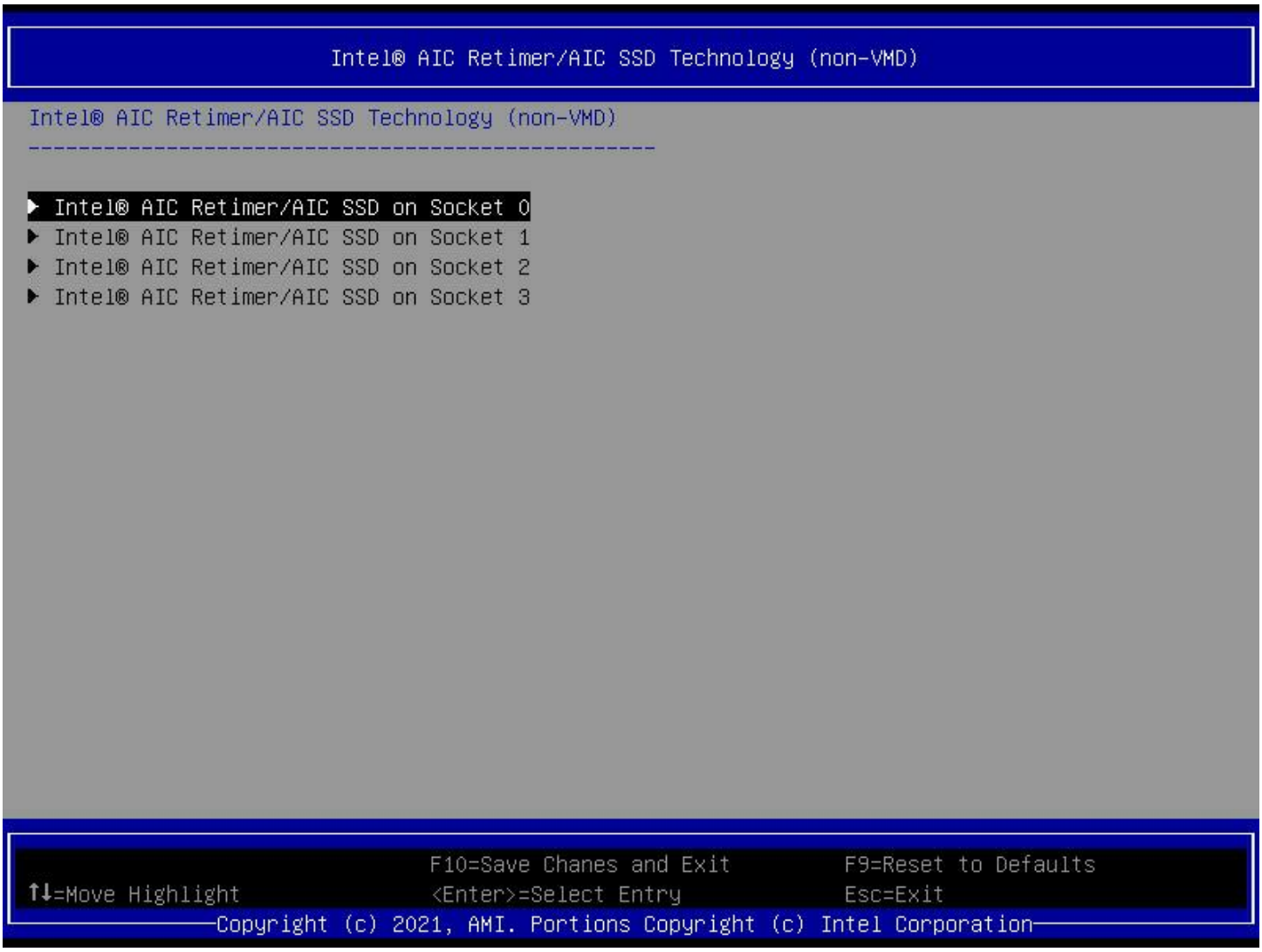

Figure 61. Intel® AIC Retimer/AIC SSD Technology (non-VMD) Screen

1. **Intel® AIC Retimer/AIC SSD on Socket 0 / 1 / 2 / 3**

Value: None.

Help text: None.

Comments: *Selection only.*

Back to: **Intel® AIC Retimer/AIC SSD Technology (non-VMD)** – **IIO Configuration** – **Socket Configuration** – **Screen Map**

7.4.3.1 Intel® AIC Retimer/AIC SSD on Socket 0

Figure 62. Intel® AIC Retimer/AIC SSD On Socket 0 Screen

1. **Intel® AIC Retimer/AIC SSD on HW at PStack0**

Value: Enable / **Disable**

Help text: `Announce Intel® AIC Retimer/AIC SSD HW at Stack0(Port1A-1D). Override IOU0 bifurcation if required.`

Comments: None.

Back to: Intel® AIC Retimer/AIC SSD on Socket 0 – Intel® AIC Retimer/AIC SSD Technology (non-VMD) – IIO Configuration – Socket Configuration – Screen Map

2. **Intel® AIC Retimer/AIC SSD on HW at PStack1**

Value: Enable / **Disable**

Help text: `Announce Intel® AIC Retimer/AIC SSD HW at Stack1(Port1A-1D). Override IOU0 bifurcation if required.`

Comments: None.

Back to: Intel® AIC Retimer/AIC SSD on Socket 0 – Intel® AIC Retimer/AIC SSD Technology (non-VMD) – IIO Configuration – Socket Configuration – Screen Map

3. Intel® AIC Retimer/AIC SSD on HW at PStack2

Value: Enable / **Disable**

Help text: `Announce Intel® AIC Retimer/AIC SSD HW at Stack2(Port2A-2D). Override IOUx bifurcation if required.`

Comments: None.

Back to: **Intel® AIC Retimer/AIC SSD on Socket 0 – Intel® AIC Retimer/AIC SSD Technology (non-VMD) – IIO Configuration – Socket Configuration – Screen Map**

7.4.3.2 Intel® AIC Retimer/AIC SSD on Socket 1

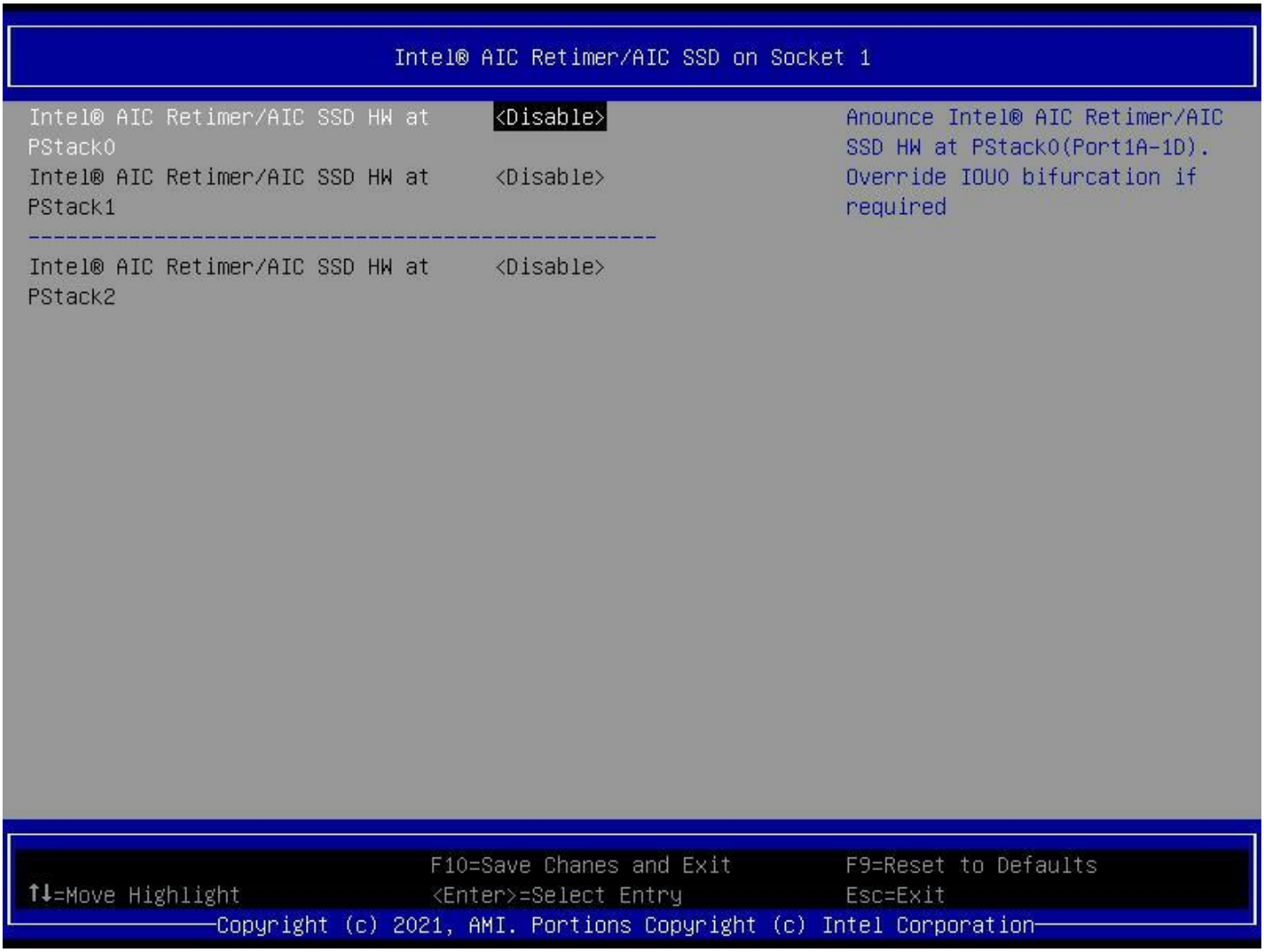

Figure 63. Intel® AIC Retimer/AIC SSD On Socket 1 Screen

Same as described in Section 7.4.3.1.

7.4.3.3 Intel® AIC Retimer/AIC SSD on Socket 2

Figure 64. Intel® AIC Retimer/AIC SSD On Socket 2 Screen

Same as described in Section 7.4.3.1.

7.4.3.4 Intel® AIC Retimer/AIC SSD on Socket 3

Figure 65. Intel® AIC Retimer/AIC SSD On Socket 3 Screen

Same as described in Section 7.4.3.1.

8. Server Mgmt

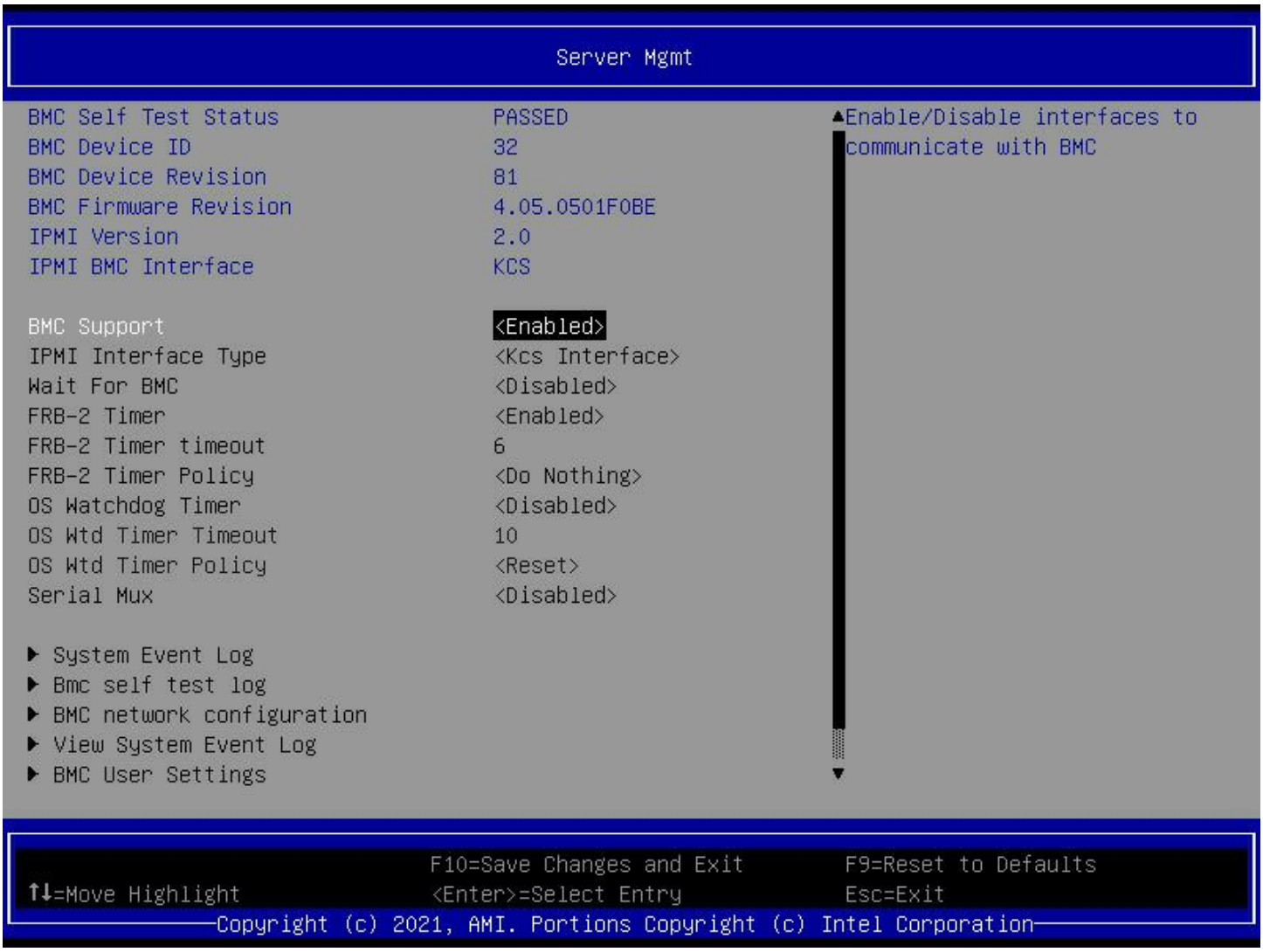

Figure 66. Server Management Screen (1)

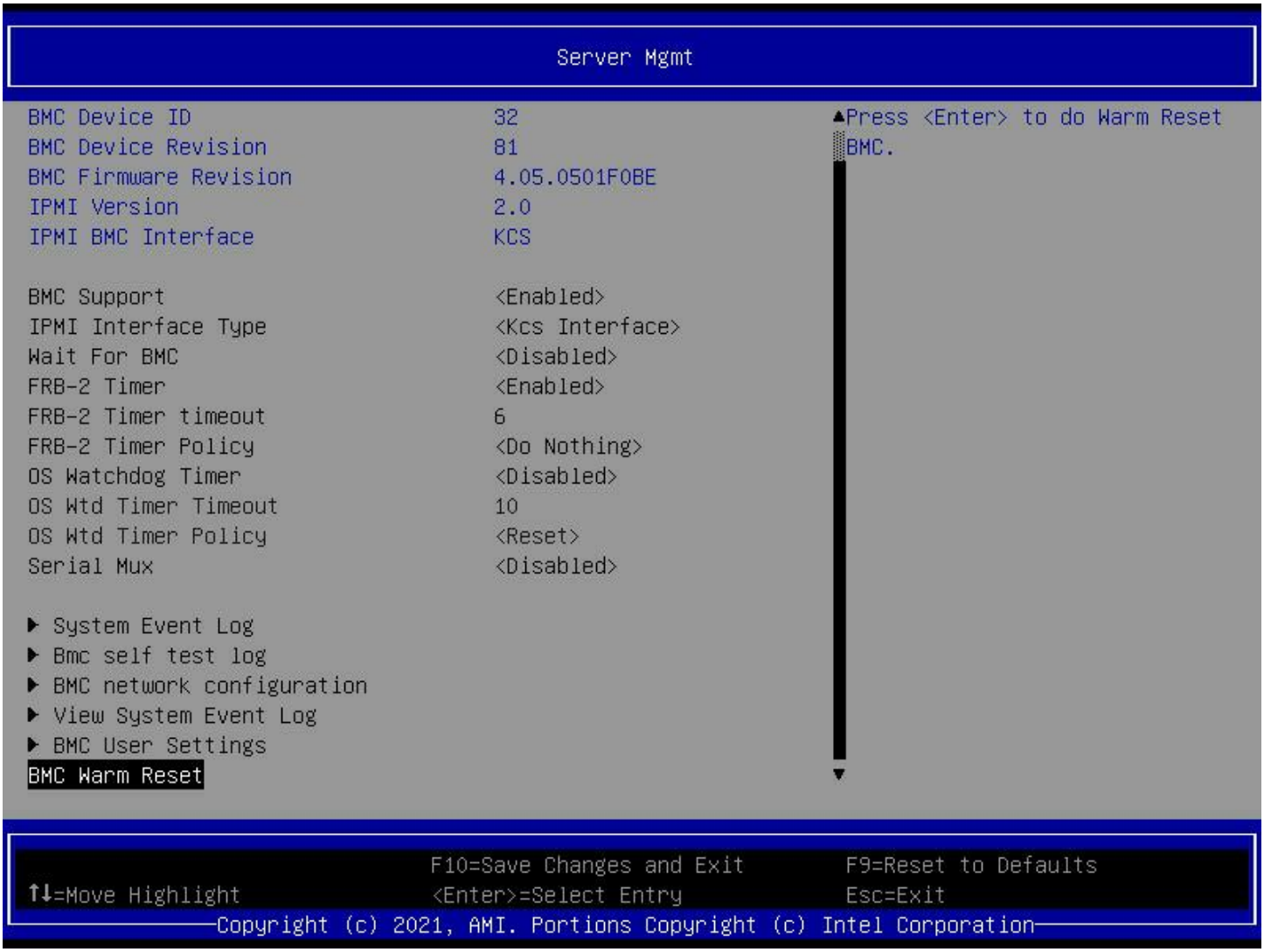

Figure 67. Server Management Screen (2)

1. BMC Support

Value: **Enabled** / Disabled

Help text: `Enable/Disable interfaces to communicate with BMC.`

Comments: None.

Back to: **Server Mgmt** – **Screen Map**

2. IPMI Interface Type

Value: <Kcs Interface> / <Bt Interface> / <Ssif Interface> / <Ipmb Interface> / <Usb Interface> / <Oem1 Interface> / <Oem2 Interface>

Help text: `Type of Interface to communicate BMC from HOST.`

Comments: None.

Back to: **Server Mgmt** – **Screen Map**

3. Wait For BMC

Value: Enabled / **Disabled**

Help text: `Wait For BMC response for specified time out. In PILOTII, BMC starts at the same time when BIOS starts during AC power ON. It takes around 30 seconds to initialize Host to BMC interfaces.`

Comments:

Note: Wait for BMC function is enabled by default, but not controlled by this option. Do not enable this knob.

Back to: **Server Mgmt – Screen Map**

4. FRB-2 Timer

Value: **Enabled** / Disabled

Help text: `Enable or Disable FRB-2 timer (POST timer).`

Comments: None.

Back to: **Server Mgmt – Screen Map**

5. FRB-2 Timer timeout

Value: 1~30

Help text: `Enter value Between 1 to 30 min for FRB-2 Timer Expiration.`

Comments: The default value is 6.

Back to: **Server Mgmt – Screen Map**

6. FRB-2 Timer Policy

Value: <**Do Nothing**> / <Reset> / <Power Down> / <Power Cycle>

Help text: `Configure how the system should respond if the FRB-2 Timer expires. Not available if FRB-2 Timer is disabled.`

Comments: None.

Back to: **Server Mgmt – Screen Map**

7. OS Watchdog Timer

Value: Enabled / **Disabled**

Help text: `If enabled, starts a BIOS timer which can only be shut off by Management Software after the OS loads. Helps determine that the OS successfully loaded or follows the OS Boot Watchdog Timer policy.`

Comments: None.

Back to: **Server Mgmt – Screen Map**

8. OS Wtd Timer Timeout

Value: 1~30

Help text: `Enter the value Between 1 to 30 min for OS Boot Watchdog Timer Expiration. Not available if OS Boot Watchdog Timer is disabled.`

Comments: None.

Back to: **Server Mgmt** – **Screen Map**

9. OS Wtd Timer Policy

Value: <**Do Nothing**> / <Reset> / <Power Down> / <Power Cycle>

Help text: `Configure how the system should respond if the OS Boot Watchdog Timer expires. Not available if OS Boot Watchdog Timer is disabled.`

Comments: None.

Back to: **Server Mgmt** – **Screen Map**

10. Serial Mux

Value: Enabled / **Disabled**

Help text: `Press <Enter> to enable or disable Serial Mux configuration.`

Comments: None.

Back to: **Server Mgmt** – **Screen Map**

11. System Event Log

Value: None.

Help text: `Press <Enter> to change the SEL event log configuration.`

Comments: *Selection only.*

Back to: **Server Mgmt** – **Screen Map**

12. Bmc self test log

Value: None.

Help text: `Logs the report returned by BMC self test command.`

Comments: *Selection only.*

Back to: **Server Mgmt** – **Screen Map**

13. BMC network configuration

Value: None.

Help text: `Configure BMC network parameters.`

Comments: *Selection only.*

Back to: **Server Mgmt** – **Screen Map**

14. View System Event Log

Value: None.

Help text: `Press <Enter> to view the System Event Log Records.`

Comments: *Selection only.*

Back to: **Server Mgmt** – **Screen Map**

15. BMC User Settings

Value: None.

Help text: `Press <Enter> to Add, Delete and Set Privilege level for users.`

Comments: *Selection only.*

Back to: **Server Mgmt** – **Screen Map**

16. BMC Warm Reset

Value: None.

Help text: `Press <Enter> to do Warm Reset BMC.`

Comments: *Selection only.*

Back to: **Server Mgmt** – **Screen Map**

8.1 System Event Log

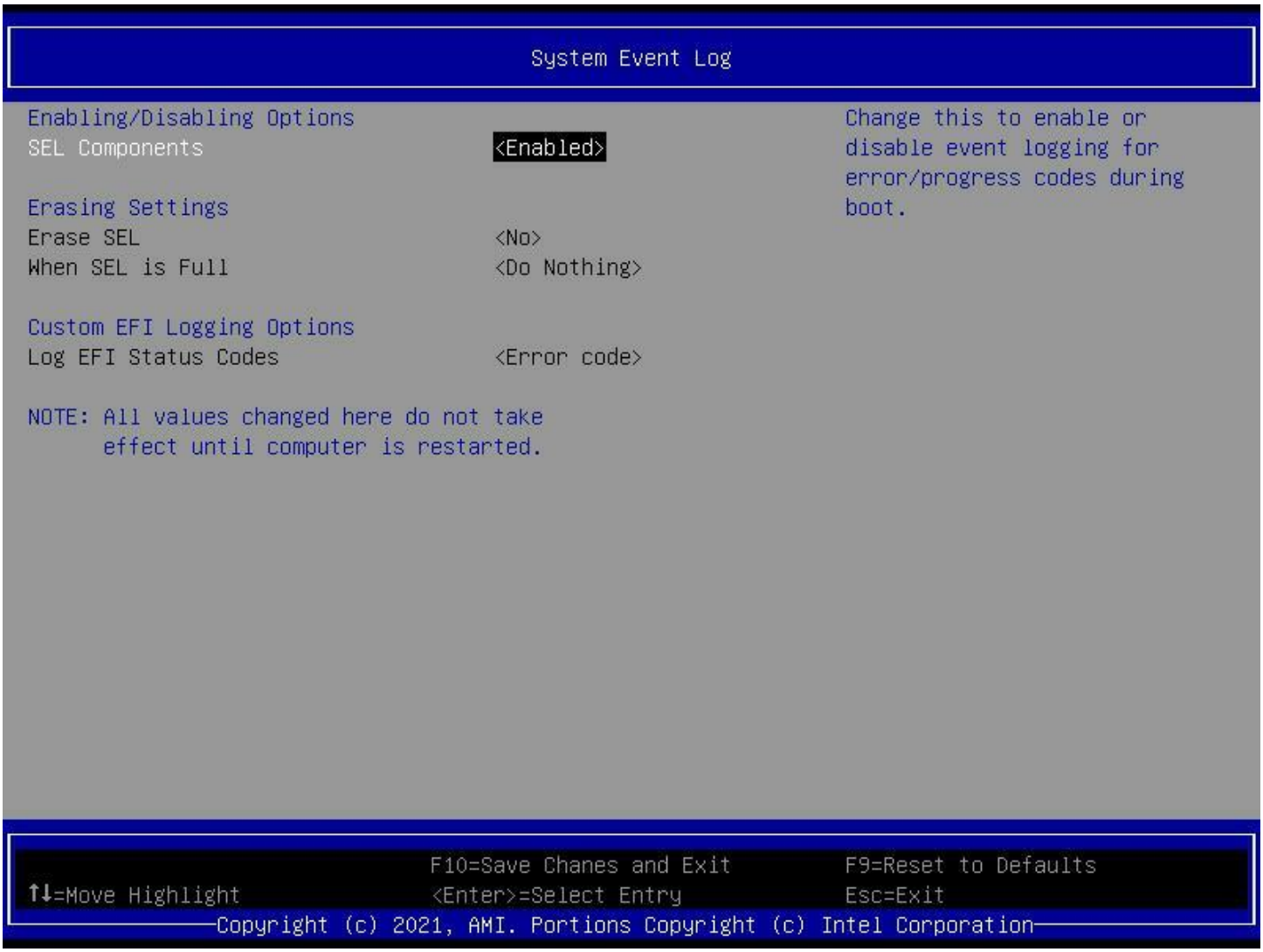

Figure 68. System Event Log Screen

1. SEL Components

Value: **Enabled** / Disabled

Help text: `Change this to enable or disable event logging for error/progress codes during boot.`

Comments: None.

Back to: System Event Log – Server Mgmt – Screen Map

2. Erase SEL

Value: <**No**> / <Yes, On next reset> / <Yes, On every reset>

Help text: `Choose options for erasing SEL.`

Comments: None.

Back to: System Event Log – Server Mgmt – Screen Map

3. When SEL is Full

Value: <**Do Nothing**> / <Erase Immediately> / <Delete Oldest Record>

Help text: `Choose options for reactions to a full SEL.`

Comments: None.

Back to: **System Event Log** – **Server Mgmt** – **Screen Map**

4. Log EFI Status Codes

Value: <Disabled> / <**Error code**> / <Progress code> / <Both>

Help text: `Disable the logging of EFI Status Codes or log only error code or only progress code or both.`

Comments: None.

Back to: **System Event Log** – **Server Mgmt** – **Screen Map**

8.2 Bmc self test log

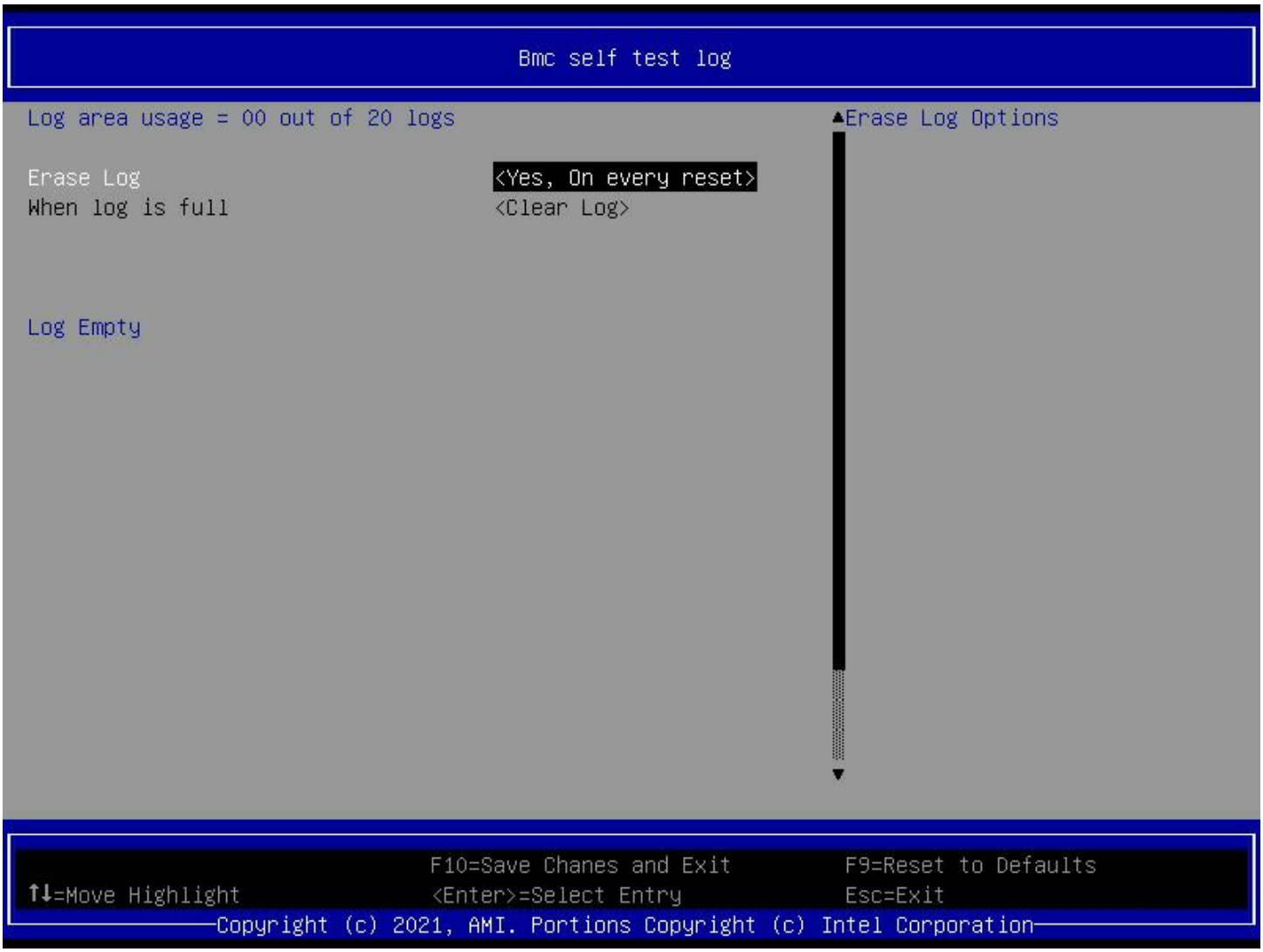

Figure 69. BMC Self-Test Log Screen

1. Erase Log

Value: <**Yes, On every reset**> / <No>

Help text: `Erase Log Options.`

Comments: None.

Back to: **Bmc self test log – Server Mgmt – Screen Map**

2. When log is full

Value: <Clear Log> / <Do not log any more>

Help text: `Select the action to be taken when log is full.`

Comments: None.

Back to: **Bmc self test log – Server Mgmt – Screen Map**

8.3 BMC network configuration

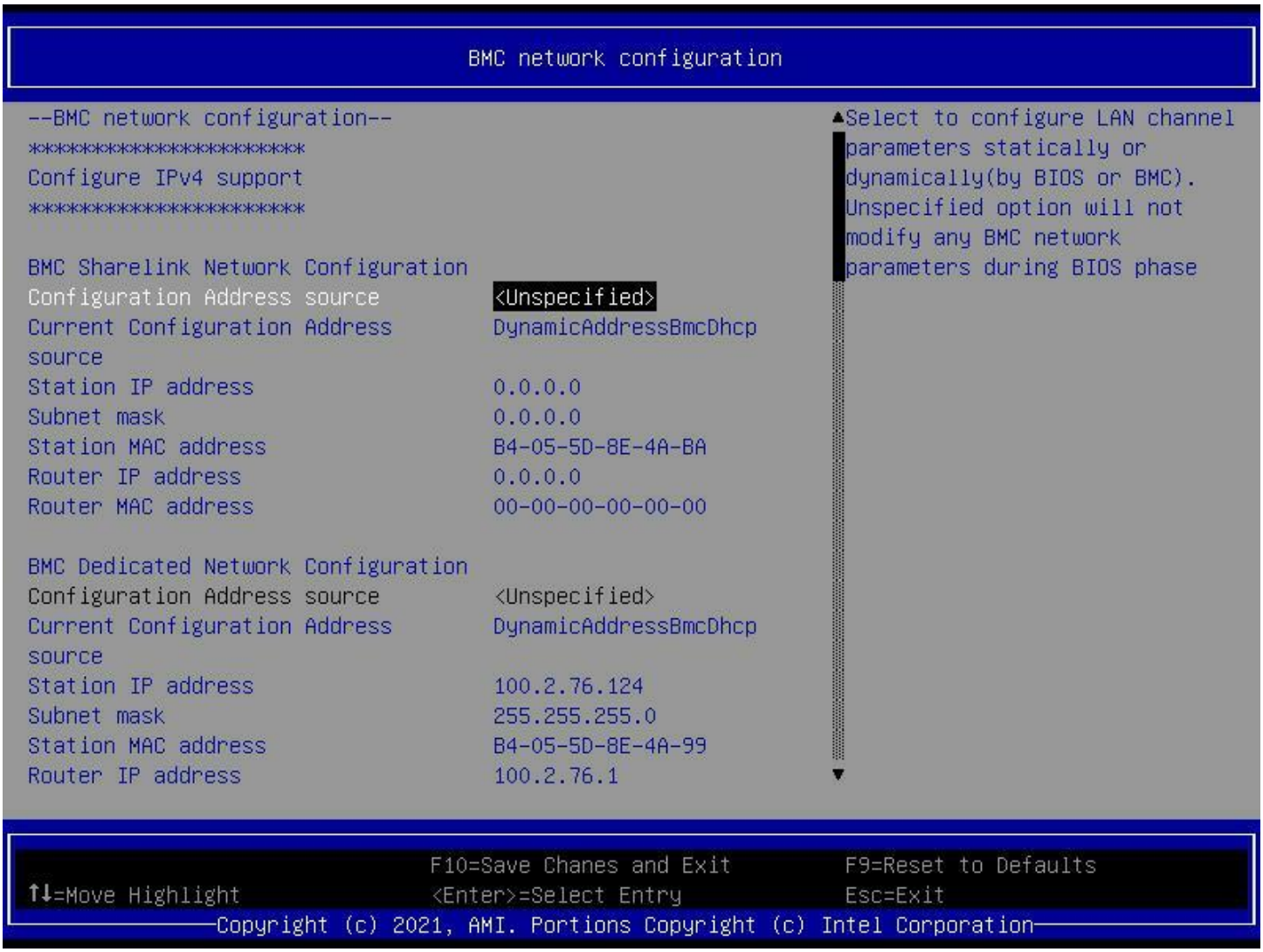

Figure 70. BMC Network Configuration Screen (1)

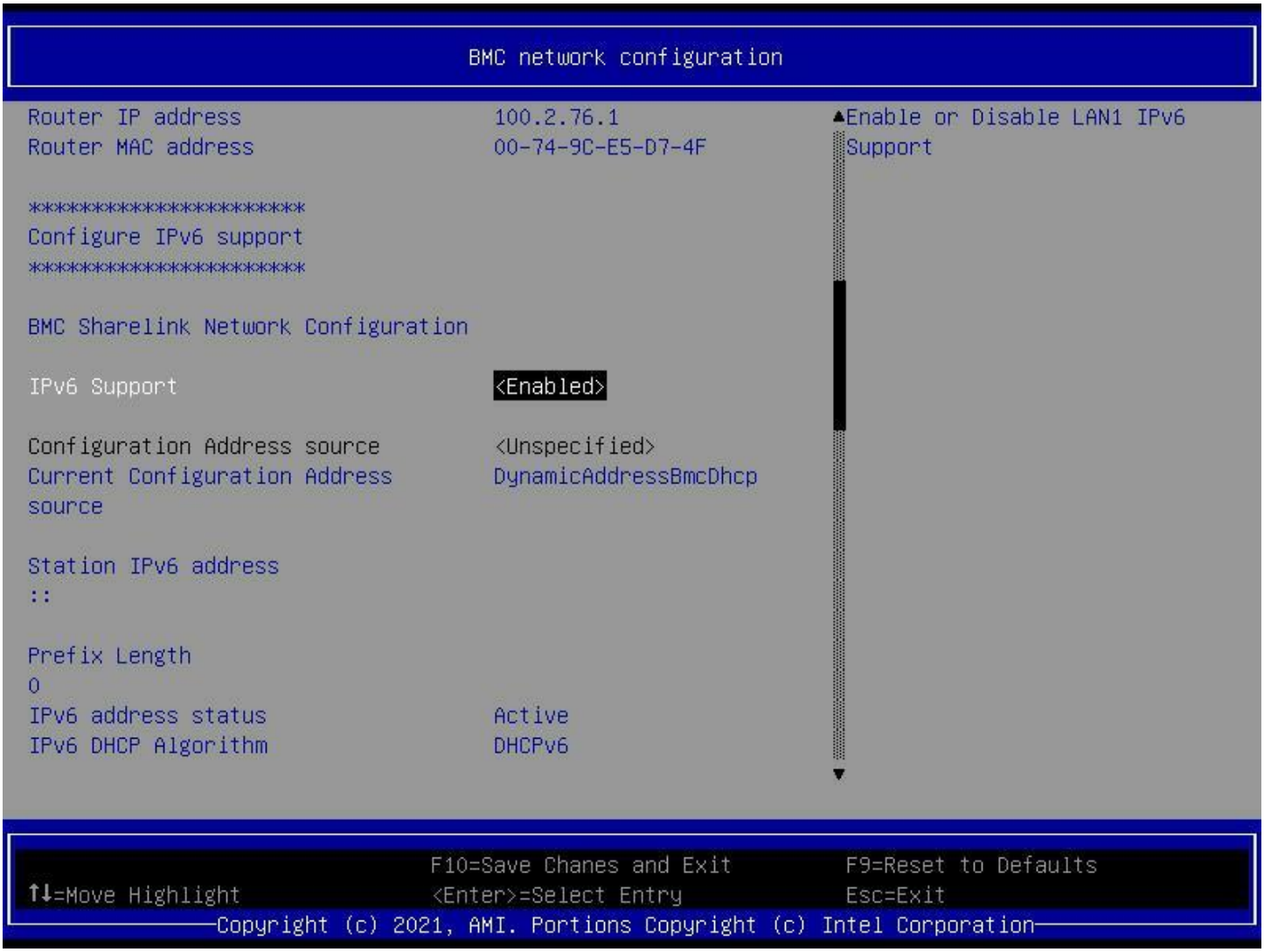

Figure 71. BMC Network Configuration Screen (2)

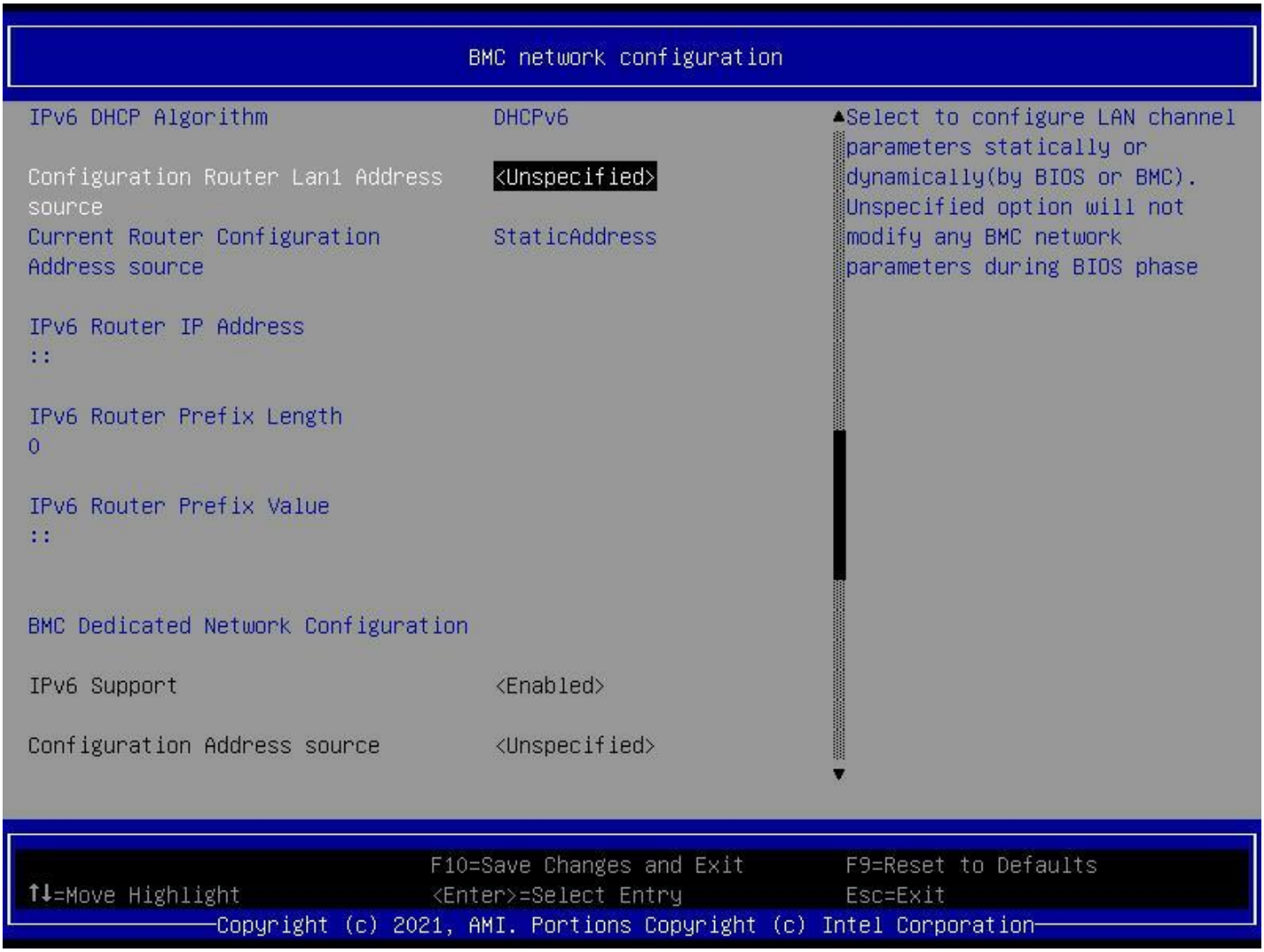

Figure 72. BMC Network Configuration Screen (3)

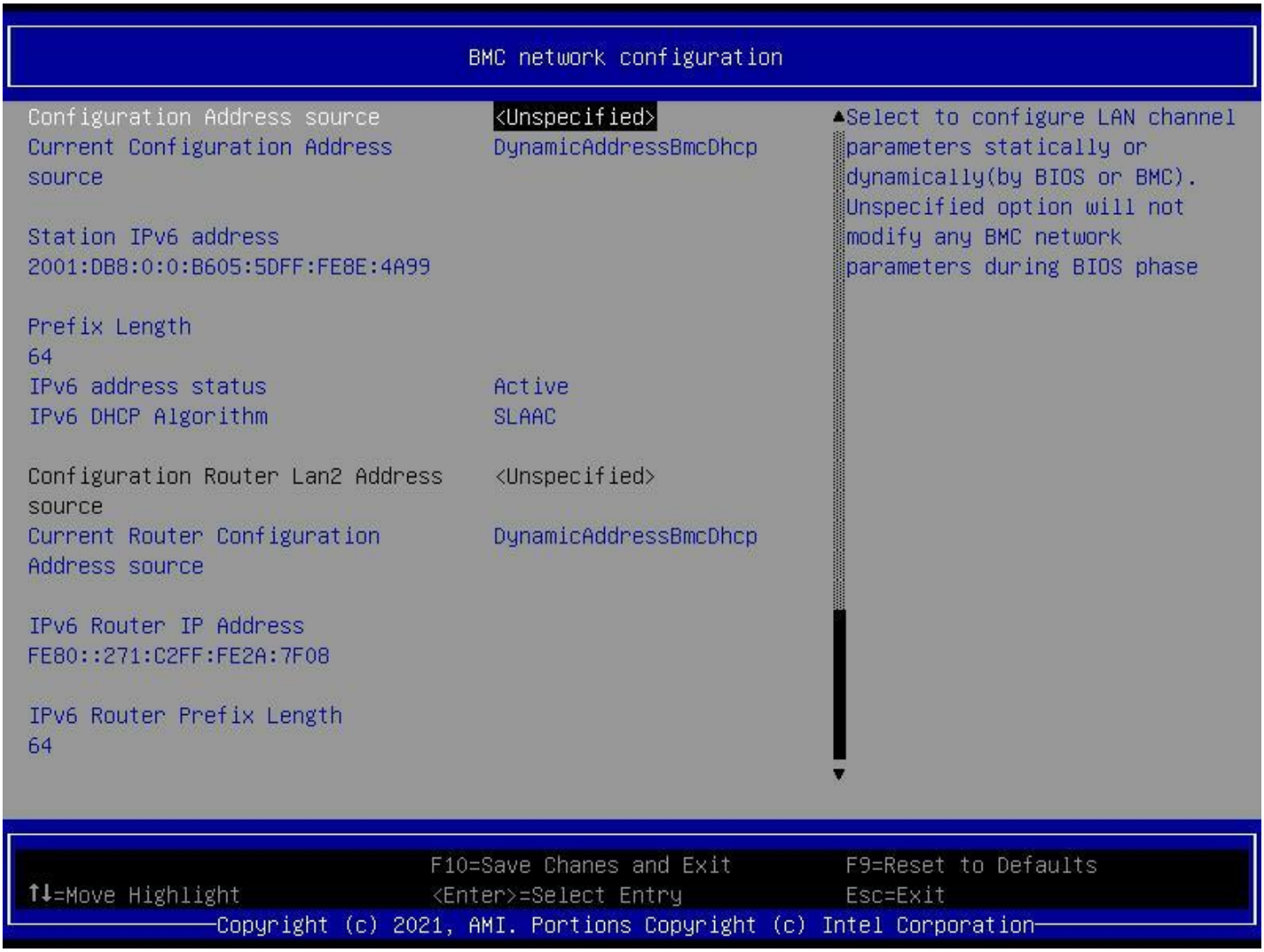

Figure 73. BMC Network Configuration Screen (4)

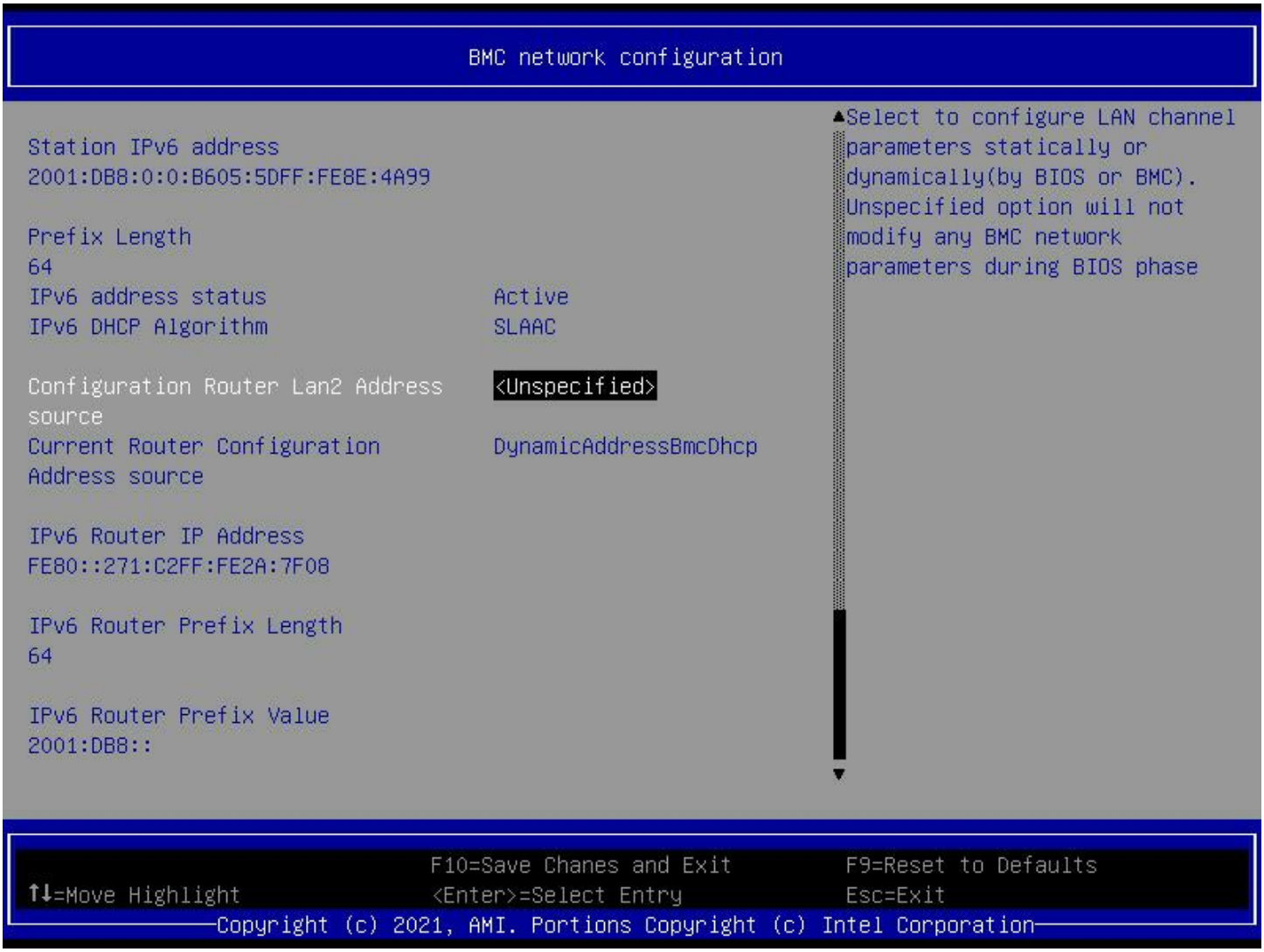

Figure 74. BMC Network Configuration Screen (5)

1. Configuration Address source

Value: **Unspecified** / Static / DynamicBmcDhcp / DynamicBmcNonDhcp

Help text: `Select to configure LAN channel parameters statically or dynamically (by BIOS or BMC). Unspecified option will not modify any BMC network parameters during BIOS phase.`

Comments: None.

Back to: **BMC network configuration** – **Server Mgmt** – **Screen Map**

2. Current Configuration Address source

Value: <current configuration address source>

Help text: `Current LAN Configuration statically or dynamically (by BIOS or BMC). Unspecified for not Configured address space.`

Comments: *Information only.* Invisible if the configuration address source option is set as static.

Back to: **BMC network configuration** – **Server Mgmt** – **Screen Map**

3. Station IP address

Value: <station IP address>

Help text: `Station IP address from BMC.`

Comments: *Information only.* Invisible if the configuration address source option is set as static.

Back to: **BMC network configuration** – **Server Mgmt** – **Screen Map**

4. Subnet Mask

Value: <subnet mask>

Help text: `Subnet mask from BMC.`

Comments: *Information only.* Invisible if the configuration address source option is set as static.

Back to: **BMC network configuration** – **Server Mgmt** – **Screen Map**

5. Station MAC address

Value: <station MAC address>

Help text: `Station MAC address from BMC.`

Comments: *Information only.* Invisible if the configuration address source option is set as static.

Back to: **BMC network configuration** – **Server Mgmt** – **Screen Map**

6. Router IP address

Value: <router IP address>

Help text: None.

Comments: *Information only.* Invisible if the configuration address source option is set as static.

Back to: **BMC network configuration** – **Server Mgmt** – **Screen Map**

7. Router MAC address

Value: <router MAC address>

Help text: `Router MAC address from BMC.`

Comments: *Information only.* Invisible if the configuration address source option is set as static.

Back to: **BMC network configuration** – **Server Mgmt** – **Screen Map**

8. Configuration Address source

Value: **Unspecified** / Static / DynamicBmcDhcp / DynamicBmcNonDhcp

Help text: `Select to configure LAN channel parameters statically or dynamically (by BIOS or BMC). Unspecified option will not modify any BMC network parameters during BIOS phase.`

Comments: None.

Back to: **BMC network configuration** – **Server Mgmt** – **Screen Map**

9. Current Configuration Address source

Value: <current configuration address source>

Help text: `Current LAN Configuration statically or dynamically (by BIOS or BMC). Unspecified for not Configured address space.`

Comments: *Information only.* Invisible if the configuration address source option is set as static.

Back to: **BMC network configuration** – **Server Mgmt** – **Screen Map**

10. Station IP address

Value: <station IP address>

Help text: `Station IP address from BMC.`

Comments: *Information only.* Invisible if the configuration address source option is set as static.

Back to: **BMC network configuration** – **Server Mgmt** – **Screen Map**

11. Subnet Mask

Value: <subnet mask>

Help text: `Subnet mask from BMC.`

Comments: *Information only.* Invisible if the configuration address source option is set as static.

Back to: **BMC network configuration** – **Server Mgmt** – **Screen Map**

12. Station MAC address

Value: <station MAC address>

Help text: `Station MAC address from BMC.`

Comments: *Information only.* Invisible if the configuration address source option is set as static.

Back to: **BMC network configuration** – **Server Mgmt** – **Screen Map**

13. Router IP address

Value: <router IP address>

Help text: None.

Comments: *Information only.* Invisible if the configuration address source option is set as static.

Back to: **BMC network configuration** – **Server Mgmt** – **Screen Map**

14. Router MAC address

Value: <router MAC address>

Help text: `Router MAC address from BMC.`

Comments: *Information only.* Invisible if the configuration address source option is set as static.

Back to: **BMC network configuration** – **Server Mgmt** – **Screen Map**

15. IPv6 support (IPv6 support)

Value: **Enabled** / Disabled

Help text: `Enable or Disable LAN1 IPv6 Support.`

Comments: None.

Back to: **BMC network configuration – Server Mgmt – Screen Map**

16. Configuration Address source (IPv6 support)

Value: **Unspecified** / Static / DynamicBmcDhcp

Help text: `Select to configure LAN channel parameters statically or dynamically (by BIOS or BMC). Unspecified option will not modify any BMC network parameters during BIOS phase.`

Comments: None.

Back to: **BMC network configuration – Server Mgmt – Screen Map**

17. Current Configuration Address source (IPv6 support)

Value: <current configuration address source>

Help text: `Current LAN Configuration statically or dynamically (by BIOS or BMC). Unspecified for not Configured address space.`

Comments: *Information only.* Invisible if the configuration address source option is set as static.

Back to: **BMC network configuration – Server Mgmt – Screen Map**

18. Station IPv6 address (IPv6 support)

Value: <station IPv6 address>

Help text: `Enter station IPv6 address.`

Comments: None.

Back to: **BMC network configuration – Server Mgmt – Screen Map**

19. Prefix Length (IPv6 support)

Value: <prefix length>

Help text: `Change the IPv6 Router Prefix Length.`

Comments: None.

Back to: **BMC network configuration – Server Mgmt – Screen Map**

20. IPv6 address status (IPv6 support)

Value: <IPv6 address status>

Help text: `Status of station IPv6 address to BMC.`

Comments: *Information only.*

Back to: **BMC network configuration – Server Mgmt – Screen Map**

21. IPv6 DHCP Algorithm (IPv6 support)

Value: <IPv6 DHCP algorithm>

Help text: `Providing the DHCP method used like DHCPv6 or StateLess Address Auto Configuration (SLAAC).`

Comments: *Information only.*

Back to: **BMC network configuration** – **Server Mgmt** – **Screen Map**

22. Configuration Router Lan1 Address source (IPv6 support)

Value: **Unspecified** / Static / DynamicBmcDhcp

Help text: `Select to configure LAN channel parameters statically or dynamically (by BIOS or BMC). Unspecified option will not modify any BMC network parameters during BIOS phase.`

Comments: None.

Back to: **BMC network configuration** – **Server Mgmt** – **Screen Map**

23. Current Router Configuration Address source (Configuration Router Lan1 Address source)

Value: <current router configuration address source>

Help text: `Current IPv6 Router LAN Configuration statically or dynamically by BMC). Unspecified for not Configured address space.`

Comments: *Information only.*

Back to: **BMC network configuration** – **Server Mgmt** – **Screen Map**

24. IPv6 Router IP address

Value: <IPv6 router IP address>

Help text: None.

Comments: *Information only.*

Back to: **BMC network configuration** – **Server Mgmt** – **Screen Map**

25. IPv6 Router Prefix Length (Configuration Router Lan1 Address source)

Value: <IPv6 Router Prefix Length>

Help text: None.

Comments: *Information only.*

Back to: **BMC network configuration** – **Server Mgmt** – **Screen Map**

26. IPv6 Router Prefix Value (Configuration Router Lan1 Address source)

Value: <IPv6 Router Prefix Value>

Help text: None.

Comments: *Information only.*

Back to: **BMC network configuration** – **Server Mgmt** – **Screen Map**

27. Configuration Address source (IPv6 support)

Value: **Unspecified** / Static / DynamicBmcDhcp

Help text: `Select to configure LAN channel parameters statically or dynamically (by BIOS or BMC). Unspecified option will not modify any BMC network parameters during BIOS phase.`

Comments: None.

Back to: **BMC network configuration – Server Mgmt – Screen Map**

28. Current Configuration Address source (IPv6 support)

Value: <current configuration address source>

Help text: `Current LAN Configuration statically or dynamically (by BIOS or BMC). Unspecified for not Configured address space.`

Comments: *Information only.* Invisible if the configuration address source option is set as static.

Back to: **BMC network configuration – Server Mgmt – Screen Map**

29. Station IPv6 address (IPv6 support)

Value: <station IPv6 address>

Help text: `Enter station IPv6 address.`

Comments: None.

Back to: **BMC network configuration – Server Mgmt – Screen Map**

30. Prefix Length (IPv6 support)

Value: <prefix length>

Help text: `Change the IPv6 Router Prefix Length.`

Comments: None.

Back to: **BMC network configuration – Server Mgmt – Screen Map**

31. IPv6 address status (IPv6 support)

Value: <IPv6 address status>

Help text: `Status of station IPv6 address to BMC.`

Comments: *Information only.*

Back to: **BMC network configuration – Server Mgmt – Screen Map**

32. IPv6 DHCP Algorithm (IPv6 support)

Value: <IPv6 DHCP algorithm>

Help text: `Providing the DHCP method used like DHCPv6 or StateLess Address Auto Configuration (SLAAC).`

Comments: *Information only.*

Back to: **BMC network configuration – Server Mgmt – Screen Map**

33. Configuration Router Lan2 Address source (IPv6 support)

Value: **Unspecified** / Static / DynamicBmcDhcp

Help text: `Select to configure LAN channel parameters statically or dynamically (by BIOS or BMC). Unspecified option will not modify any BMC network parameters during BIOS phase.`

Comments: None.

Back to: **BMC network configuration – Server Mgmt – Screen Map**

34. Current Router Configuration Address source (Configuration Router Lan2 Address source)

Value: <current router configuration address source>

Help text: `Current IPv6 Router LAN Configuration statically or dynamically by BMC). Unspecified for not Configured address space.`

Comments: *Information only.*

Back to: **BMC network configuration – Server Mgmt – Screen Map**

35. IPv6 Router IP address (Configuration Router Lan2 Address source)

Value: <IPv6 router IP address>

Help text: None.

Comments: *Information only.*

Back to: **BMC network configuration – Server Mgmt – Screen Map**

36. IPv6 Router Prefix Length (Configuration Router Lan2 Address source)

Value: <IPv6 Router Prefix Length>

Help text: None.

Comments: *Information only.*

Back to: **BMC network configuration – Server Mgmt – Screen Map**

37. IPv6 Router Prefix Value (Configuration Router Lan2 Address source)

Value: <IPv6 Router Prefix Value>

Help text: None.

Comments: *Information only.*

Back to: **BMC network configuration – Server Mgmt – Screen Map**

8.4 BMC User Settings

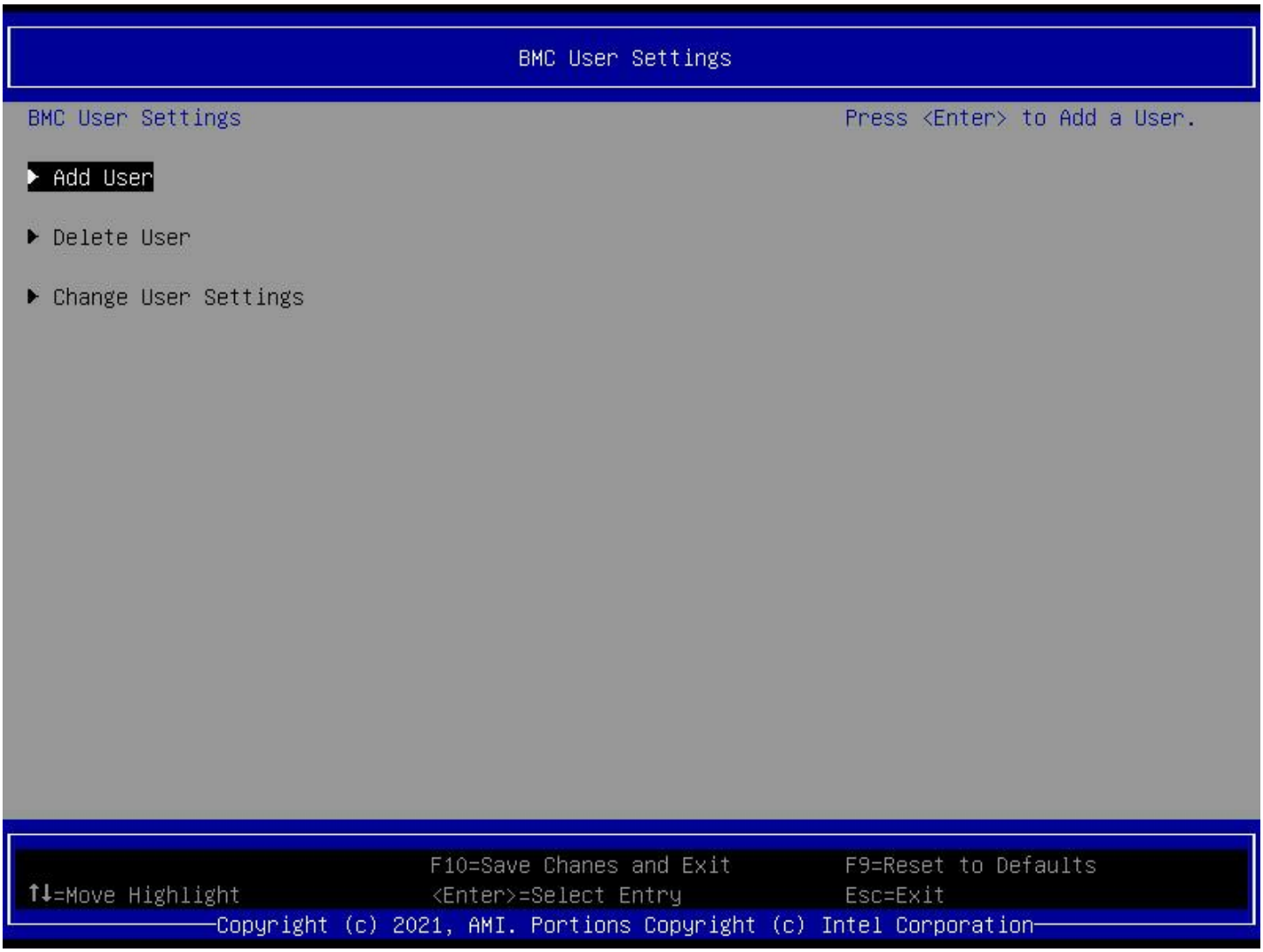

Figure 75. BMC User Settings Screen

1. Add User

Value: None.

Help text: `Press <Enter> to Add a User.`

Comments: *Selection only.*

Back to: **BMC User Settings – Server Mgmt – Screen Map**

2. Delete User

Value: None.

Help text: `Press <Enter> to Delete a User.`

Comments: *Selection only.*

Back to: **BMC User Settings – Server Mgmt – Screen Map**

3. Change User Settings

Value: None.

Help text: `Press <Enter> to Change User Settings.`

Comments: *Selection only.*

Back to: **BMC User Settings – Server Mgmt – Screen Map**

8.4.1 Add User

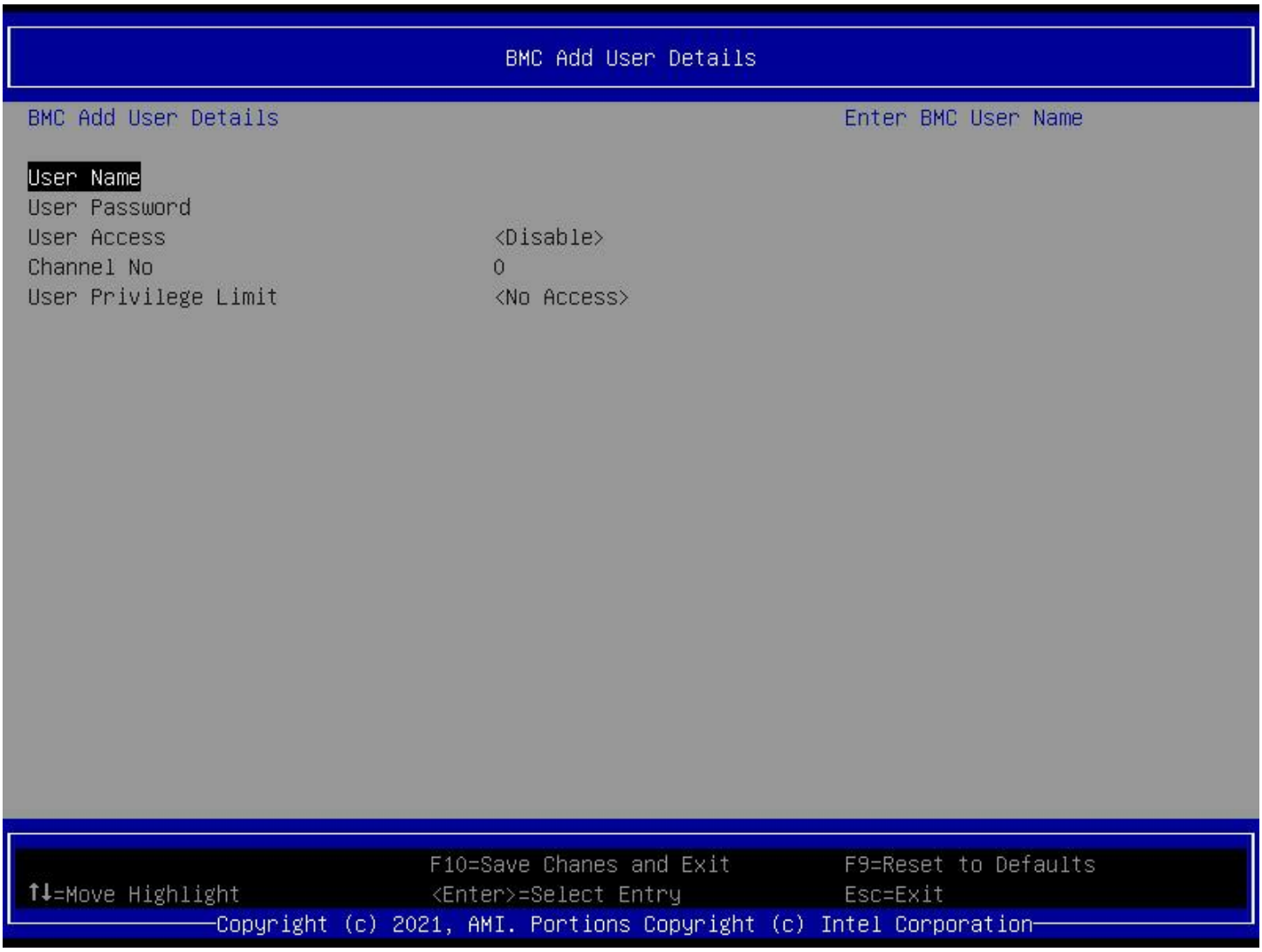

Figure 76. BMC Add User Details Screen

1. User Name

Value: None.

Help text: `Enter BMC User Name.`

Comments: *Selection only.* Username is a string of 1–16 alphanumeric characters, or '_', or '-'. This string must begin with an alphanumeric character.

Back to: **Add User** – **BMC User Settings** – **Server Mgmt** – **Screen Map**

2. User Password

Value: None.

Help text: `Enter BMC User Password.`

Comments: *Selection only.* Minimum length is 1 character. Maximum length is 20 characters. Any ASCII printable characters can be used: case-sensitive alphabetical, numeric, and special characters.

Note: The password entered overrides any previously set password.

Back to: **Add User – BMC User Settings – Server Mgmt – Screen Map**

3. User Access

Value: Enable / **Disable**

Help text: `Enable/Disable the BMC User's Access.`

Comments: None.

Back to: **Add User – BMC User Settings – Server Mgmt – Screen Map**

4. Channel No

Value: <1~15>

Help text: `Enter BMC Channel Number.`

Comments: None.

Back to: **Add User – BMC User Settings – Server Mgmt – Screen Map**

5. User Privilege Limit

Value: **<No Access>** / <Callback> / <User> / <Operator> / <Administrator> / <OEM Proprietary>

Help text: `Enter BMC User Privilege Limit for Selected Channel.`

Comments: Visible options may vary depending on BMC settings.

Back to: **Add User – BMC User Settings – Server Mgmt – Screen Map**

8.4.2 Delete User

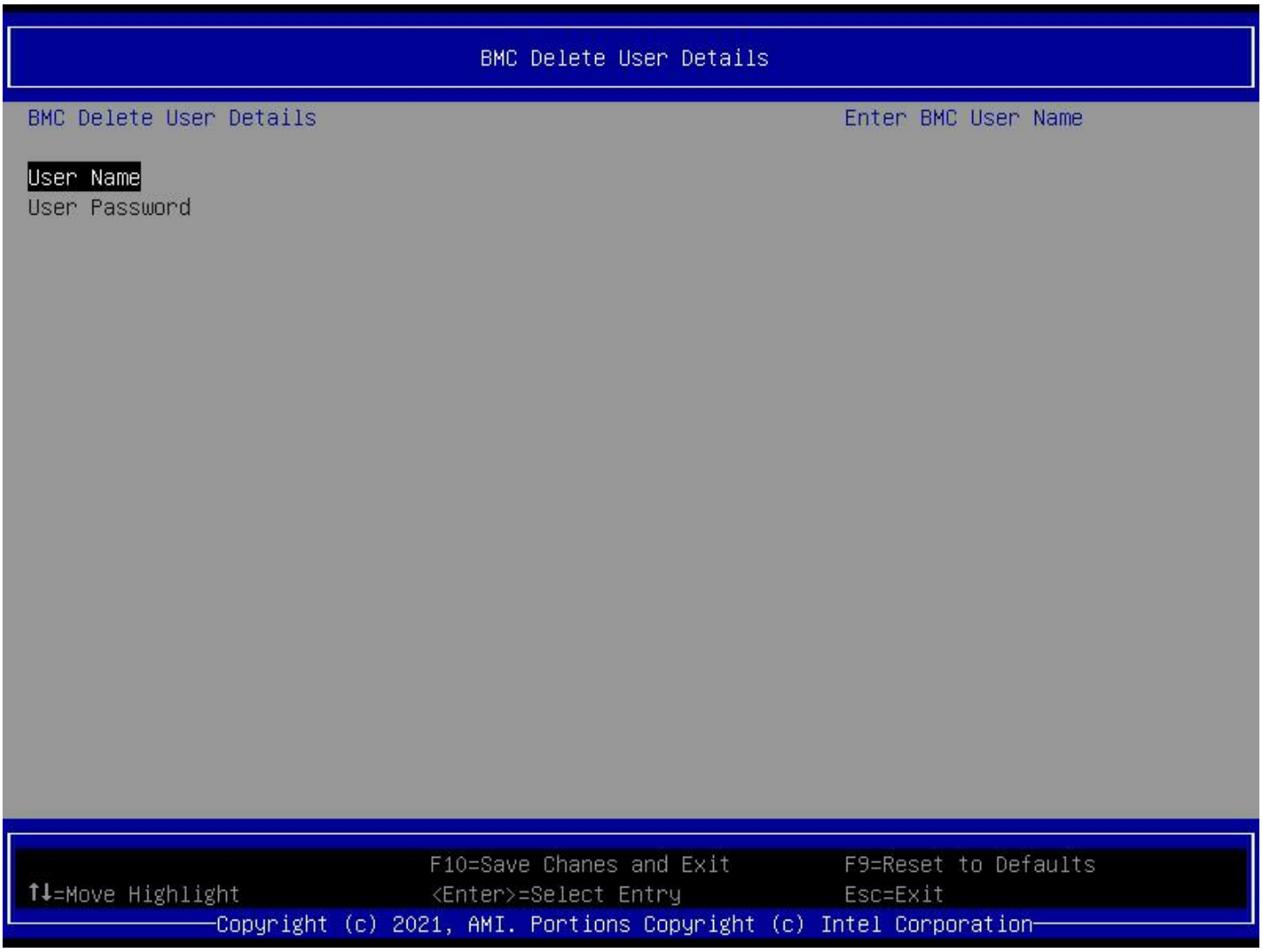

Figure 77. BMC Delete User Details Screen

1. User Name

Value: None.

Help text: `Enter BMC User Name.`

Comments: *Selection only.*

Back to: **Delete User** – **BMC User Settings** – **Server Mgmt** – **Screen Map**

2. User Password

Value: None.

Help text: `Enter BMC User Password.`

Comments: *Selection only.*

Back to: **Delete User** – **BMC User Settings** – **Server Mgmt** – **Screen Map**

8.4.3 Change User Settings

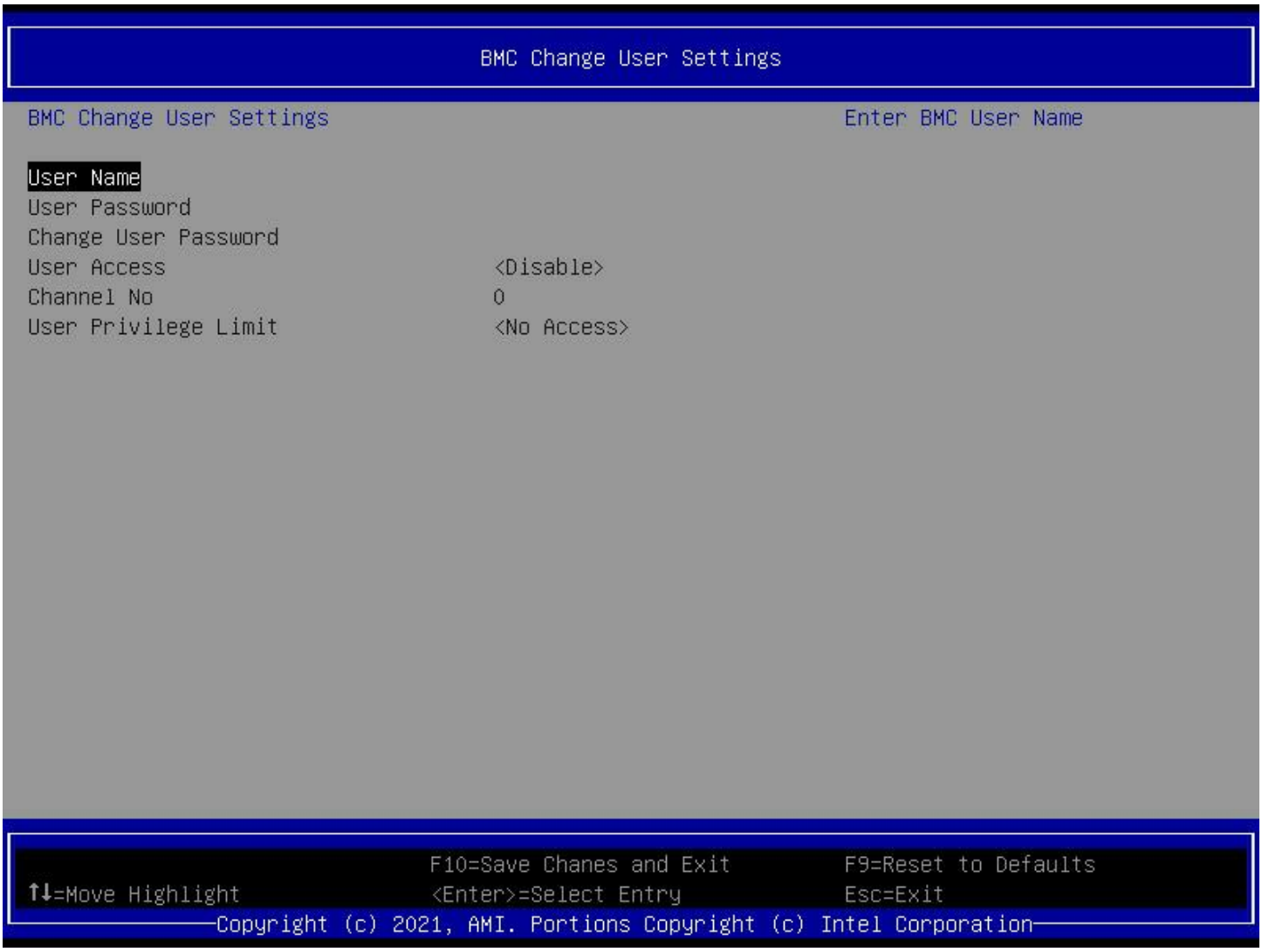

Figure 78. BMC Change User Settings Screen

1. User Name

Value: None.

Help text: `Enter BMC User Name.`

Comments: *Selection only.*

Back to: **Change User Settings** – **BMC User Settings** – **Server Mgmt** – **Screen Map**

2. User Password

Value: None.

Help text: `Enter BMC User Password.`

Comments: *Selection only.*

Back to: **Change User Settings** – **BMC User Settings** – **Server Mgmt** – **Screen Map**

3. Change User Password

Value: None.

Help text: `Enter New Password to change.`

Comments: *Selection only.*

Back to: **Change User Settings – BMC User Settings – Server Mgmt – Screen Map**

4. User Access

Value: Enable / **Disable**

Help text: `Enable/Disable the BMC User's Access.`

Comments: None.

Back to: **Change User Settings – BMC User Settings – Server Mgmt – Screen Map**

5. Channel No

Value: <1~15>

Help text: `Enter BMC Channel Number.`

Comments: None.

Back to: **Change User Settings – BMC User Settings – Server Mgmt – Screen Map**

6. User Privilege Limit

Value: **<No Access>** / <Callback> / <User> / <Operator> / <Administrator> / <OEM Proprietary>

Help text: `Enter BMC User Privilege Limit for Selected Channel.`

Comments: Visible options may vary depending on BMC settings.

Back to: **Change User Settings – BMC User Settings – Server Mgmt – Screen Map**

9. Security

Figure 79. Security Screen (1)

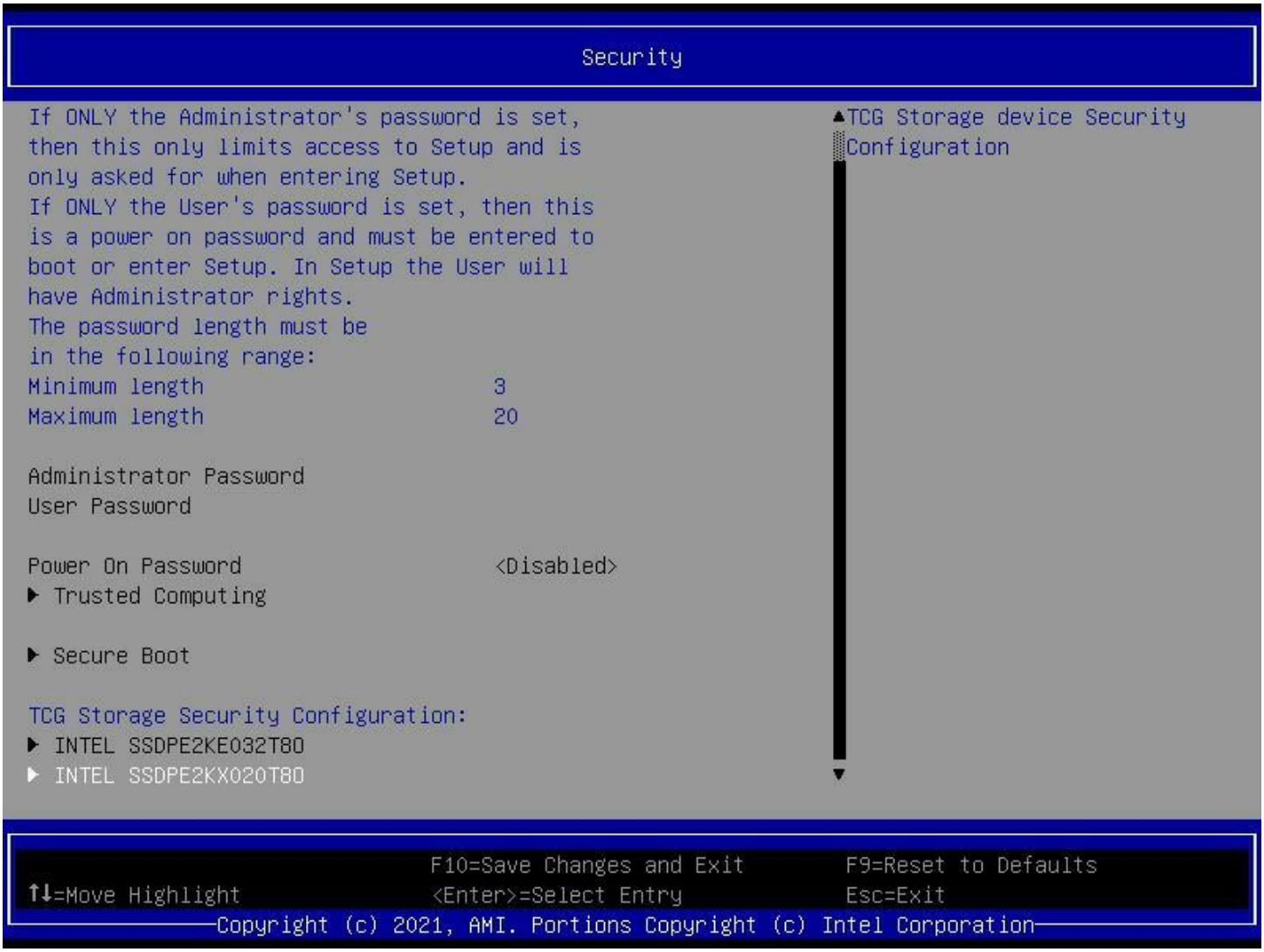

Figure 80. Security Screen (2)

1. Administrator Password

Value: None.

Help text: `Set Administrator Password.`

Comments: *Selection only.*

Back to: **Security** – **Screen Map**

2. User Password

Value: None.

Help text: `Set User Password.`

Comments: *Selection only.*

Back to: **Security** – **Screen Map**

3. Power On Password

Value: Enabled / **Disabled**

Help text: `Require a password in order to power on the system.`

Comments: None.

Back to: **Security** – **Screen Map**

4. Trusted Computing

Value: None.

Help text: `Trusted Computing Settings.`

Comments: *Selection only.*

Back to: **Security** – **Screen Map**

5. Secure Boot

Value: None.

Help text: `Secure Boot configuration.`

Comments: *Selection only.*

Back to: **Security** – **Screen Map**

6. TCG Storage Security Configuration

Value: None.

Help text: None.

Comments: TCG storages, such as OPAL SSDs, will be listed here.

Back to: **Security** – **Screen Map**

9.1 Trusted Computing

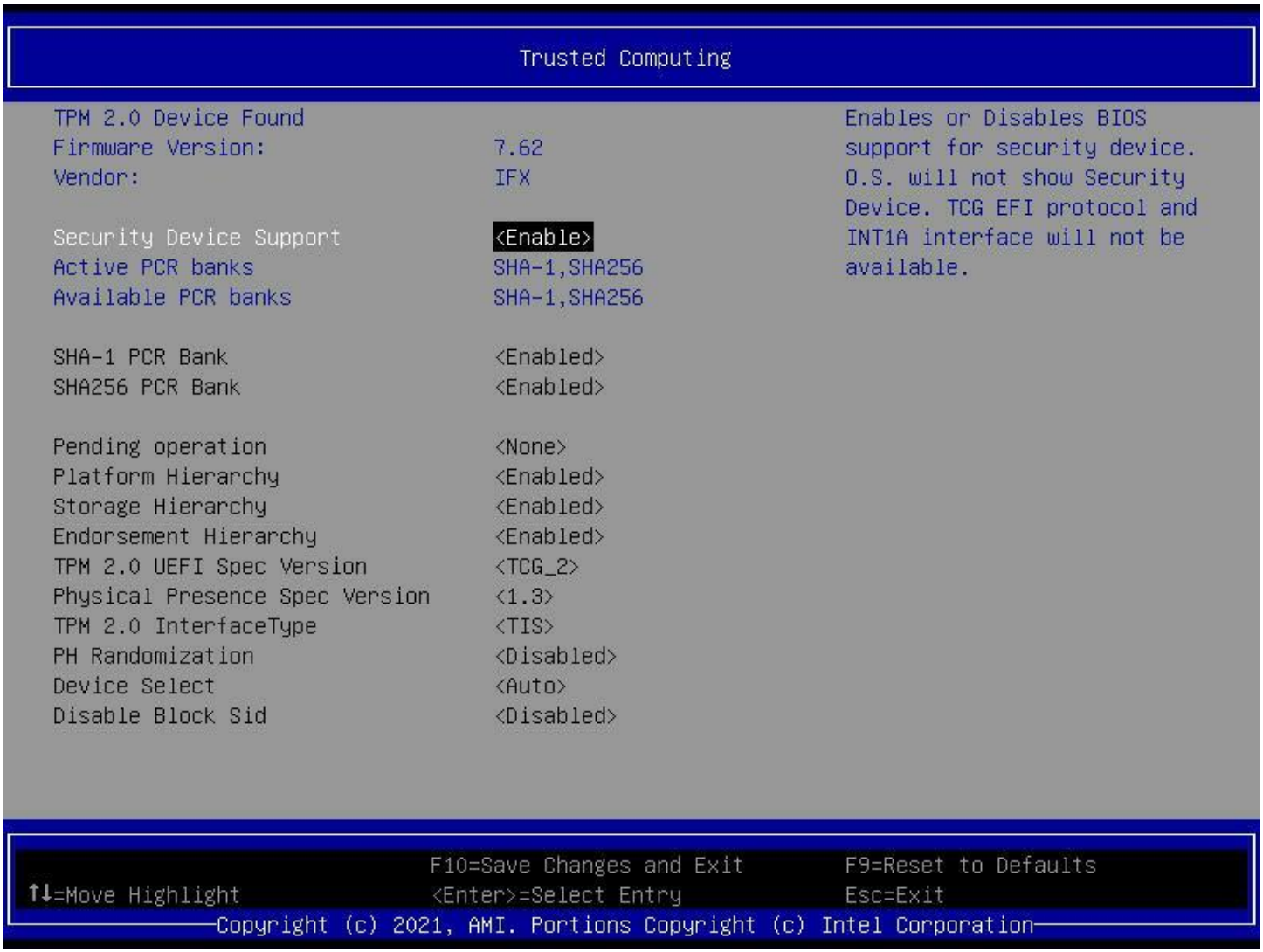

Figure 81. Trusted Computing Screen

1. Firmware Version

Value: <Firmware version>

Help text: None.

Comments: *Information only.*

Back to: **Trusted Computing** – **Security** – **Screen Map**

2. Vendor

Value: <Vendor>

Help text: None.

Comments: *Information only.*

Back to: **Trusted Computing** – **Security** – **Screen Map**

3. Security Device Support

Value: **Enable** / Disable

Help text: `Enables or Disables BIOS support for security device. O.S. will not show Security Device. TCG EFI protocol and INT1A interface will not be available.`

Comments: None.

Back to: **Trusted Computing – Security – Screen Map**

4. Active PCR banks

Value: <Active PCR banks>

Help text: None.

Comments: *Information only.*

Back to: **Trusted Computing – Security – Screen Map**

5. Available PCR banks

Value: <Available PCR banks>

Help text: None.

Comments: *Information only.*

Back to: **Trusted Computing – Security – Screen Map**

6. SHA-1 PCR Bank

Value: **Enabled** / Disabled

Help text: `Enable or Disable SHA-1 PCR Bank.`

Comments: None.

Back to: **Trusted Computing – Security – Screen Map**

7. SHA256 PCR Bank

Value: **Enabled** / Disabled

Help text: `Enable or Disable SHA256 PCR Bank.`

Comments: None.

Back to: **Trusted Computing – Security – Screen Map**

8. Pending operation

Value: **<None>** / <TPM Clear>

Help text: `Schedule an Operation for the Security Device. NOTE: Your Computer will reboot during restart in order to change State of Security Device.`

Comments: None.

Back to: **Trusted Computing – Security – Screen Map**

9. Platform Hierarchy

Value: **Enabled** / Disabled

Help text: `Enable or Disable Platform Hierarchy.`

Comments: None.

Back to: **Trusted Computing – Security – Screen Map**

10. Storage Hierarchy

Value: **Enabled** / Disabled

Help text: `Enable or Disable Storage Hierarchy.`

Comments: None.

Back to: **Trusted Computing – Security – Screen Map**

11. Endorsement Hierarchy

Value: **Enabled** / Disabled

Help text: `Enable or Disable Endorsement Hierarchy.`

Comments: None.

Back to: **Trusted Computing – Security – Screen Map**

12. TPM 2.0 UEFI Spec Version

Value: TCG_1_2 / **TCG_2**

Help text: `Select the TCG2 Spec Version Support,`
`TCG_1_2: the Compatible mode for Win8/Win10`
`TCG_2: Support new TCG2 protocol and event format for Win10 or later`

Comments: None.

Back to: **Trusted Computing – Security – Screen Map**

13. Physical Presence Spec Version

Value: 1.2 / **1.3**

Help text: `Select to Tell O.S. to support PPI Spec Version 1.2 or 1.3. Note some HCK tests might not support 1.3.`

Comments: None.

Back to: **Trusted Computing – Security – Screen Map**

14. TPM 2.0 InterfaceType

Value: CRB / **TIS**

Help text: `Select the Communication Interface to TPM 20 Device.`

Comments: None.

Back to: **Trusted Computing – Security – Screen Map**

15. PH Randomization

Value: **Disabled** / Enabled

Help text: `Enables or Disables Platform Hierarchy randomization. DO NOT ENABLE THIS QUESTION IN PRODUCTION PLATFORMS. THIS IS FOR DEVELOPMENT TESTING. OVERRIDE ChangePlatformAuth ELINK for production platforms supporting TXT.`

Comments: None.

Back to: **Trusted Computing – Security – Screen Map**

16. Device Select

Value: <TPM 1.2> / <TPM 2.0> / **<Auto>**

Help text: `TPM 1.2 will restrict support to TPM 1.2 devices, TPM 2.0 will restrict support to TPM 2.0 devices, Auto will support both with the default set to TPM 2.0 devices if not found, TPM 1.2 devices will be enumerated.`

Comments: None.

Back to: **Trusted Computing – Security – Screen Map**

17. Disable Block Sid

Value: Enabled / **Disabled**

Help text: `Override to allow SID authentication in TCG Storage device.`

Comments: None.

Back to: **Trusted Computing – Security – Screen Map**

9.2 Secure Boot

Figure 82. Secure Boot Screen

1. System Mode

Value: <System mode>

Help text: None.

Comments: *Information only.* Possible values: setup, user, audit, deployed.

Back to: Secure Boot – Security – Screen Map

2. Security Boot

Value: <Enabled> / **<Disabled>**

Help text: `Secure Boot feature is Active if Secure Boot is Enabled, Platform Key (PK) is enrolled, and the System is in User mode. The mode change requires platform reset.`

Comments: None.

Back to: Secure Boot – Security – Screen Map

3. Security Boot Mode

Value: Standard / **Custom**

Help text: `Secure Boot mode options:`

`Standard or Custom.`

`In Custom mode, Secure Boot Policy variables can be configured by a physically present user without full authentication.`

Comments: None.

Back to: **Secure Boot** – **Security** – **Screen Map**

4. Restore Factory Keys

Value: None.

Help text: `Force System to User Mode.`

`Install factory default Secure Boot key databases.`

Comments: *Selection only.*

Back to: **Secure Boot** – **Security** – **Screen Map**

5. Reset To Setup Mode

Value: None.

Help text: `Delete all Secure Boot key databases from NVRAM.`

Comments: *Selection only.*

Back to: **Secure Boot** – **Security** – **Screen Map**

6. Enter Audit Mode

Value: None.

Help text: `Enter Audit Mode workflow.`

`Transitions from User to Audit.`

`Mode will result in erasing of PK variable.`

Comments: *Selection only.*

Back to: **Secure Boot** – **Security** – **Screen Map**

7. Key Management

Value: None.

Help text: `Enables expert users to modify Secure Boot Policy variables without full authentication.`

Comments: *Selection only.*

Back to: **Secure Boot** – **Security** – **Screen Map**

9.2.1 Key Management

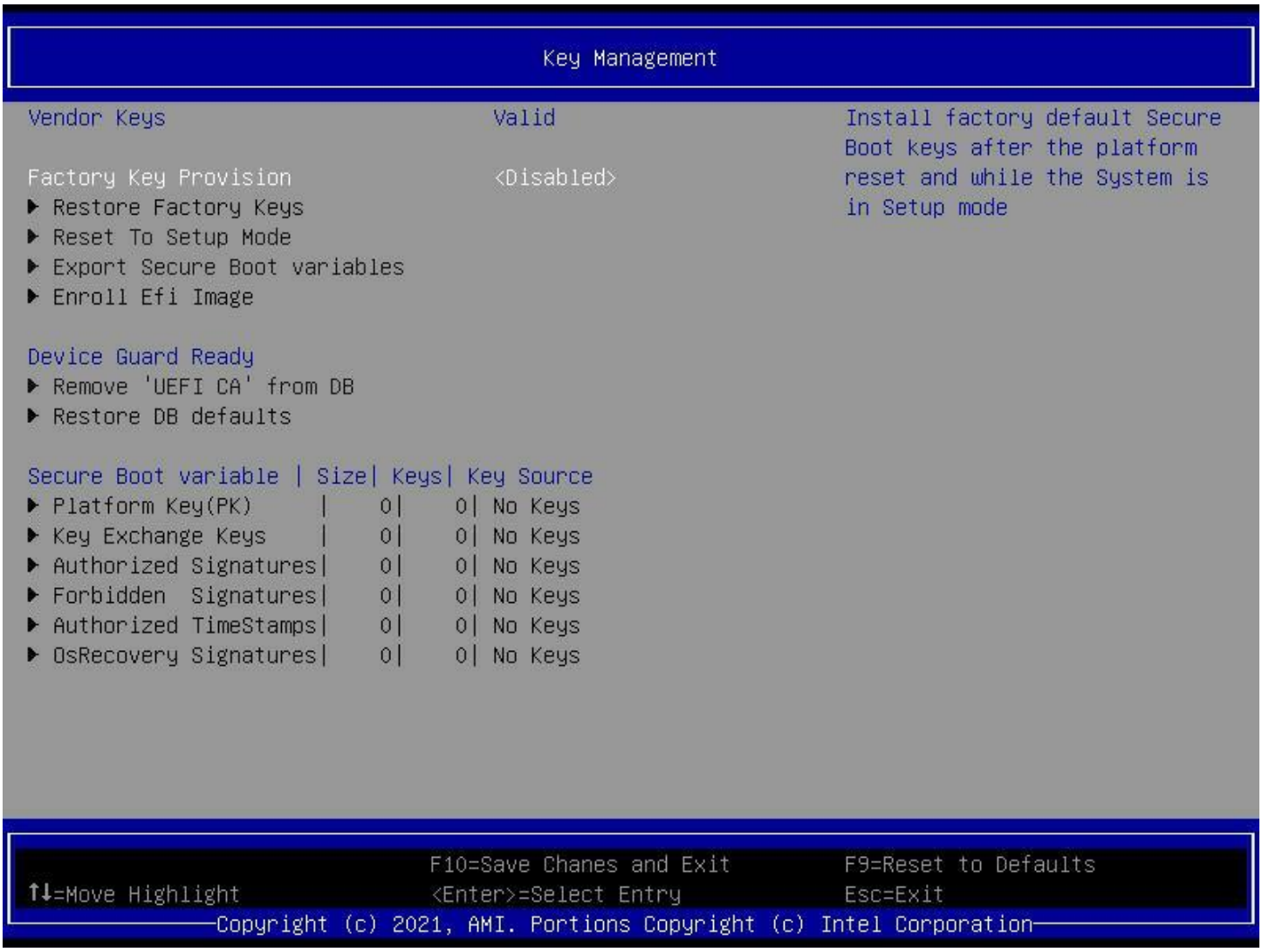

Figure 83. Key Management Screen

1. Vendor Keys

Value: <Vendor keys>

Help text: None.

Comments: *Information only.* Possible values: valid, modified.

Back to: **Key Management** – **Secure Boot** – **Security** – **Screen Map**

2. Factory Key Provision

Value: **Disabled** / Enabled

Help text: `Install factory default Secure Boot keys after the platform reset and while the System is in Setup mode.`

Comments: None.

Back to: **Key Management** – **Secure Boot** – **Security** – **Screen Map**

3. Restore Factory Keys

Value: None.

Help text: `Force System to User Mode.`

`Install factory default Secure Boot key databases.`

Comments: *Selection only.*

Back to: **Key Management** – **Secure Boot** – **Security** – **Screen Map**

4. Reset To Setup Mode

Value: None.

Help text: `Delete all Secure Boot key databases from NVRAM.`

Comments: *Selection only.*

Back to: **Key Management** – **Secure Boot** – **Security** – **Screen Map**

5. Export Secure Boot variables

Value: None.

Help text: `Copy NVRAM content of Secure Boot variables to files in a root folder on a file system device.`

Comments: *Selection only.*

Back to: **Key Management** – **Secure Boot** – **Security** – **Screen Map**

6. Enroll Efi Image

Value: None.

Help text: `Allow the image to run in Secure Boot mode.`

`Enroll SHA256 Hash certificate of a PE image into Authorized Signature Database (DB).`

Comments: *Selection only.*

Back to: **Key Management** – **Secure Boot** – **Security** – **Screen Map**

7. Remove 'UEFI CA' from DB

Value: None.

Help text: `Device Guard ready system must not list 'Microsoft UEFI CA' Certificate in Authorized Signature database (DB).`

Comments: *Selection only.*

Back to: **Key Management** – **Secure Boot** – **Security** – **Screen Map**

8. Restore DB defaults

Value: None.

Help text: `Restore DB variable to factory defaults.`

Comments: *Selection only.*

Back to: **Key Management** – **Secure Boot** – **Security** – **Screen Map**

9. Platform Key(PK)

Value: None.

Help text:
```
Enroll Factory Defaults or load certificates from a file:

1. Public Key Certificate:
   a) EFI_SIGNATURE_LIST
   b) EFI_CERT_X509 (DER)
   c) EFI_CERT_RSA2048 (bin)
   d) EFI_CERT_SHAXXX
2. Authenticated UEFI Variable
3. EFI PE/COFF Image (SHA256)

Key Source:
    Factory, External, Mixed
```

Comments: *Selection only.*

Back to: **Key Management** – **Secure Boot** – **Security** – **Screen Map**

1. Key Exchange Keys

Value: None.

Help text:
```
Enroll Factory Defaults or load certificates from a file:

1. Public Key Certificate:
   a) EFI_SIGNATURE_LIST
   b) EFI_CERT_X509 (DER)
   c) EFI_CERT_RSA2048 (bin)
   d) EFI_CERT_SHAXXX
2. Authenticated UEFI Variable
3. EFI PE/COFF Image (SHA256)

Key Source:
    Factory, External, Mixed
```

Comments: *Selection only.*

Back to: **Key Management** – **Secure Boot** – **Security** – **Screen Map**

2. Authorized Signatures

Value: None.

Help text:
```
Enroll Factory Defaults or load certificates from a file:

1. Public Key Certificate:
   a) EFI_SIGNATURE_LIST
   b) EFI_CERT_X509 (DER)
   c) EFI_CERT_RSA2048 (bin)
   d) EFI_CERT_SHAXXX
2. Authenticated UEFI Variable
3. EFI PE/COFF Image (SHA256)

Key Source:
    Factory, External, Mixed
```

Comments: *Selection only.*

Back to: **Key Management** – **Secure Boot** – **Security** – **Screen Map**

3. Forbidden Signatures

Value: None.

Help text:
```
Enroll Factory Defaults or load certificates from a file:

1. Public Key Certificate:
   a) EFI_SIGNATURE_LIST
   b) EFI_CERT_X509 (DER)
   c) EFI_CERT_RSA2048 (bin)
   d) EFI_CERT_SHAXXX
2. Authenticated UEFI Variable
3. EFI PE/COFF Image (SHA256)

Key Source:
    Factory, External, Mixed
```

Comments: *Selection only.*

Back to: **Key Management** – **Secure Boot** – **Security** – **Screen Map**

4. Authorized TimeStamps

Value: None.

Help text:
```
Enroll Factory Defaults or load certificates from a file:

1. Public Key Certificate:
   a) EFI_SIGNATURE_LIST
   b) EFI_CERT_X509 (DER)
   c) EFI_CERT_RSA2048 (bin)
   d) EFI_CERT_SHAXXX
2. Authenticated UEFI Variable
3. EFI PE/COFF Image (SHA256)

Key Source:
    Factory, External, Mixed
```

Comments: *Selection only.*

Back to: **Key Management** – **Secure Boot** – **Security** – **Screen Map**

5. OsRecovery Signatures

Value: None.

Help text:
```
Enroll Factory Defaults or load certificates from a file:

1. Public Key Certificate:
   a) EFI_SIGNATURE_LIST
   b) EFI_CERT_X509 (DER)
   c) EFI_CERT_RSA2048 (bin)
   d) EFI_CERT_SHAXXX
2. Authenticated UEFI Variable
3. EFI PE/COFF Image (SHA256)

Key Source:
    Factory, External, Mixed
```

Comments: *Selection only.*

Back to: **Key Management** – **Secure Boot** – **Security** – **Screen Map**

9.3 TCG Storage device Security Configuration

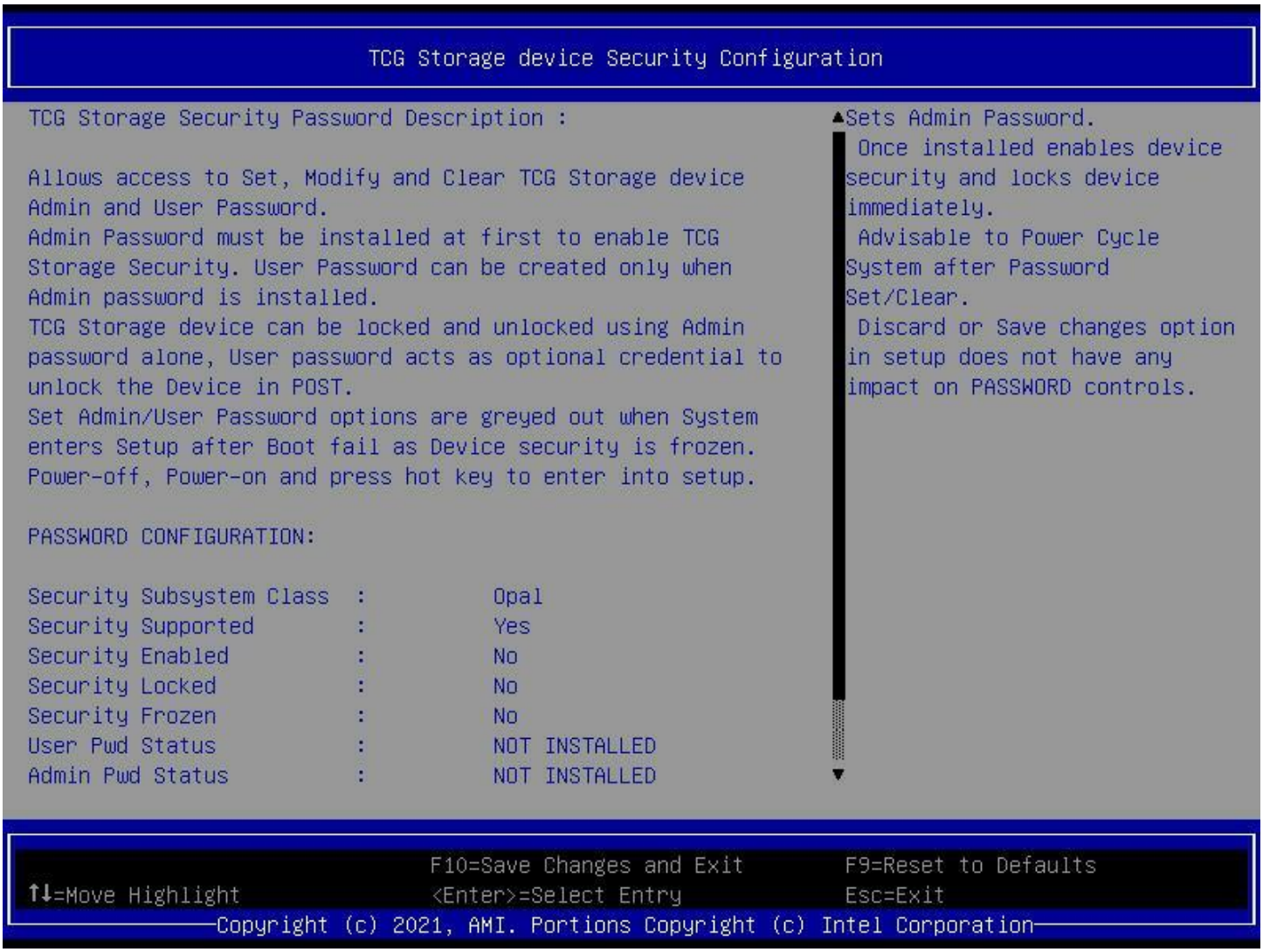

Figure 84. TCG Storage Device Security Configuration Screen (1)

Figure 85. TCG Storage Device Security Configuration Screen (2)

1. Security Subsystem Class

Value: <Security subsystem class>

Help text: None.

Comments: *Information only.*

Back to: **TCG Storage device Security Configuration** – **Security** – **Screen Map**

2. Security Supported

Value: <Security supported>

Help text: None.

Comments: *Information only.*

Back to: **TCG Storage device Security Configuration** – **Security** – **Screen Map**

3. Security Enabled

Value: <Security Enabled>

Help text: None.

Comments: *Information only.*

Back to: **TCG Storage device Security Configuration – Security – Screen Map**

4. Security Locked

Value: <Security locked>

Help text: None.

Comments: *Information only.*

Back to: **TCG Storage device Security Configuration – Security – Screen Map**

5. Security Frozen

Value: <Security Frozen>

Help text: None.

Comments: *Information only.*

Back to: **TCG Storage device Security Configuration – Security – Screen Map**

6. User Pwd Status

Value: <User password status>

Help text: None.

Comments: *Information only.*

Back to: **TCG Storage device Security Configuration – Security – Screen Map**

7. Admin Pwd Status

Value: <Admin password status>

Help text: None.

Comments: *Information only.*

Back to: **TCG Storage device Security Configuration – Security – Screen Map**

8. Set Admin Password

Value: None.

Help text: `Sets Admin Password.`

`Once installed enables device security and locks device immediately.`

`Advisable to Power Cycle System after Password Set/Clear.`

`Discard or Save changes option in setup does not have any impact on PASSWORD controls.`

Comments: *Selection only.*

Back to: **TCG Storage device Security Configuration – Security – Screen Map**

9. Set User Password

Value: None.

Help text: `Sets User Password.`

`Important: Enter Admin Password when Enter Current Password Prompt appears.`

`If 'Set User Password' option is grayed out, Set Admin password first.`

`Discard or Save changes option in setup does not have any impact on PASSWORD controls.`

Comments: *Selection only.*

Back to: **TCG Storage device Security Configuration – Security – Screen Map**

10. Boot

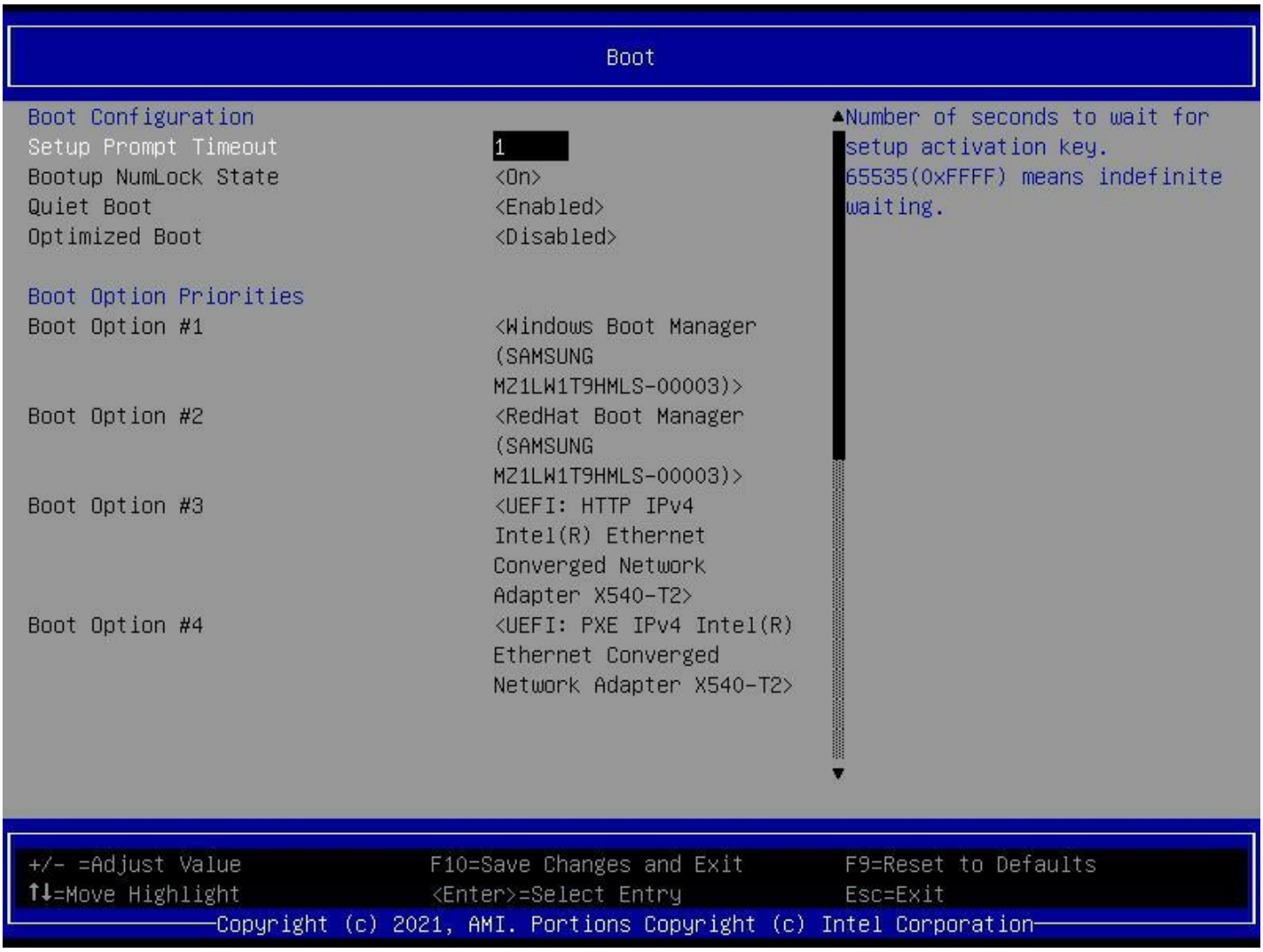

Figure 86. Boot Screen

1. Setup Prompt Timeout

Value: 1~65536

Help text: `Number of seconds to wait for setup activation key. 65535(0xFFFF) means indefinite waiting.`

Comments: None.

Back to: **Boot** – **Screen Map**

2. Bootup NumLock State

Value: **On** / Off

Help text: `Select the keyboard NumLock state.`

Comments: None.

Back to: **Boot** – **Screen Map**

3. Quiet Boot

Value: **Enabled** / Disabled

Help text: `Enables or disables Quiet Boot option.`

Comments: None.

Back to: **Boot** – **Screen Map**

4. Optimized Boot

Value: Enabled / **Disabled**

Help text: `Enables or disables Optimized Boot. Enabling Optimized Boot will disable Csm support and disable connecting Network devices to decrease boot time. While disabling Optimized Boot, make sure to restore Csm Support option to previous value before enabling Optimized Boot.`

Comments: None.

Back to: **Boot** – **Screen Map**

5. Boot Option #n

Value: <boot option>

Help text: `Sets the system boot order.`

Comments: None.

Back to: **Boot** – **Screen Map**

11. Save & Exit

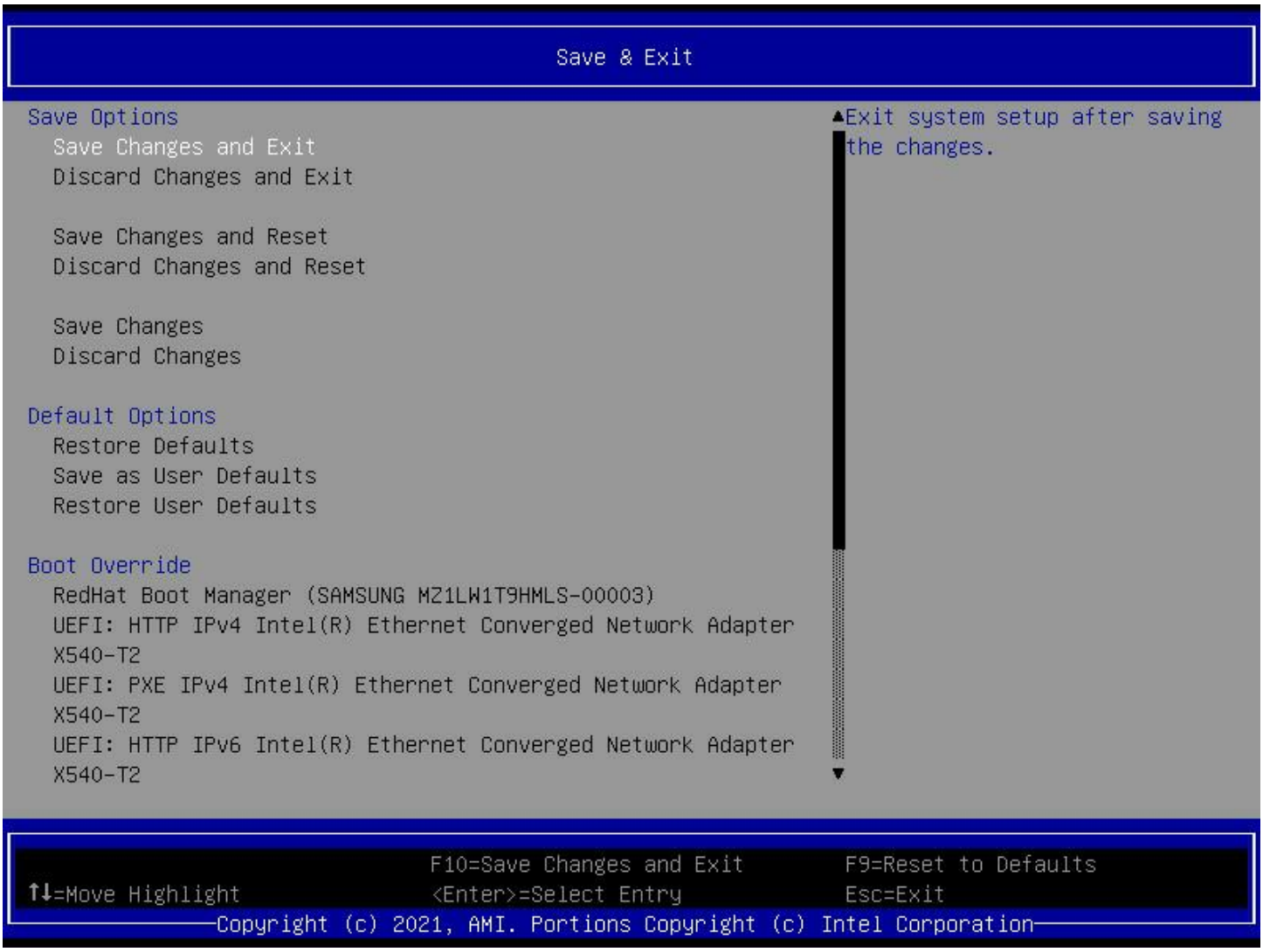

Figure 87. Save & Exit Screen

1. Save Changes and Exit

Value: None.

Help text: `Exit system setup after saving the changes.`

Comments: *Selection only.*

Back to: **Save & Exit – Screen Map**

2. Discard Changes and Exit

Value: None.

Help text: `Exit system setup without saving any changes.`

Comments: *Selection only.*

Back to: **Save & Exit – Screen Map**

3. Save Changes and Reset

Value: None.

Help text: `Reset the system after saving the changes.`

Comments: *Selection only.*

Back to: **Save & Exit** – **Screen Map**

4. Discard Changes and Reset

Value: None.

Help text: `Reset system setup without saving any changes.`

Comments: *Selection only.*

Back to: **Save & Exit** – **Screen Map**

5. Save Changes

Value: None.

Help text: `Save Changes done so far to any of the setup options.`

Comments: *Selection only.*

Back to: **Save & Exit** – **Screen Map**

6. Discard Changes

Value: None.

Help text: `Discard Changes done so far to any of the setup options.`

Comments: *Selection only.*

Back to: **Save & Exit** – **Screen Map**

7. Restore Defaults

Value: None.

Help text: `Restore/Load Default values for all the setup options.`

Comments: *Selection only.*

Back to: **Save & Exit** – **Screen Map**

8. Save as User Defaults

Value: None.

Help text: `Save the changes done so far as User Defaults.`

Comments: *Selection only.*

Back to: **Save & Exit** – **Screen Map**

9. Restore User Defaults

Value: None.

Help text: `Restore the User Defaults to all the setup options.`

Comments: *Selection only.*

Back to: **Save & Exit** – **Screen Map**

Appendix A. Glossary

Term	Definition
ACM	Authenticated code mode.
ACPI	Advanced Configuration and Power Interface. ACPI is an open industry specification proposed by Intel, Microsoft, and Toshiba. ACPI enables and supports reliable power management through improved hardware and operating system coordination.
AES	Advanced Encryption Standard (encryption algorithm).
Intel® AES-NI	Intel® AES New Instructions.
AHCI	Advanced Host Controller Interface, a USB controller standard.
ANSI	American National Standards Institute.
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.
BIOS	Basic input/output system.
BMC	Baseboard management controller.
BSP	Bootstrap processor. The processor selected at boot time to be the primary processor in a multi-processor system.
CE	Correctable error.
COM1	Communication port 1, serial port 1.
COM2	Communication port 2, serial port 2.
CSM	Compatibility support module.
DDR4	Double Data Rate 4 is a high bandwidth memory technology.
DIMM	Dual in-line memory module, a plug-in memory module with signal and power pins on both sides of the internal printed circuit board (front and back).
DMA	Direct memory access.
DMAR	DMA resource.
DRAM	Dynamic random access memory, memory chips from which DIMMs are constructed.
ECC	Error correction code. Refers to a memory system that has extra bit(s) to support limited detection or correction of memory errors.
EFI	Extensible Firmware Interface (see also UEFI).
EPS	External product specification.
Formset	Framework term for display pages, which includes setup pages.
FRB	Fault resilient booting.
Gb	Gigabit, 1,073,741,824 bits. **Note:** 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.
GUID	Globally unique identifier.
KB	Kilobyte, 1024 bytes.
Intel® HT Technology	Intel® Hyper-Threading Technology.
IDE	Integrated Drive Electronics, a disk interface standard.
IMC	Integrated memory controller.
I/O	Input/output.

Term	Definition
IPMI	Intelligent Platform Management Interface. This is an industry standard that defines standardized, abstracted interfaces to platform management hardware.
IRQ	Interrupt request.
iSCSI	Internet small computer system interface, a connection usually used for disks of various types.
KB	Kilobyte, 1024 bytes.
KCS	Keyboard controller style.
LAN	Local area network.
MAC	Media access control.
Mb	Megabit, 1,048,576 bits. **Note:** Lowercase “b” distinguishes “bits” from uppercase “B” for “bytes”.
MB	Megabyte, 1024 kilobytes (1,048,576 bytes).
Intel® ME	Intel® Management Engine.
MHz	Megahertz, a frequency measurement, a million cycles/second.
MRC	Memory reference code.
MSR	Model specific register.
NIC	Network interface card.
Intel® NM	Intel® Node Manager (now Intel® Intelligent Power Node Manager).
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.
OS	Operating system.
PCI	Peripheral Component Interconnect, or PCI standard.
PCIe*	PCI Express*.
PCR	Platform configuration register.
POR	Process of record.
POST	Power on self-test.
PXE	Pre-execution environment.
RAID	Redundant array of inexpensive disks. Provides data security by spreading data over multiple disk drives. RAID 0, RAID 1, RAID 10, and RAID 5 are different patterns of data on varying numbers of disks to provide varying degrees of security and performance.
RAS	Reliability, availability, serviceability.
RTS	Root of trust storage.
SATA	Serial ATA, a high speed serial data version of the disk ATA interface.
SDR	Sensor data record.
SEC	Security component of Intel® Platform Innovation Framework for EFI architecture.
SEL	System event log.
SMBIOS	System management BIOS.
SMM	System management mode.
TCG	Trusted Computing Group.
TPM	Trusted platform module.

Term	Definition
Intel® TXT	Intel® Trusted Execution Technology.
UEFI	Unified Extensible Firmware Interface. This is the replacement for legacy BIOS and legacy DOS interface.
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 for Directed I/O.