



NETAŞ Server

BIOS User Guide (Intel EagleStream)

Version: R1.3

NETAŞ TELEKOMÜNİKASYON A.Ş
Yenişehir Mahallesi Osmanlı Bulvarı Aeropark Sitesi
B Blok No:11B İç Kapı No:40
Postcode: 34912
Tel: +90 (216) 522 20 00
URL: <https://destek.netas.com.tr>
E-mail: info@netas.com.tr

LEGAL INFORMATION

Copyright 2025 NETAŞ CORPORATION.

The contents of this document are protected by copyright laws and international treaties. Any reproduction or distribution of this document or any portion of this document, in any form by any means, without the prior written consent of NETAŞ CORPORATION is prohibited. Additionally, the contents of this document are protected by contractual confidentiality obligations.

All company, brand and product names are trade or service marks, or registered trade or service marks, of NETAŞ CORPORATION or of their respective owners.

This document is provided as is, and all express, implied, or statutory warranties, representations or conditions are disclaimed, including without limitation any implied warranty of merchantability, fitness for a particular purpose, title or non-infringement. NETAŞ CORPORATION and its licensors shall not be liable for damages resulting from the use of or reliance on the information contained herein.

NETAŞ CORPORATION or its licensors may have current or pending intellectual property rights or applications covering the subject matter of this document. Except as expressly provided in any written license between NETAŞ CORPORATION and its licensee, the user of this document shall not acquire any license to the subject matter herein.

NETAŞ CORPORATION reserves the right to upgrade or make technical change to this product without further notice. Users may visit the NETAŞ technical support website <https://destek.netas.com.tr> to inquire for related information. The ultimate right to interpret this product resides in NETAŞ CORPORATION.

Statement on the Use of Third-Party Embedded Software:

If third-party embedded software such as Oracle, Sybase/SAP, Veritas, Microsoft, VMware, and Redhat is delivered together with this product of NETAŞ, the embedded software must be used as only a component of this product. If this product is discarded, the licenses for the embedded software must be void either and must not be transferred. NETAŞ will provide technical support for the embedded software of this product.

Revision History

Revision No.	Revision Date	Revision Reason
R1.3	2025-11-28	Updated "1.3 Applicable Server Models".
R1.2	2025-02-08	Update "2 Common Operations" and "4 Setup Parameter Descriptions".
R1.1	2024-08-12	Update "3.4.5.4 Intel VMD technology".

Revision No.	Revision Date	Revision Reason
R1.0	2023-09-07	First edition.

Serial Number: SJ-20230907115354-005

Publishing Date: 2025-11-28 (R1.3)

Contents

1 BIOS Overview.....	1
1.1 Basic Concepts.....	1
1.2 Precautions.....	1
1.3 Applicable Server Models	2
2 Common Operations	3
2.1 Entering the BIOS	4
2.2 Setting the BIOS Language	6
2.3 Querying Server Parameter Settings	7
2.4 Querying the CPU Information.....	8
2.5 Querying Memory Information.....	9
2.6 Querying NIC Information	10
2.7 Querying RAID Card Information.....	15
2.8 Querying Hard Disk Information.....	22
2.9 Setting the BIOS Time	24
2.10 Setting the Boot Mode	26
2.11 Setting the Boot Order.....	28
2.12 Setting the BIOS Password	30
2.13 Deleting a BIOS Password.....	33
2.14 Setting the PCIe Function for a Port	34
2.15 Setting Serial Port Console Redirection.....	37
2.16 Querying BMC Network Parameter Settings	38
2.17 Setting BMC Network Parameters	39
2.18 Setting the PXE Function for a NIC.....	41
2.19 Setting Virtualization Parameters.....	43
2.20 Setting Memory Parameters.....	49
2.21 Setting Power Parameters.....	51
2.22 Setting the TPM Type	58
2.23 Setting the Port Mode for a RAID Card.....	60
2.24 Creating a RAID Volume for SATA Drives	69
2.25 Restoring the Default BIOS Settings	73
3 Setup Parameter Descriptions.....	75
3.1 Main.....	75
3.2 Advanced.....	78

3.2.1 Mainboard Information.....	81
3.2.2 Trusted Computing.....	86
3.2.3 ACPI Settings	90
3.2.4 Redfish Host Interface Settings	91
3.2.5 Serial Port Console Redirection Settings	92
3.2.6 SIO Common Setting	100
3.2.7 SIO Configuration.....	101
3.2.8 PCI Subsystem Settings	103
3.2.9 USB Configuration.....	104
3.2.10 Network Stack Configuration.....	106
3.2.11 CSM Configuration.....	109
3.2.12 NVMe Configuration.....	111
3.2.13 Emulation Configuration	111
3.2.14 PXE Configuration	113
3.2.15 Tls Auth Configuration.....	114
3.2.16 RAM Disk Configuration.....	117
3.2.17 Driver Health.....	119
3.3 Platform Configuration	120
3.3.1 PCH-IO Configuration.....	121
3.3.2 Miscellaneous Configuration.....	136
3.3.3 Server ME Configuration.....	137
3.3.4 Runtime Error Logging.....	141
3.4 Socket Configuration.....	168
3.4.1 Processor Configuration	170
3.4.2 Common RefCode Configuration.....	184
3.4.3 Uncore Configuration.....	186
3.4.4 Memory Configuration	195
3.4.5 IIO Configuration	230
3.4.6 Advanced Power Management Configuration.....	270
3.5 Server Mgmt.....	295
3.5.1 System Event Log.....	299
3.5.2 View FRU information	300
3.5.3 BMC network configuration.....	301
3.5.4 BMC User Settings	312
3.6 Security	316
3.6.1 HDD Security Configuration	319
3.6.2 Secure Boot	319

3.6.3 Secure Flash Update.....	322
3.7 Boot.....	324
3.7.1 Add New Boot Option	329
3.7.2 Delete Boot Option	331
3.7.3 Hard Disk Boot Sequence	331
3.7.4 UEFI NETWORK Drive BBS Priorities	332
3.7.5 UEFI Other Drive BBS Priorities	333
3.8 Save & Exit	334
4 Reference: Control Keys for BIOS Setup.....	337
Figures	338
Tables.....	348
Glossary.....	354

About This Manual

Purpose

This manual describes the common operations and parameters of the BIOS of the Eagle Stream platform to provide you with guidance about server BIOS configuration and management.

Intended Audience

This manual is intended for:

- Planning engineers
- Network management and monitoring engineers
- Maintenance engineers

What Is in This Manual

This manual contains the following chapters:

Chapter 1, BIOS Overview	Describes basic BIOS concepts, the precautions for BIOS setup, and the server models that this manual applies to.
Chapter 2, Common Operations	Describes the common operations on the BIOS.
Chapter 3, Setup Parameter Descriptions	Describes parameters on the Setup screens.
Chapter 4, Reference: Control Keys for BIOS Setup	Describes common control keys used for BIOS setup.

Conventions

This manual uses the following conventions.

	Notice: indicates equipment or environment safety information. Failure to comply can result in equipment damage, data loss, equipment performance degradation, environmental contamination, or other unpredictable results. Failure to comply will not result in personal injury.
	Note: provides additional information about a topic.

Chapter 1

BIOS Overview

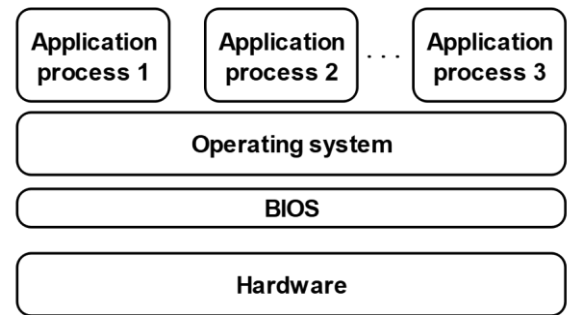
Table of Contents

Basic Concepts.....	1
Precautions.....	1
Applicable Server Models.....	2

1.1 Basic Concepts

As a server's most basic program, the **BIOS** is pre-loaded on a **ROM** chip on the motherboard. **Figure 1-1** shows the BIOS in a system, which bridges server hardware and an **OS**. It initializes server hardware before booting an OS.

Figure 1-1 BIOS in a System



The main functions of the BIOS include:

- Performing **POST**.
- Initializing **CPUs** and memory.
- Checking **I/O** devices and boot devices.
- Booting an OS.

1.2 Precautions

Before modifying the **BIOS** setting of a server, you must record the corresponding initial settings so that the original settings can be restored if the modification results in improper operation of the server.



Notice

In general, the factory default settings are the optimal settings. Do not modify any parameter unless you are clear about it. Any improper modification may result in hardware resource conflicts or reduce the system performance.

1.3 Applicable Server Models

This document is applicable to rack servers based on the **Eagle Stream** platform, including but not limited to the following models:

- NCS6712 N4
- NCS6722 N4
- NCS6742 N4
- NCS6742G N4
- NCS6744 N4
- NCS6782G N4
- ...

Chapter 2

Common Operations

Table of Contents

Entering the BIOS.....	4
Setting the BIOS Language	6
Querying Server Parameter Settings.....	7
Querying the CPU Information.....	8
Querying Memory Information.....	9
Querying NIC Information.....	10
Querying RAID Card Information.....	15
Querying Hard Disk Information	22
Setting the BIOS Time.....	24
Setting the Boot Mode	26
Setting the Boot Order	28
Setting the BIOS Password.....	30
Deleting a BIOS Password.....	33
Setting the PCIe Function for a Port.....	34
Setting Serial Port Console Redirection	37
Querying BMC Network Parameter Settings.....	38
Setting BMC Network Parameters	39
Setting the PXE Function for a NIC.....	41
Setting Virtualization Parameters.....	43
Setting Memory Parameters.....	49
Setting Power Parameters.....	51
Setting the TPM Type	58
Setting the Port Mode for a RAID Card	60
Creating a RAID Volume for SATA Drives.....	69
Restoring the Default BIOS Settings	73

2.1 Entering the BIOS

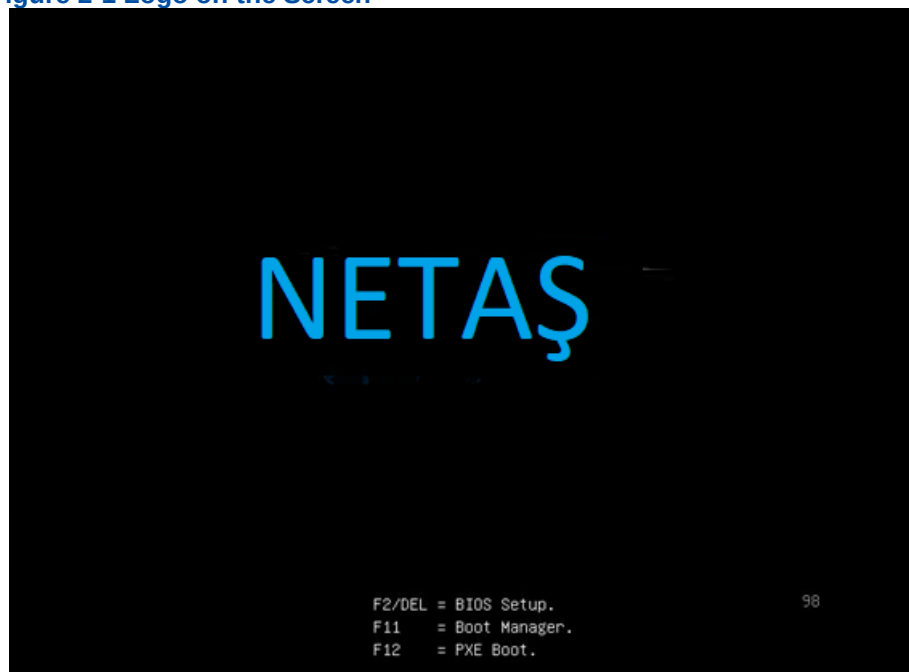
Abstract

This procedure describes how to enter the [BIOS](#) so that you can view and set BIOS information.

Steps

1. Connect to a server in either of the following ways:
 - Connect a monitor, mouse, and keyboard to the server.
 - Start the KVM on the Web portal of the BMC.
For details, refer to "7.4 Starting the KVM" in the *NETAŞ Server BMC User Guide (BMC V4)*.
2. Power on the server. The server starts and the [POST](#) is performed. The logo of the server is displayed on the screen, see [Figure 2-1](#).

Figure 2-1 Logo on the Screen



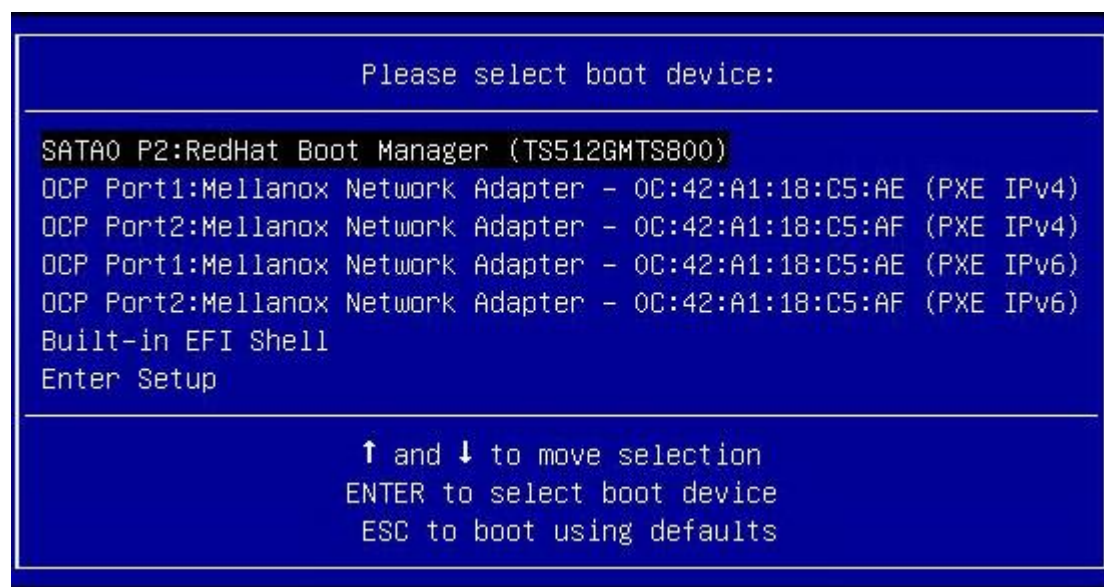
For a description of the hot keys for BIOS startup, refer to [Table 2-1](#).

Table 2-1 Descriptions of Hot Keys for BIOS Startup

Hot Key	Description
F2/DEL	Press the key to enter the Aptio Setup screen.
F11	Press the key to enter the Boot Manager screen.
F12	Press the key to enter the PXE Boot environment.

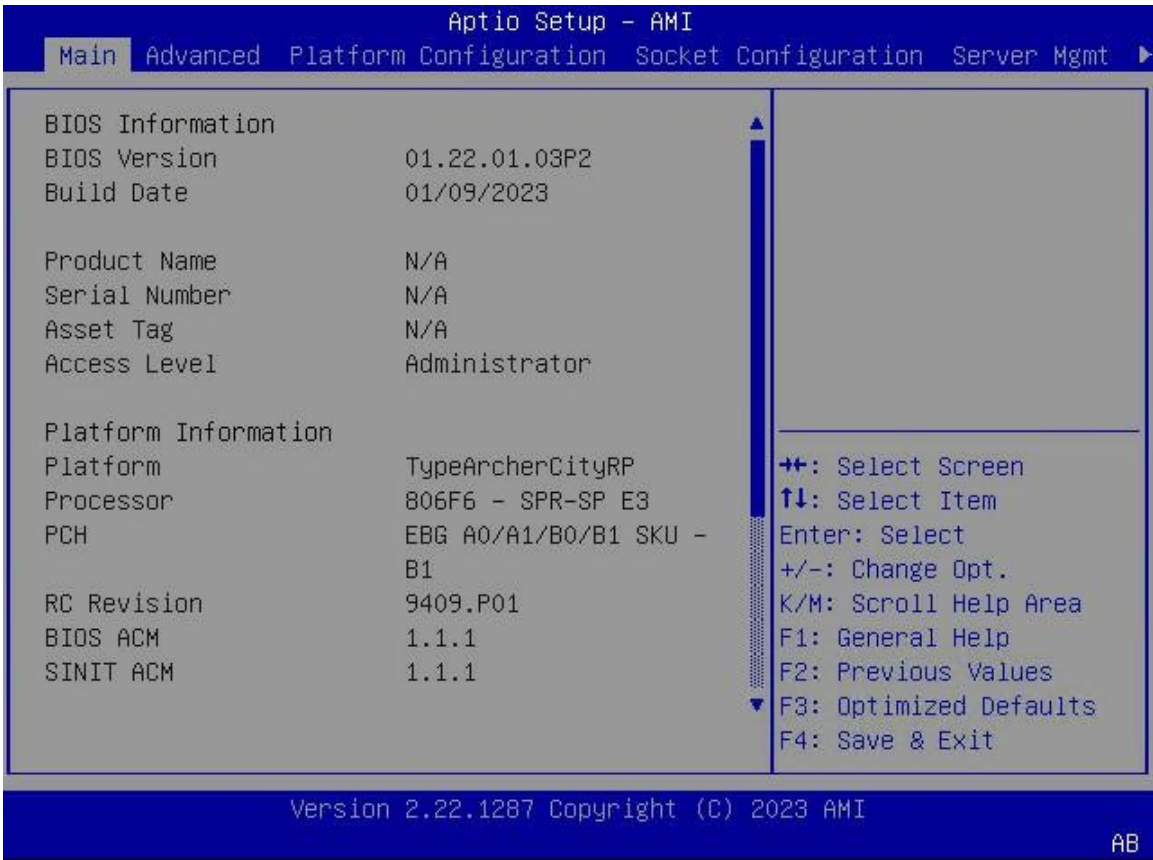
3. Perform the following operations as required.

To...	Do...
Enter the Boot Manager screen	Press the F11 key. The Boot Manager screen is displayed, see Figure 2-2 .
Enter the Aptio Setup screen	Press F2 or DEL . The Aptio Setup screen is displayed, see Figure 2-3 .

Figure 2-2 Boot Manager Screen**Note**

The **Boot Manager** screen displays the currently configured boot devices of the server. You can select the desired boot device on this screen.

Figure 2-3 Aptio Setup Screen



 Note

- For a description of the **Aptio Setup** screen, refer to [3 Setup Parameter Descriptions](#).
- For a description of the control keys on the **Aptio Setup** screen, refer to [4 Reference: Control Keys for BIOS Setup](#).

2.2 Setting the BIOS Language

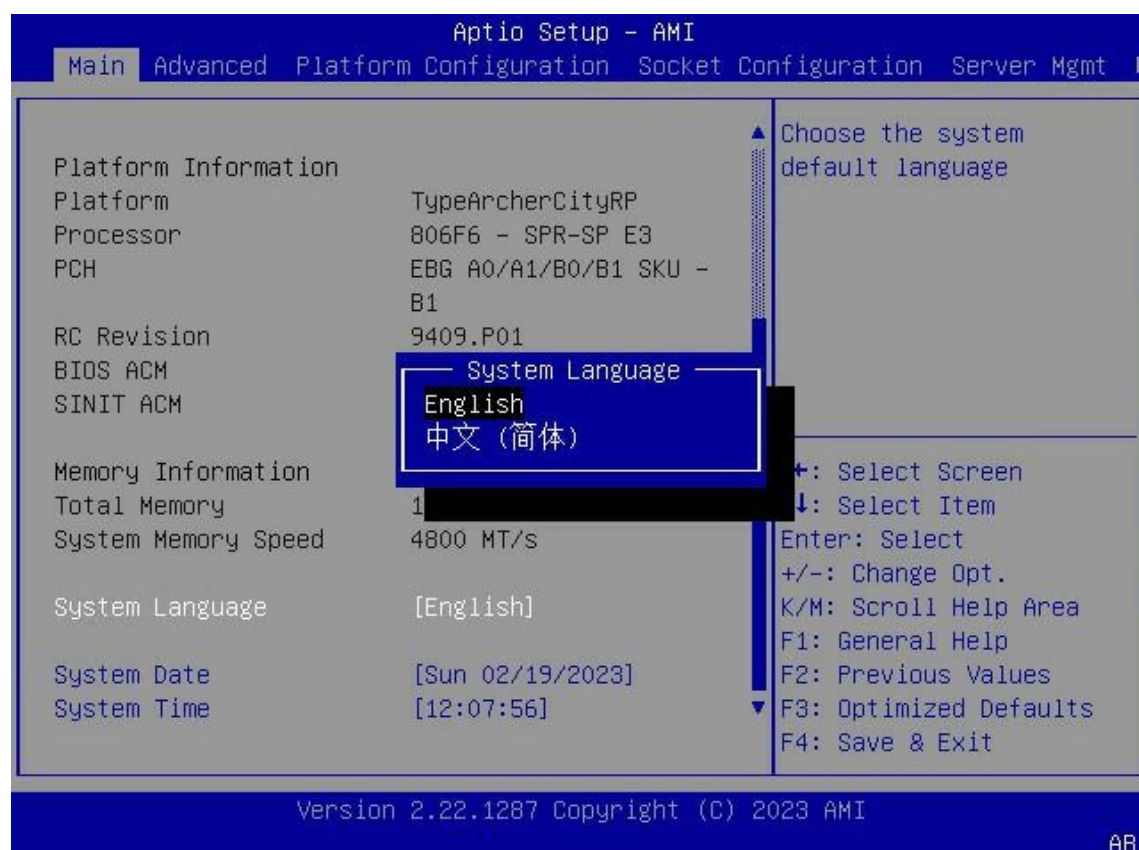
Abstract

This procedure describes how to set the **BIOS** language that the BIOS information is displayed in.

Steps

1. On the **Aptio Setup** screen, select the **Main** menu. The **Main** screen is displayed.
2. Select **System Language**. Press **Enter**. The **System Language** dialog box is displayed, see [Figure 2-4](#).

Figure 2-4 System Language Dialog Box



3. Select **English**.
4. Press **F4**. In the displayed dialog box, select **Yes**.

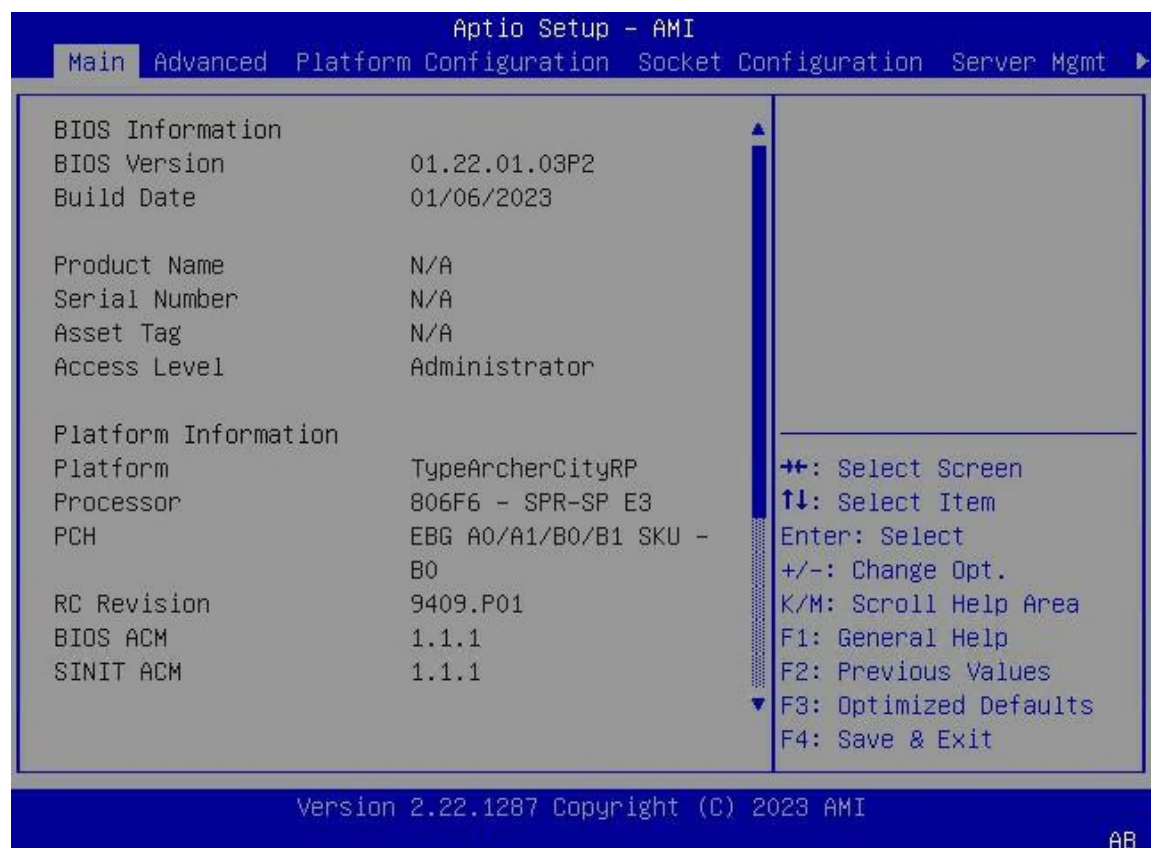
2.3 Querying Server Parameter Settings

Abstract

This procedure describes how to query server parameter settings, including the [BIOS](#) version number and product name.

Steps

1. On the **Aptio Setup** screen, select the **Main** menu. On the **Main** screen, the server configuration information is displayed, see [Figure 2-5](#).

Figure 2-5 Server Configuration Information

2.4 Querying the CPU Information

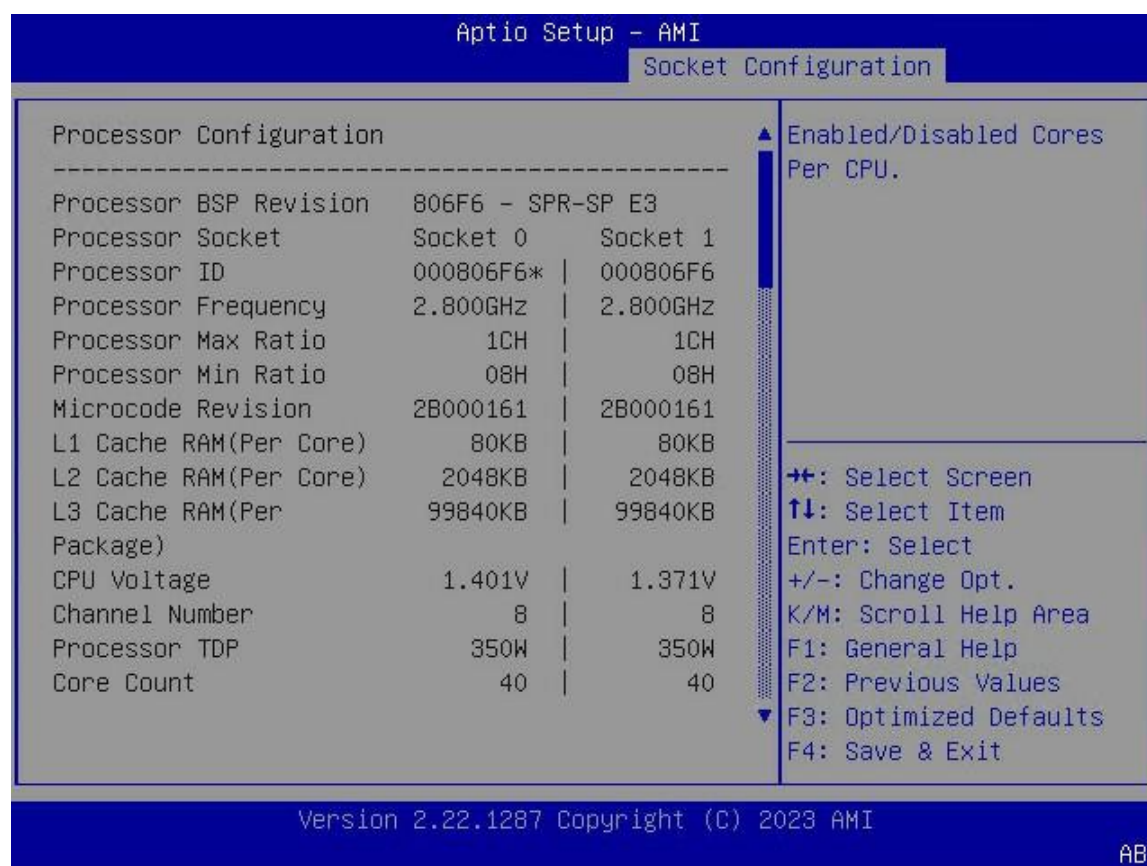
Abstract

This procedure describes how to query the [CPU](#) information so that you can learn about the parameters of CPUs.

Steps

1. On the **Aptio Setup** screen, select the **Socket Configuration** menu. The **Socket Configuration** window is displayed.
2. Select **Processor Configuration** and press **Enter**. The CPU information is displayed, see [Figure 2-6](#).

Figure 2-6 CPU Information



2.5 Querying Memory Information

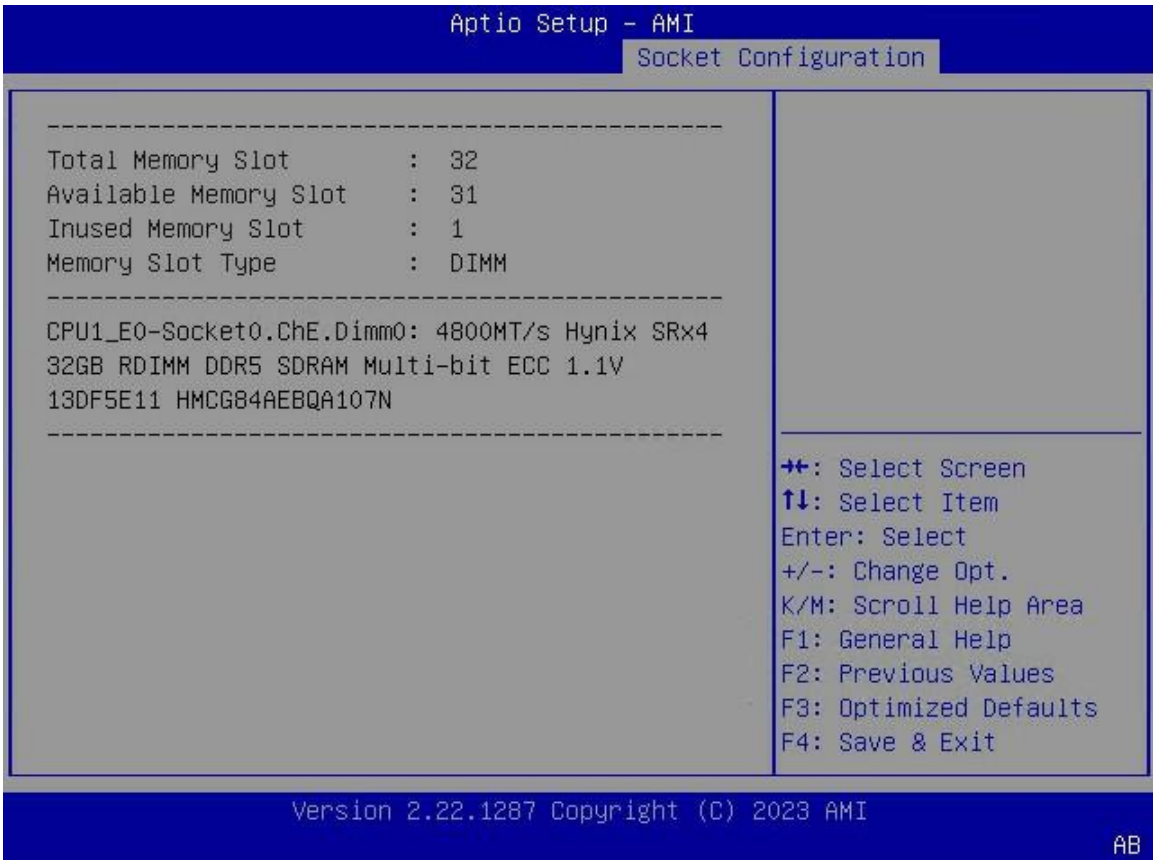
Abstract

This procedure describes how to query memory parameter settings.

Steps

1. On the **Aptio Setup** screen, select the **Socket Configuration** menu. The **Socket Configuration** window is displayed.
2. Select **Memory Configuration > Memory Topology** and press **Enter**. The memory information is displayed, see [Figure 2-7](#).

Figure 2-7 Memory Information



2.6 Querying NIC Information

Abstract

This procedure describes how to query [NIC](#) information to learn about the NIC configurations, such as the [MAC](#) address, slot status, and NIC details.

Prerequisite

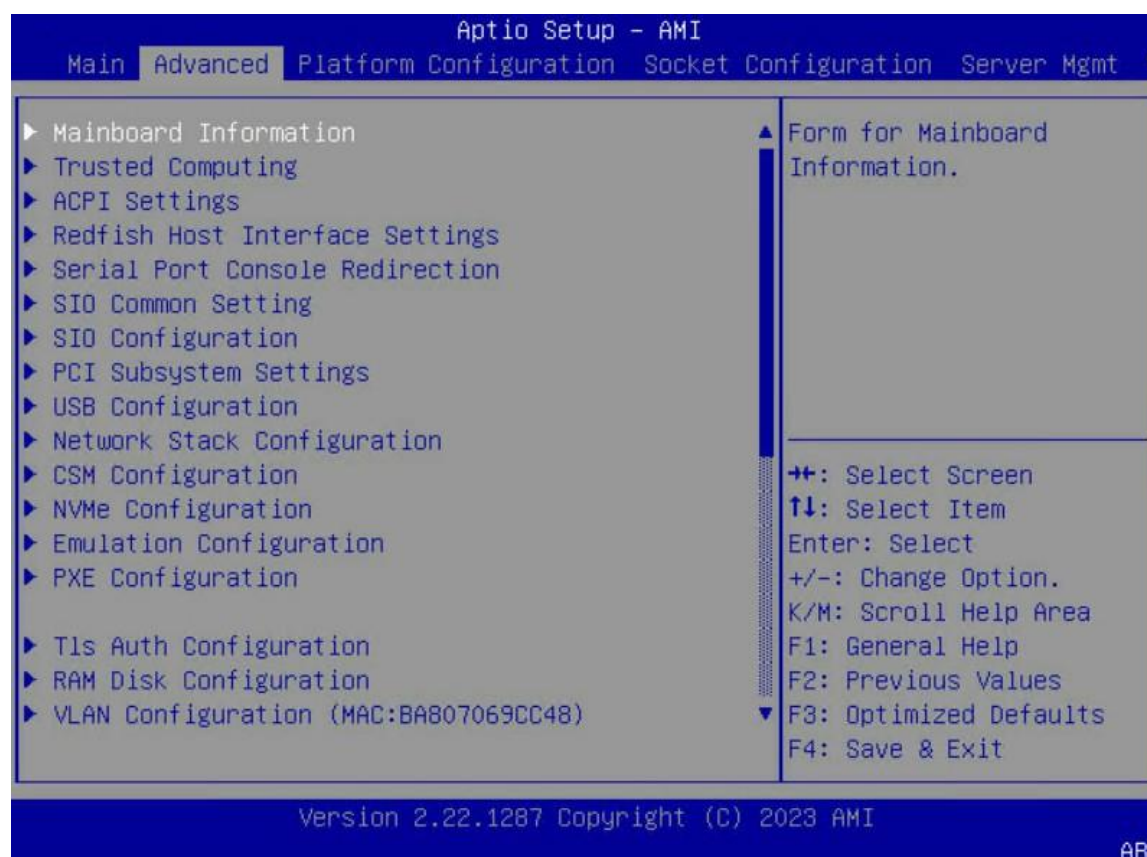
The boot mode is already set to [UEFI](#) in the [BIOS](#). For details, refer to [2.10 Setting the Boot Mode](#).

Steps

Querying Slot Number, Port Number, and MAC Address Information

1. On the **Aptio Setup** screen, select **Advanced**. The **Advanced** screen is displayed, see [Figure 2-8](#).

Figure 2-8 Advanced Screen

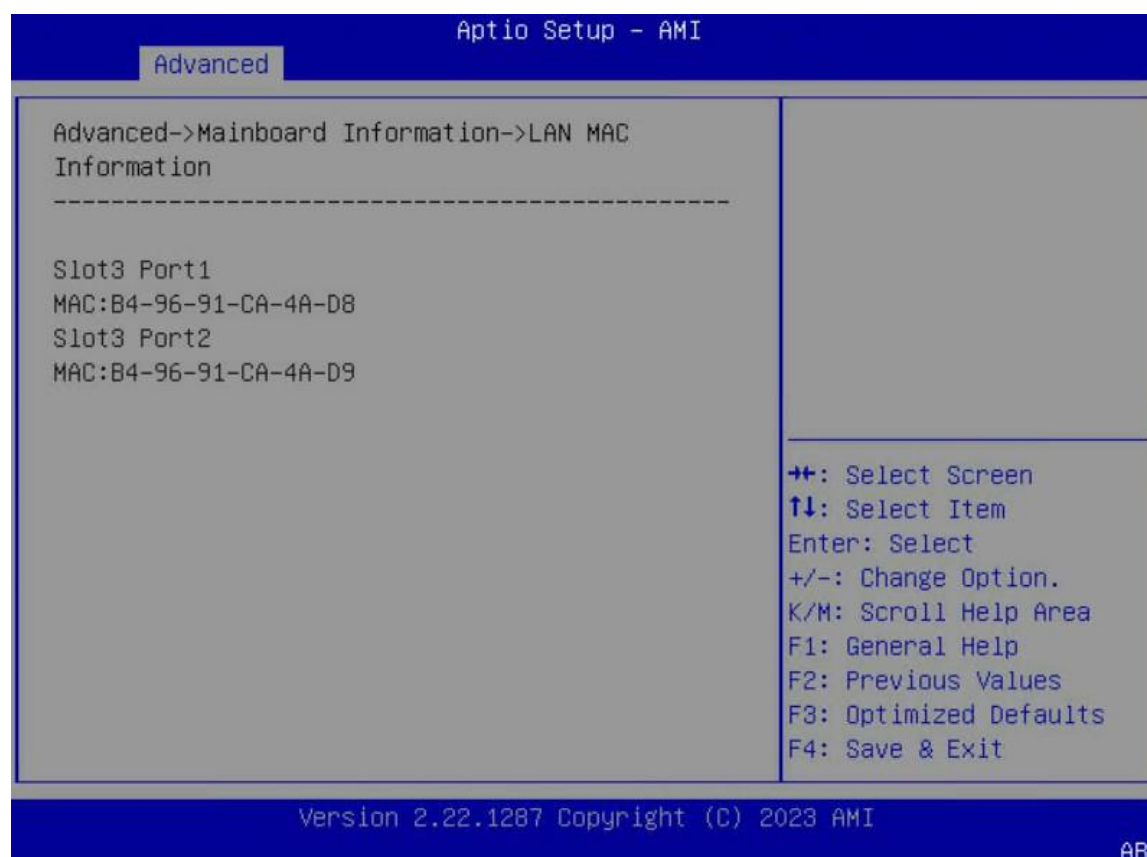


2. Select **Mainboard Information**, and then press **Enter**. The **Mainboard Information** screen is displayed, see [Figure 2-9](#).

Figure 2-9 Mainboard Information Screen

3. Select **LAN MAC Information**, and then press **Enter**. The **LAN MAC Information** screen is displayed, see [Figure 2-10](#).

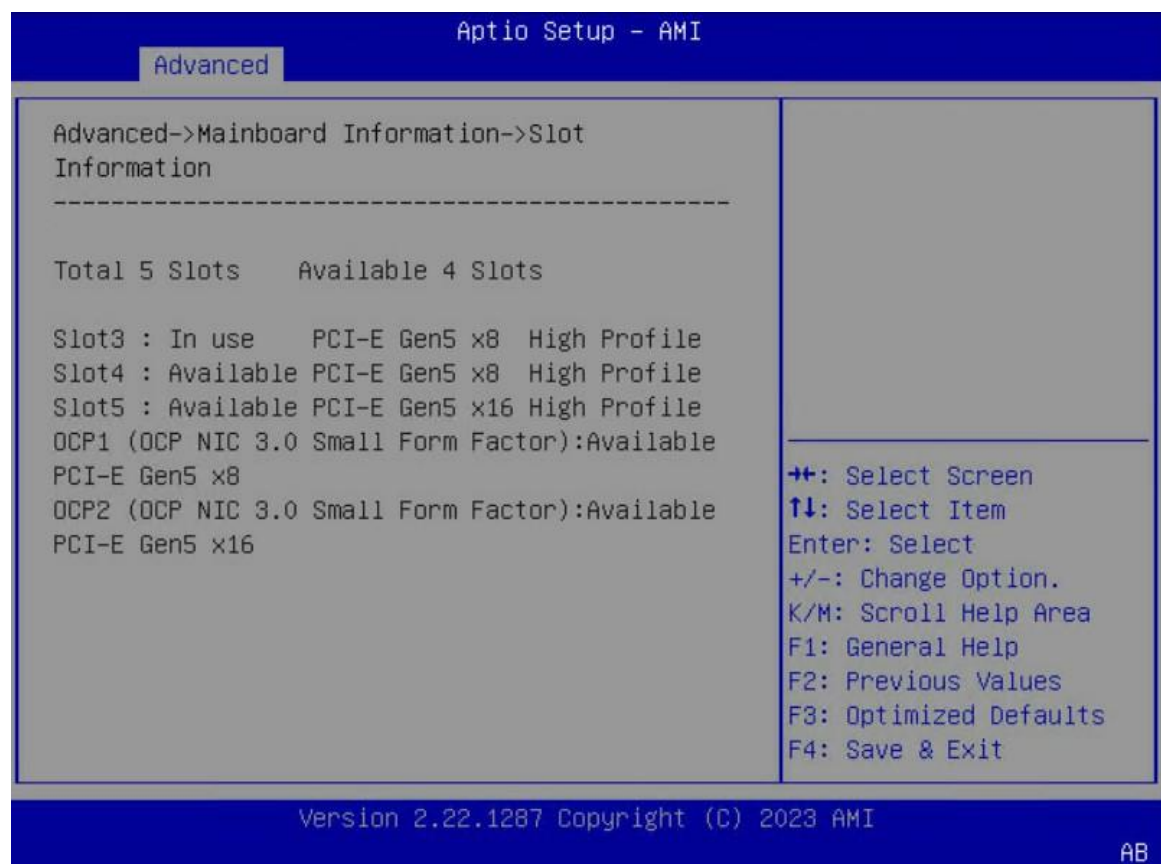
Figure 2-10 LAN MAC Information Screen



4. Press **Esc** to return to the **Mainboard Information** screen.

Querying Slot Status

5. Select **Slot Information**, and then press **Enter**. The **Slot Information** screen is displayed, see [Figure 2-11](#).

Figure 2-11 Slot Information Screen

Note

The slot status is described as follows:

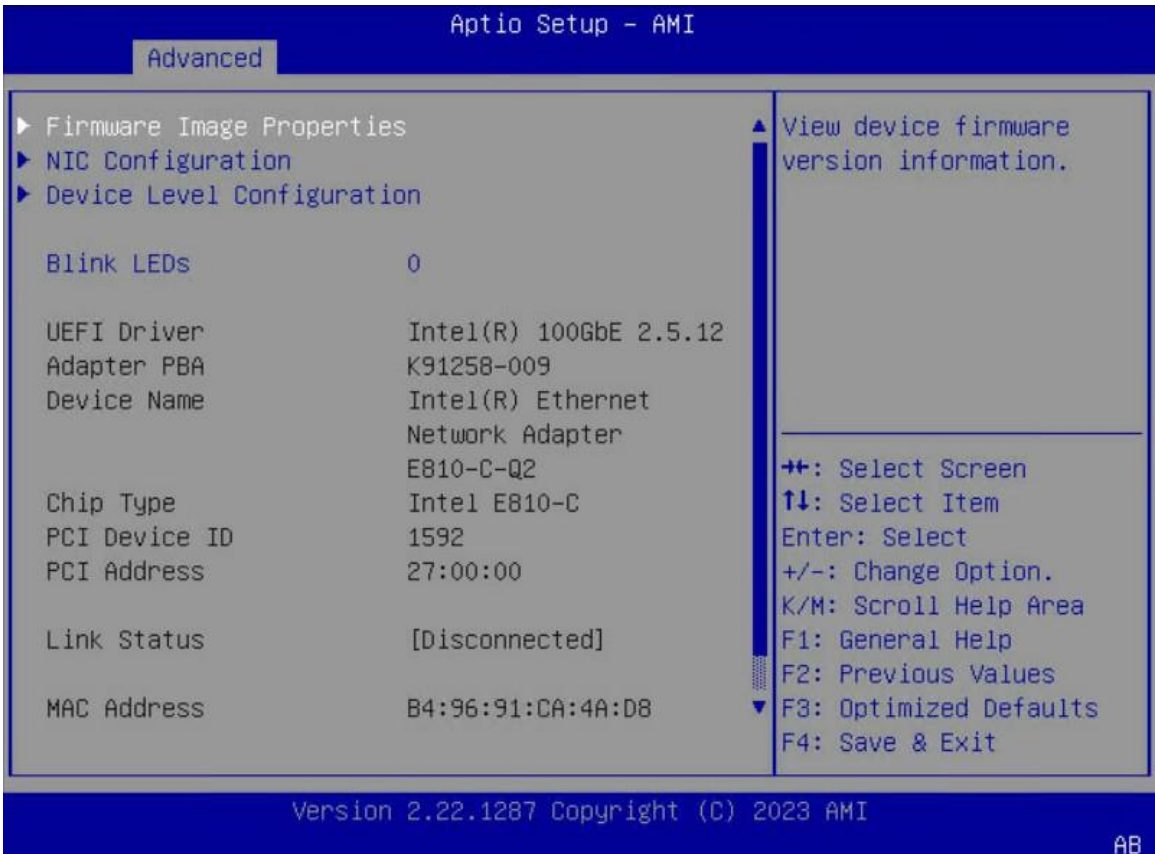
- **In Use:** indicates that a PCIe device is already installed in the slot.
- **Available:** indicates that the slot is available and no PCIe device is installed in it.

- Press **Esc** twice to return to the **Advanced** screen.

Querying NIC Details

- Select the desired NIC, for example, **Inter(R) Ethernet Network Adapter E810-C-Q2**, and then press **Enter**. The detailed information about the NIC is displayed, see [Figure 2-12](#).

Figure 2-12 Detailed NIC Information



2.7 Querying RAID Card Information

Abstract

This procedure describes how to query RAID card information to learn about the RAID card configurations.

RAID cards are divided into the following types by installation position:

- Onboard RAID card
- Standard RAID card

 Note

A RAID card connected to a PCIe slot is called a standard RAID card.

The methods for querying the information about the above two types of RAID cards are different.

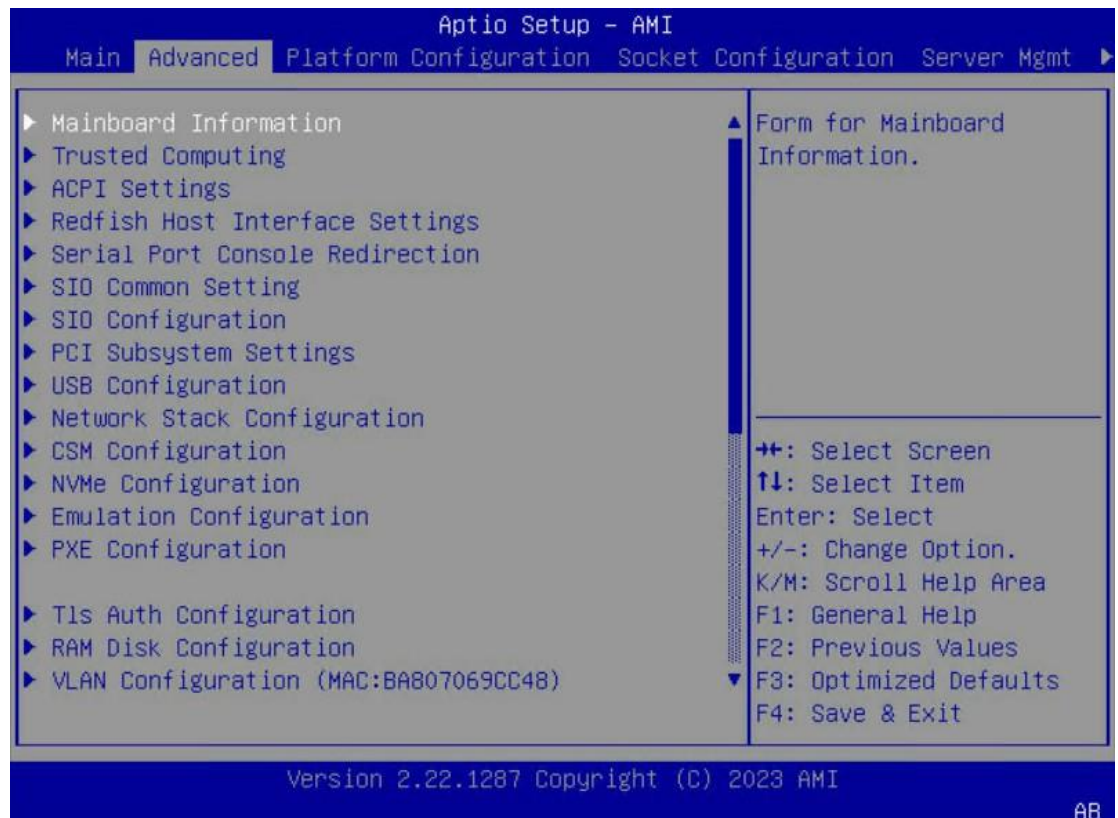
Prerequisite

The boot mode is already set to UEFI in the BIOS. For details, refer to [2.10 Setting the Boot Mode](#).

Steps

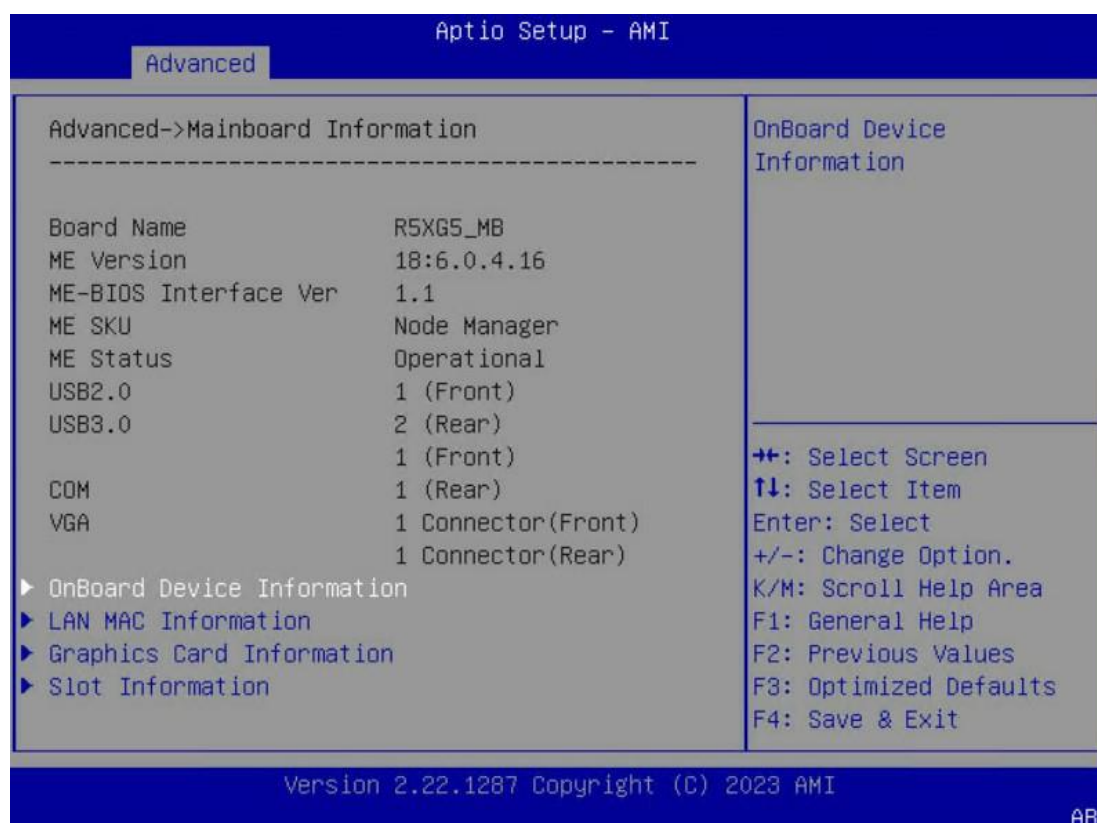
- Querying Onboard RAID Card Information
 1. On the **Aptio Setup** screen, select **Advanced**. The **Advanced** screen is displayed, see [Figure 2-13](#).

Figure 2-13 Advanced Screen

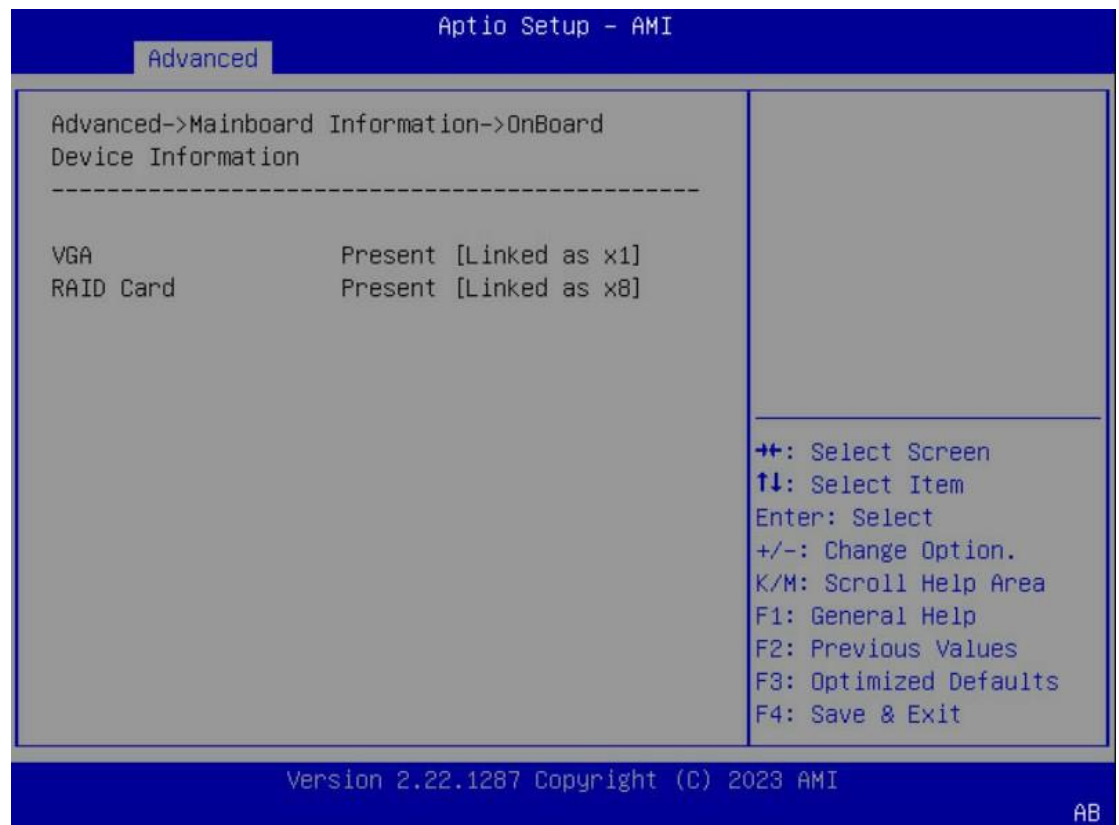


2. Select **Mainboard Information**, and then press **Enter**. The **Mainboard Information** screen is displayed, see [Figure 2-14](#).

Figure 2-14 Mainboard Information Screen



3. Select **OnBoard Device Information**, and then press **Enter**. The **OnBoard Device Information** screen is displayed, see [Figure 2-15](#).

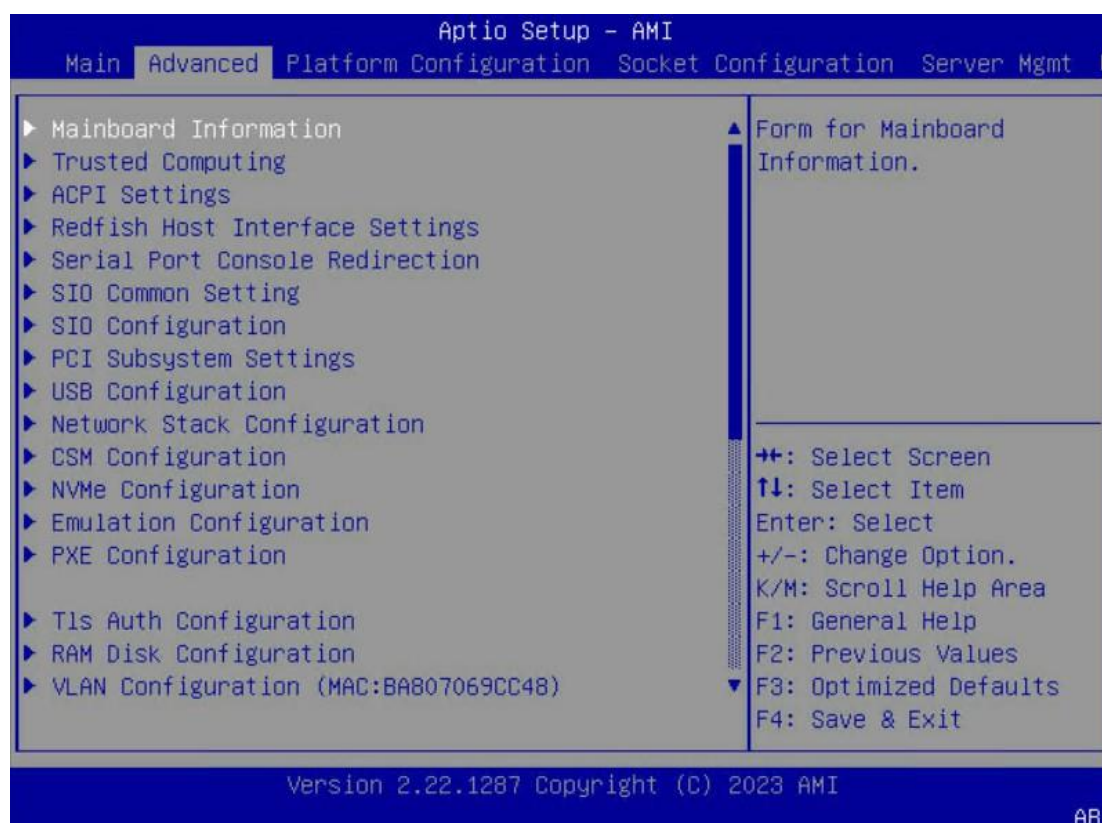
Figure 2-15 OnBoard Device Information Screen**Note**

The presence status of an onboard RAID card is described as follows:

- **Present:** The onboard RAID card is present and its bandwidth information is displayed.
- **Not Present:** The onboard RAID card is not present.

- Querying Standard RAID Card Information
 1. On the **Aptio Setup** screen, select **Advanced**. The **Advanced** screen is displayed, see [Figure 2-16](#).

Figure 2-16 Advanced Screen

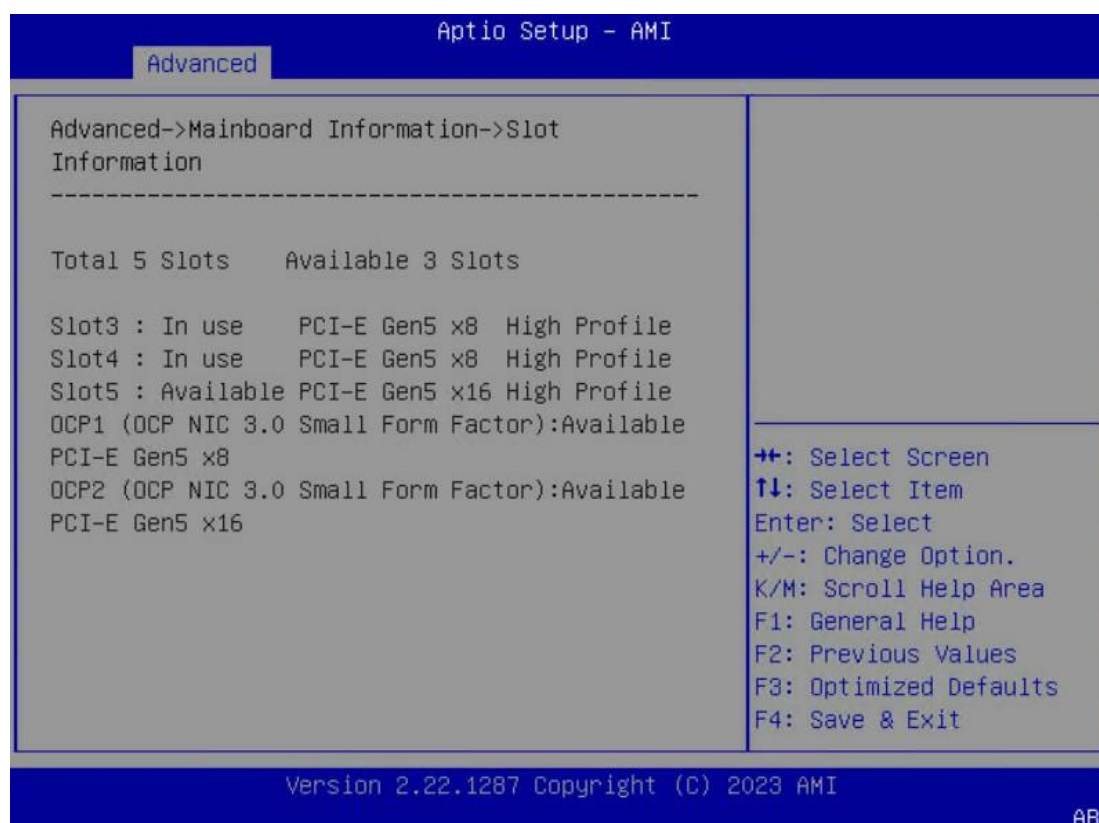


2. Select **Mainboard Information**, and then press **Enter**. The **Mainboard Information** screen is displayed, see [Figure 2-17](#).

Figure 2-17 Mainboard Information Screen

3. Select **Slot Information**, and then press **Enter**. The **Slot Information** screen is displayed, see [Figure 2-18](#).

Figure 2-18 Slot Information Screen

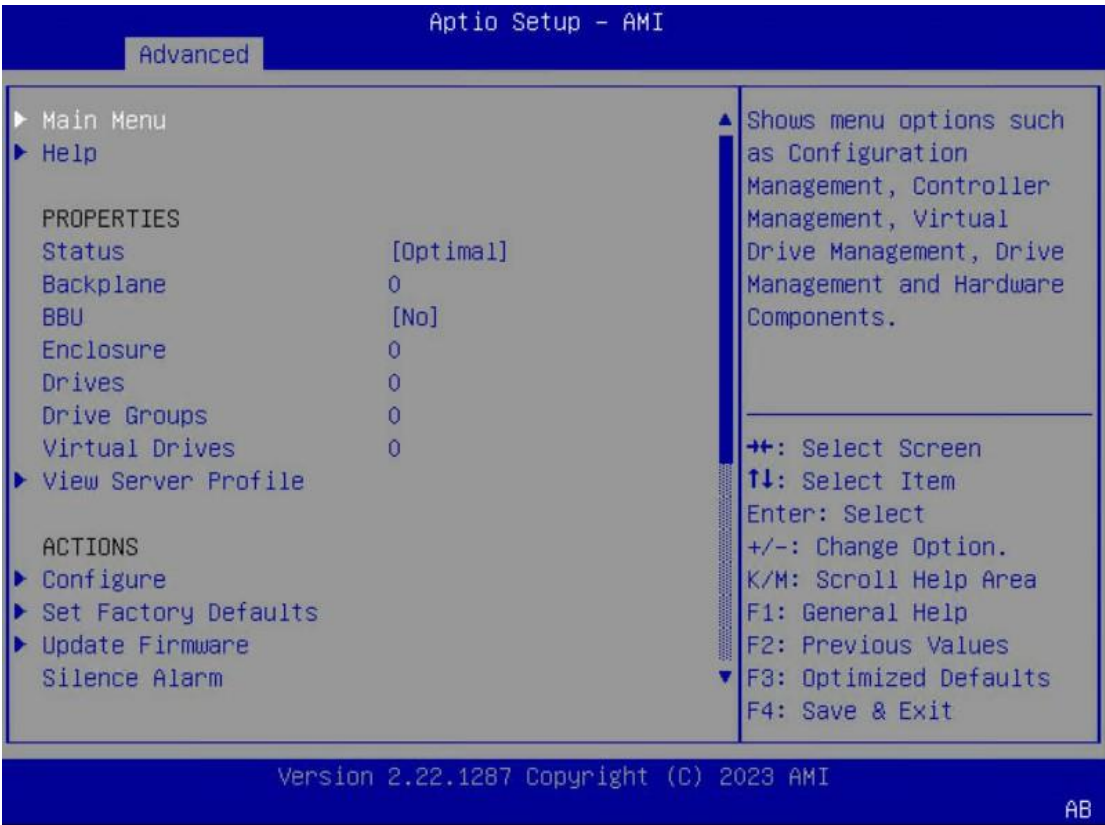
**Note**

The slot status is described as follows:

- ➔ **In Use:** indicates that a PCIe device is already installed in the slot.
- ➔ **Available:** indicates that the slot is available and no PCIe device is installed in it.

4. Press **Esc** twice to return to the **Advanced** screen.
5. Select a standard RAID card (for example, **AVAGO MegaRAID**), and then press **Enter**.
The detailed information about the standard RAID card is displayed, see [Figure 2-19](#).

Figure 2-19 Detailed Standard RAID Card Information



2.8 Querying Hard Disk Information

Abstract

This procedure describes how to query the hard disk information so that you can learn about the parameter settings of hard disks.

Steps

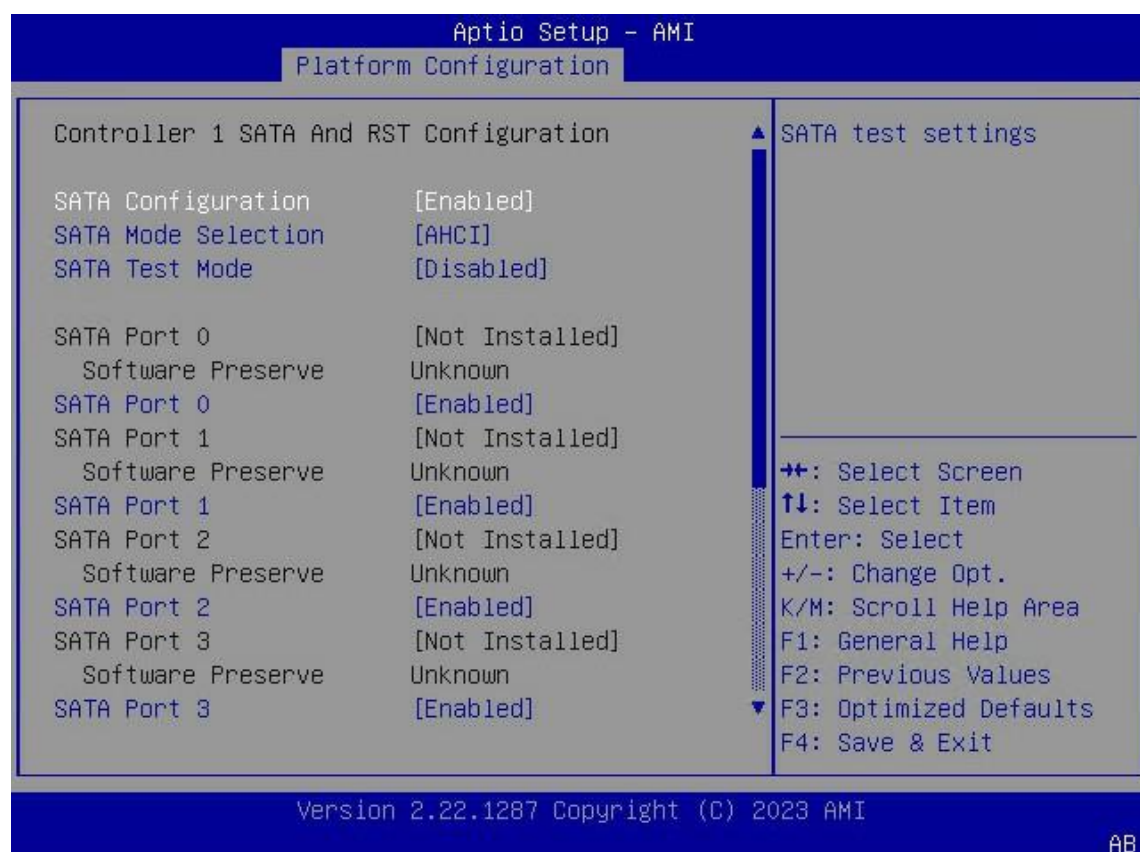
1. On the **Aptio Setup** screen, select the **Platform Configuration** menu. The **Platform Configuration** window is displayed.
2. Select **PCH-IO Configuration > SATA And RST Configuration > Controller x SATA And RST Configuration** and press **Enter**. The hard disk information is displayed, see [Figure 2-20](#).



Note

This procedure uses **Controller 1 SATA And RST Configuration** as an example.

Figure 2-20 Hard Disk Information



For a description of the parameters about hard disk information, refer to [Table 2-2](#).

Table 2-2 Hard Disk Information Parameter Descriptions

Parameter	Description	Default
SATA Configuration	Enables or disables the SATA configuration feature. Options: - Enabled: enables the SATA configuration feature. - Disabled: disables the SATA configuration feature. After the feature is disabled, the parameters below are hidden.	Enabled
SATA Mode Selection	Select a SATA mode. Options: AHCI: AHCI mode. When AHCI mode is selected, the SATA Interrupt Selection and RAID Device ID parameters are hidden. RAID: RAID mode.	AHCI

Parameter	Description	Default
SATA Interrupt Selection	Select the interrupt that the OS will use. This parameter takes effect only when the SAT controller is in RAID mode. Options: ● Msix ● Msi ● Legacy	Msix
SATA Test Mode	Enables or disables SATA Test mode. Options: ● Enabled: enables SATA Test mode. ● Disabled: disables SATA Test mode.	Disabled
RAID Device ID	Select the ID of the RAID device. This parameter takes effect only when the SATA controller is in RAID mode. Options: ● Client ● Alternate ● Server	Server
SATA Port 0	Name of the device installed in SATA port 0. If the device is present, the device information is displayed. If the device is not present, the information shows that the device is not installed.	-
Software Preserve	Software preservation.	Unknown
SATA Port 0	Enables or disables the SATA port. Options: ● Enabled ● Disabled	Enabled
Spin Up Device	If interleaving boot for any port is enabled, interleaving boot is performed only on the ports with the driver enabled. Options: ● Enabled ● Disabled	Disabled

2.9 Setting the BIOS Time

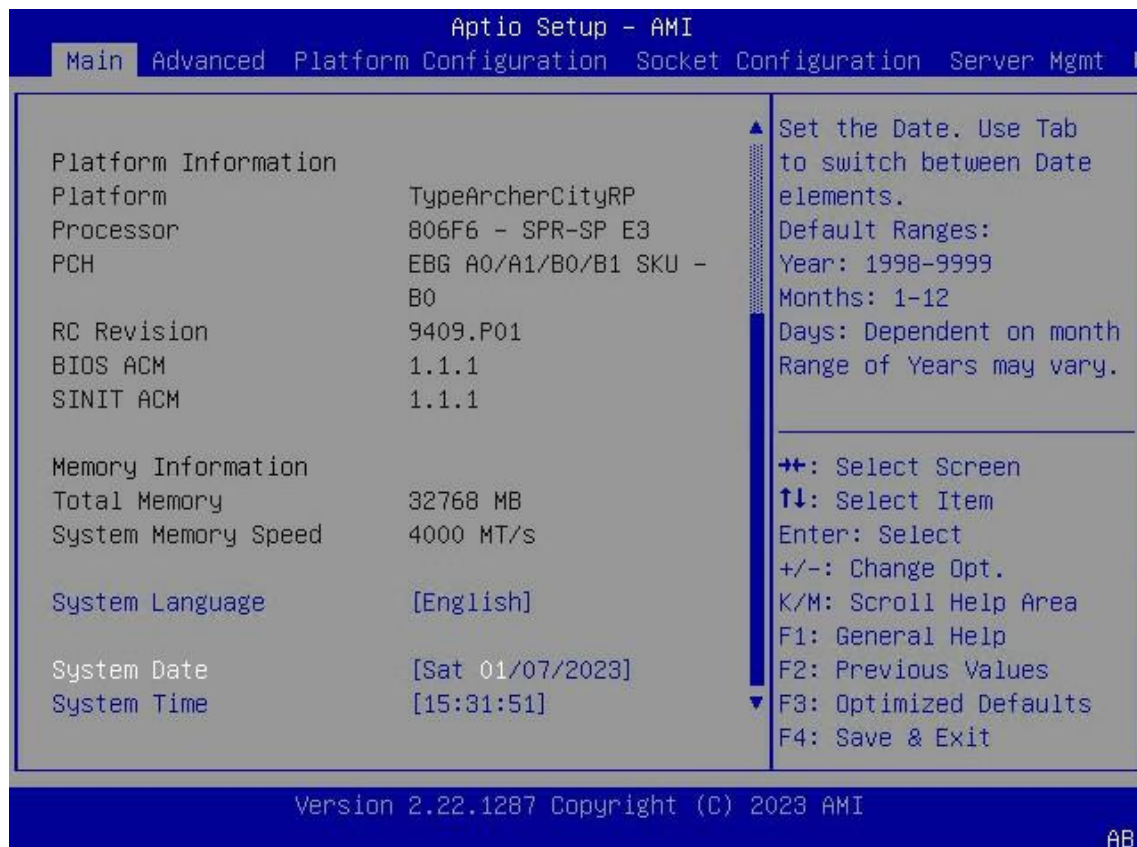
Abstract

This procedure describes how to set the **BIOS** time to the local time.

Steps

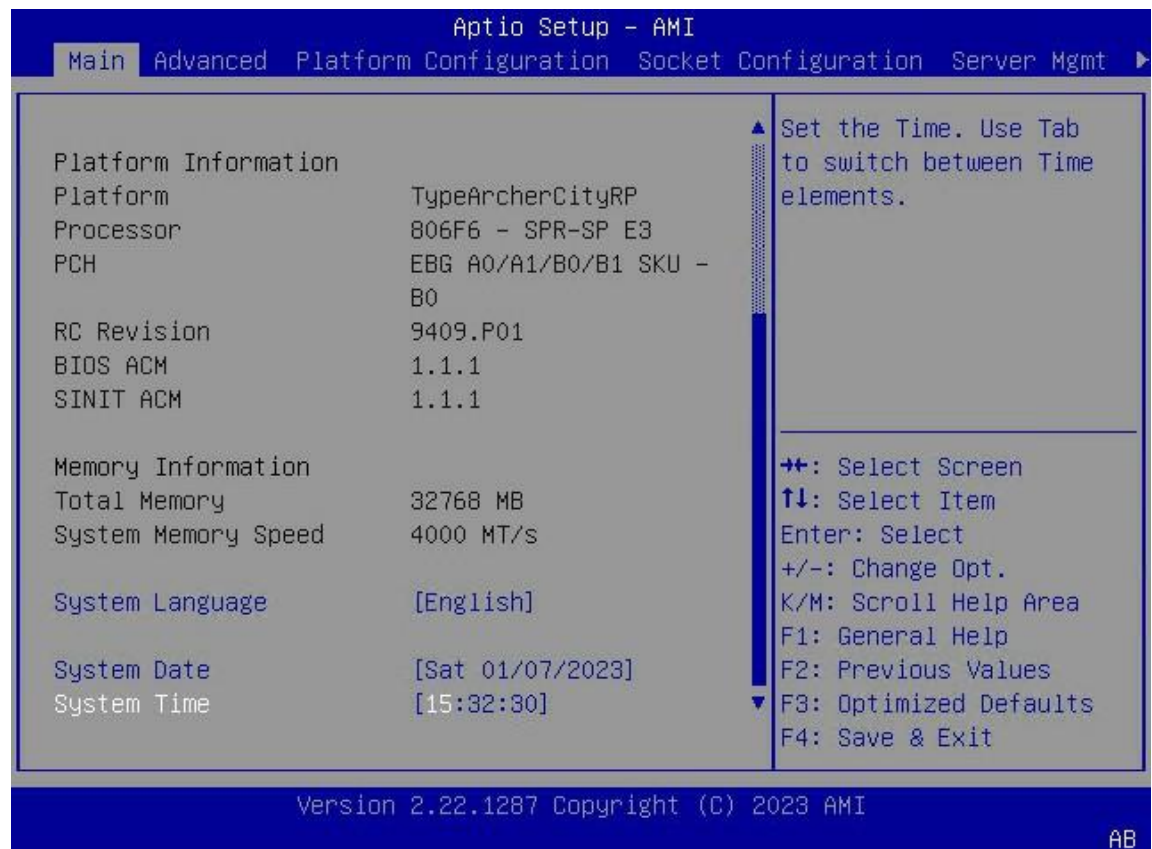
1. On the **Aptio Setup** screen, select the **Main** menu. The **Main** screen is displayed.
2. Select **System Date** and press **Enter** to move the cursor to the date, see [Figure 2-21](#).

Figure 2-21 Setting the Date



3. Set the date.
The date is displayed in MM/DD/YYYY format. Press **Enter** or **Tab** to switch between the month, date, and year items and change the settings as follows:
 - To increase the value by one, press **+**.
 - To decrease the value by one, press **-**.
 - To specify a value, press the corresponding number key.
4. Select **System Time** and press **Enter** to move the cursor to the time, see [Figure 2-22](#).

Figure 2-22 Setting the Time



5. Set the time.

The time is displayed in HH:MM:SS format based on a 24-hour clock system.

Press **Enter** or **Tab** to switch between the hour, minute, and second items and change the settings as follows:

- To increase the value by one, press **+**.
- To decrease the value by one, press **-**.
- To specify a value, press the corresponding number key.

6. Press **F4**. In the displayed dialog box, select **Yes**.

2.10 Setting the Boot Mode

Abstract

The server boot modes include:

- Legacy mode: a relatively old boot mode with certain limitations.
- **UEFI** mode: a relatively new boot mode that supports **PXE** over **IPv6** or **IPv4** and provides the UEFI Shell environment.

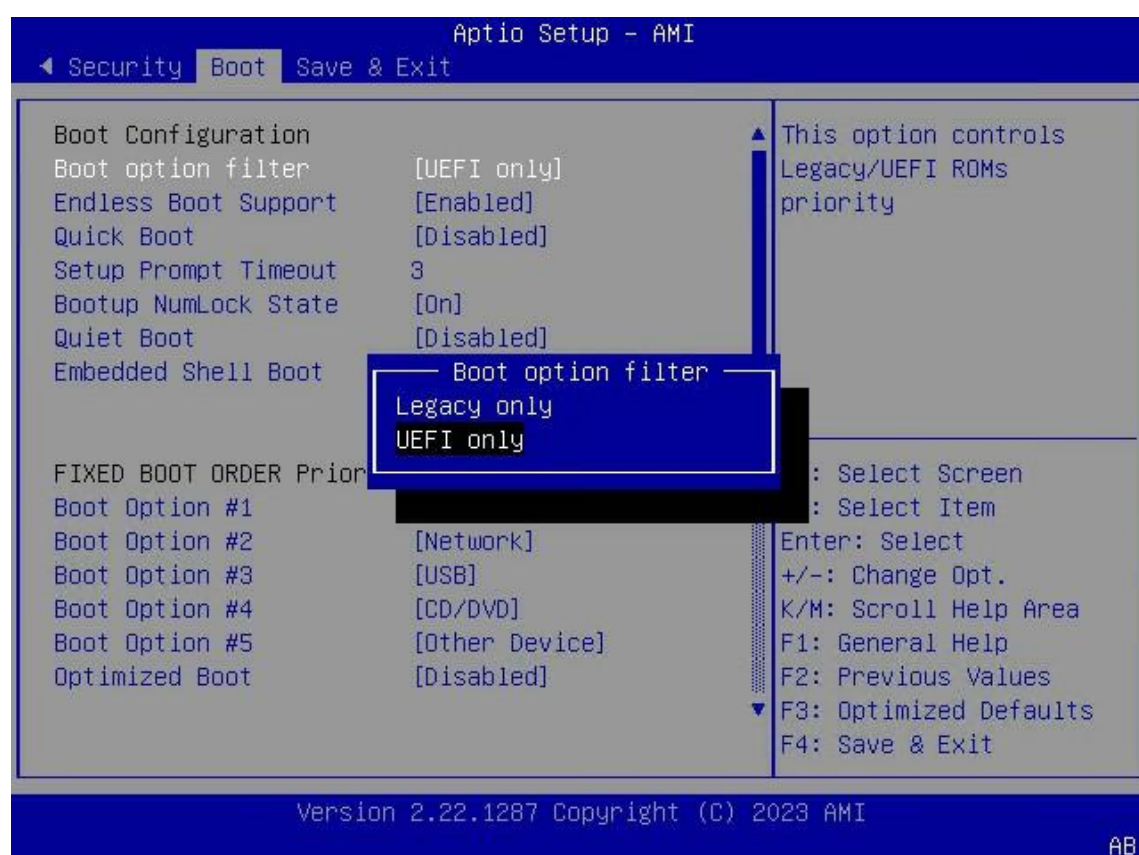
**Note**

UEFI mode is recommended.

Steps

1. On the **Aptio Setup** screen, select the **Boot** menu. The **Boot** screen is displayed.
2. Select **Boot option filter** and press the **Enter** key. The **Boot option filter** dialog box is displayed, see [Figure 2-23](#).

Figure 2-23 Boot Option Filter Dialog Box



3. Select **Legacy only** or **UEFI only** as needed.

**Note**

After the boot mode is changed, some configuration parameters of the BIOS are changed accordingly.

4. Press **F4**. In the displayed dialog box, select **Yes**.

2.11 Setting the Boot Order

Abstract

In most cases, a server is configured with multiple boot devices, for example, a hard disk, a [CD](#), or a [DVD](#).

This procedure describes how to adjust the priorities of these boot devices in the [BIOS](#) to set the boot order.

Context

By default, the boot order of the server is as follows:

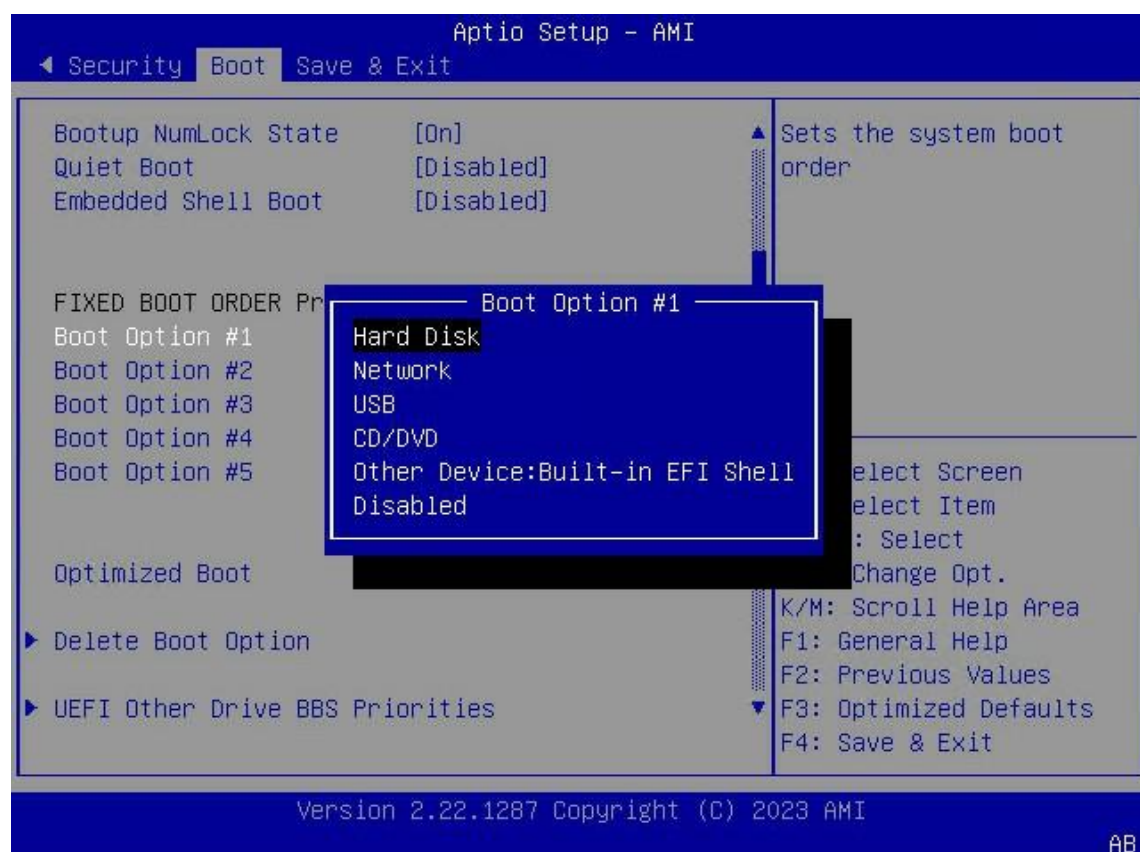
1. Hard disk
2. Network
3. [USB](#)
4. CD/DVD drive
5. Other devices

Steps

1. On the **Aptio Setup** screen, select the **Boot** menu. The **Boot** screen is displayed.
2. Under **FIXED BOOT ORDER Priorities**, select the option for which you want to adjust the boot order.

For example, to adjust the boot device with the first priority, select **Boot Option #1** and press the **Enter** key. The **Boot Option #1** dialog box is displayed, see [Figure 2-24](#).

Figure 2-24 Boot Option #1 Dialog Box



For a description of the boot devices, refer to [Table 2-3](#).

Table 2-3 Boot Device Descriptions

Boot Device	Description
Hard Disk	Boots the server from a hard disk.
Network	Boots the server from a network device.
USB	Boots the server from a USB device.
CD/DVD	Boots the server from a CD/DVD-ROM drive.
Other Device:Built-in EFI Shell	Boots the server from another device.
Disabled	Disables this option.

- Press the up/down key to select another device that will serve as the first boot device in the boot sequence. Press **Enter**.
- (Optional) Adjust boot devices with other priorities by referring to [Step 2](#) through [Step 3](#).
- Press **F4**. In the displayed dialog box, select **Yes**.

2.12 Setting the BIOS Password

Abstract

BIOS passwords include an administrator password and a user password. By default, neither the administrator password nor the user password is set.

To ensure server security, it is recommended that you set BIOS passwords immediately at first login and properly keep the passwords.



Note

This procedure describes how to set the administrator password. You can set the user password by using the same method.

Context

After you log in to the BIOS by using the administrator password, you can perform operations by using the administrator permission. After you log in to the BIOS by using the user password, you can perform operations by using the user permission. For the items that cannot be set by the user, refer to [Table 2-4](#).

Table 2-4 Descriptions of the Items Not Available for the User

Level-1 Menu	Level-2 menu	Level-3 menu
Advance	ACPI Settings	Enabled ACPI Auto Configuration
		Hibernation
	Redfish Host Interface Settings	IP address
		IP Mask address
		IP Port
	PCI Subsystem Settings	Above 4G Decoding
		SR-IOV Support
	USB Configuration	Legacy USB Support
		XHCI Hand-off
		USB Boot
Server Mgmt	POST Timer	-
	POST Timer timeout	-
	POST Timer Policy	-
	OS Watchdog Timer	-
	OS Wtd Timer Timeout	-

Level-1 Menu	Level-2 menu	Level-3 menu
	OS Wtd Timer Policy	-
	Restore on AC power loss	-
	Set BMC to default	-
	View FRU information	-
	BMC network configuration	-
	BMC User Settings	-
Security	Administrator Password	-

Steps

1. On the **Aptio Setup** screen, select the **Security** menu. The **Security** screen is displayed.
2. Select **Administrator Password** and press **Enter**. The **Create New Password** dialog box is displayed, see [Figure 2-25](#).

Figure 2-25 Create New Password Dialog Box



3. Enter the password and press **Enter**. In the displayed **Confirm New Password** dialog box, enter the password again and then press **Enter**.

**Note**

The password consists of 8 to 32 characters, including uppercase and lowercase letters, digits, and special characters.

4. Press **F4**. In the displayed dialog box, select **Yes**.

Related Tasks

To change the password, perform the following steps:

1. On the **Security** screen, select **Administrator Password** and press **Enter**. The **Enter Current Password** dialog box is displayed, see [Figure 2-26](#).

Figure 2-26 Enter Current Password Dialog Box



2. Enter the current BIOS password and press the **Enter** key. In the two dialog boxes that are displayed, enter the new password and then press the **Enter** key.

**Note**

The new password cannot be the same as the last three passwords used for the account.

3. Press **F4**. In the displayed dialog box, select **Yes**.

2.13 Deleting a BIOS Password

Abstract

In a special case, a **BIOS** password can be cleared.

Note

After a BIOS password is set, you must enter the password if you want to delete it. If you do not enter it, you cannot delete it. Therefore, you must properly keep the password. This procedure describes how to delete the administrator password. You can delete the user password by using the same method.

Steps

1. On the **Aptio Setup** screen, select the **Security** menu. The **Security** screen is displayed.
2. Select **Administrator Password** and press **Enter**. The **Enter Current Password** dialog box is displayed, see [Figure 2-27](#).

Figure 2-27 Enter Current Password Dialog Box



3. Enter the current BIOS password and press **Enter**. In the displayed dialog box, do not enter any password. Directly press **Enter**. The **WARNING** dialog box is displayed, see [Figure 2-28](#).

Figure 2-28 WARNING Dialog Box



4. Select **Yes**. The **Security** screen is displayed.
5. Press **F4**. In the displayed dialog box, select **Yes**.

2.14 Setting the PCIe Function for a Port

Abstract

After the **PCIe** feature of a port is enabled, the port adapts to different PCIe cards to maximize port resource utilization.

Steps

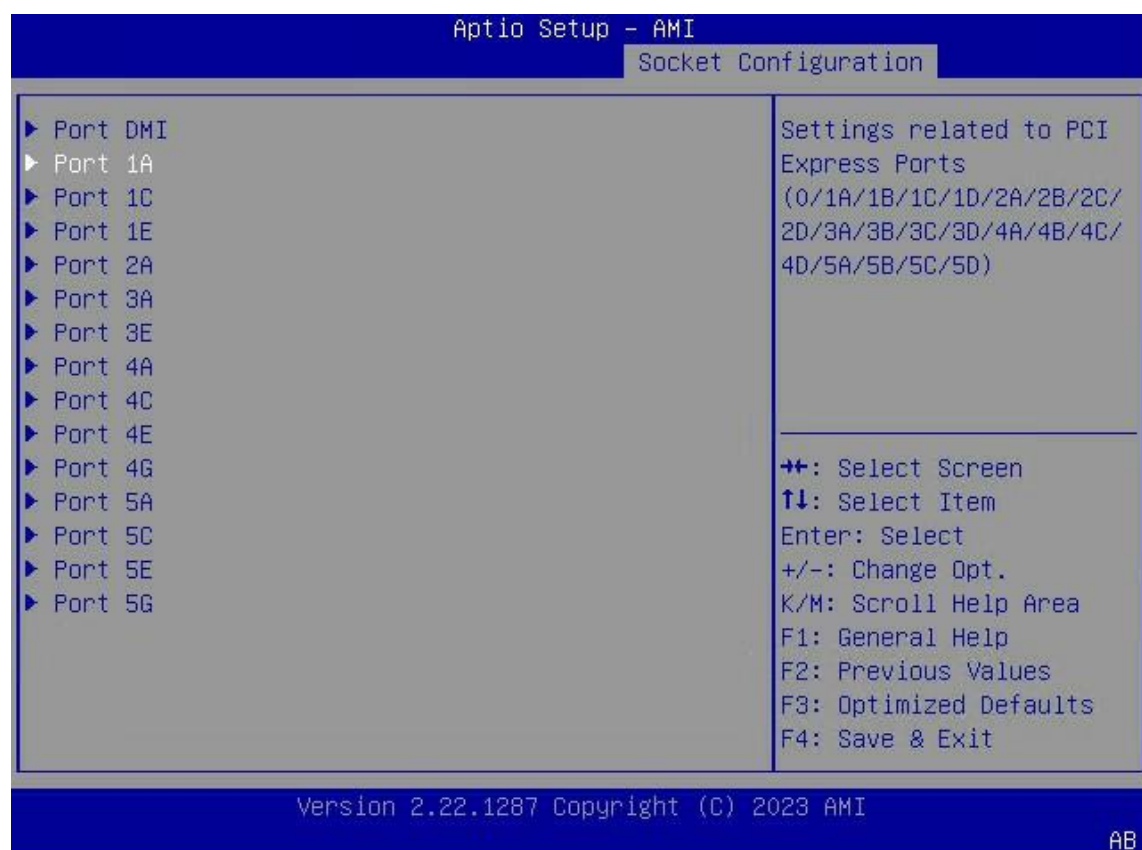
1. On the **Aptio Setup** screen, select the **Socket Configuration** menu. The **Socket Configuration** window is displayed.
2. Select **IIO Configuration > Socketx Configuration** and press **Enter**. The **Socketx Configuration** screen is displayed, see [Figure 2-29](#).



Note

This procedure uses **Socket1 Configuration** as an example.

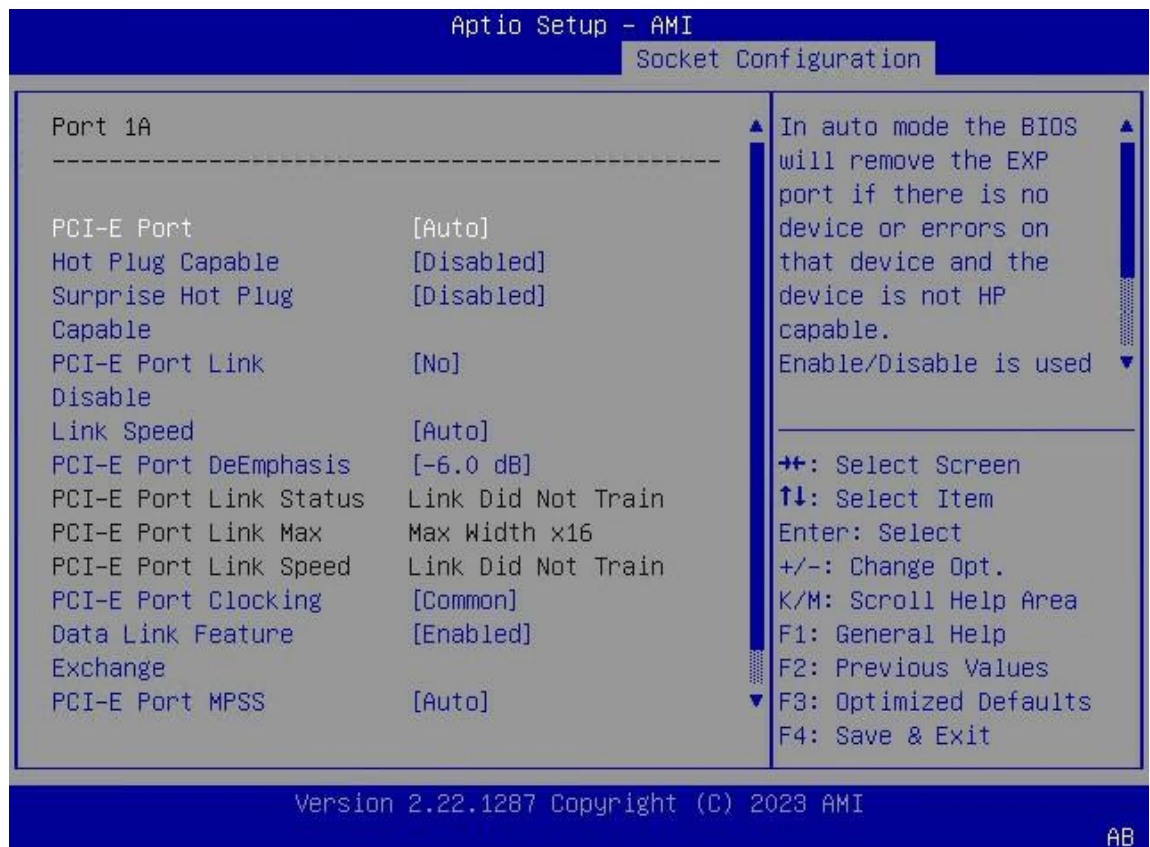
Figure 2-29 Socket1 Configuration Screen



3. Select the port that you want to configure and then press **Enter**. The screen for configuring the port is displayed, see [Figure 2-30](#).

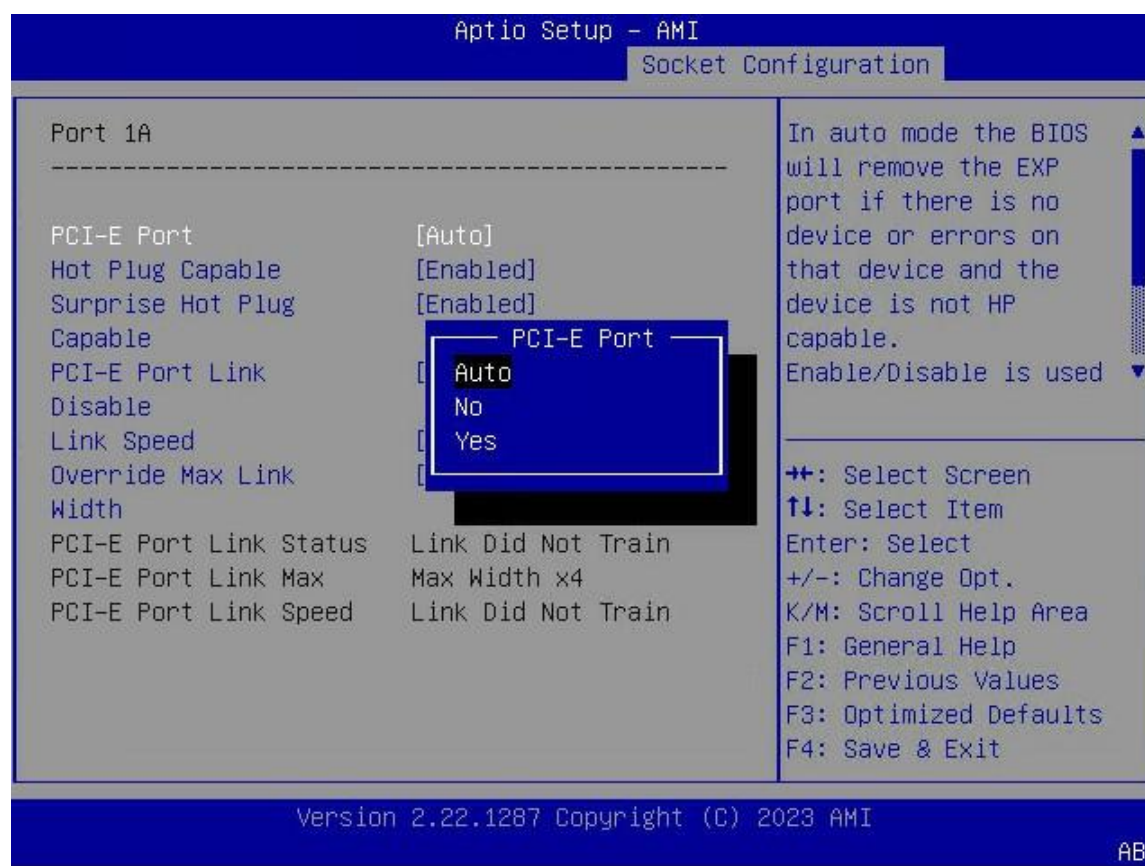
Note

This procedure uses **Port 1A** as an example.

Figure 2-30 Port 1A Screen

4. Select **PCI-E Port** and press **Enter**. The **PCI-E Port** dialog box is displayed, see [Figure 2-31](#).

Figure 2-31 PCI-E Port Dialog Box



5. Select the desired PCIe feature as needed and then press **Enter**.
 - Auto: automatic
 - No: disabled
 - Yes: enabled
6. Press **F4**. In the displayed dialog box, select **Yes**.

2.15 Setting Serial Port Console Redirection

Abstract

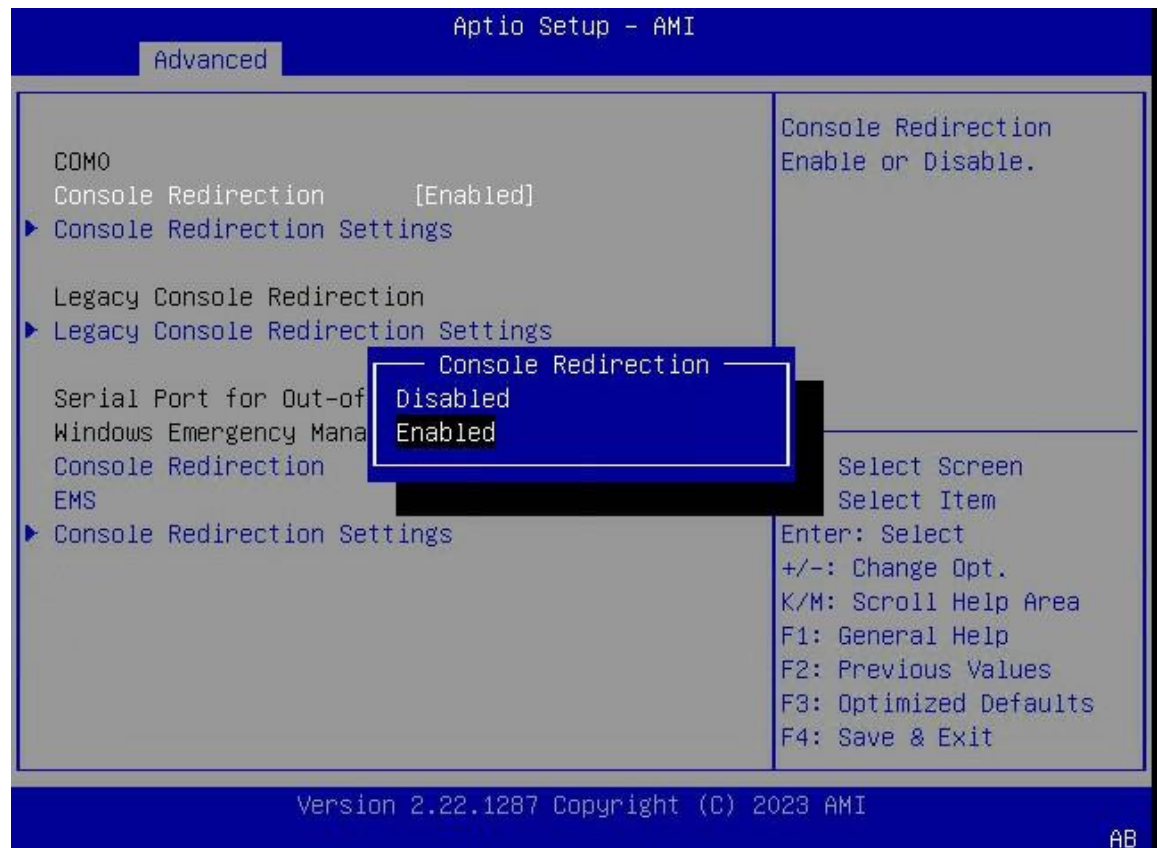
This procedure describes how to set serial port console redirection to redirect the console output to a serial port.

Steps

1. On the **Aptio Setup** screen, select the **Advanced** menu. The **Advanced** screen is displayed.
2. Select **Serial Port Console Redirection** and press **Enter**. The **Serial Port Console Redirection** screen is displayed.

3. Select **Console Redirection** and press **Enter**. The **Console Redirection** dialog box is displayed, see [Figure 2-32](#).

Figure 2-32 Console Redirection Dialog Box



4. Select **Enabled** and press **Enter**.
5. Press **F4**. In the displayed dialog box, select **Yes**.

2.16 Querying BMC Network Parameter Settings

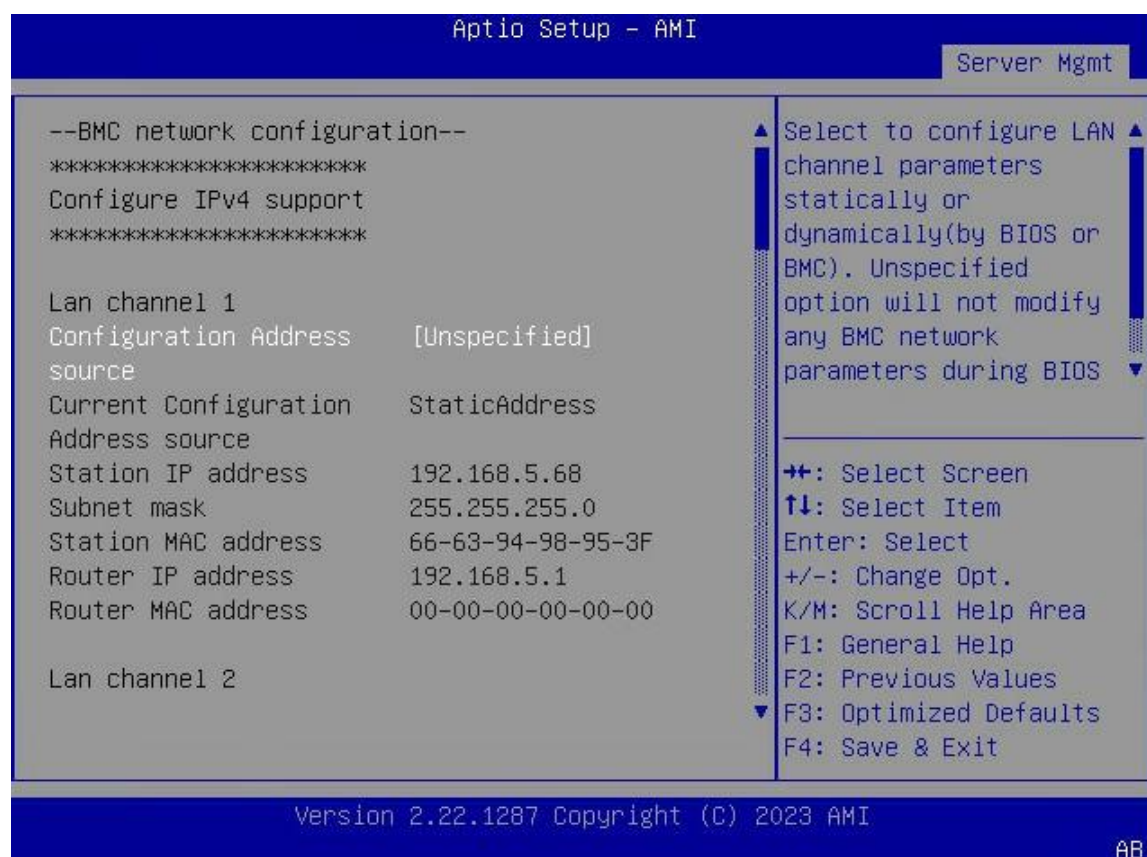
Abstract

This procedure describes how to query **BMC** network parameter settings.

Steps

1. On the **Aptio Setup** screen, select the **Server Mgmt** menu. The **Server Mgmt** screen is displayed.
2. Select **BMC network Configuration** and press **Enter**. The **BMC network Configuration** screen is displayed, see [Figure 2-33](#).

Figure 2-33 BMC Network Configuration Screen



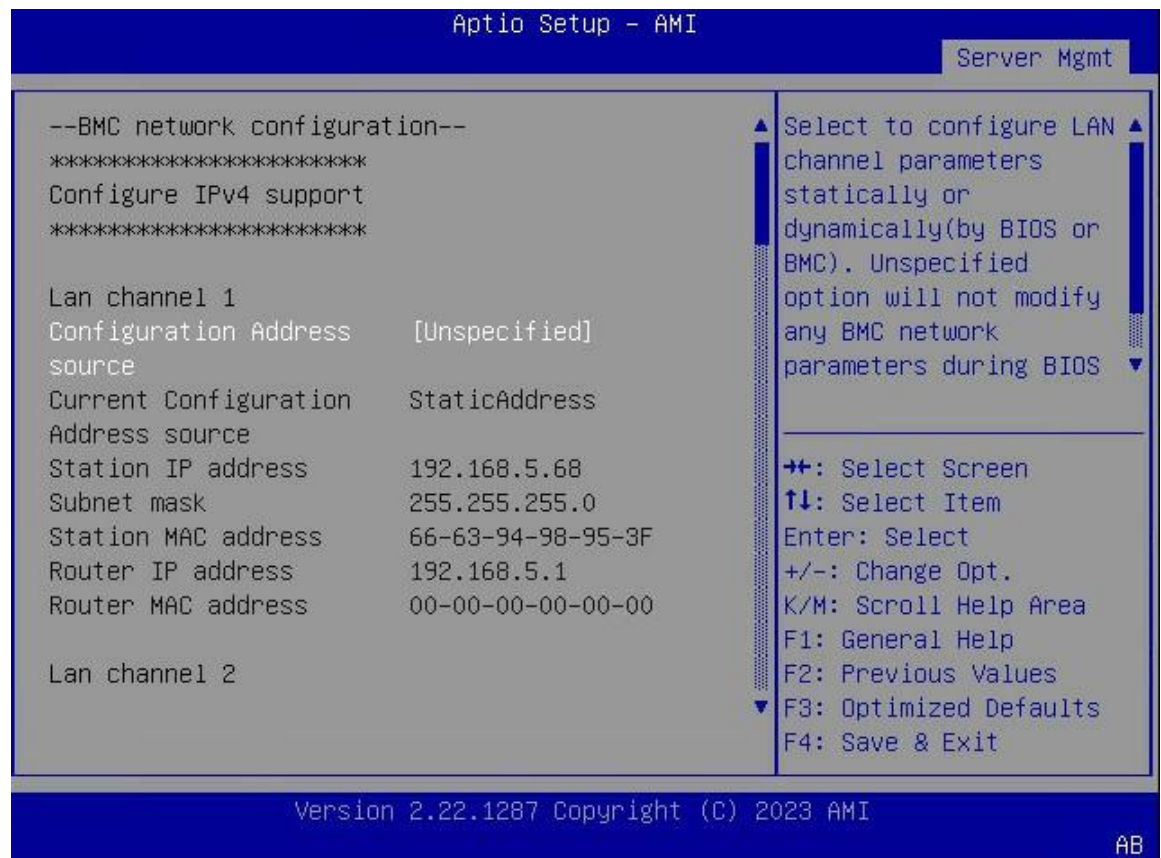
2.17 Setting BMC Network Parameters

Abstract

This procedure describes how to set the **BMC** network parameters so that the local **PC**, as a client, can connect to the BMC.

Steps

1. On the **Aptio Setup** screen, select the **Server Mgmt** menu. The **Server Mgmt** screen is displayed.
2. Select **BMC network configuration** and press **Enter**. The **BMC network configuration** screen is displayed, see [Figure 2-34](#).

Figure 2-34 BMC Network Configuration Screen

3. Select each parameter that you need to set and press the **Enter** key. The screen for setting the parameter is displayed. Set the parameter. For a description of the parameters, refer to [Table 2-5](#).

Table 2-5 BMC Network Parameter Descriptions

Parameter	Description
Configure IPv4 support	
Configuration Address source	Sets the IPv4 address configuration method of Channel 1/Channel 2: ● Unspecified: undefined. ● Static: static mode, in which the IP address is manually set. ● DynamicBmcDhcp: The IP address is dynamically obtained through BMC DHCP. ● DynamicBmcNonDhcp: The IP address is dynamically obtained through the BMC.
Configure IPv6 support	
IPv6 Support	Sets whether or not Channel 1/Channel 2 supports the IPv6 configuration. ● Enabled: IPv6 configuration is supported. The following IPv6 parameters can be configured only when Enabled is selected. ● Disabled: IPv6 configuration is not supported.

Parameter	Description
	If Disabled is selected, the following IPv6 parameters cannot be configured.
Configuration Address source	Sets the IPv6 address configuration method of Channel 1 or Channel 2: ● Unspecified: undefined. ● Static: static mode, in which the IP address is manually set. ● DynamicBmcDhcp: The IP address is dynamically obtained through BMC DHCP.
Configure VLAN support	
VLAN Support	Sets whether or not Channel/Channel 2 supports the VLAN configuration. ● Enabled: VLAN configuration is supported. The following VLAN parameters can be configured only when Enabled is selected. ● Disabled: VLAN configuration is not supported. If Disabled is selected, the following VLAN parameters cannot be configured.

4. Press **F4**. In the displayed dialog box, select **Yes**.

2.18 Setting the PXE Function for a NIC

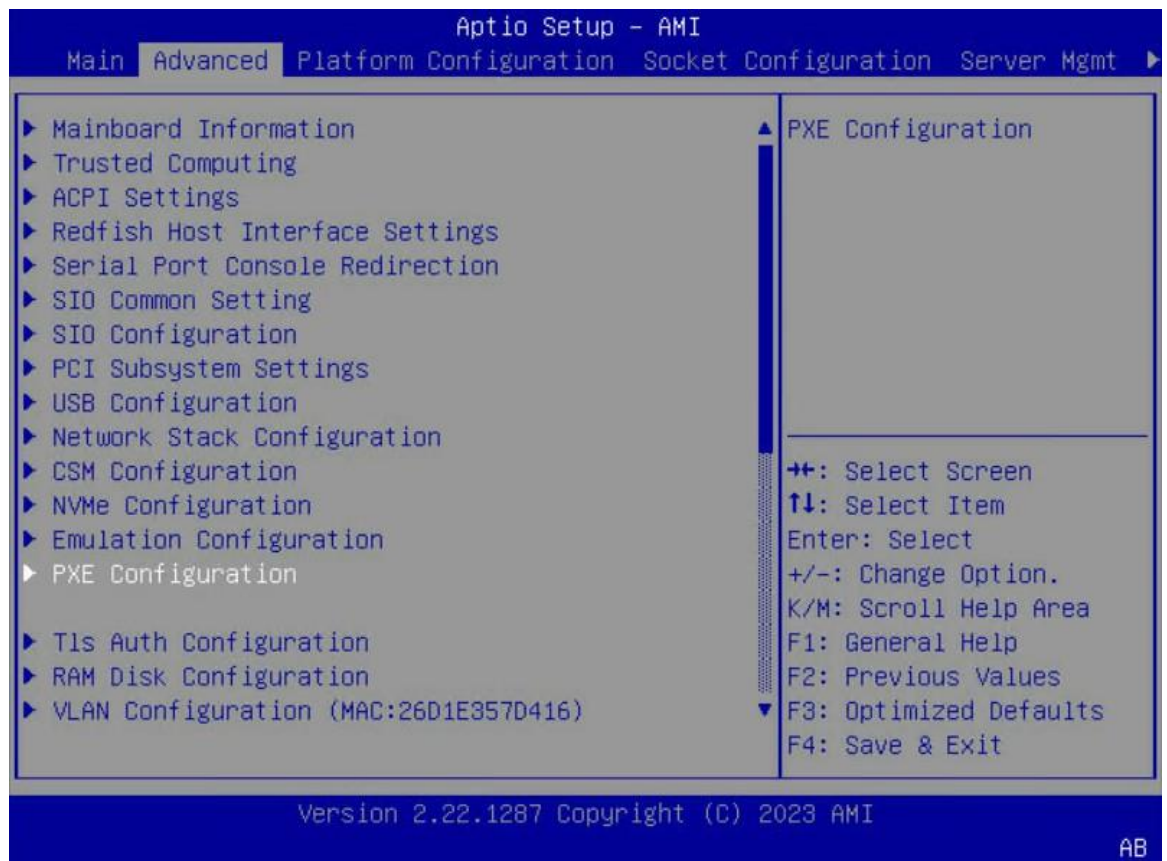
Abstract

This procedure describes how to enable the **PXE** function for a **NIC** in a server to control the server over the network.

Steps

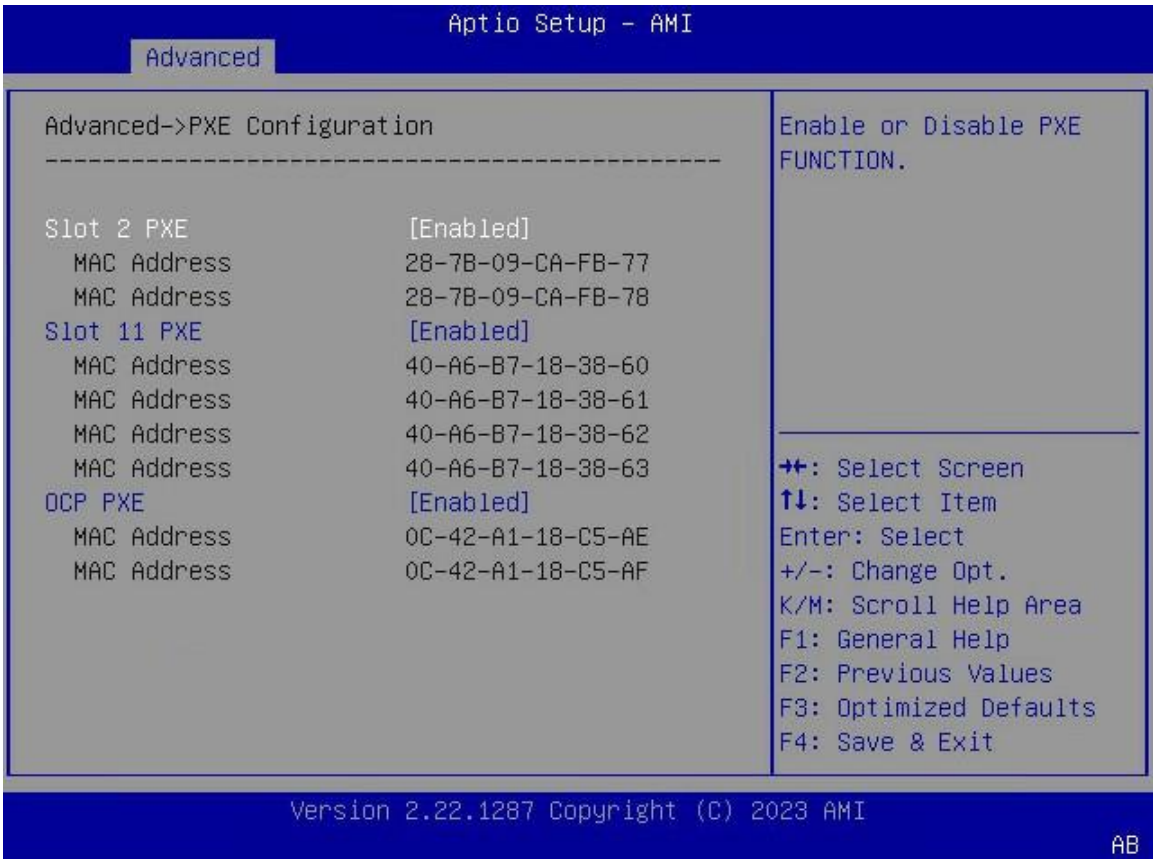
1. On the **Aptio Setup** screen, select **Advanced**. The **Advanced** screen is displayed, see [Figure 2-35](#).

Figure 2-35 Advanced Screen



2. Select **PXE Configuration**, and then press **Enter**. The **PXE Configuration** screen is displayed, see [Figure 2-36](#).

Figure 2-36 PXE Configuration Screen



 Note

The **PXE Configuration** screen only displays the NIC information about the server, which is for reference only. The NIC information depends on the actual configuration.

- 3. Select the desired NIC, and then press **Enter**. In the displayed dialog box, select **Enabled** to enable the PXE function for the NIC.
- 4. Press **F4**. In the displayed dialog box, select **Yes**.

2.19 Setting Virtualization Parameters

Abstract

This procedure describes how to set virtualization parameters to improve server performance.

Context

For a description of common virtualization parameters, refer to [Table 2-6](#).

Table 2-6 Common Virtualization Parameter Descriptions

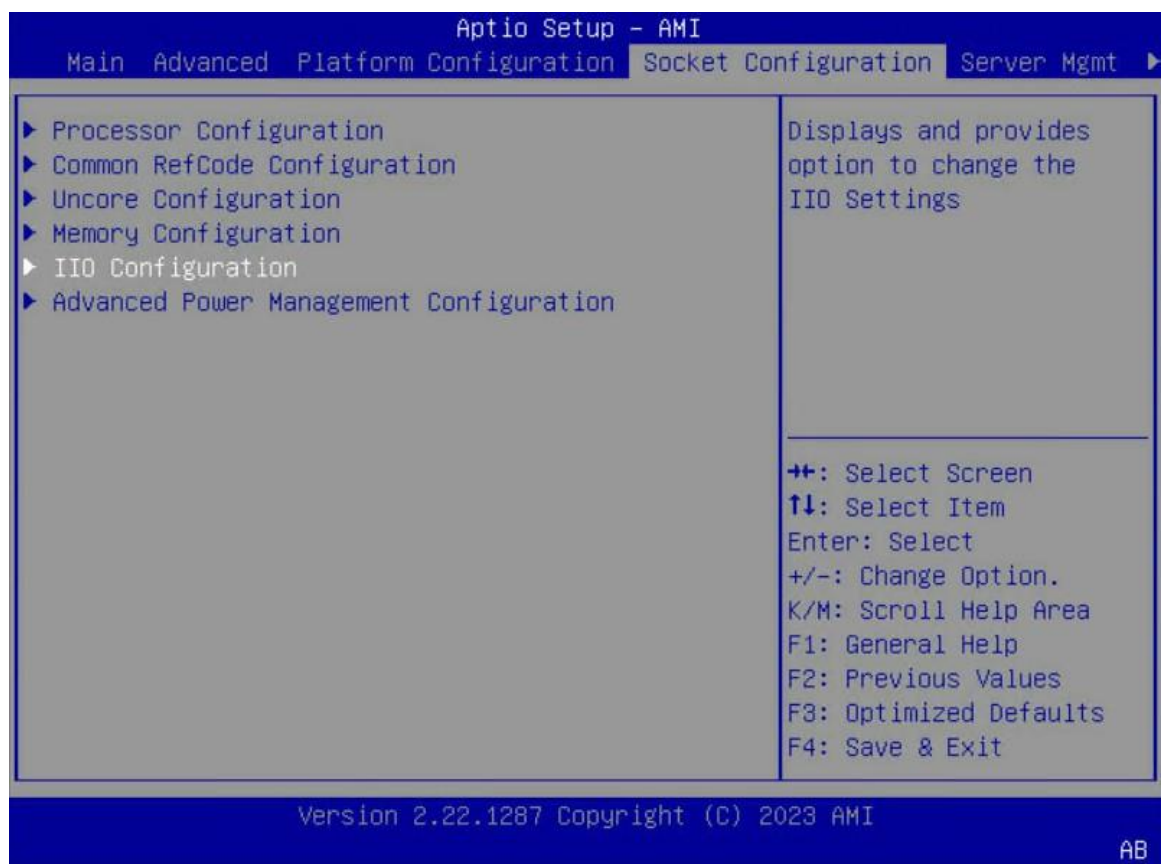
Parameter	Description	Recommended Configuration
Intel VT for Directed I/O	Specifies whether to enable the I/O virtualization function (namely, the VT-d function). After the VT-d function is enabled, the VMM manages the access of multiple VMs to the same physical I/O device through this function.	Enabled
VMX	Specifies whether to enable the CPU virtualization function. After the CPU virtualization function is enabled, the virtualization layer or operating system that supports the CPU virtualization technology can use the hardware capabilities of Intel's virtualization technologies.	Enabled
SR-IOV Support	Specifies whether to enable the SR-IOV function. After the SR-IOV function is enabled, a physical I/O device (typically a network adapter) can be virtualized into multiple independent I/O devices that can be used by multiple VMs. This reduces the CPU load of the host and network latency, improving network performance.	Enabled

Steps

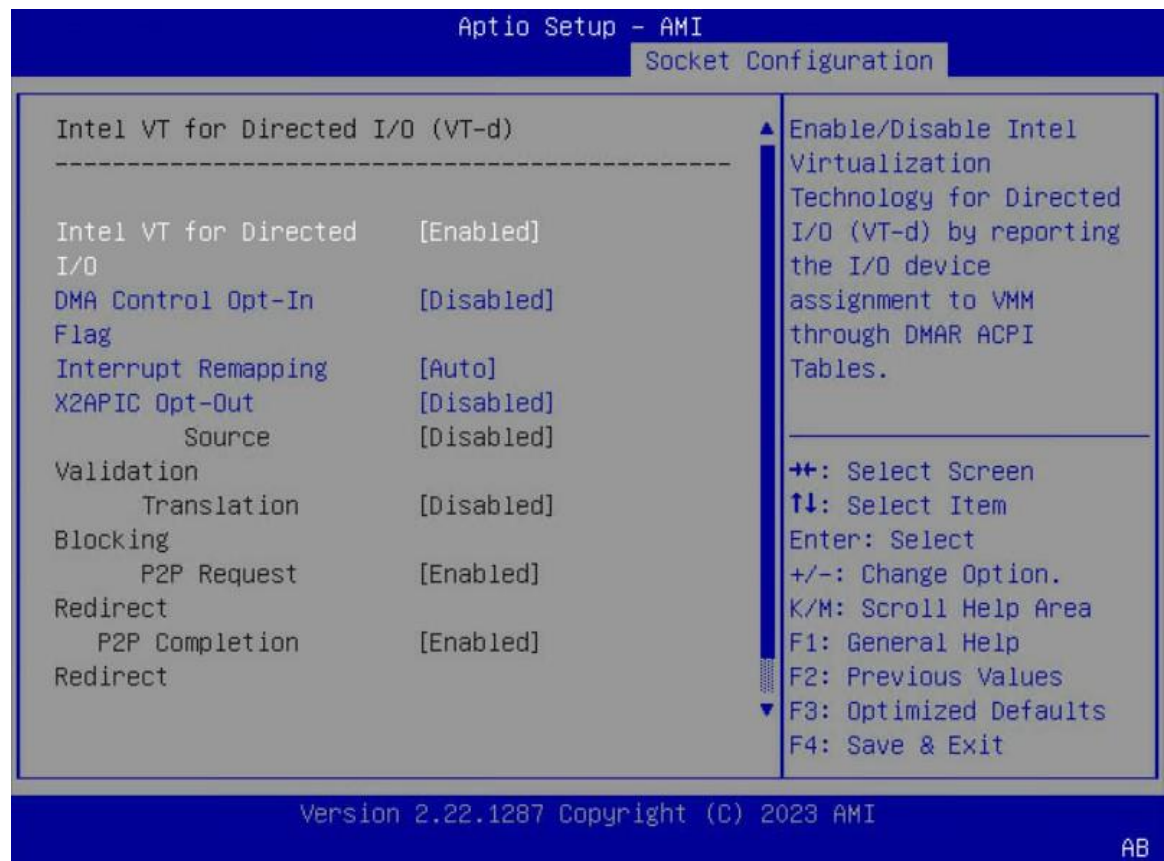
Configuring Intel VT for Directed I/O

1. On the **Aptio Setup** screen, select **Socket Configuration**. The **Socket Configuration** screen is displayed, see [Figure 2-37](#).

Figure 2-37 Socket Configuration Screen



2. Select **IIO Configuration > Intel VT for Directed I/O (VT-d)**, and then press **Enter**. The **Intel VT for Directed I/O (VT-d)** screen is displayed, see [Figure 2-38](#).

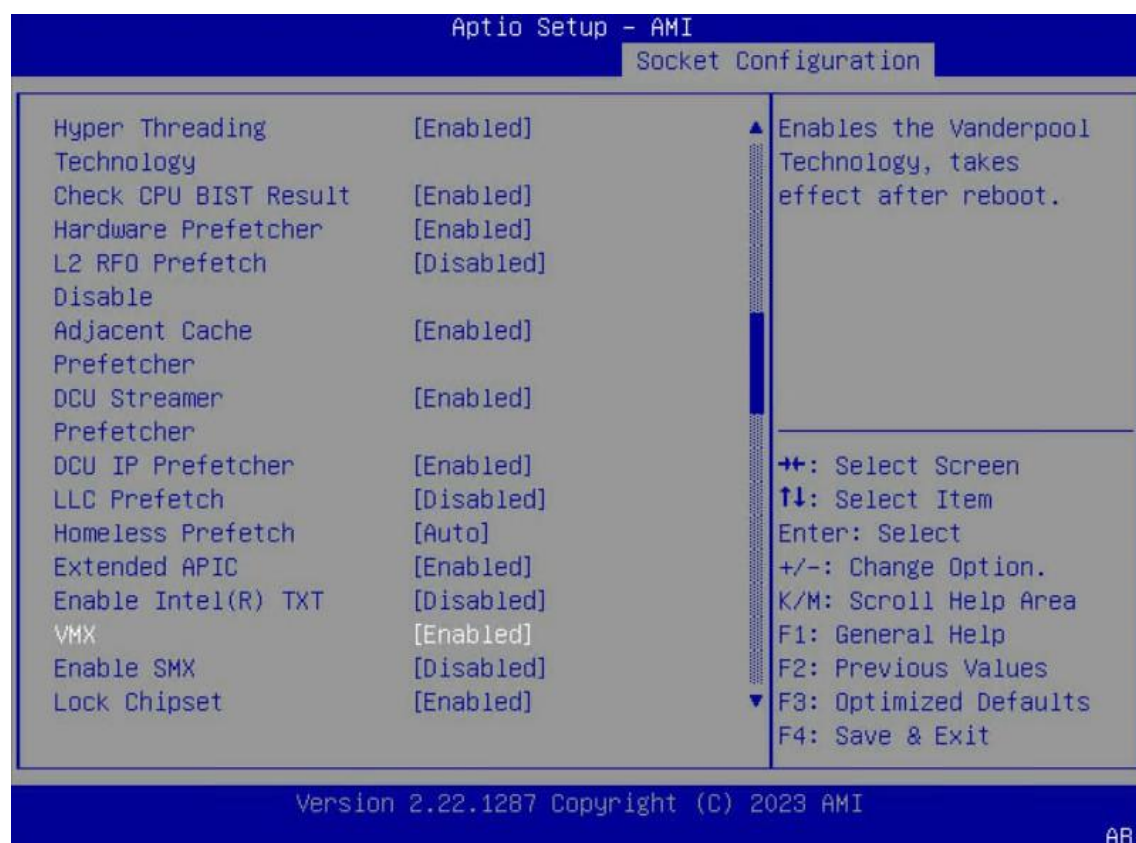
Figure 2-38 Intel VT for Directed I/O (VT-d) Screen

3. Select **Intel VT for Directed I/O**, and then press **Enter**. In the displayed dialog box, select **Enabled** to enable the VT-d function.

Configuring VMX

4. On the **Socket Configuration** screen, select **Processor Configuration**, and then press **Enter**. The **Processor Configuration** screen is displayed, see [Figure 2-39](#).

Figure 2-39 Processor Configuration Screen

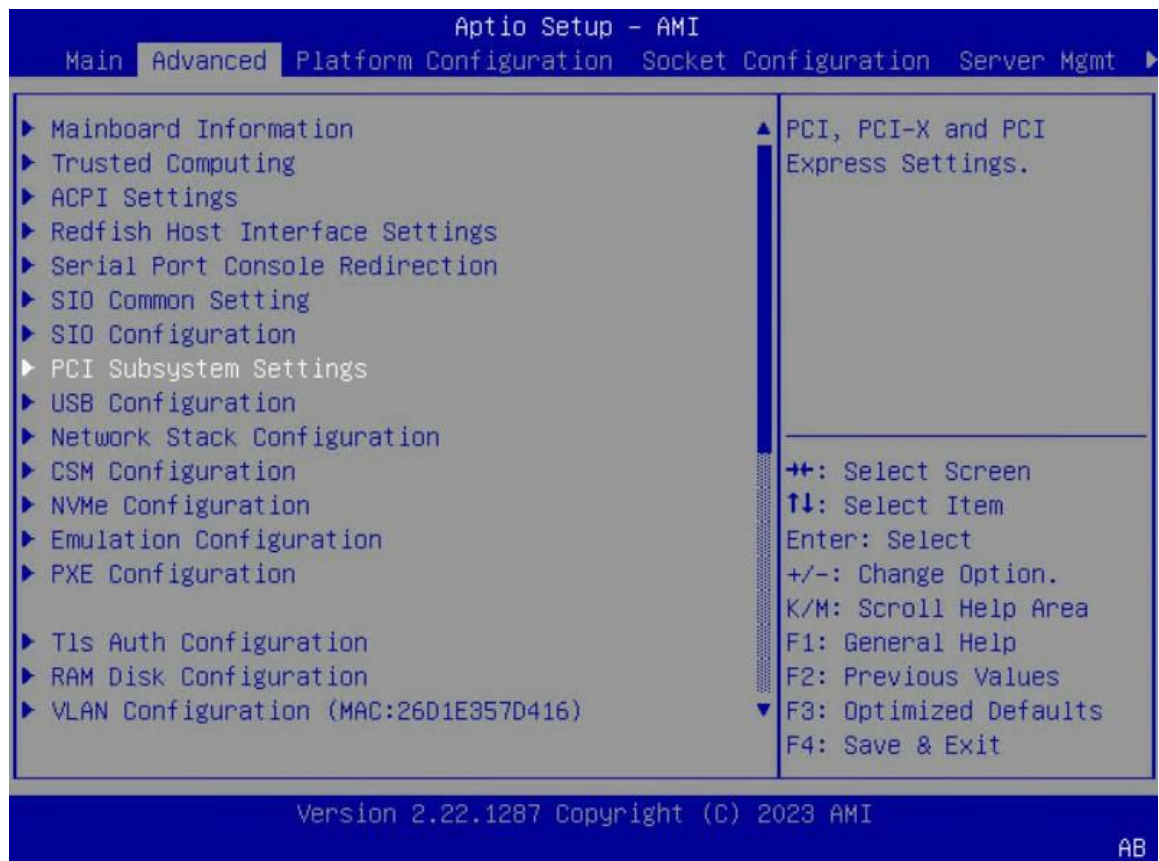


5. Select **VMX**, and then press **Enter**. In the displayed dialog box, select **Enabled** to enable the CPU virtualization function.

Configuring SR-IOV Support

6. On the **Setup** screen, select **Advanced**. The **Advanced** screen is displayed, see [Figure 2-40](#).

Figure 2-40 Advanced Screen



7. Select **PCI Subsystem Settings**, and then press **Enter**. The **PCI Subsystem Settings** screen is displayed, see [Figure 2-41](#).

Figure 2-41 PCI Subsystem Settings Screen



8. Select **SR-IOV Support**, and then press **Enter**. In the displayed dialog box, select **Enabled** to enable the SR-IOV function.
9. Press **F4**. In the displayed dialog box, select **Yes**.

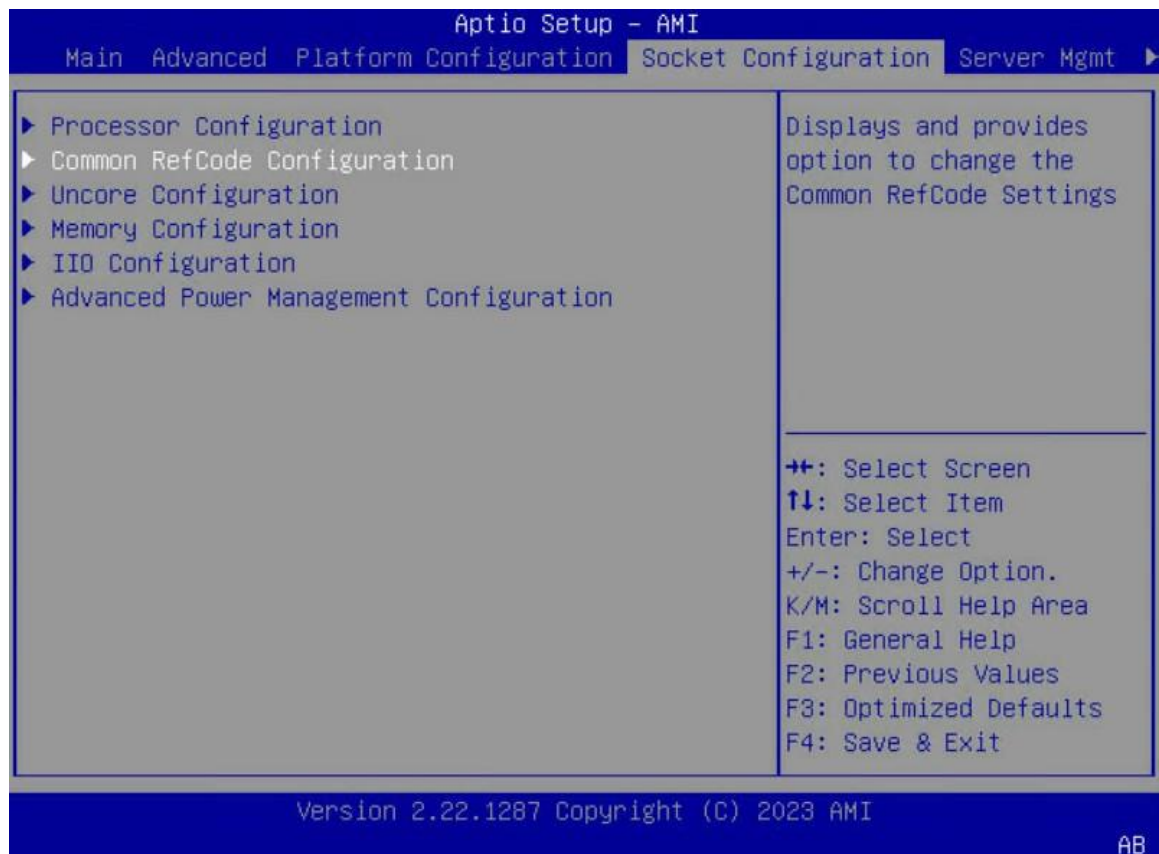
2.20 Setting Memory Parameters

Abstract

This procedure describes how to set memory parameters to improve server performance.

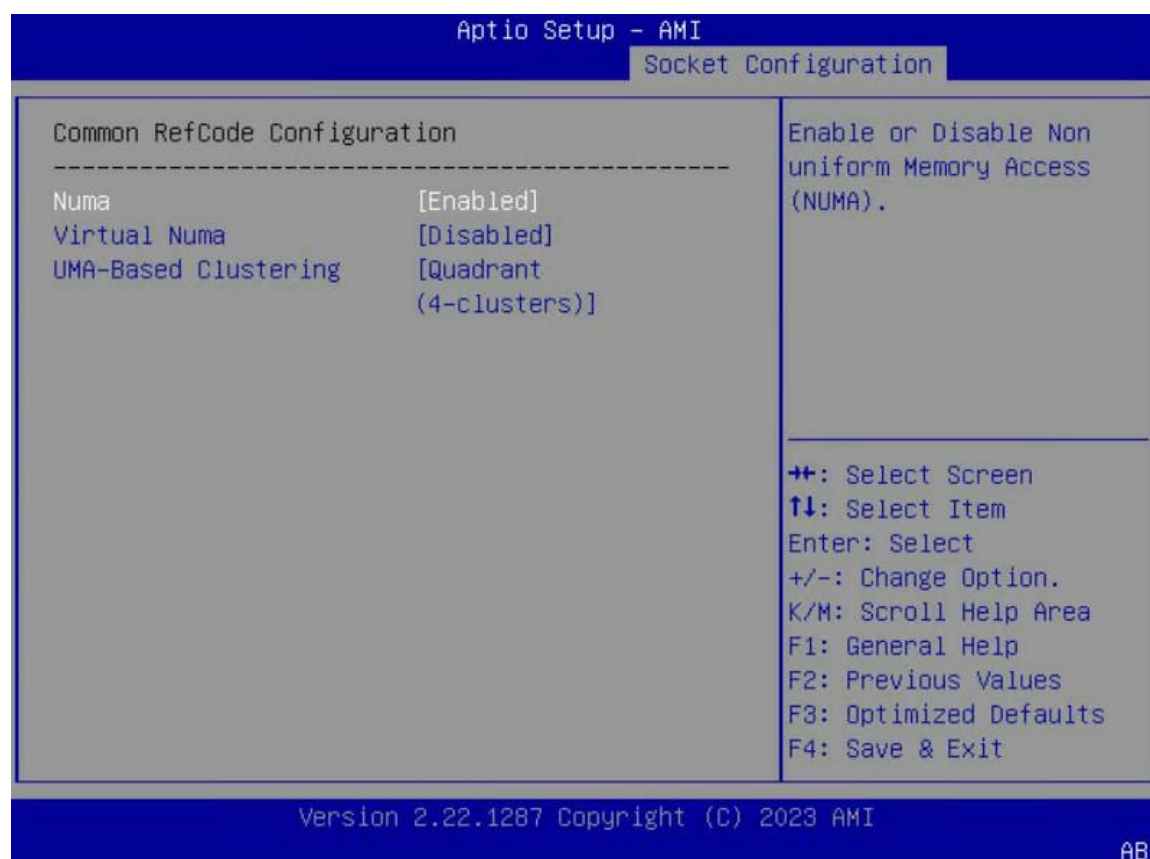
Steps

1. On the **Aptio Setup** screen, select **Socket Configuration**. The **Socket Configuration** screen is displayed, see [Figure 2-42](#).

Figure 2-42 Socket Configuration Screen

2. Select **Common RefCode Configuration**, and then press **Enter**. The **Common RefCode Configuration** screen is displayed, see [Figure 2-43](#).

Figure 2-43 Common RefCode Configuration Screen



3. Select **Numa**, and then press **Enter**. In the displayed dialog box, select **Enabled** to enable the **NUMA** function.
4. Select **Virtual Numa**, and then press **Enter**. In the displayed dialog box, select **Disabled** to disable the virtual NUMA function.
5. Press **F4**. In the displayed dialog box, select **Yes**.

2.21 Setting Power Parameters

Abstract

This procedure describes how to set power parameters to improve server performance.

Context

For a description of common power parameters, refer to [Table 2-7](#).

Table 2-7 Common Power Parameter Descriptions

Parameter	Description	Recommended Configuration
Power Policy Select	Power mode. Options: ● Performance: performance mode.	Performance

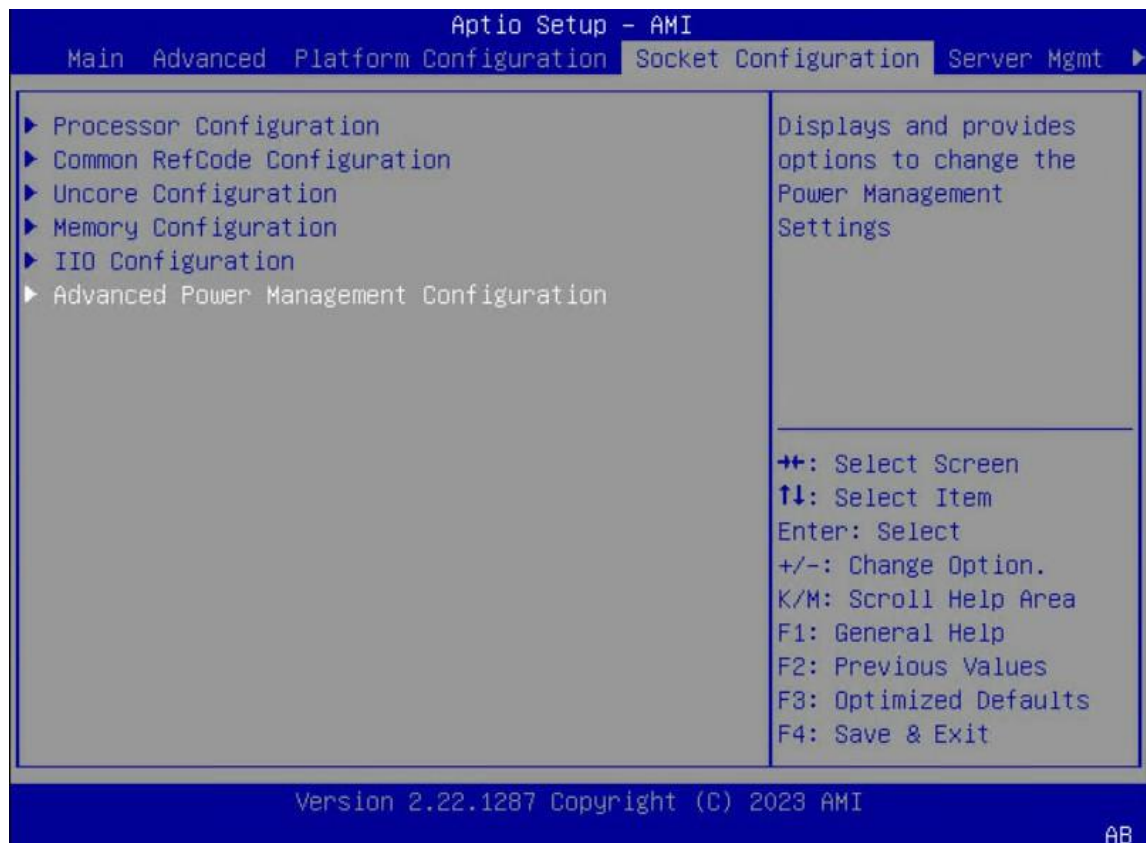
Parameter	Description	Recommended Configuration
	This mode is applicable to high-performance scenarios characterized by high load, multiple threads and low latency. In this mode, the CPU usage and memory usage are high and energy saving is automatically disabled, and therefore the overall power consumption is increased. ● Efficient: energy-saving mode. This mode is applicable to most common scenarios. In this mode, the server enables energy saving with minimal impact on performance and puts some CPU cores to sleep at a low load, to increase energy savings while delivering good performance. ● Custom: user-defined mode. This mode is applicable to the scenarios where you need to customize the power management policy as required. ● Latency-Performance: low-latency mode. This mode is applicable to the scenarios with strict requirements for latency and jitter, for example, the real-time operating system. In this mode, the server disables energy saving and other management functions that may cause latency, and keeps idle CPUs at their highest frequency for faster response. ● Maximum-Performance: maximum-performance mode. In this mode, the CPU remains stable at the Max Turbo frequency.	
EIST (Pstates)	Specifies whether to enable the EIST function. EIST is used to adjust the voltage and frequency of the CPUs and reduce both the power consumption and the heat generated in accordance with different workloads.	Enabled
Turbo Mode	Specifies whether to enable the Turbo mode. The Turbo mode increases CPU frequency and thus maximizes CPU performance. This parameter is displayed when EIST (Pstates) is set to Enabled.	Enabled

Parameter	Description	Recommended Configuration
Monitor/MWAIT Support	Specifies whether to enable the Monitor/Mwait instruction. Enabling the Monitor/Mwait instruction optimizes the instruction operation of a CPU. ● If the C-State needs to be disabled for a CPU, and this instruction needs to be disabled in some operating systems, set this parameter to Disabled. ● If an Enhanced VMotion Compatibility (EVC) error is reported when a VM is added to a cluster or is migrated, set this parameter to Enabled to enable this instruction.	Disabled
CPU C6 report	Specifies whether to report the C6 state to the operating system.	Disabled
Enhanced Halt State (C1E)	Specifies whether to enable the C1E function.	Disabled
Package C State	Sets the package C-State limit. Options: ● C0/C1 state ● C2 state ● C6 (non-retention) state ● Auto C0 indicates that the CPU is actively running. Other C-States indicate the idleness of different levels. From C0 to C6, the higher the C number is, the deeper into sleep mode the CPU goes. In a deeper sleep mode, the CPU saves more power but needs more time to get active again.	C0/C1 state

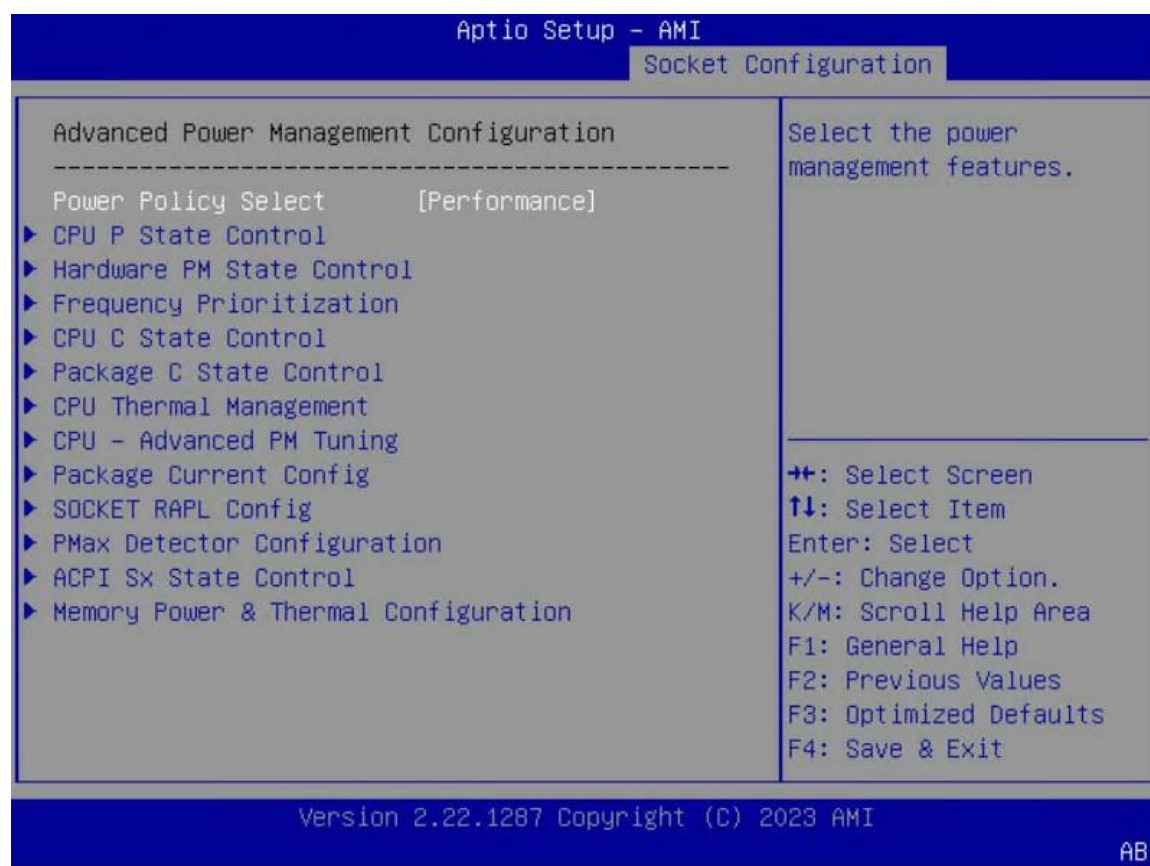
Steps

Configuring the Power Policy Select Parameter

1. On the **Aptio Setup** screen, select **Socket Configuration**. The **Socket Configuration** screen is displayed, see [Figure 2-44](#).

Figure 2-44 Socket Configuration Screen

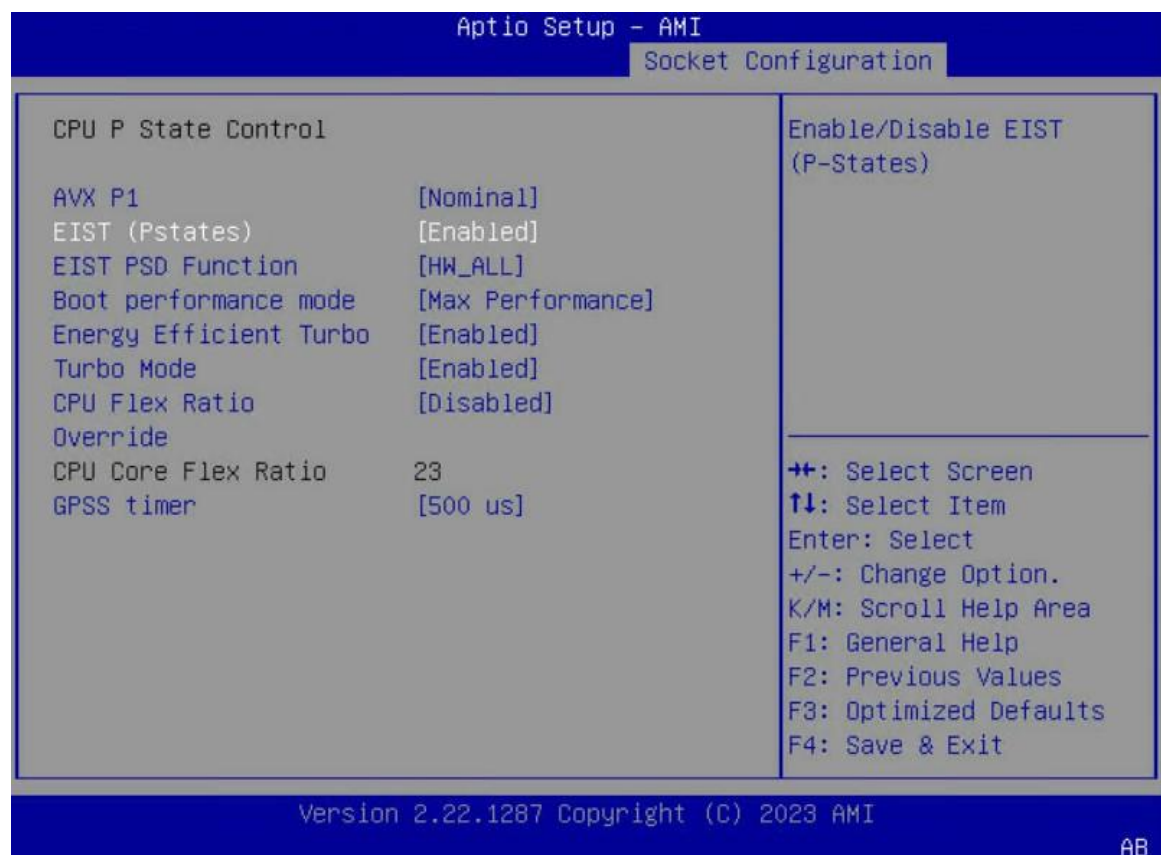
2. Select **Advanced Power Management Configuration**, and then press **Enter**. The **Advanced Power Management Configuration** screen is displayed, see [Figure 2-45](#).

Figure 2-45 Advanced Power Management Configuration Screen

3. Select **Power Policy Select**, and then press **Enter**. In the displayed dialog box, select **Performance**.

Configuring the EIST (Pstates) and Turbo Mode Parameters

4. On the **Advanced Power Management Configuration** screen, select **CPU P State Control**, and then press **Enter**. The **CPU P State Control** screen is displayed, see [Figure 2-46](#).

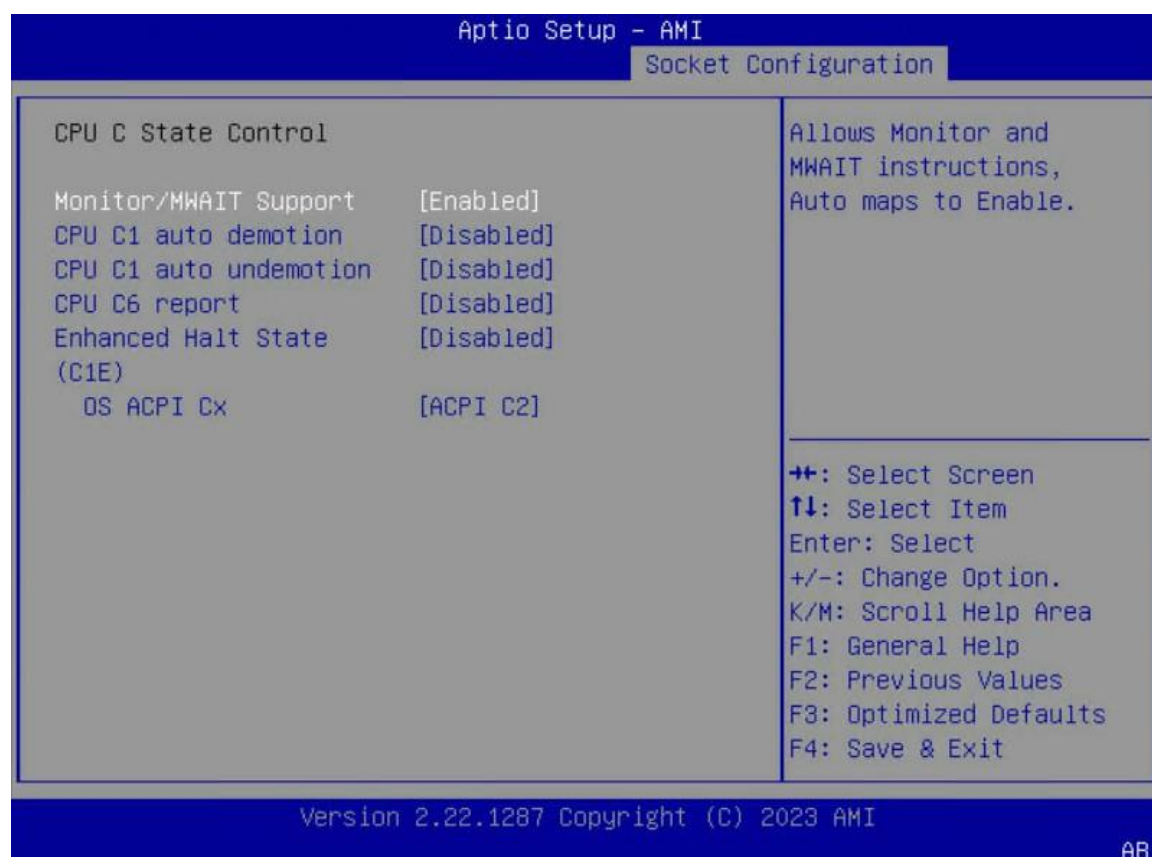
Figure 2-46 CPU P State Control Screen

5. Select **EIST (Pstates)**, and then press **Enter**. In the displayed dialog box, select **Enabled** to enable the **EIST** function.
6. Select **Turbo Mode**, and then press **Enter**. In the displayed dialog box, select **Enabled** to enable the Turbo mode.

Configuring the Monitor/MWAIT Support, CPU C6 report, and Enhanced Halt State (C1E) Parameters

7. On the **Advanced Power Management Configuration** screen, select **CPU C State Control**, and then press **Enter**. The **CPU C State Control** screen is displayed, see [Figure 2-47](#).

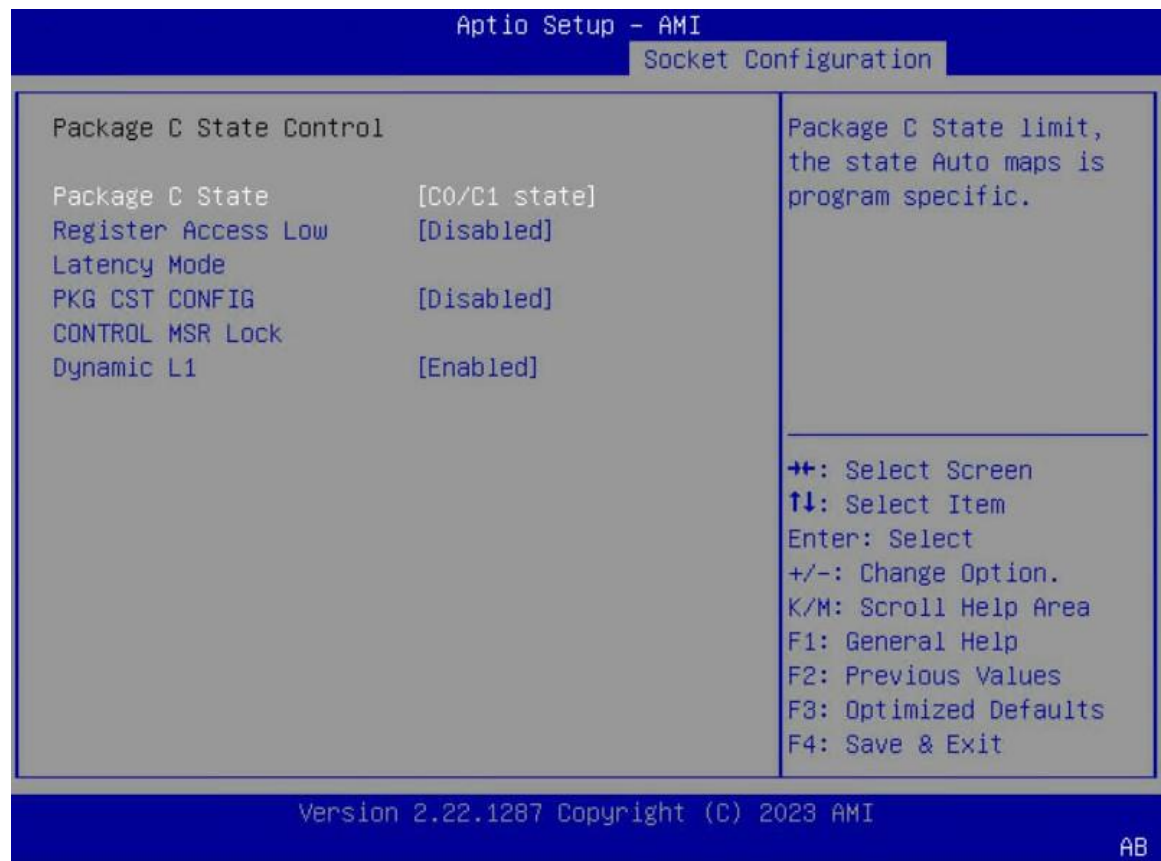
Figure 2-47 CPU C State Control Screen



8. Select **Monitor/MWAIT Support**, and then press **Enter**. In the displayed dialog box, select **Disabled** to disable the Monitor/Mwait instruction.
9. Select **CPU C6 report**, and then press **Enter**. In the displayed dialog box, select **Disabled** to not report the C6 state to the operating system.
10. Select **Enhanced Halt State (C1E)**, and then press **Enter**. In the displayed dialog box, select **Disabled** to disable the C1E function.

Configuring the Package C State Parameter

11. On the **Advanced Power Management Configuration** screen, select **CPU C State Control**, and then press **Enter**. The **Package C State Control** screen is displayed, see [Figure 2-48](#).

Figure 2-48 Package C State Control Screen

12. Select **Package C State Control**, and then press **Enter**. In the displayed dialog box, select **C0/C1 state** and then press **Enter**.
13. Press **F4**. In the displayed dialog box, select **Yes**.

2.22 Setting the TPM Type

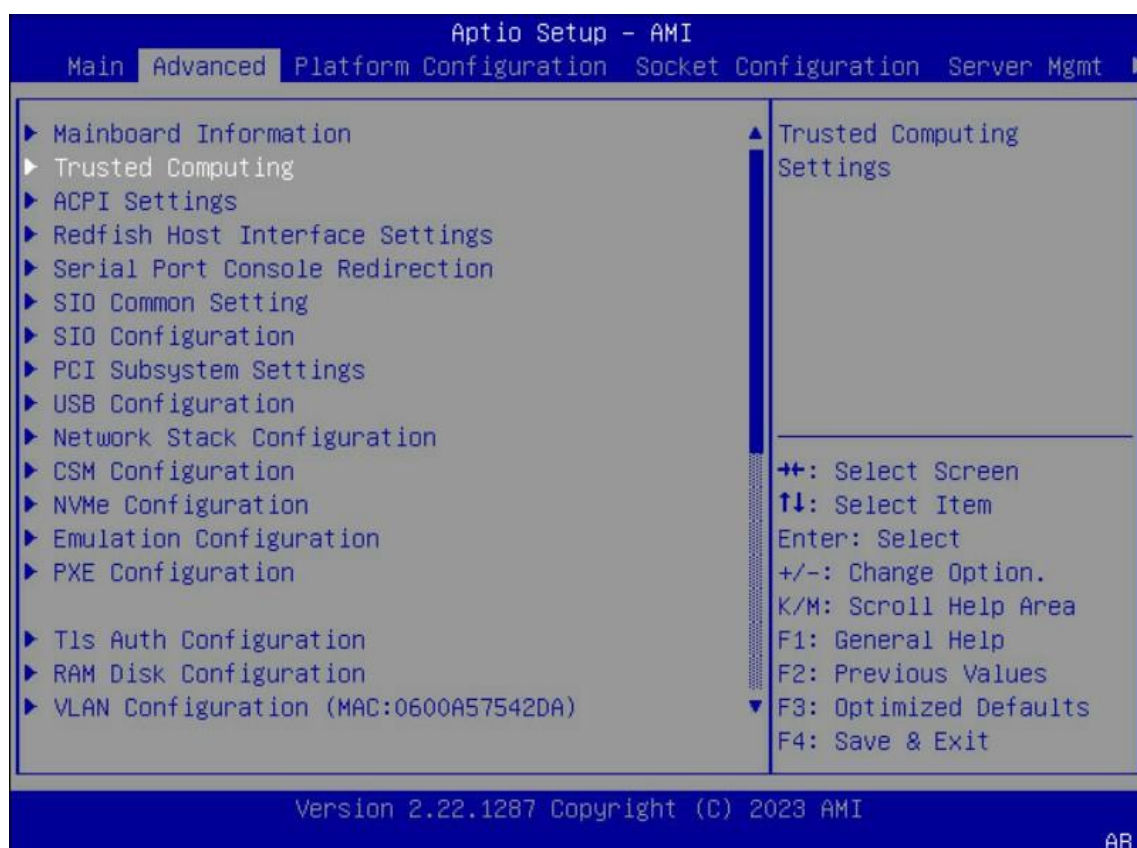
Abstract

The **TPM** installed on a server can be used properly only if the supported TPM type is correctly set. This procedure describes how to set the TPM type.

Steps

1. On the **Aptio Setup** screen, select **Advanced**. The **Advanced** screen is displayed, see [Figure 2-49](#).

Figure 2-49 Advanced Screen



2. Select **Trusted Computing**, and then press **Enter**. The **Trusted Computing** screen is displayed, see [Figure 2-50](#).

Figure 2-50 Trusted Computing Screen

3. Select **Device Select**, and then press **Enter**. A dialog box for selecting the TPM type is displayed.
4. Select the supported TPM type, and then press **Enter**.
Options:
 - **TPM1.2**: TPM 1.2 is supported.
 - **TPM2.0**: TPM 2.0 is supported.
 - **Auto**: Both TPM 1.2 and TPM 2.0 are supported. By default, the system first checks whether the installed TPM uses TPM version 2.0. If not, the system check whether the installed TPM uses TPM version 1.2.
5. Press **F4**. In the displayed dialog box, select **Yes**.

2.23 Setting the Port Mode for a RAID Card

Abstract

The ports (namely the ports connected to the disk backplane and disk cables) of a NETAŞ SmartROC3100 **RAID** card support three modes: RAID, **HBA** and Mixed. Before adding the disk corresponding to a port to a logical RAID volume, you need to set the port mode. This procedure describes how to set the port mode.



This procedure uses a NETAŞ SmartROC3100 RAID card as an example to describe how to set the port mode. For how to configure the port mode for other RAID cards, refer to the *NETAŞ Server RAID User Guide (Intel EagleStream)*.

The NETAŞ SmartROC3100 RAID card supports port mode configuration in the following two ways:

- Setting the mode of ports in batches
- Setting the mode of a single port



This procedure uses setting the mode of a single port as an example. For how to set the mode of ports in batches, refer to the *NETAŞ Server RAID User Guide (Intel EagleStream)*.

Prerequisite

The boot mode is already set to [UEFI](#) in the BIOS. For details, refer to [2.10 Setting the Boot Mode](#).

Context

Port modes include **RAID**, **HBA** and **Mixed**, which are described as follows:

- In **RAID** mode, the connected disks can be used only after they are used to build a RAID volume.
- In **HBA** mode, the connected disks are pass-through disks (directly used only) and cannot be used to build a RAID volume.
- In **Mixed** mode, the connected disks support both **RAID** and **HBA** modes.
 - ➔ The **RAID** mode is applicable to the disks that have been used to build a RAID volume.
 - ➔ The **HBA** mode (pass-through) is applicable to the disks that are not used to build a RAID volume.

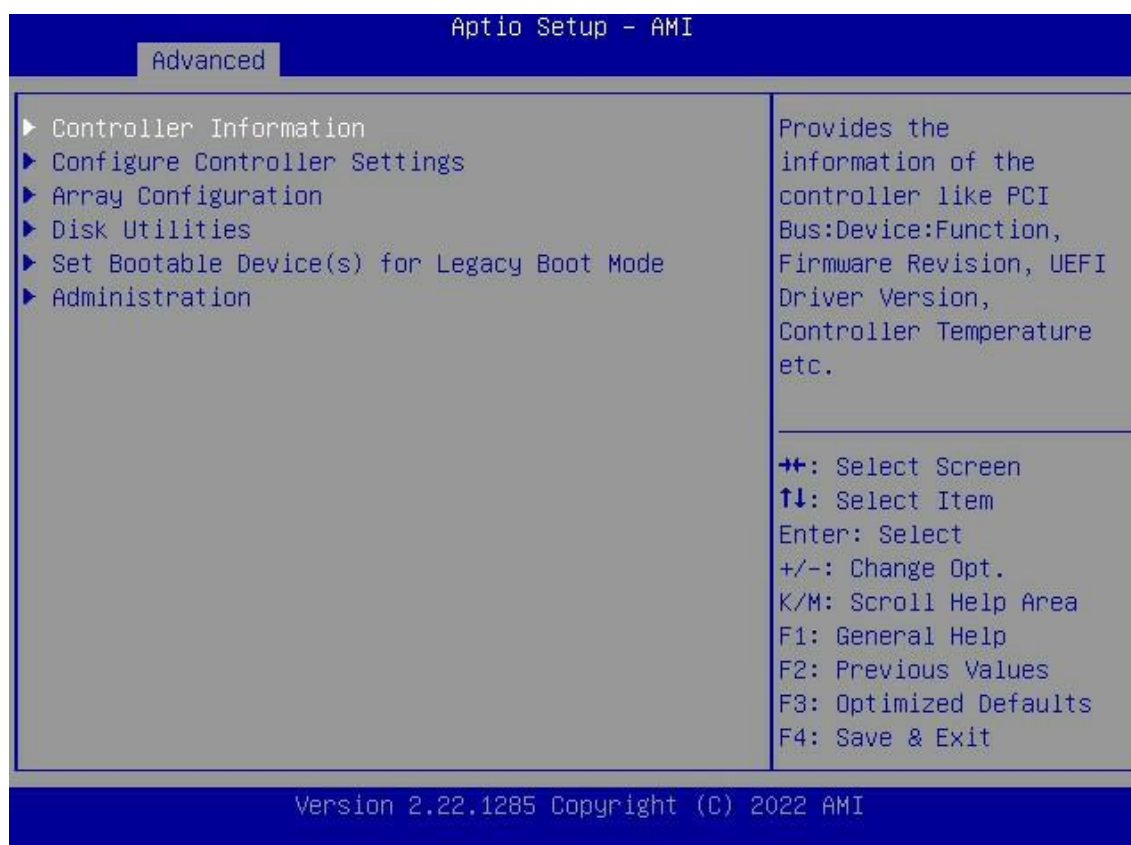
Steps

1. On the **Aptio Setup** screen, select **Advanced**. The **Advanced** screen is displayed, see [Figure 2-51](#).

Figure 2-51 Advanced Screen



2. Select **NETAŞ SmartROC3100 RM241B-18i 2G**, and then press **Enter**. The controller management screen is displayed, see [Figure 2-52](#).

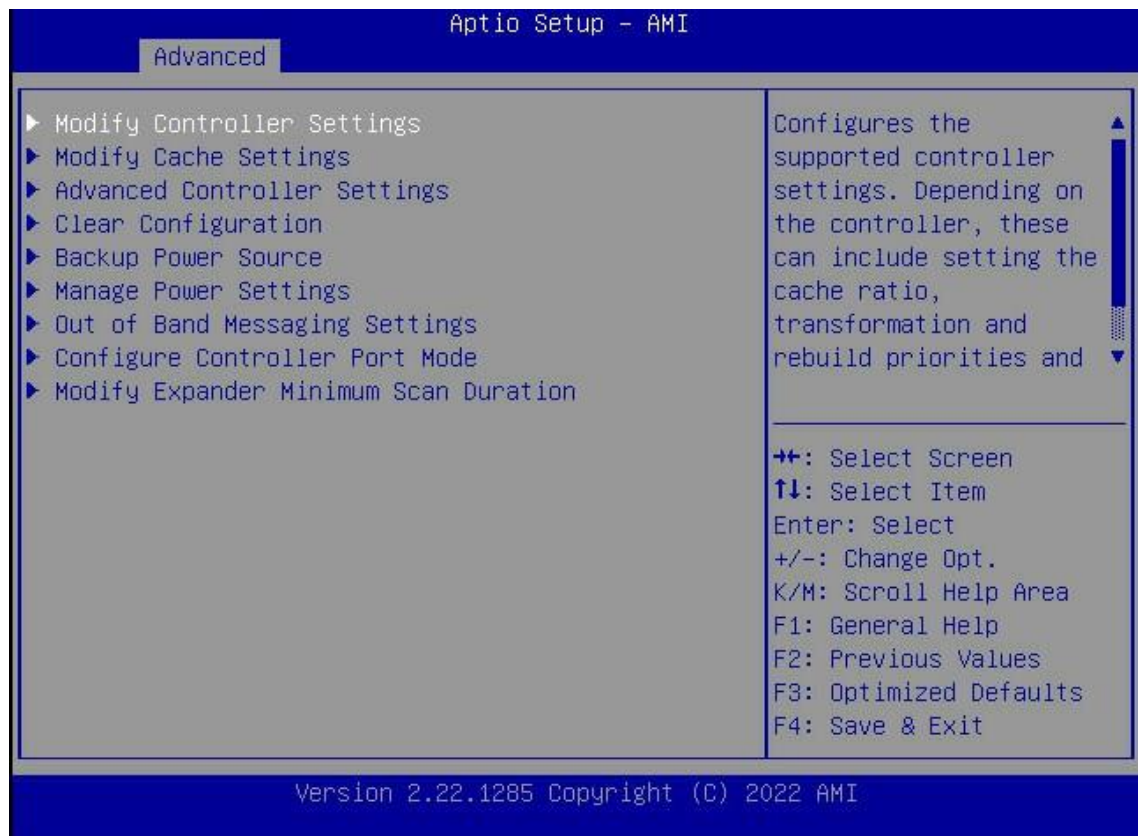
Figure 2-52 Managing a RAID Controller

For a description of the functions of the menus on the controller management screen, refer to [Table 2-8](#).

Table 2-8 Functions of the Menus on the Controller Management Screen

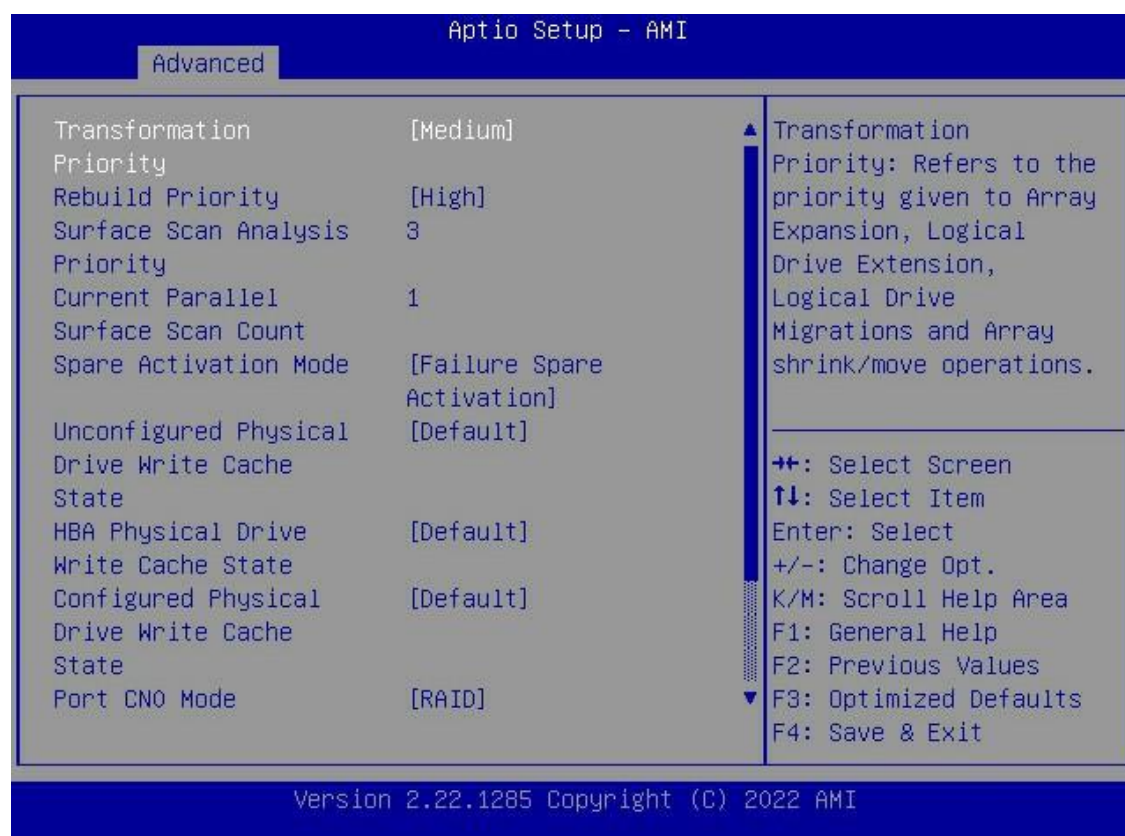
Menu	Function
Controller Information	Displays the basic information, firmware, current temperature, and port configuration of the controller.
Configure Controller Settings	Provides advanced configuration options for the controller.
Array Configuration	Creates a RAID array.
Disk Utilities	Displays the list of disks controlled by the controller as well as the basic disk information, and allows you to turn on the disk positioning indicator, erase disk data, and upgrade the firmware.
Set Bootable Device(s) for Legacy Boot Mode	Configures, or clears the primary and secondary boot disks.
Administration	Allows you to perform such operations as upgrading firmware and restoring to factory defaults.

3. Select **Configure Controller Settings**, and then press **Enter**. The advanced configuration option screen is displayed, see [Figure 2-53](#).

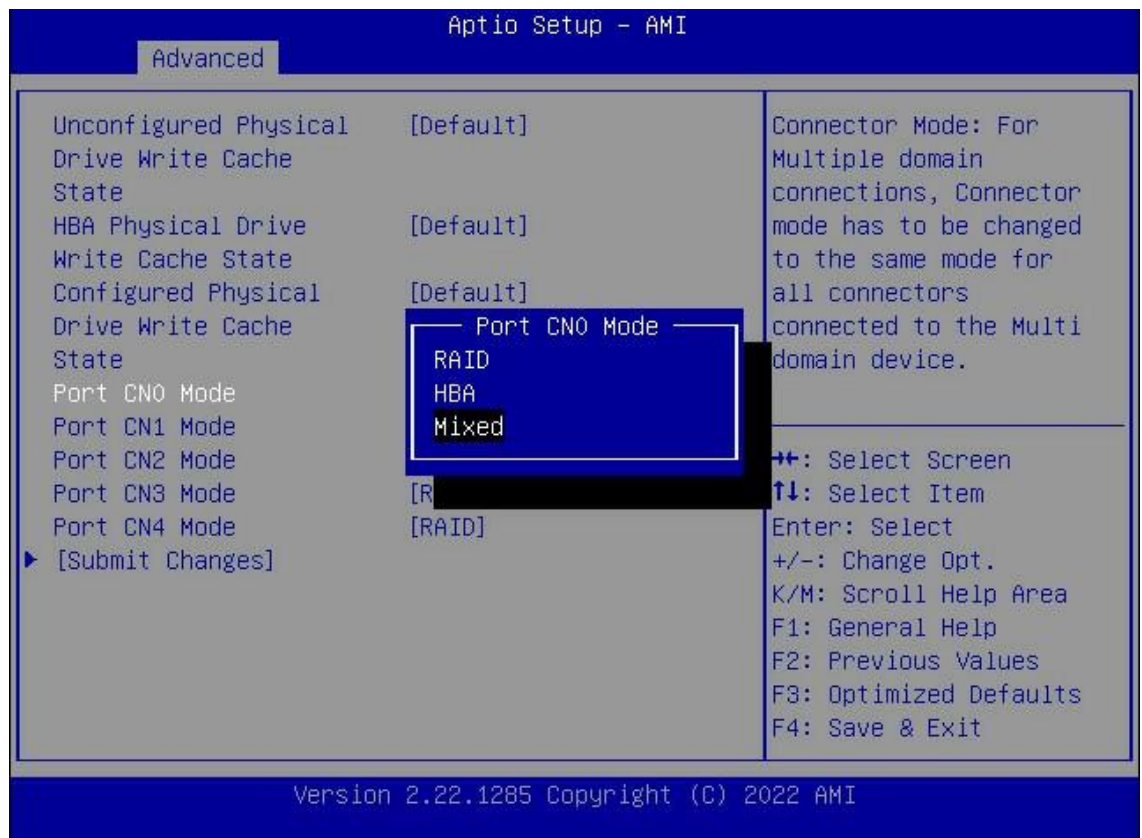
Figure 2-53 Setting Advanced Configuration Options for the RAID Controller

4. Select **Modify Controller Settings**, and then press **Enter**. The controller configuration screen is displayed, see [Figure 2-54](#).

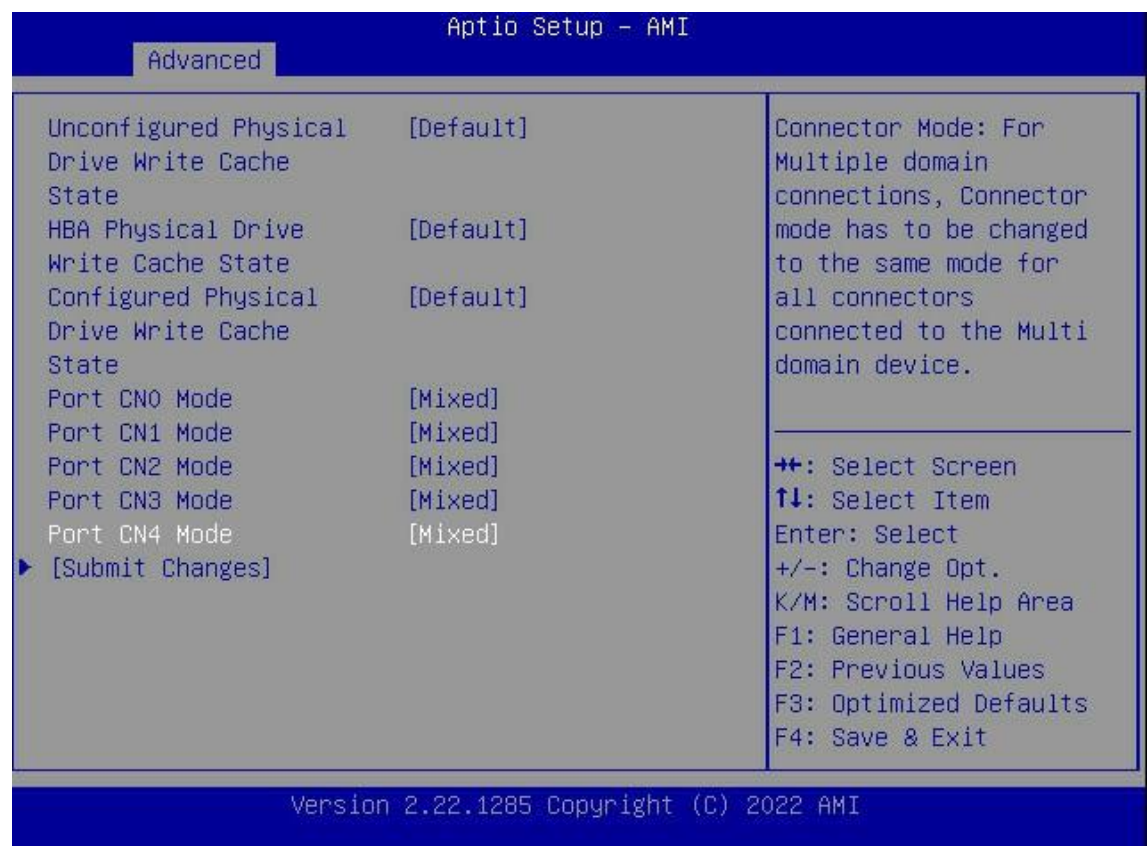
Figure 2-54 Configuring the RAID Controller



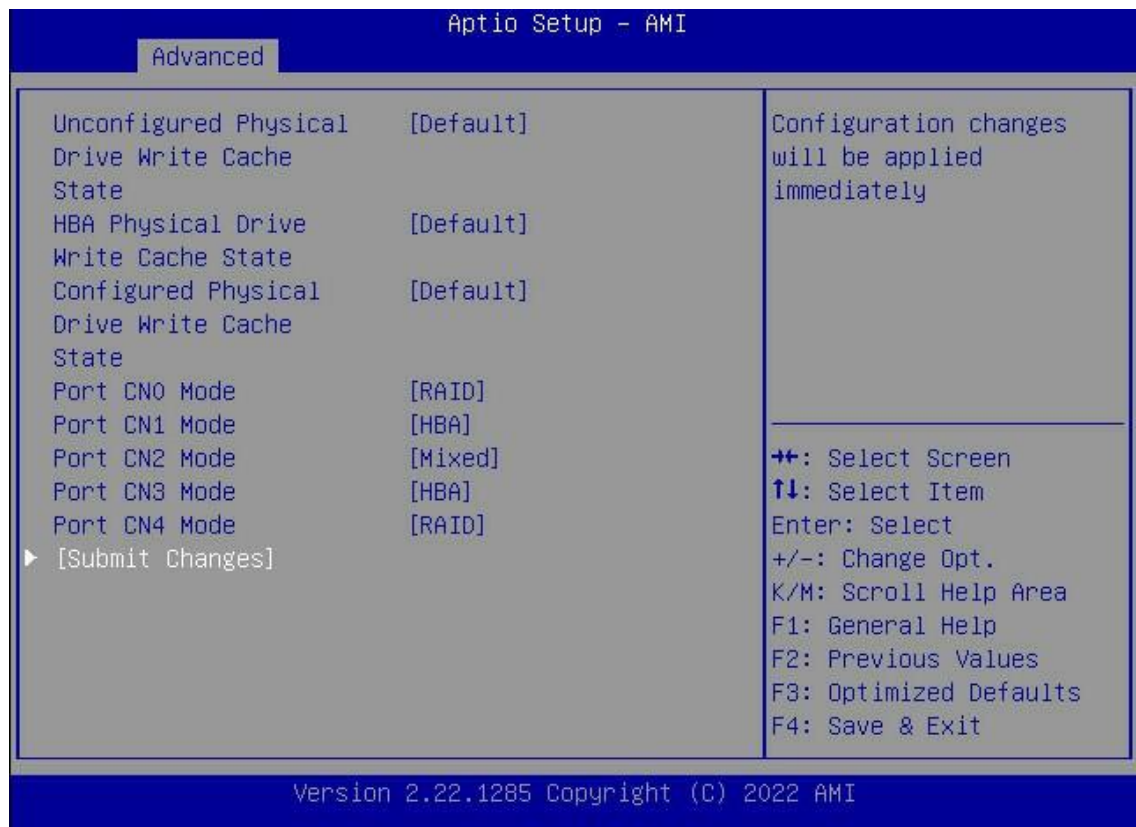
5. Select **Port CN0 Mode**, and then press **Enter**. The **Port CN0 Mode** dialog box is displayed, see [Figure 2-55](#).

Figure 2-55 Port CN0 Mode Dialog Box

6. Select the desired port mode, and then press **Enter**, see [Figure 2-56](#).

Figure 2-56 Configuring the Mode of a Port

- Repeat [Step 5](#) through [Step 6](#) to set the mode of another port, see [Figure 2-57](#).

Figure 2-57 Configuring the Mode of Another Port

8. Select **Submit Changes**, and then press **Enter**. The port mode is set successfully, see [Figure 2-58](#).

Figure 2-58 Port Mode Set Successfully



9. Select **Back to Main Menu**, and then press **Enter** to return to the controller management screen.
10. Press **Esc** to exit the controller management screen and return to the **Advanced** screen.
11. Press **F4** to save the port configuration, exit the BIOS, and continue the server startup program.

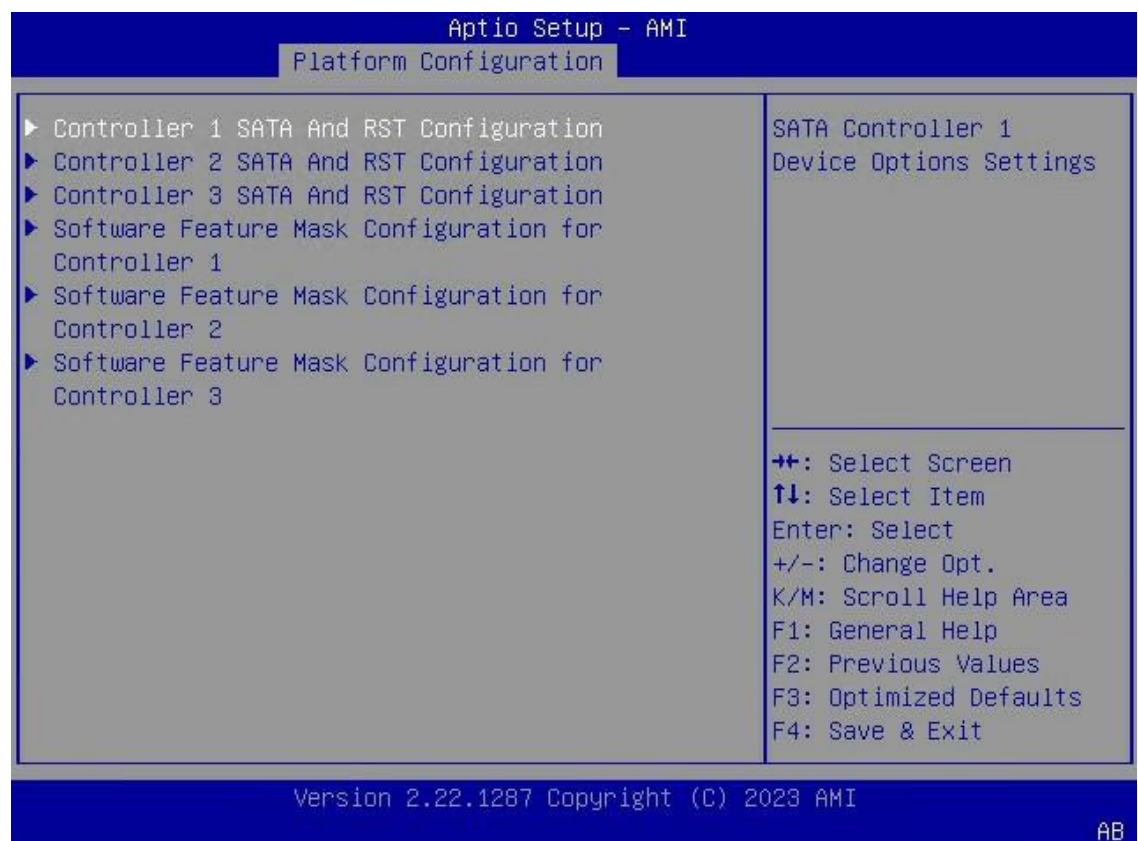
2.24 Creating a RAID Volume for SATA Drives

Abstract

This procedure describes how to create a [RAID](#) volume for multiple [SATA](#) drives to meet service requirements.

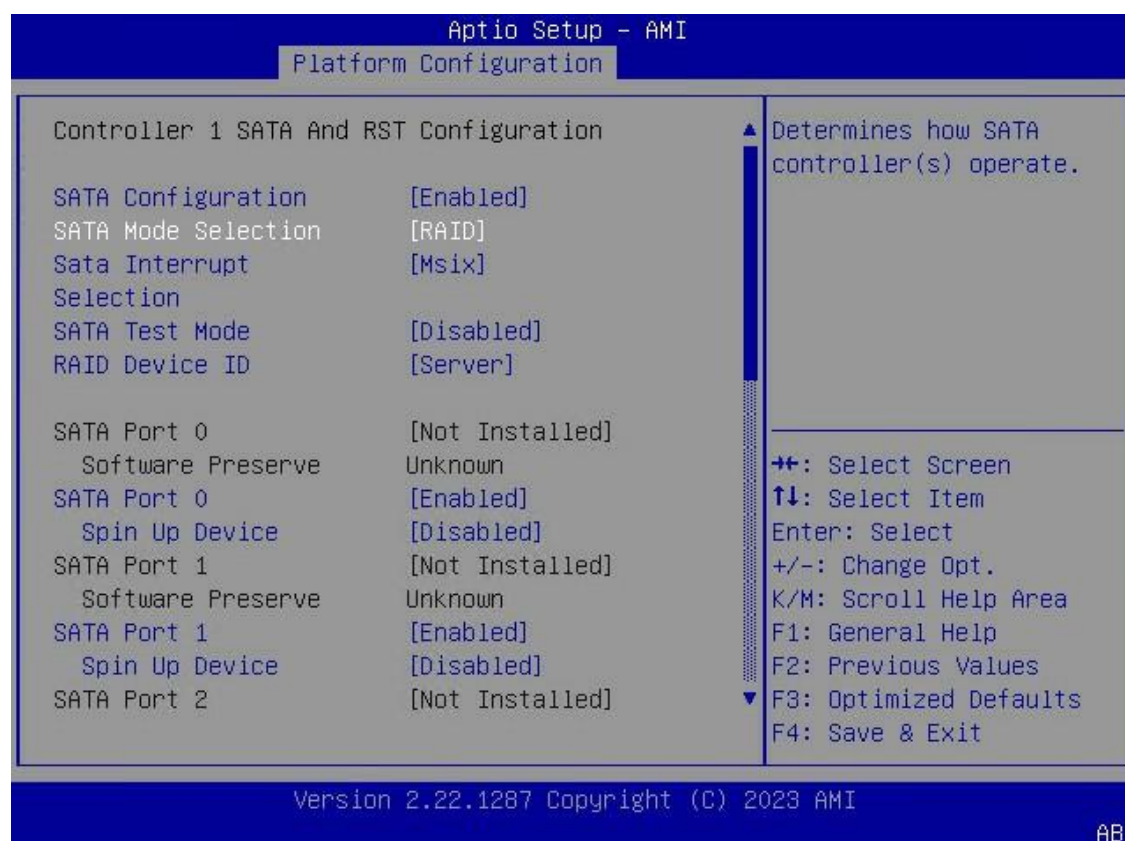
Steps

1. On the **Aptio Setup** screen, select the **Platform Configuration** menu. The **Platform Configuration** window is displayed.
2. Select **PCH-IO Configuration > SATA And RST Configuration**. The **SATA And RST Configuration** screen is displayed, see [Figure 2-59](#).

Figure 2-59 SATA And RST Configuration Screen

3. Select the corresponding controller and press **Enter**. The screen for the controller is displayed.

For example, select **Controller 1 SATA And RST Configuration**. The **Controller 1 SATA And RST Configuration** screen is displayed, see [Figure 2-60](#).

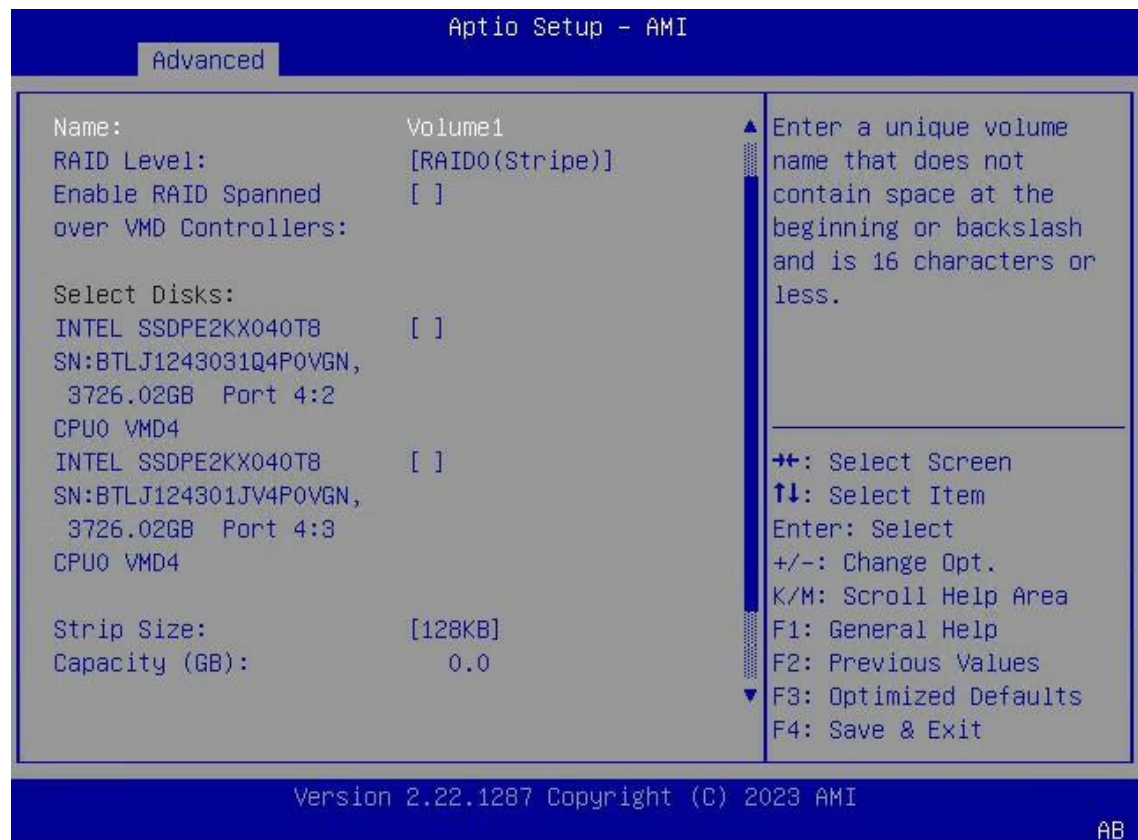
Figure 2-60 Controller 1 SATA And RST Configuration Screen

4. Select **SATA Mode Selection** and press **Enter**. In the displayed dialog box, select **RAID** and press **Enter**.
5. Press **F4**. In the displayed dialog box, select **Yes**.
6. During the server restart process, the **Aptio Setup** screen is displayed.

**Note**

For a description of the operations on the **Aptio Setup** screen, refer to [2.1 Entering the BIOS](#).

7. Select **Advanced**. The **Advanced** screen is displayed.
8. Select **Intel Virtual RAID on CPU > All Intel VMD Controllers > Create RAID Volume** and press **Enter**. The **Create RAID Volume** screen is displayed, see [Figure 2-61](#).

Figure 2-61 Create RAID Volume Screen

9. Set the parameters. For a description of the parameters, refer to [Table 2-9](#).

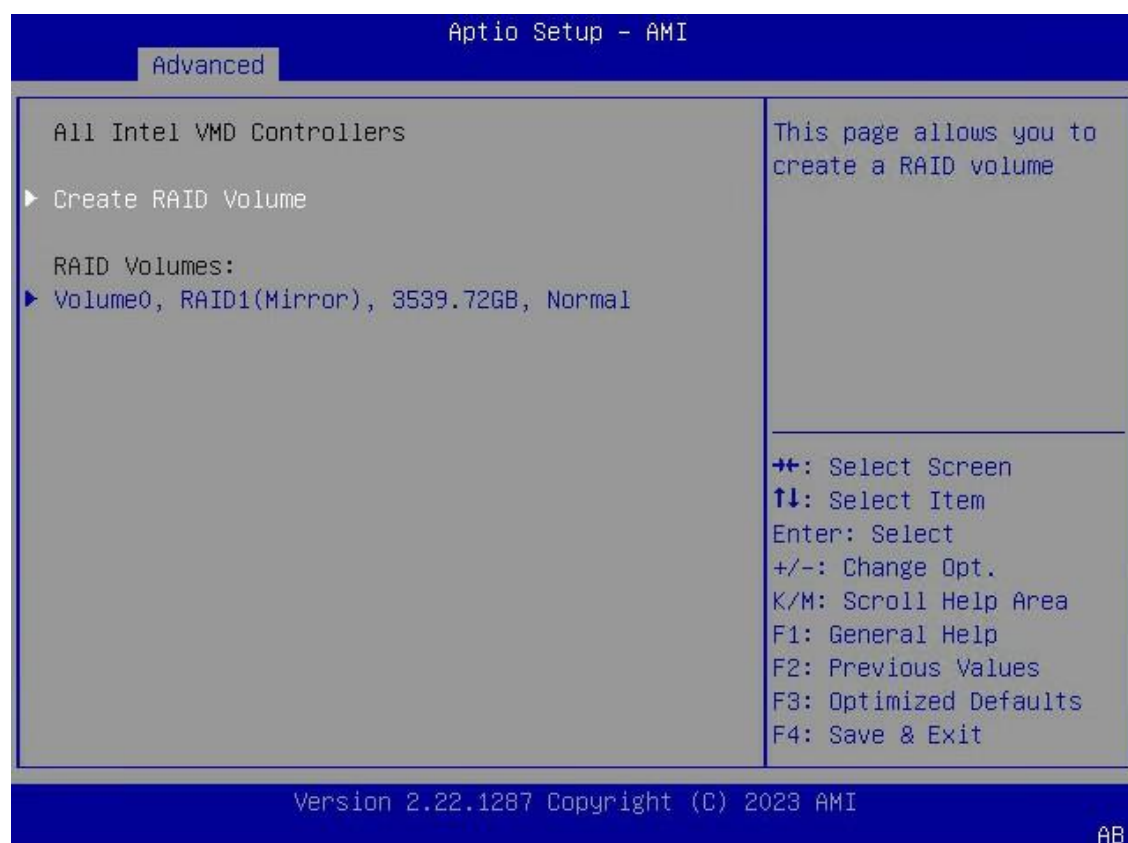
Table 2-9 RAID Volume Parameter Descriptions

Parameter	Description
Name	Enter a unique RAID volume name that contains no more than 16 characters. The name cannot start or end with a space.
RAID Level	Select a RAID level.
Select Disks	Select the member SATA drives of the RAID volume.
Strip Size	Select the stripe size.
Capacity (GB)	Enter the capacity of the RAID volume.

10. Press **Enter**. In the displayed dialog box, select **Yes**.

When the RAID volume is displayed below **Create RAID Volume** on the **All Intel VMD Controllers** screen (see [Figure 2-62](#)), it indicates that the RAID volume is created successfully.

Figure 2-62 RAID Volume Successfully Created



11. Press **F4**. In the displayed dialog box, select **Yes**.

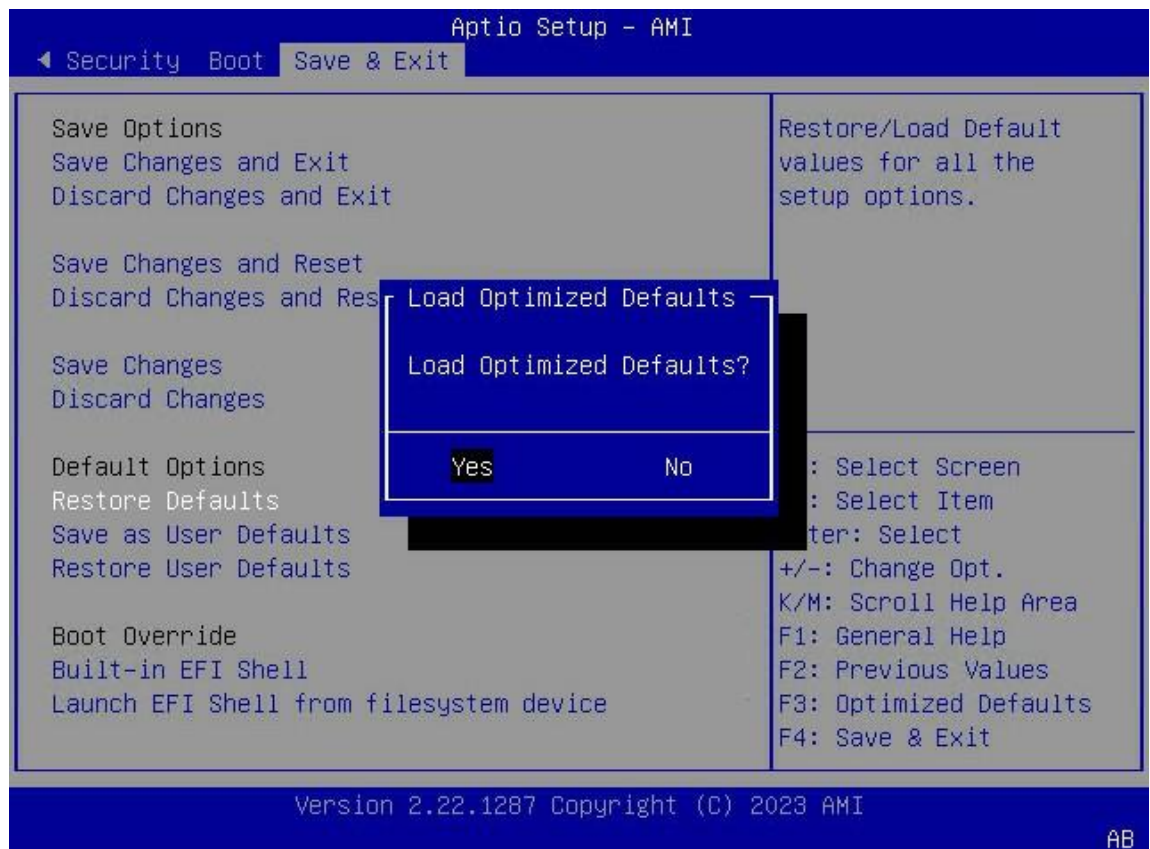
2.25 Restoring the Default BIOS Settings

Abstract

This procedure describes how to restore the default [BIOS](#) settings when a system error occurs because of unknown changes to the BIOS.

Steps

1. On the **Aptio Setup** screen, perform either of the following operations. The **Load Optimized Defaults** dialog box is displayed, see [Figure 2-63](#).
 - Press **F3**.
 - Select **Save & Exit**. The **Save & Exit** screen is displayed. Select **Restore Defaults**.

Figure 2-63 Load Optimal Defaults Dialog Box

2. Click **Yes**.
3. Press **F4**. In the displayed dialog box, select **Yes**.

Chapter 3

Setup Parameter Descriptions

Table of Contents

Main	75
Advanced	78
Platform Configuration	120
Socket Configuration.....	168
Server Mgmt.....	295
Security	316
Boot	324
Save & Exit	334

3.1 Main

The **Main** screen provides the basic BIOS information including the BIOS version, memory capacity, and system time. [Figure 3-1](#) through [Figure 3-2](#) show the **Main** screen.

Figure 3-1 Main Screen—1

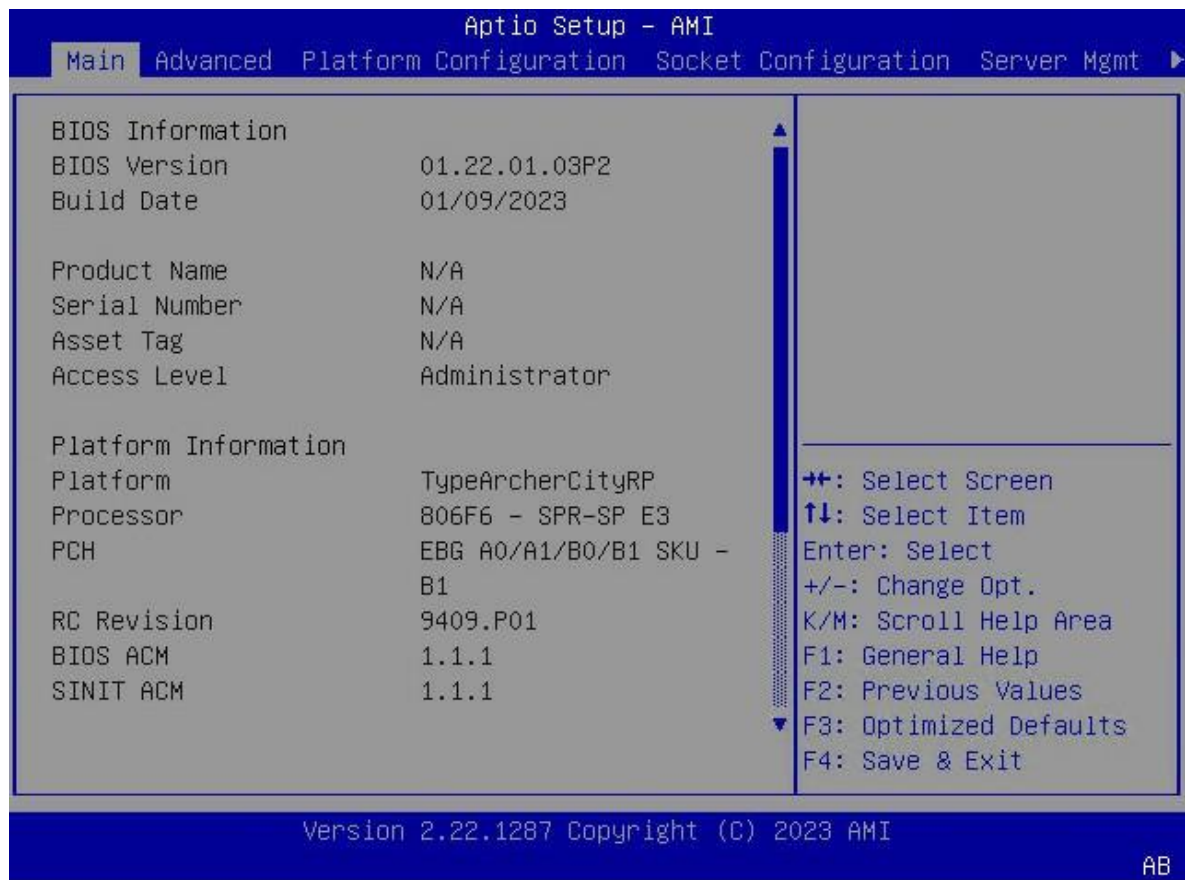
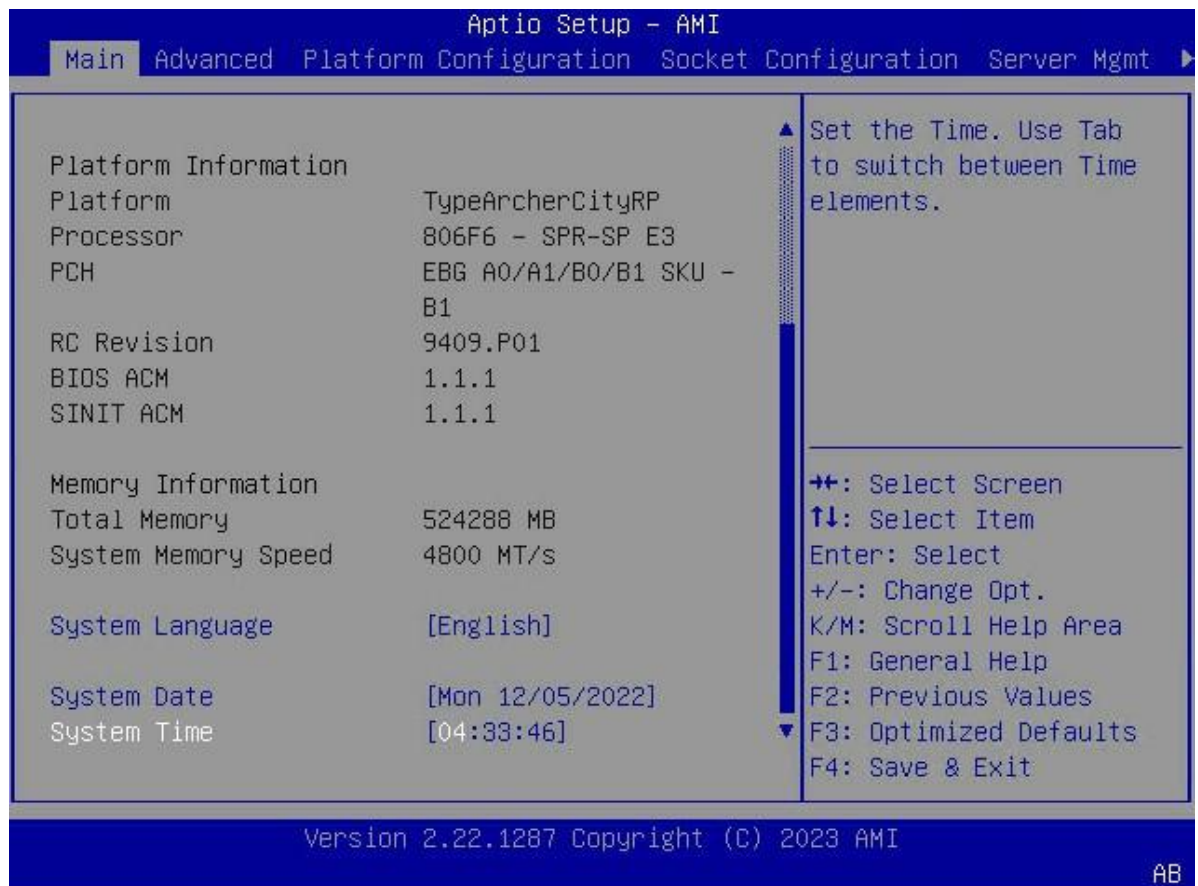


Figure 3-2 Main Screen—2



For a description of the parameters on the **Main** screen, refer to [Table 3-1](#).

Table 3-1 Main Screen Parameter Descriptions

Parameter	Description
BIOS Version	BIOS version.
Build Date	BIOS creation date (format: MM/DD/YYYY).
Product Name	Product name.
Serial Number	Serial number of the product.
Asset Tag	Asset tag.
Access Level	Access permission.
Platform	Platform name.
Processor	Processor model.
PCH	Bridge chip model.
RC Revision	RC version.
BIOS ACM	Firmware version information about the BIOS ACM.

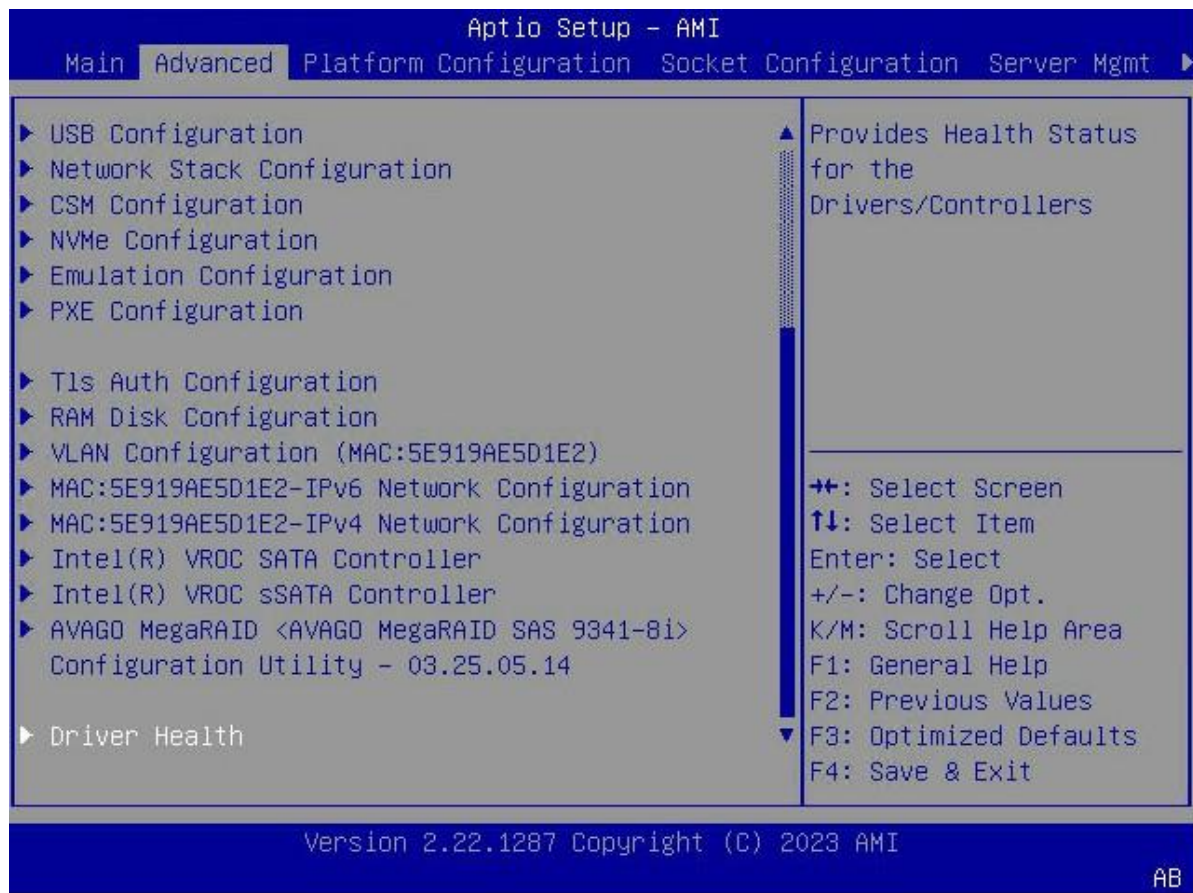
Parameter	Description
SINIT ACM	Firmware version information about the SINIT ACM.
Total Memory	Total memory capacity.
System Memory Speed	Memory speed.
System Language	System language ● English ● Simplified Chinese
System Date	Current system date. You can change the setting. System date format: day of week month/day of the month (in numbers)/year. Press Enter to switch between the day of the month (in numbers), month, and year items and change the settings as follows: ● To increase the value by one, press +. ● To decrease the value by one, press -. ● To specify a value, press the corresponding number key.
System Time	Current system time. You can change the setting. The system time is displayed in HH:MM:SS format based on a 24-hour clock system. You can press Enter to switch between the hour, minute, and second items and change the settings as follows: ● To increase the value by one, press +. ● To decrease the value by one, press -. ● To specify a value, press the corresponding number key.

3.2 Advanced

The **Advanced** screen provides advanced BIOS settings, such as mainboard information and console redirection. [Figure 3-3](#) through [Figure 3-4](#) show the **Advanced** screen.

Figure 3-3 Advanced Screen—1



Figure 3-4 Advanced Screen—2

For a description of the parameters on the **Advanced** screen, refer to [Table 3-2](#).

Table 3-2 Advanced Parameter Descriptions

Parameter	Description
Mainboard Information	Mainboard information. For details, refer to 3.2.1 Mainboard Information .
Trusted Computing	Trusted computing. For details, refer to 3.2.2 Trusted Computing .
ACPI Settings	ACPI settings. For details, refer to 3.2.3 ACPI Settings .
Redfish Host Interface Settings	Host Redfish interface settings. For details, refer to 3.2.4 Redfish Host Interface Settings .
Serial Port Console Redirection	Console redirection. For details, refer to 3.2.5 Serial Port Console Redirection Settings .
SIO Common Setting	SIO common settings. For details, refer to 3.2.6 SIO Common Setting .
SIO Configuration	SIO settings.

Parameter	Description
	For details, refer to 3.2.7 SIO Configuration .
PCI Subsystem Settings	PCI subsystem settings. For details, refer to 3.2.8 PCI Subsystem Settings .
USB Configuration	USB settings. For details, refer to 3.2.9 USB Configuration .
Network Stack Configuration	Network protocol stack settings. For details, refer to 3.2.10 Network Stack Configuration .
CSM Configuration	CSM settings. For details, refer to 3.2.11 CSM Configuration .
NVMe Configuration	NVMe settings. For details, refer to 3.2.12 NVMe Configuration .
Emulation Configuration	Emulation settings. For details, refer to 3.2.13 Emulation Configuration .
PXE Configuration	PXE settings. For details, refer to 3.2.14 PXE Configuration .
Tls Auth Configuration	Tls authentication settings. For details, refer to 3.2.15 Tls Auth Configuration .
RAM Disk Configuration	RAM disk settings. For details, refer to 3.2.16 RAM Disk Configuration .
Driver Health	Health status of drivers and controllers. For details, refer to 3.2.17 Driver Health .

**Note**

Other parameters on the **Advanced** screen are generated by related devices. For example, for **MAC:5 E919AE5D1E2-IPv4 Network Configuration** in [Figure 3-4](#), if the corresponding NIC exists, the parameter is displayed, and if the corresponding NIC does not exist, this parameter is not displayed.

3.2.1 Mainboard Information

The **Mainboard Information** screen contains board interface and device information. [Figure 3-5](#) shows the **Mainboard Information** screen.

Figure 3-5 Mainboard Information Screen



For a description of the parameters on the **Mainboard Information** screen, refer to [Table 3-3](#).

Table 3-3 Parameter Descriptions for the Mainboard Information screen

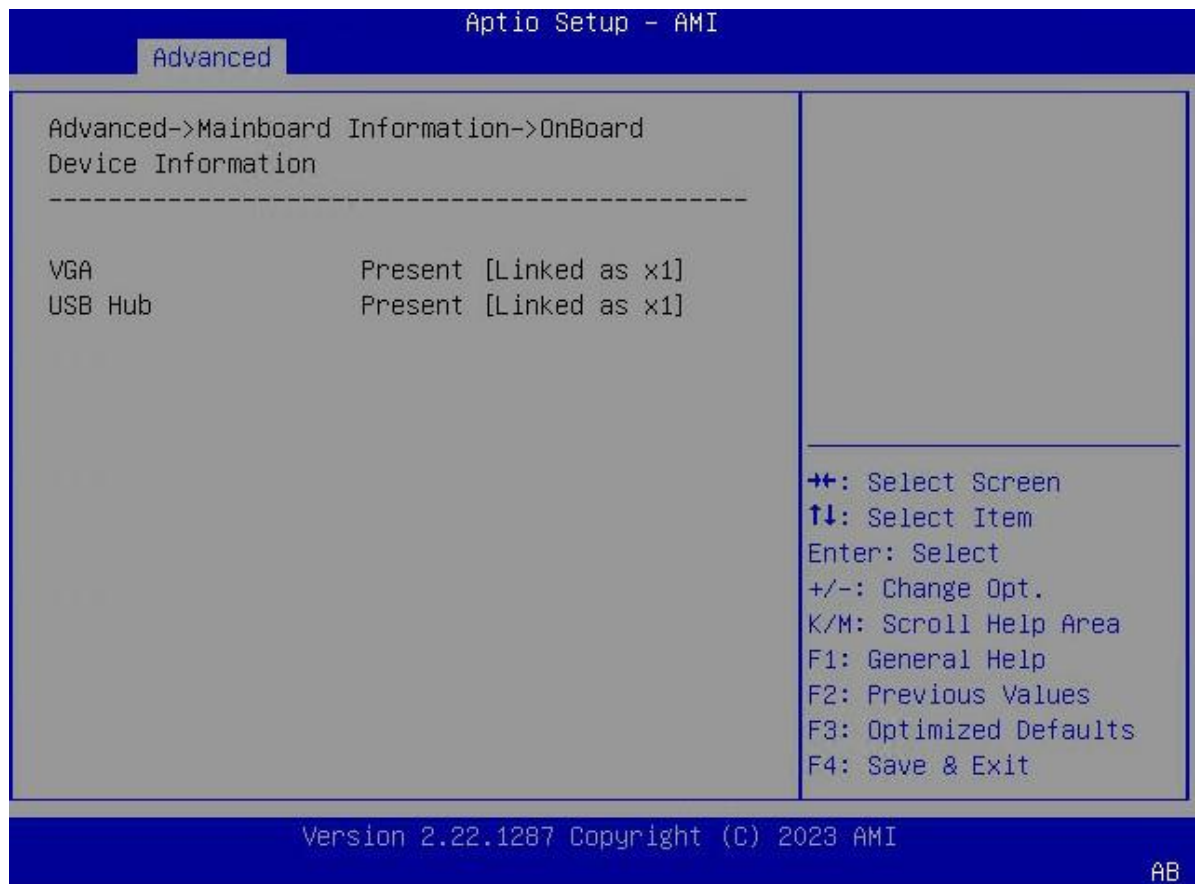
Parameter	Description	Default
Board Name	Mainboard name.	MI05102A
ME Version	ME version.	-
ME-BIOS Interface Ver	ME-BIOS interface version.	1.1
ME SKU	ME module.	Node Manager
ME Status	ME status.	Operational
USB2.0	Number and physical locations of USB 2.0 interfaces.	1 (Front)
USB3.0	Number and physical locations of USB 3.0 interfaces.	● 2 (Rear) ● 1 (Front)
COM	Number and physical locations of COM interfaces.	1 (Rear)
VGA	Number and physical locations of VGA interfaces.	● 1 Connector (Front)

Parameter	Description	Default
		● 1 Connector (Rear)
OnBoard Device Information	Onboard device information. For details, refer to 3.2.1.1 OnBoard Device Information .	-
LAN MAC Information	MAC address of the Ethernet port. For details, refer to 3.2.1.2 LAN MAC Information .	-
Graphics Card Information	Information about onboard graphics cards. For details, refer to 3.2.1.3 Graphics Card Information .	-
Slot Information	Information about PCIe card slots. For details, refer to 3.2.1.4 Slot Information .	-

3.2.1.1 OnBoard Device Information

Figure 3-6 shows the **OnBoard Device Information** screen.

Figure 3-6 OnBoard Device Information Screen



For a description of the parameters on the **OnBoard Device Information** screen, refer to [Table 3-4](#).

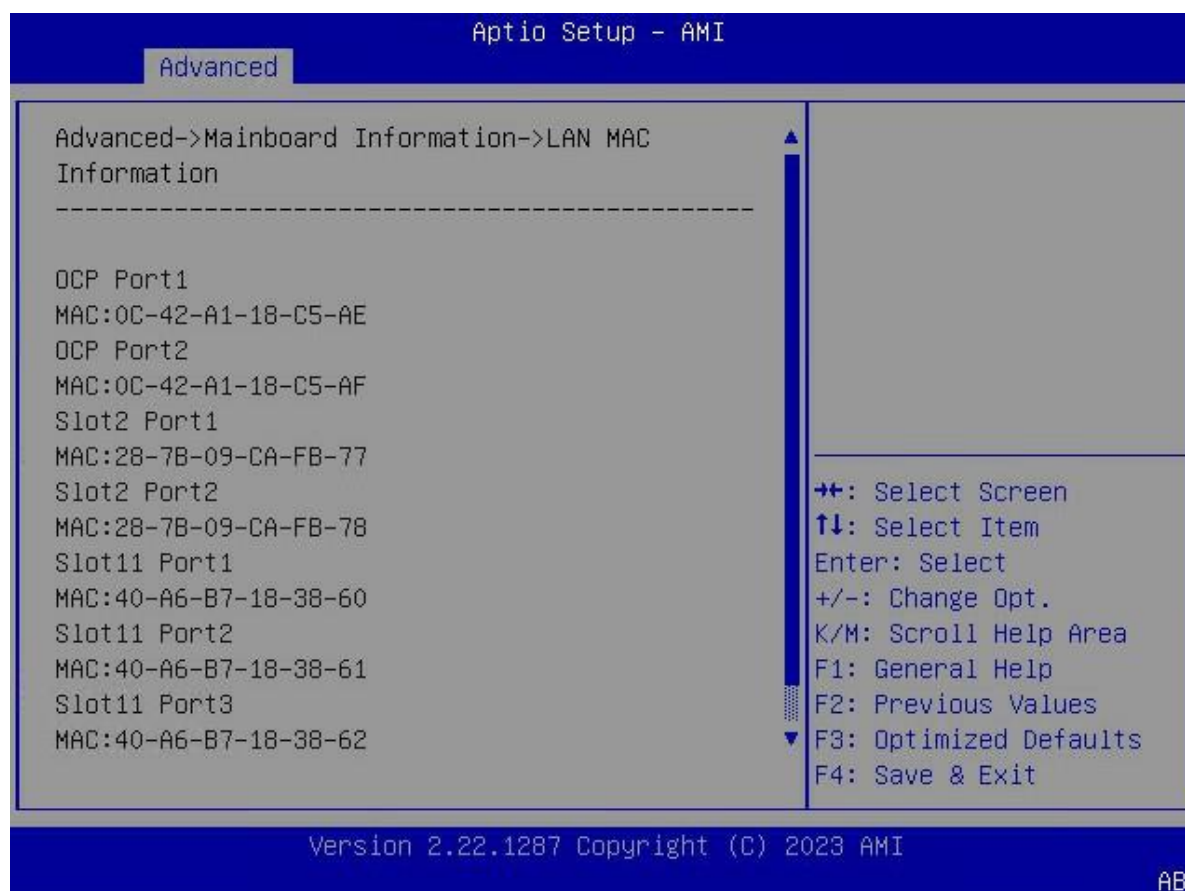
Table 3-4 Parameter Descriptions for the OnBoard Device Information Screen

Parameter	Description
VGA	Displays whether the VGA card on the mainboard is present. If the VGA card is not present on the mainboard, Not Present is displayed.
USB Hub	Displays whether the USB Hub on the mainboard is present. If the USB Hub is not present on the mainboard, Not Present is displayed.

3.2.1.2 LAN MAC Information

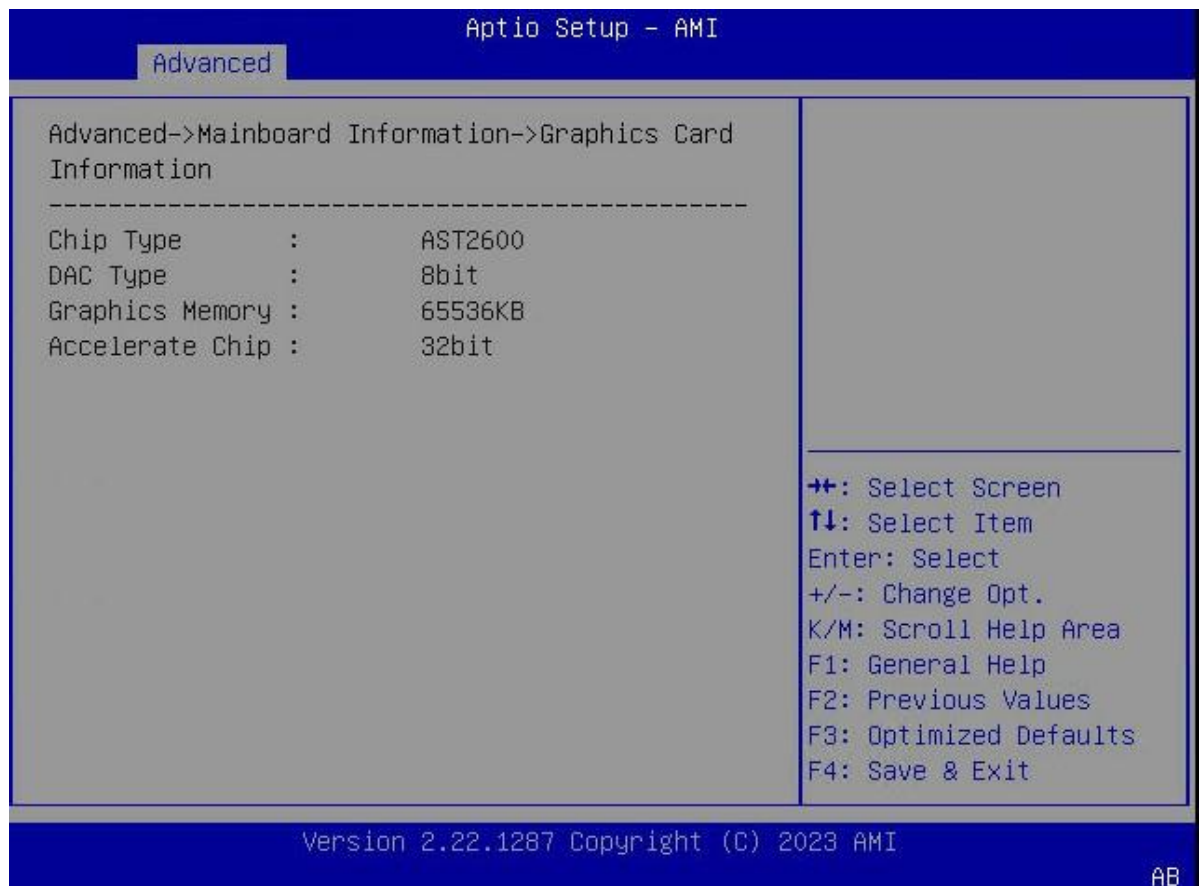
The **LAN MAC Information** screen displays MAC addresses of NICs. [Figure 3-7](#) shows the **LAN MAC Information** screen.

Figure 3-7 LAN MAC Information Screen



3.2.1.3 Graphics Card Information

[Figure 3-8](#) shows the **Graphics Card Information** screen.

Figure 3-8 Graphics Card Information Screen

For a description of the parameters on the **Graphics Card Information** screen, refer to [Table 3-5](#).

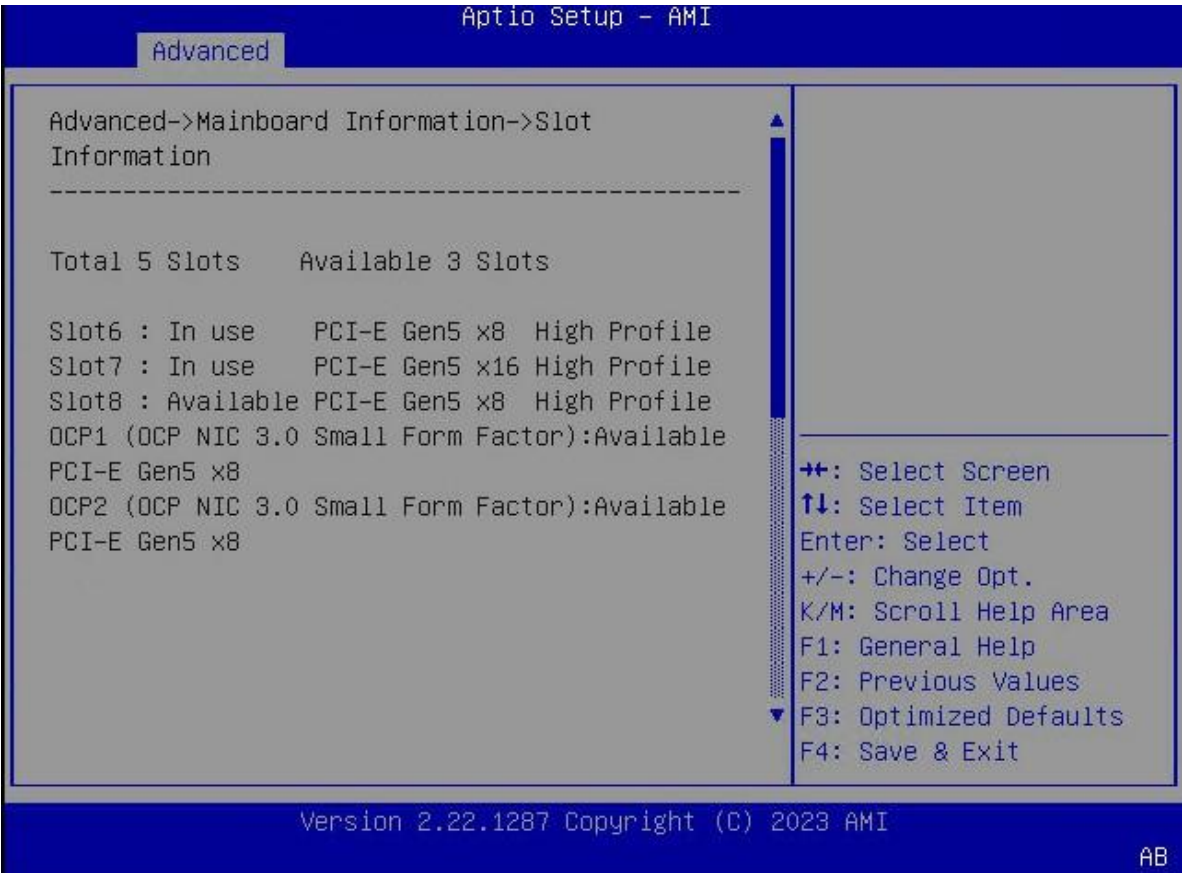
Table 3-5 Parameter Descriptions for the Graphics Card Information Screen

Parameter	Description
Chip Type	Chip type of the graphics card.
DAC Type	DAC type.
Graphics Memory	Graphics memory.
Accelerate Chip	Type of graphics accelerator.

3.2.1.4 Slot Information

[Figure 3-9](#) shows the **Slot Information** screen.

Figure 3-9 Slot Information Screen



For a description of the parameters on the **Slot Information** screen, refer to [Table 3-6](#).

Table 3-6 Parameter Descriptions for the Slot Information Screen

Parameter	Description
Total 5 Slots, Available 3 Slots	Total number of PCIe standard card slots on the mainboard and the number of available slots.

 Note

- Slot states are described as follows:
- **In use**: indicates that a device is installed in the current slot.
 - **Available**: indicates that no device is installed in the current slot.

3.2.2 Trusted Computing

[Figure 3-10](#) through [Figure 3-11](#) show the **Trusted Computing** screen.

Figure 3-10 Trusted Computing Screen—1

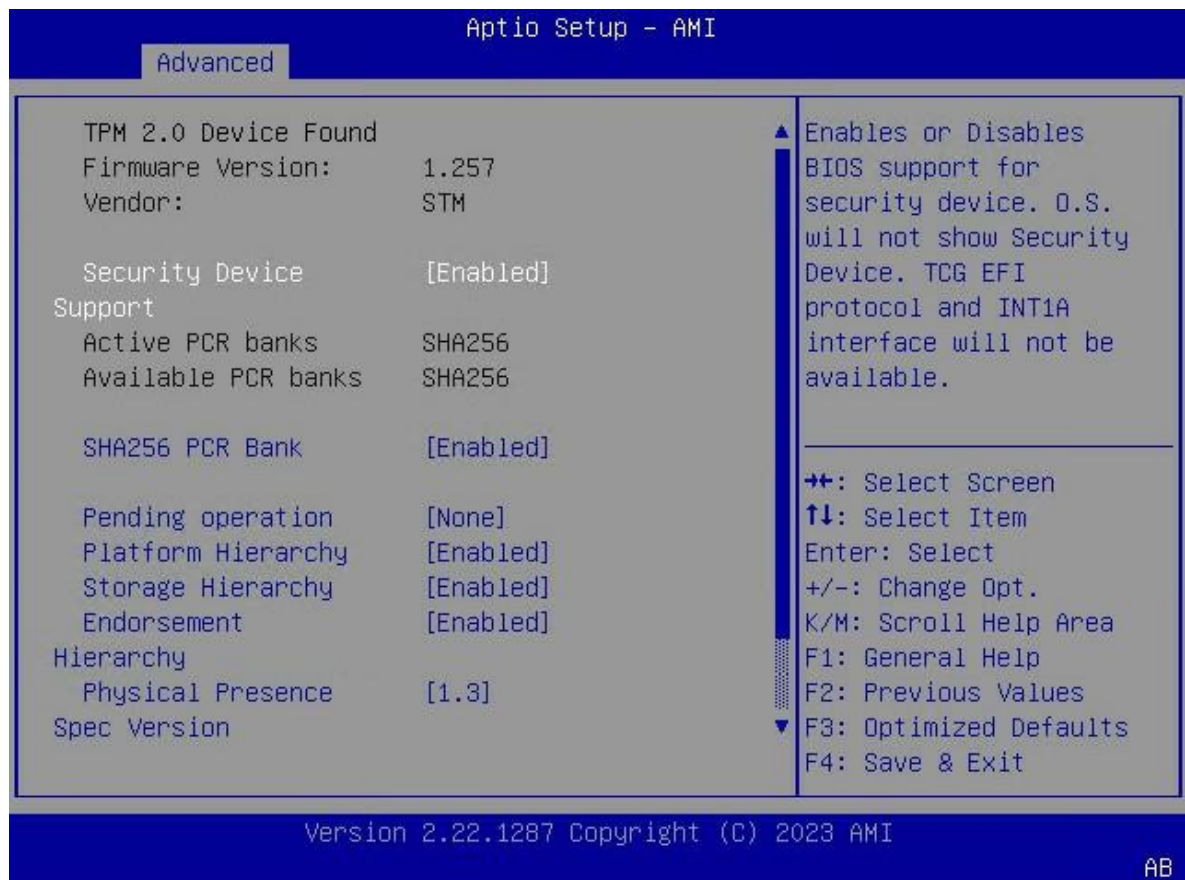
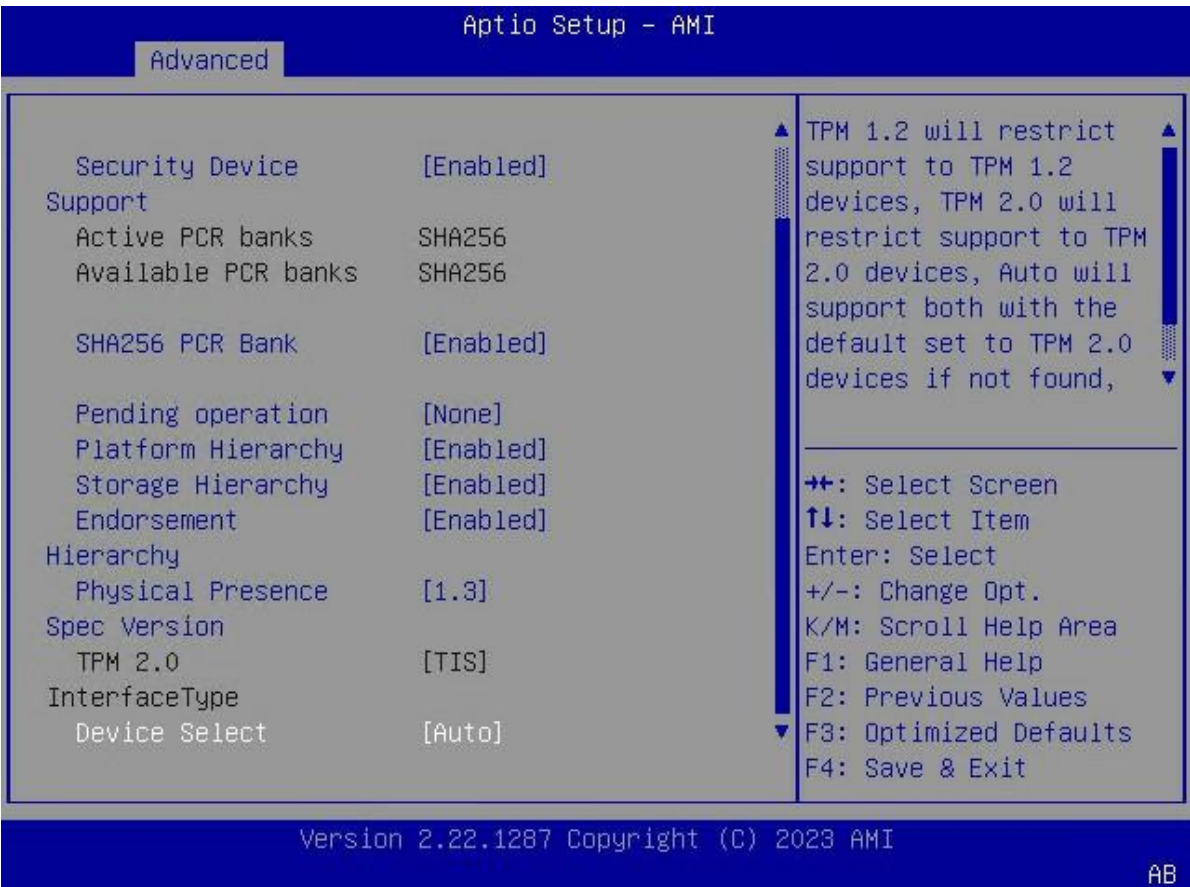


Figure 3-11 Trusted Computing Screen—2



For a description of the parameters on the **Trusted Computing** screen, refer to [Table 3-7](#).

Table 3-7 Parameter Descriptions for the Trusted Computing Screen

Parameter	Description	Default
Firmware Version	Firmware version number.	-
Vendor	Vendor name.	-
Security Device Support	Enables or disables BIOS support for the security device. Options: - Enabled: enables BIOS support for the security device. When this parameter is set to Enabled, the OS captures and displays security device information. - Disabled: disables BIOS support for the security device. When this parameter is set to Disabled, the TGG EFI protocol and the INT1A interface are unavailable.	Enabled
Active PCR banks	PCR Banks being used.	-

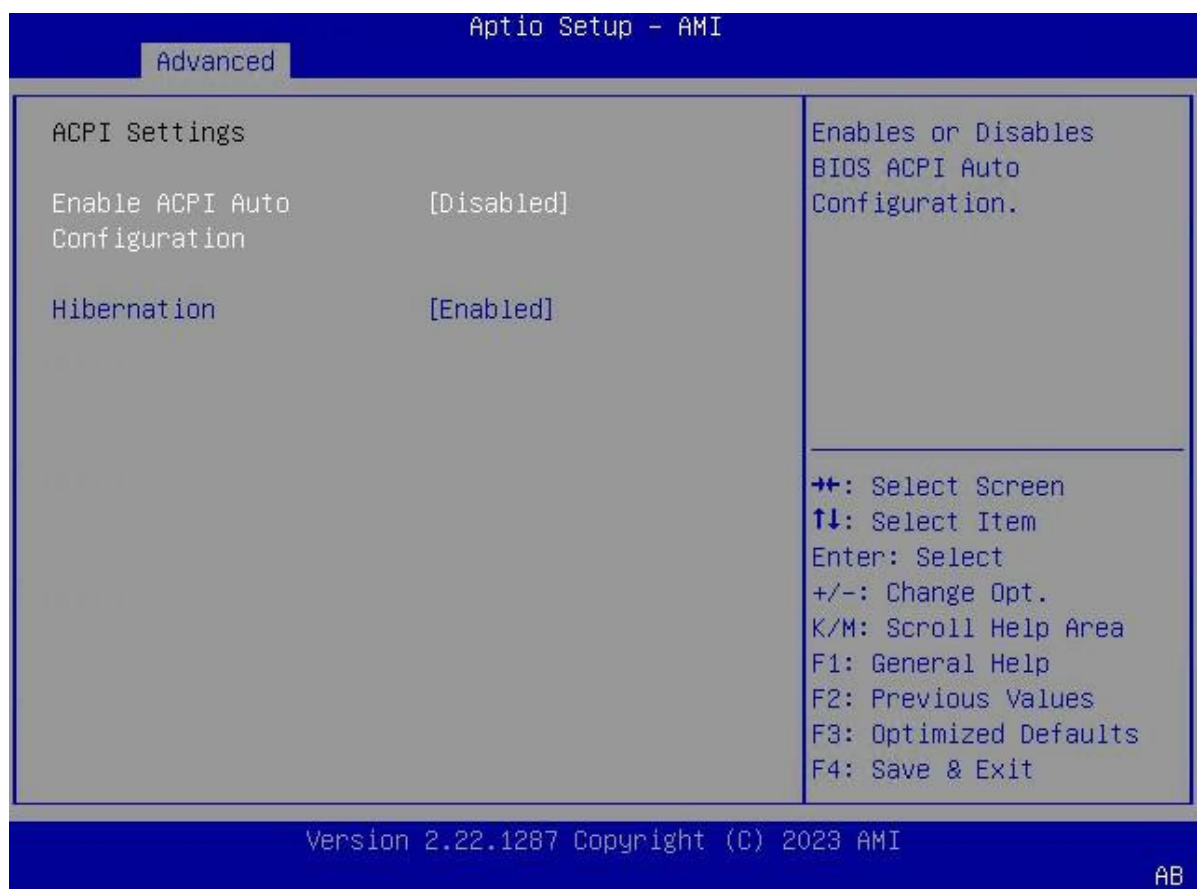
Parameter	Description	Default
Available PCR banks	Available PCR Banks.	-
SHA256 PCR Bank	Enables or disables the SHA256 PCR Bank configuration feature. Options: ● Enabled: enables the SHA256 PCR Bank configuration feature. ● Disabled: disables the SHA256 PCR Bank configuration feature.	Enabled
Pending operation	Schedules an operation for device security control. Options: ● None: no operation. ● TPM Clear: clears the TPM metric value.	None
Platform Hierarchy	Enables or disables the platform hierarchy feature. Options: ● Enabled: enables the platform hierarchy feature. ● Disabled: disables the platform hierarchy feature.	Enabled
Storage Hierarchy	Enables or disables the storage hierarchy feature. The storage hierarchy is controlled by the platform firmware. Options: ● Enabled: enables the storage hierarchy feature. ● Disabled: disables the storage hierarchy feature.	Enabled
Endorsement Hierarchy	Enables or disables the endorsement hierarchy feature. Options: ● Enabled: enables the endorsement hierarchy feature. ● Disabled: disables the endorsement hierarchy feature.	Enabled
Physical Presence Spec Version	Select the PPI specification version number reported to the OS. Options: ● 1.2: Version 1.2 is supported. ● 1.3: Version 1.3 is supported.	1.3
TPM 2.0 InterfaceType	TPM 2.0 interface type. This parameter cannot be configured.	TIS
Device Select	Select a supported device type. Options: ● TPM1.2: supports TPM 1.2 devices.	Auto

Parameter	Description		Default
	- TPM2.0: supports TPM 2.0 devices. - Auto: supports both types of devices. By default, TPM 2.0 devices are searched for. If no TPM 2.0 device is found, TPM 1.2 devices are searched for.		

3.2.3 ACPI Settings

Figure 3-12 shows the **ACPI Settings** screen.

Figure 3-12 ACPI Settings Screen



For a description of the parameters on the **ACPI Settings** screen, refer to [Table 3-8](#).

Table 3-8 Parameter Descriptions for the ACPI Settings Screen

Parameter	Description	Default
Enabled ACPI Auto Configuration	Enables or disables the ACPI auto-configuration feature. Options: Enabled: enables the ACPI auto-configuration feature.	Disabled

Parameter	Description	Default
	this parameter is set to Enabled, hibernate configuration items are hidden. Disabled: disables the ACPI auto-configuration feature.	
Hibernation	Enables or disables the system hibernation feature. Options: - Enabled: enables the system hibernation feature. - Disabled: disables the system hibernation feature.	Enabled

3.2.4 Redfish Host Interface Settings

Figure 3-13 shows the **Redfish Host Interface Settings** screen.

Figure 3-13 Redfish Host Interface Settings Screen



For a description of the parameters on the **Redfish Host Interface Settings** screen, refer to Table 3-9.

Table 3-9 Parameter Descriptions for the Redfish Host Interface Settings Screen

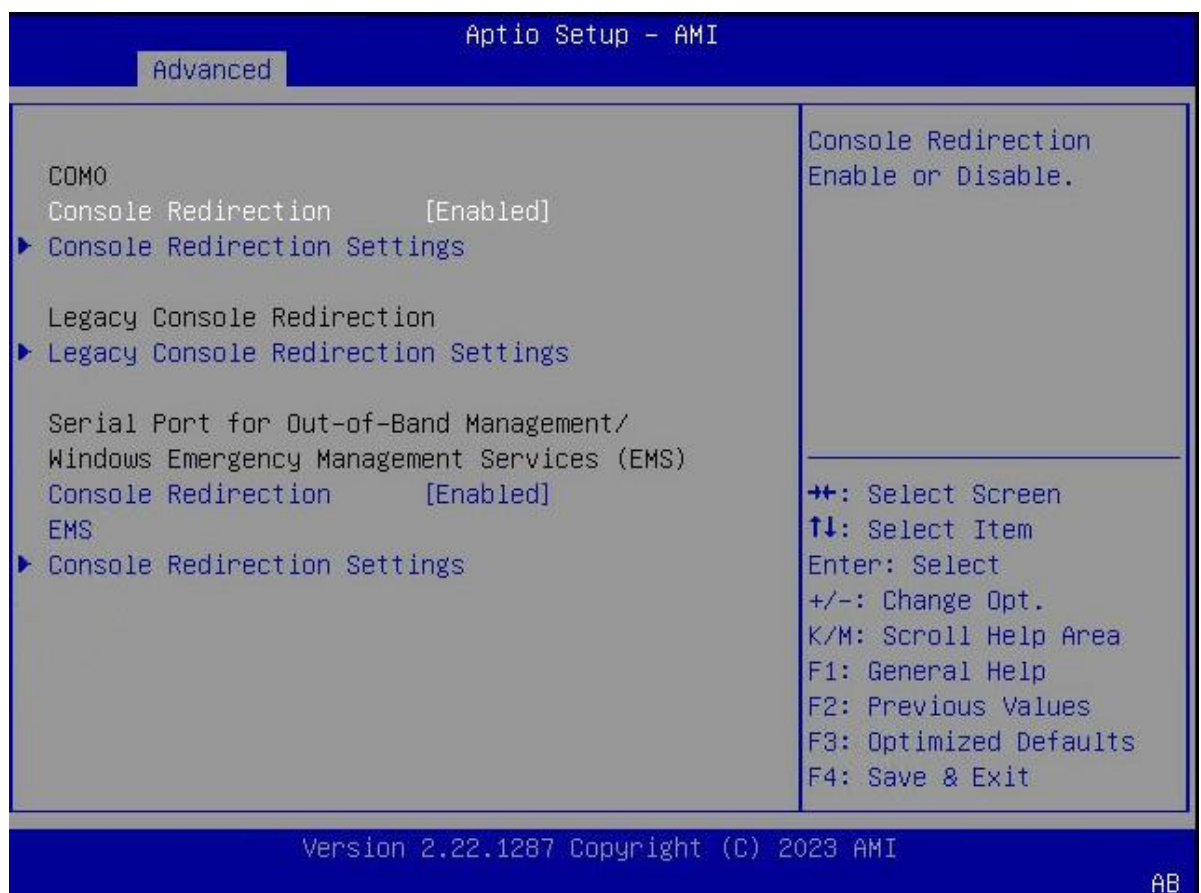
Parameter	Description	Default
BMC Redfish Version	BMC Redfish version number.	-

Parameter	Description	Default
BIOS Redfish Version	BIOS Redfish version number.	-
BIOS RTP Version	BIOS RTP version number.	-
Authentication mode	Select an authentication mode. Options: - Basic Authentication. - Session Authentication.	Basic Authentication

3.2.5 Serial Port Console Redirection Settings

Figure 3-14 shows the **Serial Port Console Redirection** screen.

Figure 3-14 Serial Port Console Redirection Screen



For a description of the parameters on the **Serial Port Console Redirection** screen, refer to Table 3-10.

Table 3-10 Parameter Descriptions for the Serial Port Console Redirection Screen

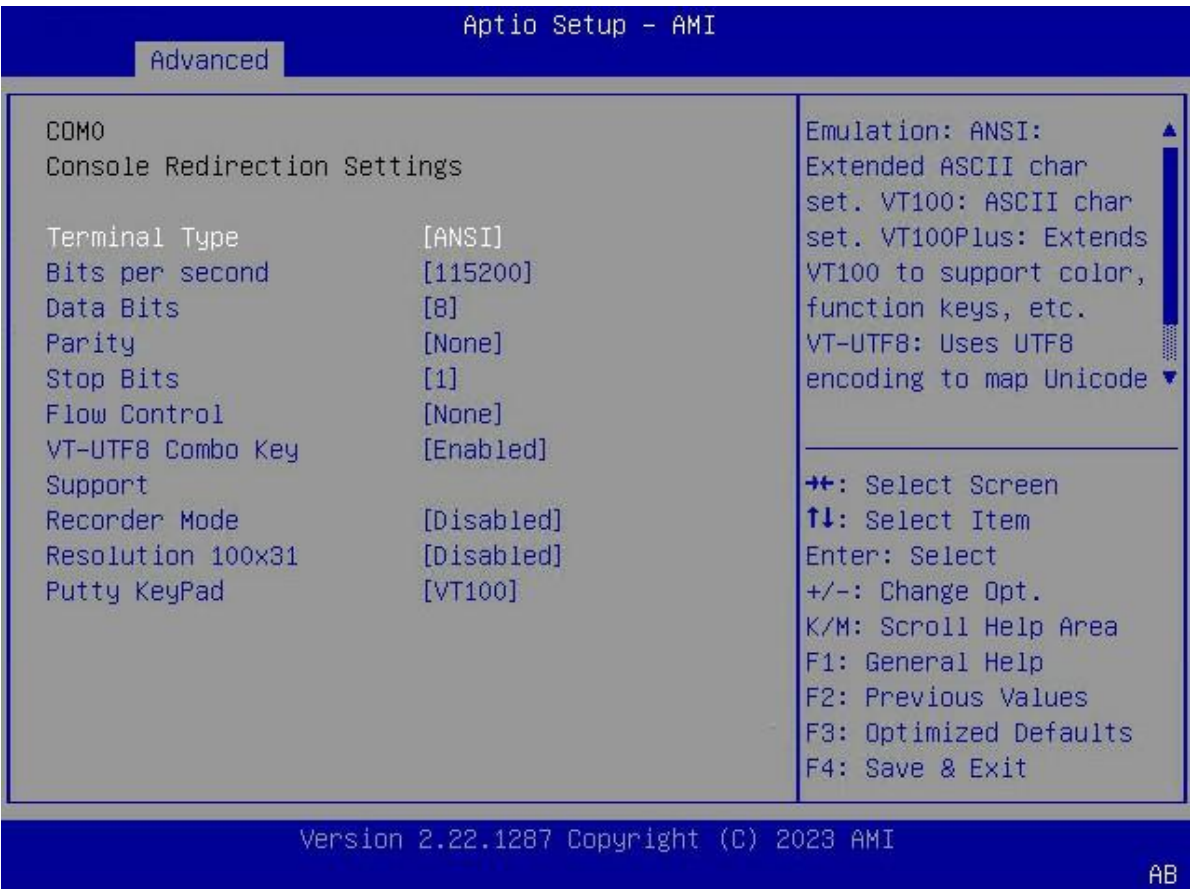
Parameter	Description	Default
Console Redirection	Enables or disables the serial port redirection feature. Options:	Enabled

Parameter	Description	Default
	- Enabled: enables the serial port redirection feature. - Disabled: disables the serial port redirection feature. When this parameter is set to Disabled, Console Redirection Settings below is not configurable.	
Console Redirection Settings	Configures serial port redirection to specify how the host and a remote computer exchange data. The host and the remote computer should have the same or compatible settings. For details, refer to 3.2.5.1 Console Redirection Settings (COM0).	-
Legacy Console Redirection Settings	Configures the serial port redirection feature in Legacy mode. For details, refer to 3.2.5.2 Legacy Console Redirection Settings.	-
Console Redirection EMS	Enables or disables the serial port redirection feature of the EMS. Options: - Enabled: enables the serial port redirection feature of the EMS. - Disabled: disables the serial port redirection feature of the EMS. When this parameter is set to Disabled, Console Redirection Settings below is not configurable.	Enabled
Console Redirection Settings	Configures the console redirection feature of the EMS. For details, refer to 3.2.5.3 Console Redirection Settings (EMS).	-

3.2.5.1 Console Redirection Settings (COM0)

[Figure 3-15](#) shows the **Console Redirection Settings** screen.

Figure 3-15 Console Redirection Settings Screen



For a description of the parameters on the **Console Redirection Settings** screen, refer to [Table 3-11](#).

Table 3-11 Parameter Descriptions for the Console Redirection Settings Screen

Parameter	Description	Default
Terminal Type	Terminal type. Options: - ANSI: extended ASCII character set. - VT100: ASCII character set. - VT100+: extended VT100, which is used to support color display and functional keys. - VT-UTF8: UTF8 is used to map unicode characters to one or more bytes.	ANSI
Bits per Second	Number of bits transmitted per second. The transmission speed must match the serial port, and very long lines or lines with noise may require lower speeds. Options: 9600 19200	115200

Parameter	Description	Default
	● 38400 ● 57600 ● 115200	
Data Bits	Number of bits used by the actual data in a byte. Options: ● 7 ● 8	8
Parity	Parity bit, which can be transmitted together with data bits to detect transmission errors. Options: ● None: No parity bit is transmitted. ● Even: If the number of 1s in the data bits is an even number, the parity bit is 0. ● Odd: If the number of 1s in the data bits is an odd number, the parity bit is 0. ● Mark: The parity bit is always a binary 1. ● Space: The parity bit is always a binary 0. For Mark and Space, error detection is not performed. Mark or Space can be used as an additional data bit.	None
Stop Bits	Stop bit, which indicates the end of a packet. The start bit indicates the start of a packet. Select the number of stop bits. The standard setting is one stop bit. More than one stop bit may be required for communication with a slow speed device. Options: ● 1: 1 stop bit ● 2: 2 stop bits	1
Flow Control	Flow control, which can prevent data loss caused by buffer overflow. During data transmission, if the receive buffer is full, a "stop" signal can be sent to stop the data flow. Once the buffer is empty, a "start" signal can be sent to restart the process. Select a flow control mode. Options: ● None: no flow control. ● Hardware RTS/CTS: hardware flow control. Hardware flow control uses two lines. One is used to send the "stop" signal and the other is used to send the "start" signal.	None

Parameter	Description	Default
VT-UTF8 Combo Key Support	Enables or disables the VT-UTF8 combination key support for ANSI/VT 100 terminals. Options: ● Enabled: enables the VT-UTF8 combination key support. ● Disabled: disables the VT-UTF8 combination key support.	Enabled
Recorder Mode	Enables or disables recorder mode for capturing terminal text data. Options: ● Enabled: enables recorder mode. ● Disabled: disables recorder mode.	Disabled
Resolution 100×31	Enables or disables the extended terminal resolution feature. Options: ● Enabled: enables the extended terminal resolution feature. ● Disabled: disables the extended terminal resolution feature.	Disabled
Putty KeyPad	Sets FunctionKey and KeyPad in PuTTY. Options: ● VT100 ● LINUX ● XTERMR6 ● SCO ● ESCN ● VT400	VT100

3.2.5.2 Legacy Console Redirection Settings

Figure 3-16 shows the **Legacy Console Redirection Settings** screen.

Figure 3-16 Legacy Console Redirection Settings Screen



For a description of the parameters on the **Legacy Console Redirection Settings** screen, refer to [Table 3-12](#).

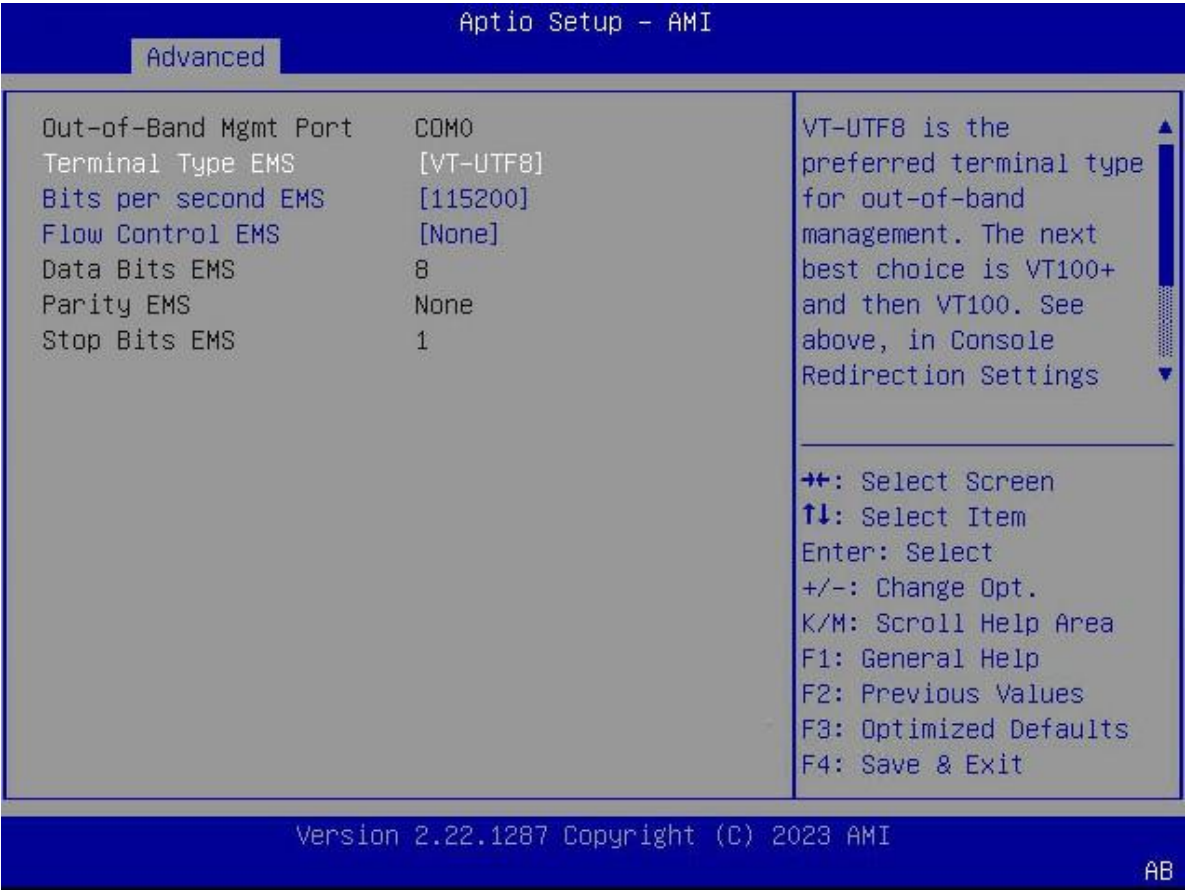
Table 3-12 Parameter Descriptions for the Legacy Console Redirection Settings Screen

Parameter	Description	Default
Redirection COM Port	COM port for redirection of OS, Option, and ROM information in Legacy mode.	COM0
Resolution	Select the number of rows and columns that can be redirected in Legacy mode. Options: 80×24 80×25	80×24
Redirect After POST	Select redirection after POST. Options: - Always Enable: enables legacy console redirection for the legacy OS. - BootLoader: disables legacy console redirection before the legacy OS is loaded.	Always Enable

3.2.5.3 Console Redirection Settings (EMS)

Figure 3-17 shows the **Console Redirection Settings** screen.

Figure 3-17 Console Redirection Settings Screen



For a description of the parameters on the **Console Redirection Settings** screen, refer to Table 3-13.

Table 3-13 Parameter Descriptions for the Console Redirection Settings Screen

Parameter	Description	Default
Out-of-Band Mgmt Port	Out-of-band management serial port.	COM0
Terminal Type EMS	Select an EMS terminal type. Options: ● ANSI: extended ASCII character set. ● VT100: ASCII character set. ● VT100+: extended VT100, which is used to support color display and function keys.	VT-UTF8

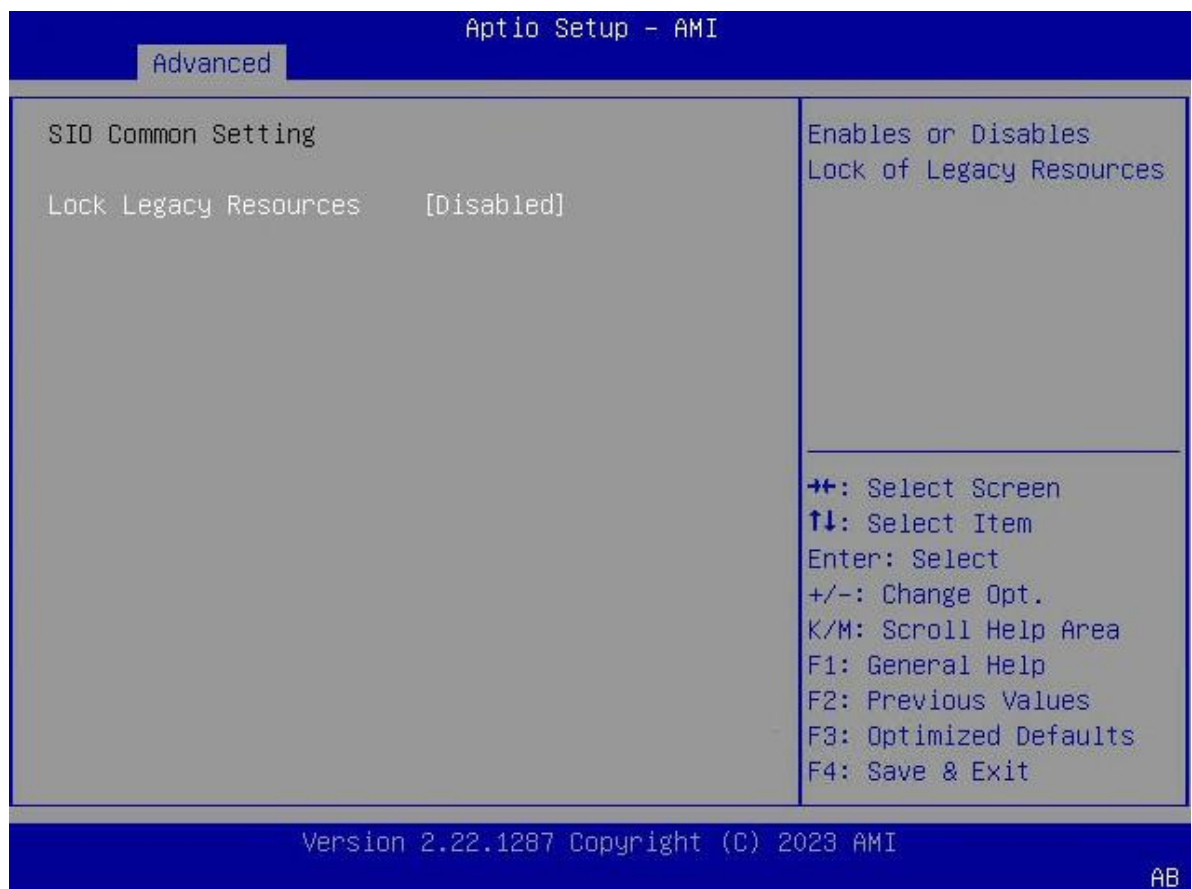
Parameter	Description	Default
	● VT-UTF8: UTF8 is used to map unicode characters to one or more bytes. EMS terminal types are sorted as follows: 1. VT-UTF8 2. VT100+ 3. VT100	
Bits per second EMS	Select the number of bits transmitted per second by the EMS. The transmission speed must match the serial port, and very long lines or lines with noise may require lower speeds. Options: ● 9600 ● 19200 ● 57600 ● 115200	115200
Flow Control EMS	Flow control of the EMS to prevent data loss caused by buffer overflow. During data transmission, if the receive buffer is full, a "stop" signal can be sent to stop the data flow. Once the buffer is empty, a "start" signal can be sent to restart the process. Select a flow control mode. Options: ● None: no flow control. ● Hardware RTS/CTS: hardware flow control. Hardware flow control uses two lines. One is used to send the "stop" signal and the other is used to send the "start" signal. ● Software Xon/Xoff: software flow control.	None

Parameter	Description	Default
Data Bits EMS	The number of bits used by the actual data in the EMS.	8
Parity EMS	Parity of the EMS.	None
Stop Bits EMS	Stop bit of the EMS.	1

3.2.6 SIO Common Setting

Figure 3-18 shows the **SIO Common Setting** screen.

Figure 3-18 SIO Common Setting Screen



For a description of the parameters on the **SIO Common Setting** screen, refer to [Table 3-14](#).

Table 3-14 Parameter Descriptions for the SIO Common Setting Screen

Parameter	Description	Default
Lock Legacy Resources	Locks or unlocks legacy resources. Options: - Enabled: locks legacy resources. - Disabled: unlocks legacy resources.	Disabled

3.2.7 SIO Configuration

Figure 3-19 shows the **SIO Configuration** screen.

Figure 3-19 SIO Configuration Screen



Note

Super IO Chip Logical Device(s) Configuration on the **SIO Configuration** screen is displayed based on the particular situation.

For example, **Serial Port 1** and **Serial Port 2** contain the basic attributes of the SIO logical device. By configuring the basic attributes, you can enable or disable the SIO devices and modify device resources.

For a description of the parameters on the **SIO Configuration** screen, refer to [Table 3-15](#).

Table 3-15 Parameter Descriptions for the SIO Configuration Screen

Parameter	Description
AMI SIO Driver Version	Version number of the AMI SIO driver.
[*Active*] Serial Port 1	Allows you to view and set the basic attributes of the SIO logical devices, such as IO Base , DMA Channel , and Device Mode . For details, refer to 3.2.7.1 Serial Port 1 .
[*Active*] Serial Port 2	Allows you to view and set the basic attributes of the SIO logical devices, such as IO Base , DMA Channel , and Device Mode .

Parameter	Description
	For details, refer to 3.2.7.1 Serial Port 1 .

3.2.7.1 Serial Port 1

Figure 3-20 shows the **Serial Port 1** screen.

Figure 3-20 Serial Port 1 Screen



 Note

The items on the **Serial Port 1** screen are the same as those on the **Serial Port 2** screen. This procedure uses **Serial Port 1** as an example.

For a description of the parameters on the **Serial Port 1** screen, refer to [Table 3-16](#).

Table 3-16 Parameter Descriptions for the Serial Port 1 Screen

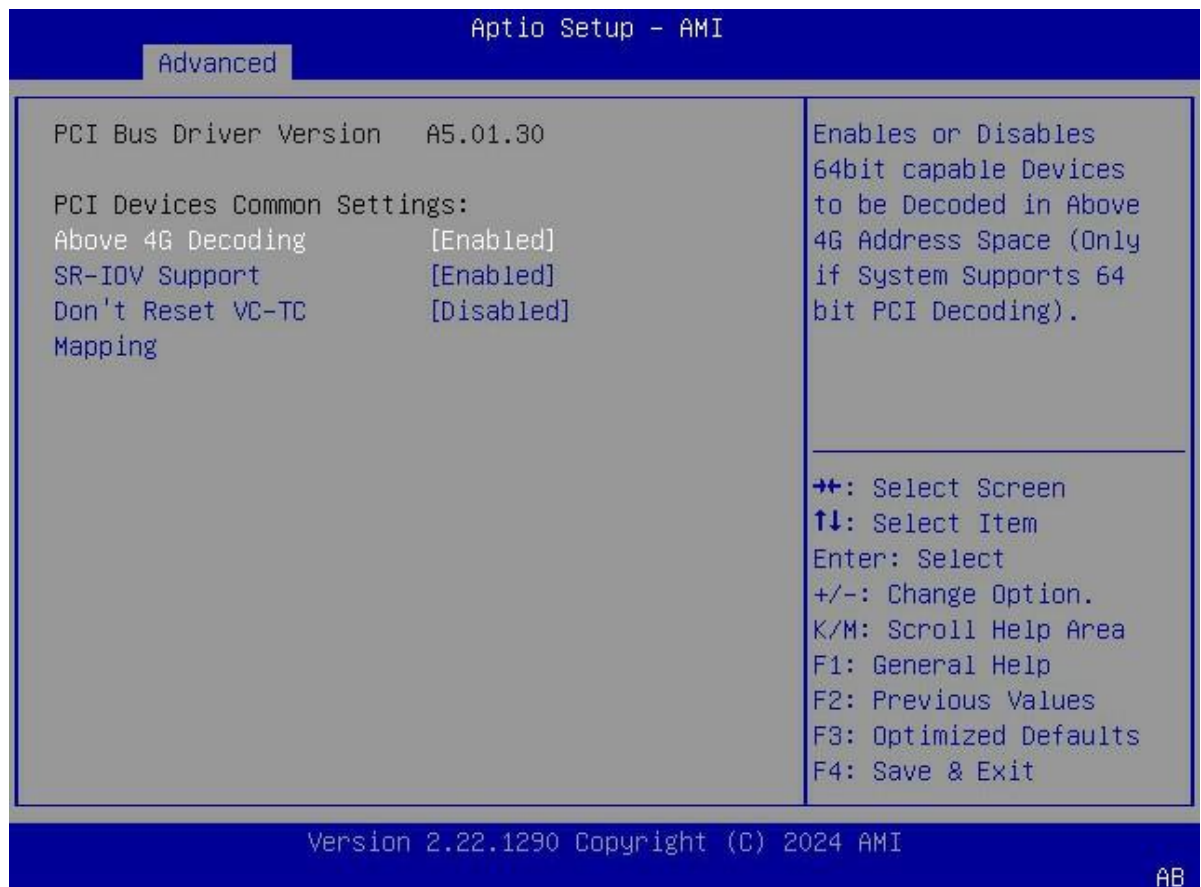
Parameter	Description	Default
Use This Device	Enables or disables this device. Options: ● Enabled: enables this device. ● Disabled: disables this device.	Enabled

Parameter	Description	Default
	When this parameter is set to Disabled , the parameters below Use This Device are hidden.	
Current	Current configuration.	IO=3F8H; IRQ=4;
Possible	Allows you to change the device resource settings. After the system reboots, the new settings are displayed on the Serial Port 1 screen. Options: ● Use Automatic Settings ● IO=3F8h; IRQ=4; DMA; ● IO=2F8h; IRQ=4; DMA; ● IO=3E8h; IRQ=4; DMA; ● IO=2E8h; IRQ=4; DMA;	Use Automatic Settings

3.2.8 PCI Subsystem Settings

Figure 3-21 shows the **PCI Subsystem Settings** screen.

Figure 3-21 PCI Subsystem Settings Screen



For a description of the parameters on the **PCI Subsystem Settings** screen, refer to [Table 3-17](#).

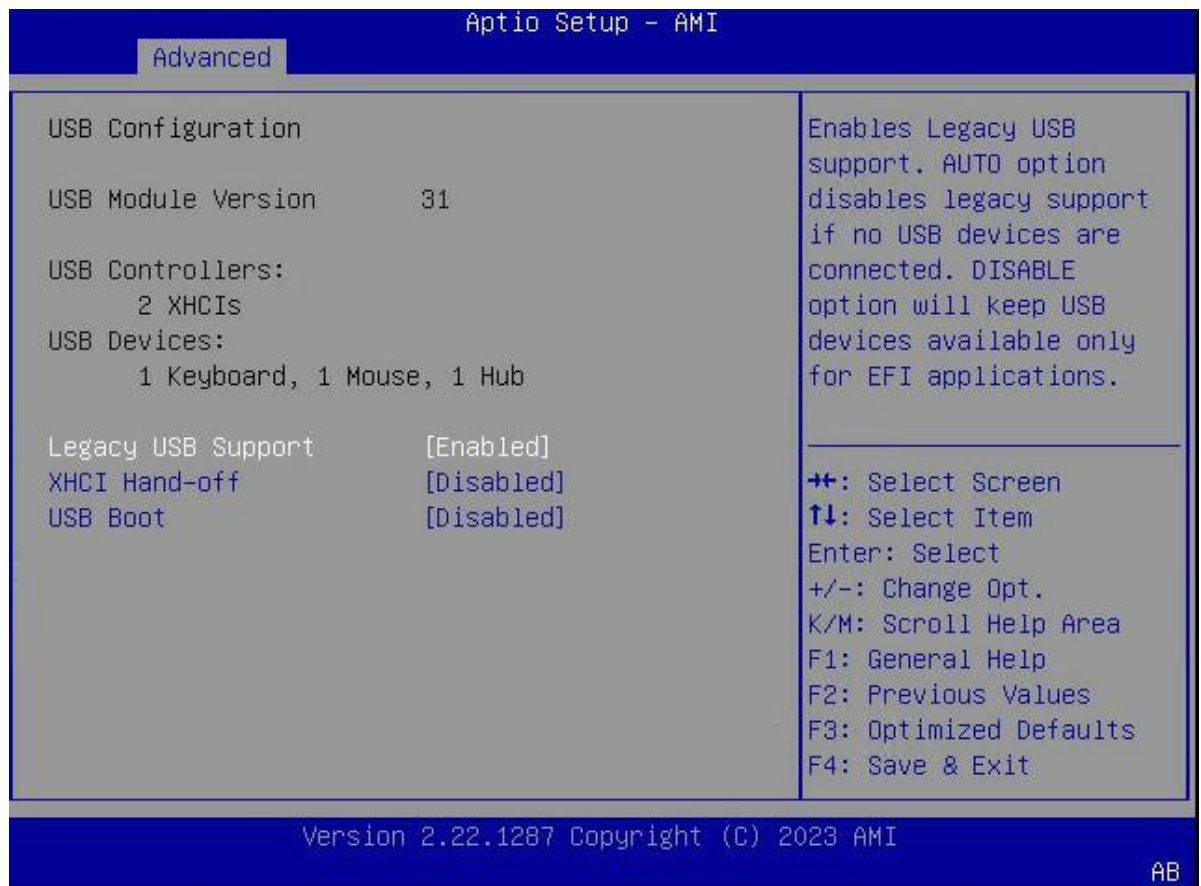
Table 3-17 Parameter Descriptions for the PCI Subsystem Settings Screen

Parameter	Description	Default
PCI Bus Driver Version	Version number of the PCI bus driver.	-
Above 4G Decoding	Enables or disables decoding of 64-bit devices in the address space above 4G (only when the system supports 64-bit PCI decoding). Options: ● Enabled: enables decoding of 64-bit devices in the address space above 4G. ● Disabled: disables decoding of 64-bit devices in the address space above 4G.	Enabled
SR-IOV Support	If the system has PCIe devices that support SR-IOV, set this parameter to enable or disable SR-IOV support. Options: ● Enabled: enables SR-IOV support. ● Disabled: disables SR-IOV support.	Enabled
Don't Reset VC-TC Mapping	Controls whether software can reset the traffic class mapping to the default state through a virtual channel (the system needs to have a virtual channel). Options: ● Enabled: enables software to reset the traffic class mapping to the default state through a virtual channel. When this parameter is set to Enabled, VC resources are not modified. ● Disabled: disables software from resetting the traffic class mapping to the default state through a virtual channel.	Disabled

3.2.9 USB Configuration

Figure 3-22 shows the **USB Configuration** screen.

Figure 3-22 USB Configuration Screen



For a description of the parameters on the **USB Configuration** screen, refer to [Table 3-18](#).

Table 3-18 Parameter Descriptions for the USB Configuration Screen

Parameter	Description	Default
USB Module Version	USB module version number.	-
USB Controllers	USB controllers.	-
USB Devices	USB devices.	-
Legacy USB Support	Enables or disables USB support in Legacy mode. Options: - Enabled: enables USB support in Legacy mode. - Disabled: disables USB support in Legacy mode. When this parameter is set to Disabled, USB devices are available only for EFI applications. - Auto: If there are no USB devices, USB support in Legacy mode is disabled.	Enabled
XHCI Hand-off	Enables or disables the XHCI feature, which provides a viable solution for OSs that do not support XHCI.	Enabled

Parameter	Description	Default
	XHCI ownership changes shall be declared by the XHCI driver. Options: • Enabled: enables the XHCI feature. • Disabled: disables the XHCI feature.	
USB Boot	Enables or disables support for USB mass storage drivers. Options: • Enabled: enables support for USB mass storage drivers. • Disabled: disables support for USB mass storage drivers.	Enabled

3.2.10 Network Stack Configuration

Figure 3-23 shows the **Network Stack Configuration** screen.

Figure 3-23 Network Stack Configuration Screen



For a description of the parameters on the **Network Stack Configuration** screen, refer to [Table 3-19](#).

Table 3-19 Parameter Descriptions for the Network Stack Configuration Screen

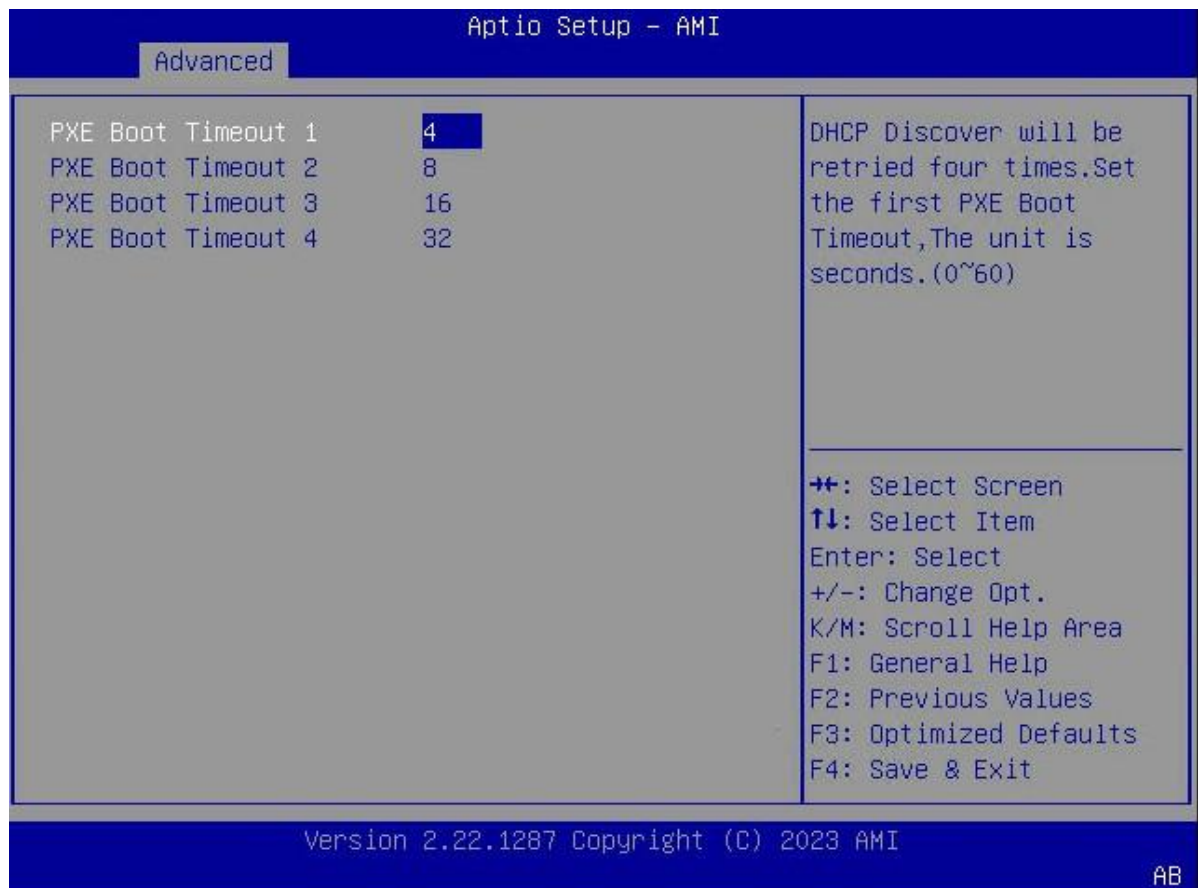
Parameter	Description	Default
IPv4 PXE Support	Enables or disables the IPv4 PXE boot feature. Options: ● Enabled: enables the IPv4 PXE boot feature. ● Disabled: disables the IPv4 PXE boot feature.	Enabled
IPv4 HTTP Support	Enables or disables the IPv4 HTTP boot feature. Options: ● Enabled: enables the IPv4 HTTP boot feature. ● Disabled: disables the IPv4 HTTP boot feature.	Disabled
IPv4 PXE Boot Timeout	Sets IPv4 PXE boot timeout parameters. For details, refer to 3.2.10.1 IPv4 PXE Boot Timeout .	-
IPv6 PXE Support	Enables or disables the IPv6 PXE boot feature. Options: ● Enabled: enables the IPv6 PXE boot feature. ● Disabled: disables the IPv6 PXE boot feature.	Enabled
IPv6 HTTP Support	Enables or disables the IPv6 HTTP boot feature. Options: ● Enabled: enables the IPv6 HTTP boot feature. ● Disabled: disables the IPv6 HTTP boot feature.	Disabled
PXE boot wait time	Sets the PXE boot wait time in seconds. When the system is booting, press Esc to terminate the PXE boot wait time. ● To increase the value by one, press +. ● To decrease the value by one, press -. ● To specify a value, press the corresponding number key.	0
Media detect count	Number of media device detection times, range: 1–50. ● To increase the value by one, press +. ● To decrease the value by one, press -. ● To specify a value, press the corresponding number key.	3
PXE Retry Count	Number of PXE retry times. Range: 1–50. Only UEFI mode is supported. When set to 50, PXE retries are always performed. ● To increase the value by one, press +. ● To decrease the value by one, press -. ● To specify a value, press the corresponding number key.	1

Parameter	Description	Default
PXE Only	PXE only. Options: - Enabled: attempts to boot from the PXE setting only. - Disabled: The PXE device has a higher boot priority.	Enabled

3.2.10.1 IPv4 PXE Boot Timeout

Figure 3-24 shows the **IPv4 PXE Boot Timeout** screen.

Figure 3-24 IPv4 PXE Boot Timeout Screen



For a description of the parameters on the **IPv4 PXE Boot Timeout** screen, refer to [Table 3-20](#).

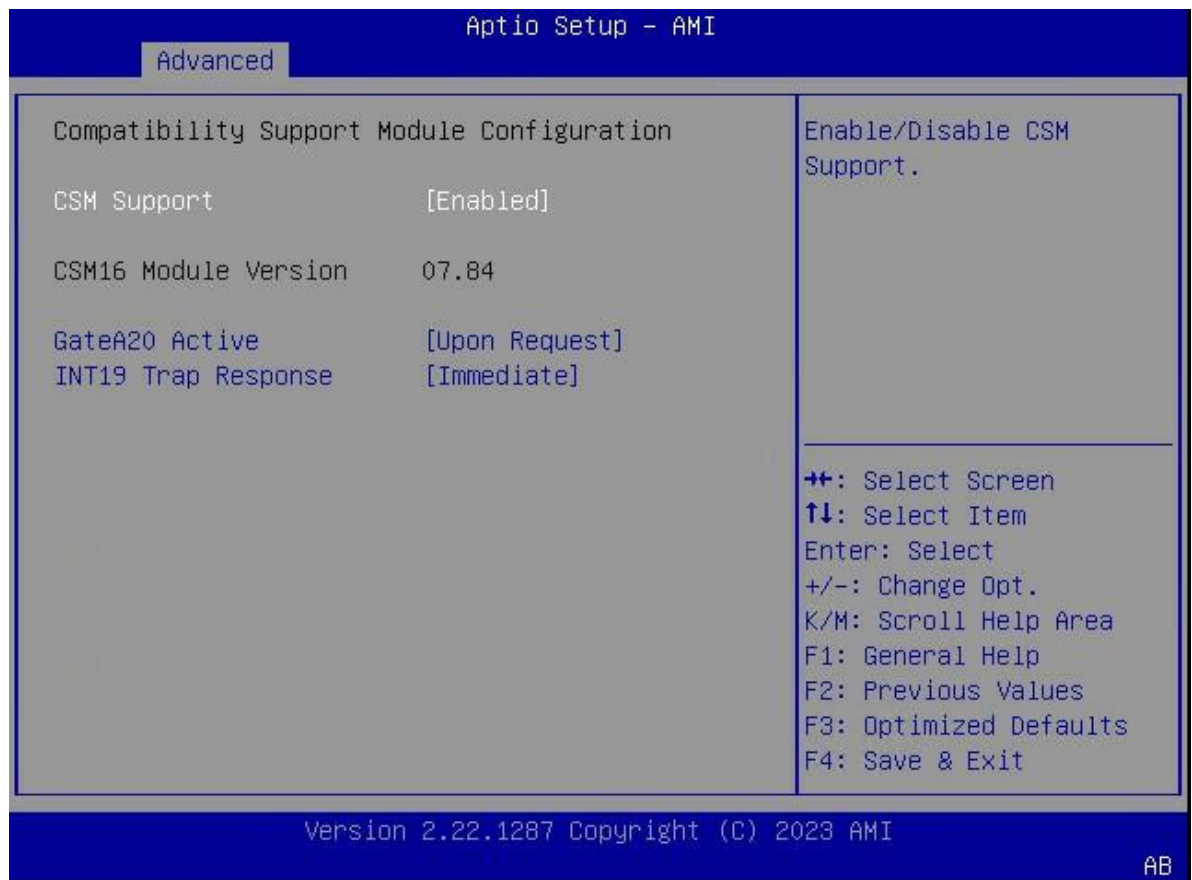
Table 3-20 Parameter Descriptions for the IPv4 PXE Boot Timeout Screen

Parameter	Description	Default
PXE Boot Timeout 1	First PXE boot timeout time, unit: s, range: 0–60. - To increase the value by one, press +. - To decrease the value by one, press -.	4

Parameter	Description	Default
	● To specify a value, press the corresponding number key.	
PXE Boot Timeout 2	Second PXE boot timeout time, unit: s, range: 0–60. ● To increase the value by one, press +. ● To decrease the value by one, press -. ● To specify a value, press the corresponding number key.	8
PXE Boot Timeout 3	Third PXE boot timeout time, unit: s, range: 0–60. ● To increase the value by one, press +. ● To decrease the value by one, press -. ● To specify a value, press the corresponding number key.	16
PXE Boot Timeout 4	Fourth PXE boot timeout time, unit: s, range: 0–60. ● To increase the value by one, press +. ● To decrease the value by one, press -. ● To specify a value, press the corresponding number key.	32

3.2.11 CSM Configuration

Figure 3-25 shows the **CSM Configuration** screen.

Figure 3-25 CSM Configuration Screen

For a description of the parameters on the **CSM Configuration** screen, refer to [Table 3-21](#).

Table 3-21 Parameter Descriptions for the CSM Configuration Screen

Parameter	Description	Default
CSM Support	Enables or disables CSM support. Options: - Enabled: enables CSM support. - Disabled: disables CSM support. When this parameter is set to Disabled , the parameters below are hidden.	Enabled
CSM16 Module Version	Version number of the CSM16 module.	-
GateA20 Active	GateA20 status. Options: - Upon Request: GateA20 can be disabled using the BIOS service. - Always: Disabling GateA20 is not allowed. The Always option is useful when any RT code is executed above 1 MB.	Upon Request
INT19 Trap Response	BIOS reaction on INT19 trapping by Option ROM.	Immediate

Parameter	Description	Default
	Options: ● Immediate: executes the trap immediately. ● Postponed: executes the trap during legacy boot.	

3.2.12 NVMe Configuration

Figure 3-26 shows the **NVMe Configuration** screen.

Figure 3-26 NVMe Configuration Screen



Note

If an **NVMe** drive is mounted on the mainboard, the NVMe drive information is displayed.

3.2.13 Emulation Configuration

Figure 3-27 shows the **Emulation Configuration** screen.

Figure 3-27 Emulation Configuration Screen



For a description of the parameters on the **Emulation Configuration** screen, refer to [Table 3-22](#).

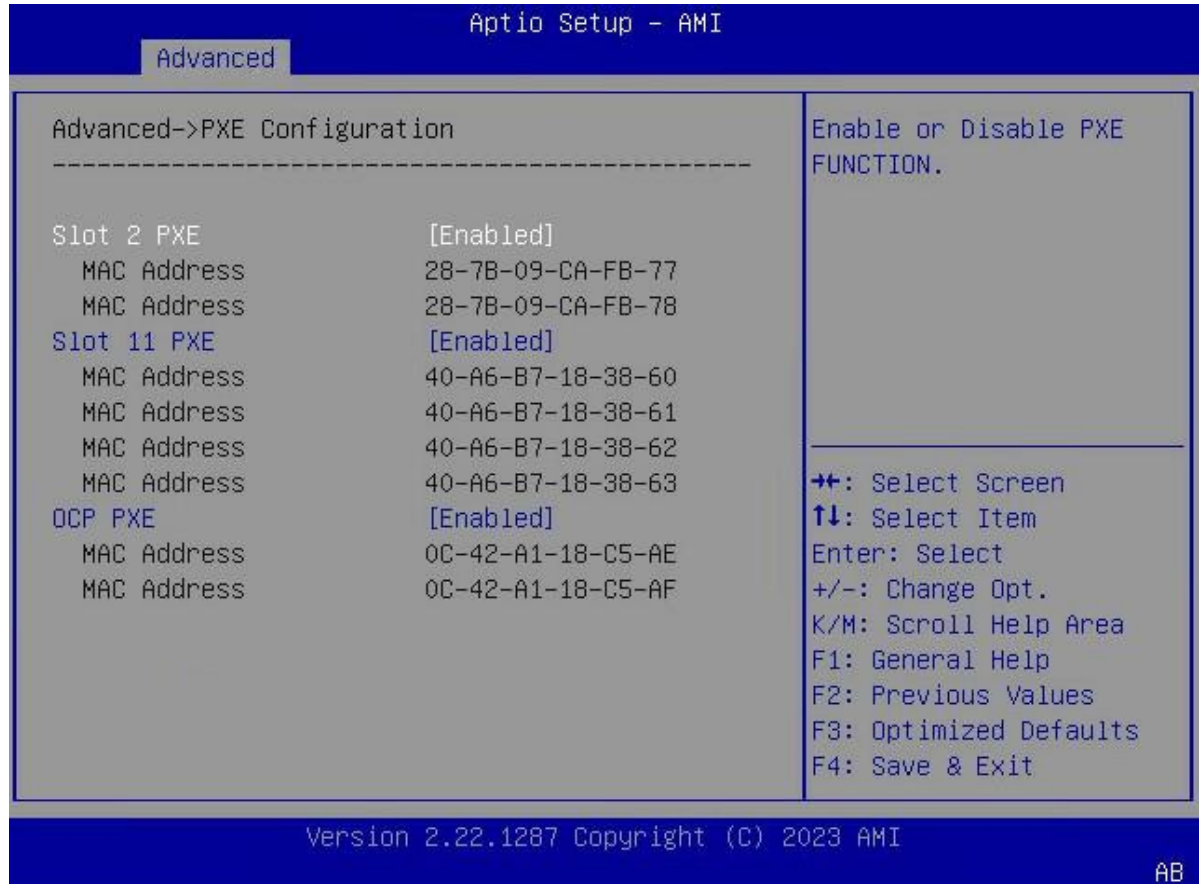
Table 3-22 Parameter Descriptions for the Emulation Configuration Screen

Parameter	Description	Default
MSR Trace for PM	Enables or disables the MSR trace feature for PM in uBIOS. ● Enabled: enables the MSR trace feature for PM in uBIOS. When this parameter is set to Enabled, the uBIOS is allowed to record MSR changes related to power management. ● Disabled: disables the MSR trace feature for PM in uBIOS. When this parameter is set to Disabled, the uBIOS cannot record MSR changes related to power management. ● Auto: disables the MSR trace feature for PM in uBIOS.	Auto

3.2.14 PXE Configuration

Figure 3-28 shows the **PXE Configuration** screen.

Figure 3-28 PXE Configuration Screen



Note

The **PXE Configuration** screen is displayed based on the connected device.

For a description of the parameters on the **PXE Configuration** screen, refer to [Table 3-23](#).

Table 3-23 Parameter Descriptions for the PXE Configuration Screen

Parameter	Description	Default
Slot 2 PXE	Enables or disables the PXE feature of the standard NIC in slot 2. - Enabled: enables the PXE feature on all NICs. - Disabled: disables the PXE feature on all NICs.	Enabled
Slot 11 PXE	Enables or disables the PXE feature of the standard NIC in slot 11. - Enabled: enables the PXE feature on all NICs. - Disabled: disables the PXE feature on all NICs.	Enabled

Parameter	Description	Default
OCB PXE	Enables or disables the PXE feature of the OCB NIC. - Enabled: enables the PXE feature on all NICs. - Disabled: disables the PXE feature on all NICs.	Enabled

3.2.15 Tls Auth Configuration

Figure 3-29 shows the **Tls Auth Configuration** screen.

Figure 3-29 Tls Auth Configuration Screen



For a description of the parameters on the **Tls Auth Configuration** screen, refer to [Table 3-24](#).

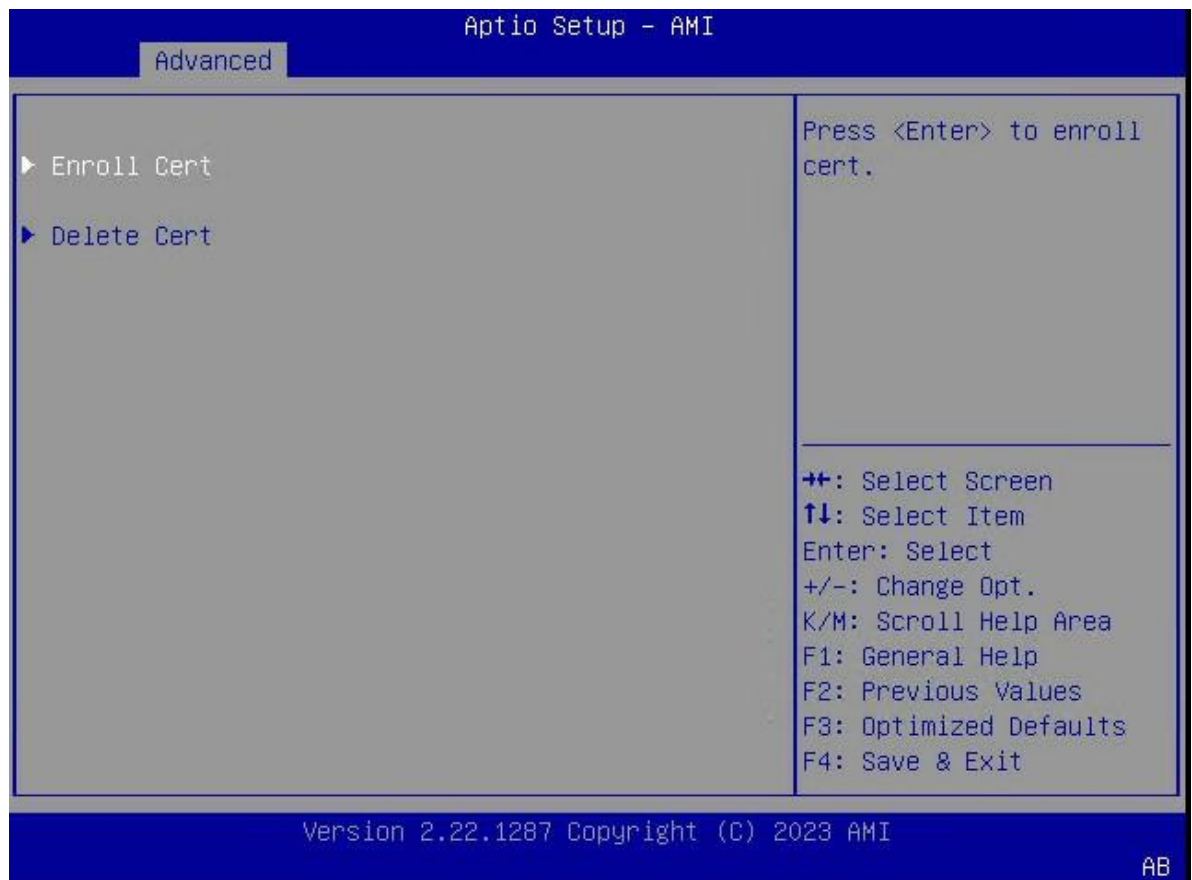
Table 3-24 Parameter Descriptions for the Tls Auth Configuration Screen

Parameter	Description
Server CA Configuration	Sets server CA parameters. For details, refer to 3.2.15.1 Server CA Configuration .
Client Cert Configuration	Client certificate configuration. Cannot be set.

3.2.15.1 Server CA Configuration

Figure 3-30 shows the **Server CA Configuration** screen.

Figure 3-30 Server CA Configuration Screen

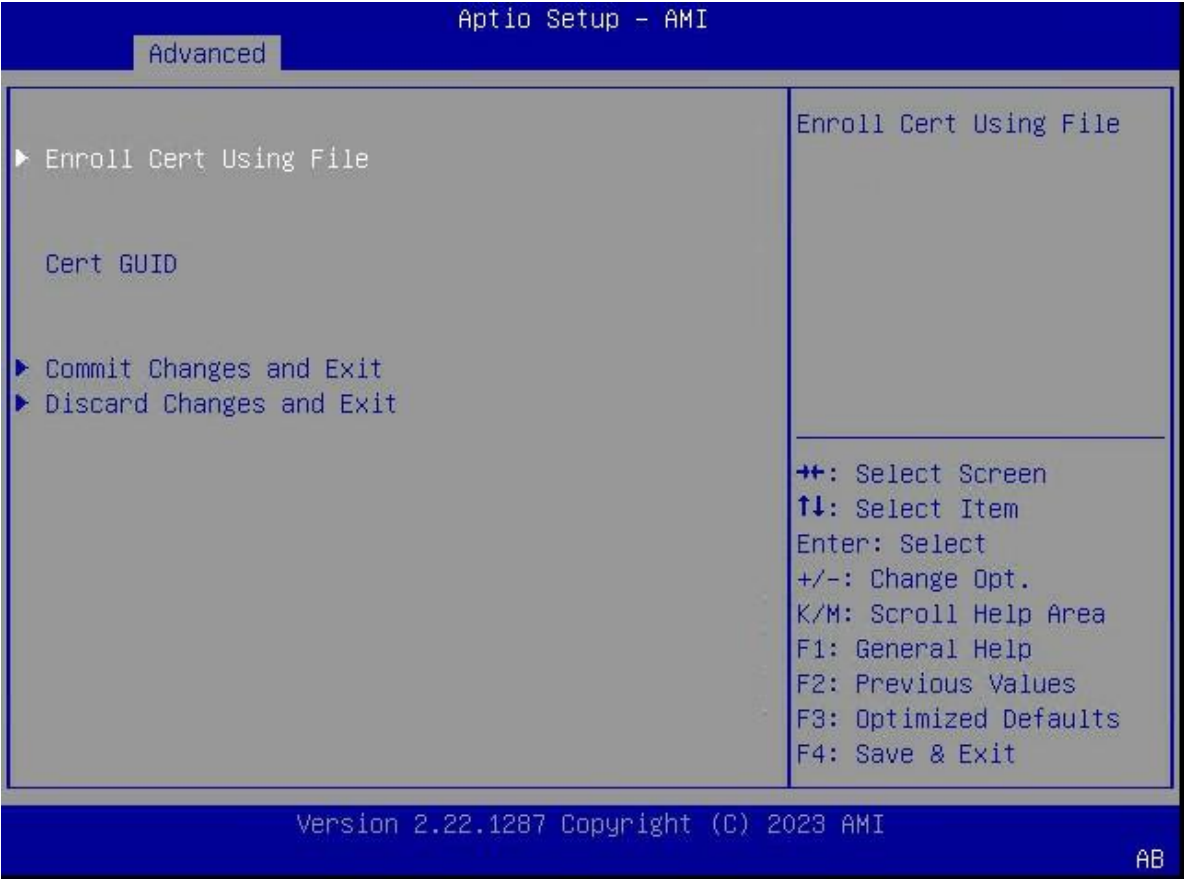


For a description of the parameters on the **Server CA Configuration** screen, refer to [Table 3-25](#).

Table 3-25 Parameter Descriptions for the Server CA Configuration Screen

Parameter	Description
Enroll Cert	Enrolls for certificates. Press the Enter key. The Enroll Cert screen is displayed, see Figure 3-31 .
Delete Cert	Deletes certificates. Press the Enter key. The Delete Cert screen is displayed, see Figure 3-32 .

Figure 3-31 Enroll Cert Screen



For a description of the parameters on the **Enroll Cert** screen, refer to [Table 3-26](#).

Table 3-26 Parameter Descriptions for the Enroll Cert Screen

Parameter	Description
Enroll Cert Using File	Enrolls for a certificate by using a file. Press the Enter key and then select a file.
Cert GUID	Enter alphanumeric characters as the GUID of the certificate in the following format: <i>11111111- 2222-3333-4444-1234567890ab</i>
Commit Changes and Exit	Submits the changes and exits.
Discard Changes and Exit	Discards the changes and exits.

Figure 3-32 Delete Cert Screen



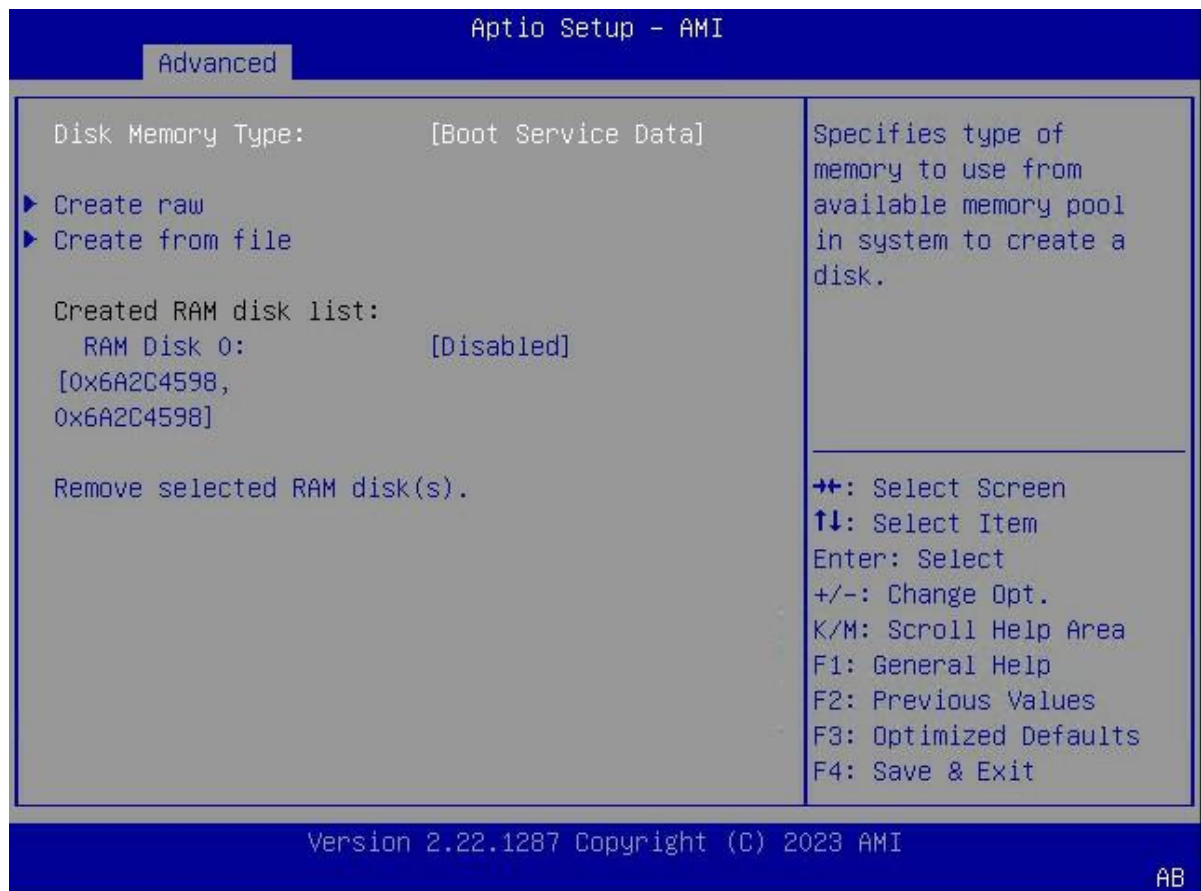
For a description of the parameters on the **Delete Cert** screen, refer to [Table 3-27](#).

Table 3-27 Parameter Descriptions for the Delete Cert Screen

Parameter	Description	Default
GUID of the certificate.	Enables or disables certificate deletion. Options: • Enabled: enables certificate deletion. • Disabled: disables certificate deletion.	Disabled

3.2.16 RAM Disk Configuration

[Figure 3-33](#) shows the **RAM Disk Configuration** screen.

Figure 3-33 RAM Disk Configuration Screen

For a description of the parameters on the **RAM Disk Configuration** screen, refer to [Table 3-28](#).

Table 3-28 Parameter Descriptions for the RAM Disk Configuration Screen

Parameter	Description	Default
Disk Memory Type	In the system available memory pool, specify the type of memory required to create the disk. Options: ● Boot Service Data ● Reserved	Boot Service Data
Create raw	Creates a raw RAM disk. For details, refer to 3.2.16.1 Create raw .	-
Create from file	Creates a RAM disk from a given file. Press the Enter key and then select a file.	-
RAM Disk 0	Sets whether to delete the created RAM disk. Options: ● Enabled: deletes the selected RAM disk. ● Disabled: does not delete the selected RAM disk.	Disabled

Parameter	Description	Default
Remove selected RAM disk(s)	Deletes the enabled disks from the list of created RAM disks.	-

3.2.16.1 Create raw

Figure 3-34 shows the **Create raw** screen.

Figure 3-34 Create Raw Screen



For a description of the parameters on the **Create raw** screen, refer to Table 3-29.

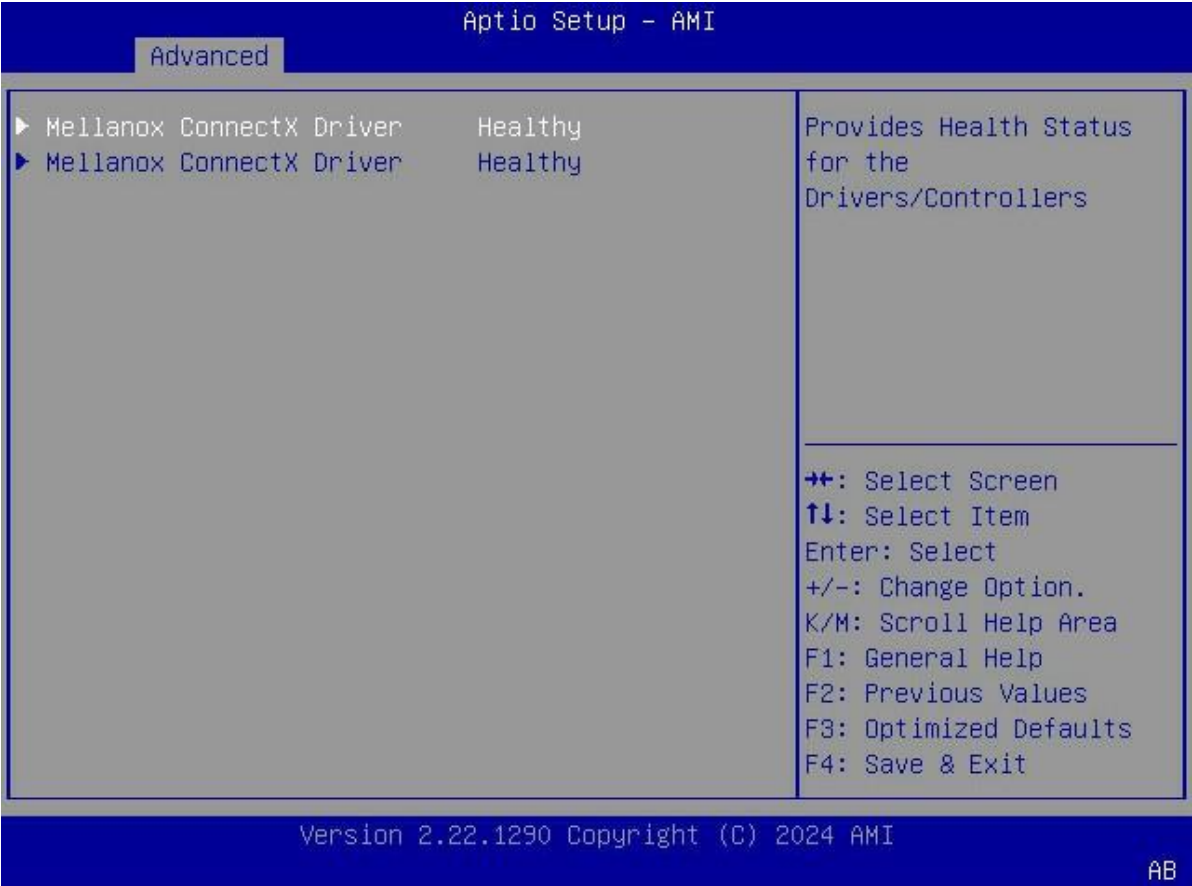
Table 3-29 Parameter Descriptions for the Create Raw Screen

Parameter	Description	Default
Size (Hex)	Enter the disk size.	1
Create & Exit	Creates the disk and exits.	-
Discard & Exit	Discards disk creation and exits.	-

3.2.17 Driver Health

The **Driver Health** screen contains the health status of drivers and controllers. Figure 3-35 shows the **Driver Health** screen.

Figure 3-35 Driver Health Screen



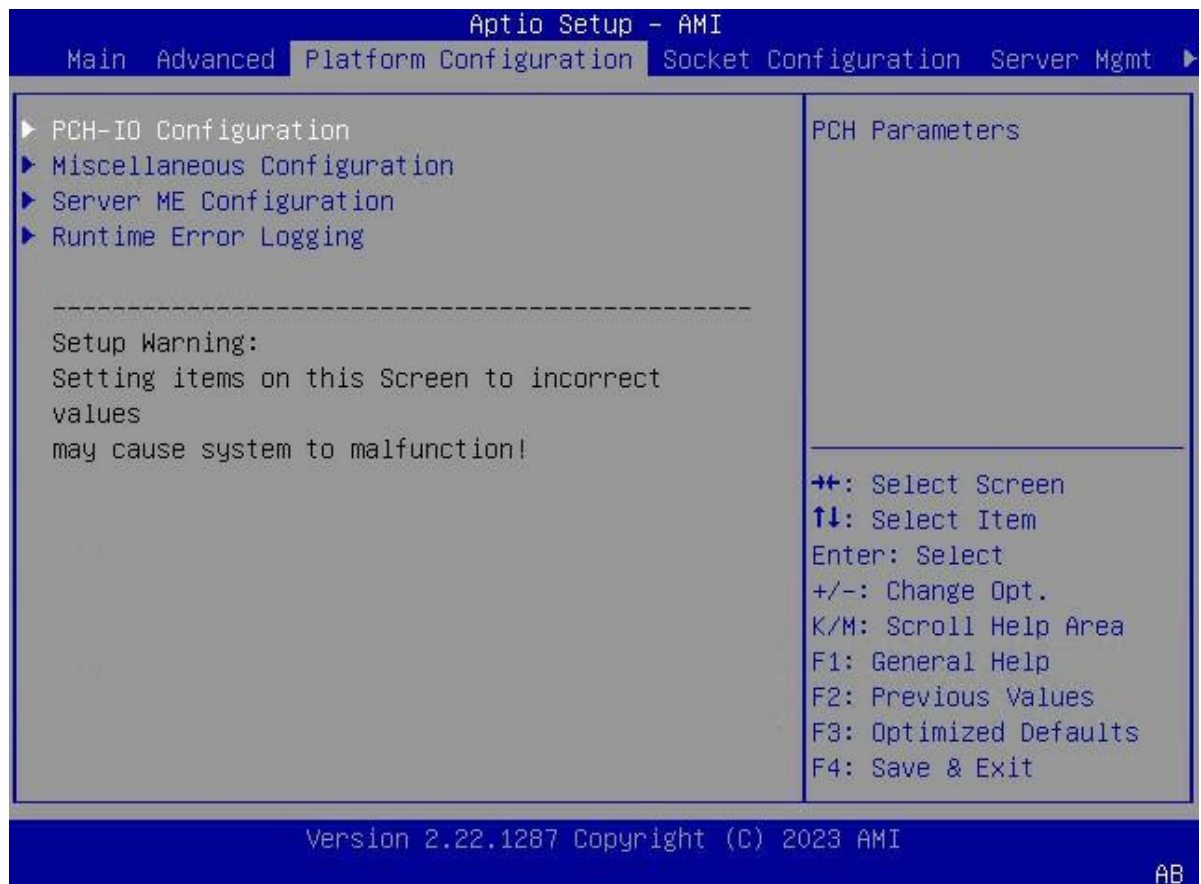
 Note

Parameters on the **Driver Health** screen vary with server configurations.

3.3 Platform Configuration

Figure 3-36 shows the **Platform Configuration** screen.

Figure 3-36 Platform Configuration Screen



For a description of the parameters on the **Platform Configuration** screen, refer to [Table 3-30](#).

Table 3-30 Parameter Descriptions for the Platform Configuration Screen

Parameter	Description
PCH-IO Configuration	Sets PCH-IO parameters. For details, refer to 3.3.1 PCH-IO Configuration .
Miscellaneous Configuration	Sets miscellaneous parameters. For details, refer to 3.3.2 Miscellaneous Configuration .
Server ME Configuration	Sets server ME parameters. For details, refer to 3.3.3 Server ME Configuration .
Runtime Error Logging	Checks or modifies runtime error logging parameters. For details, refer to 3.3.4 Runtime Error Logging .

3.3.1 PCH-IO Configuration

[Figure 3-37](#) through [Figure 3-38](#) show the **PCH-IO Configuration** screen.

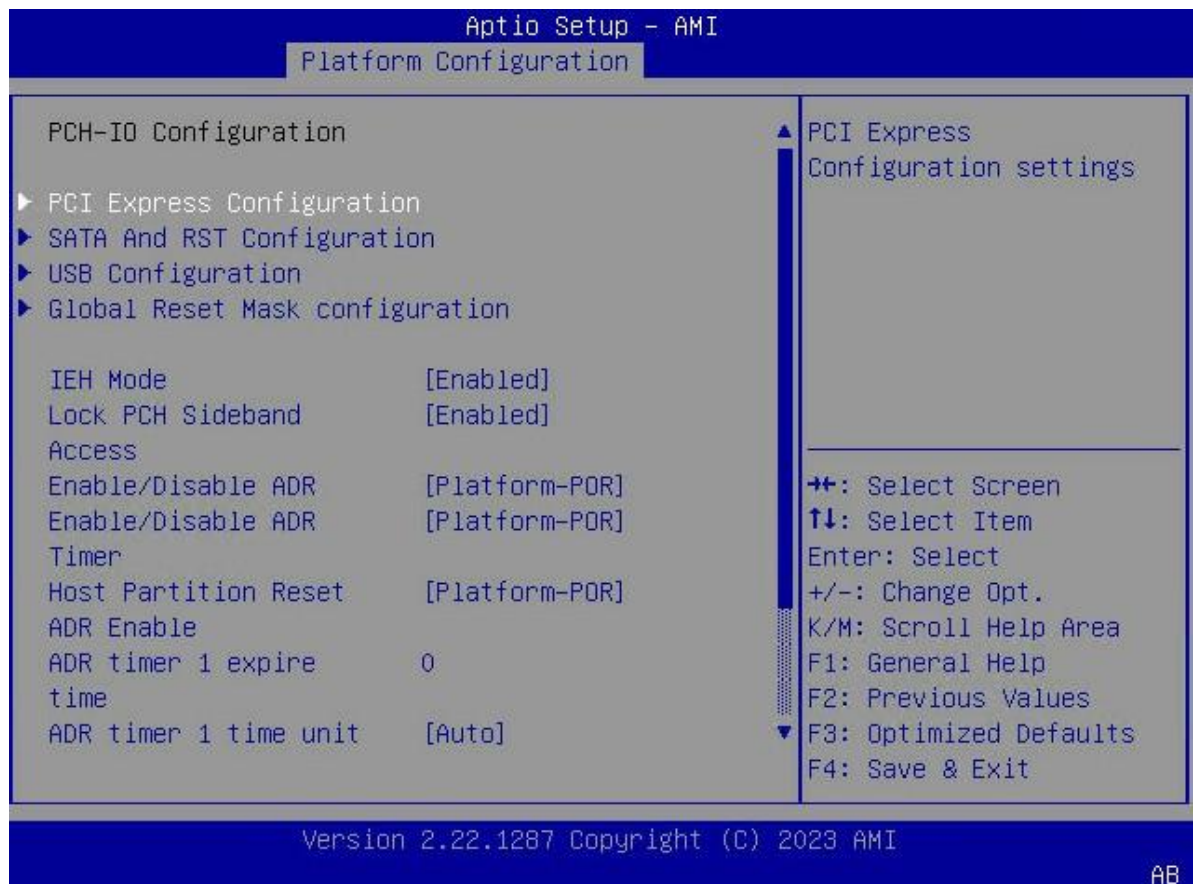
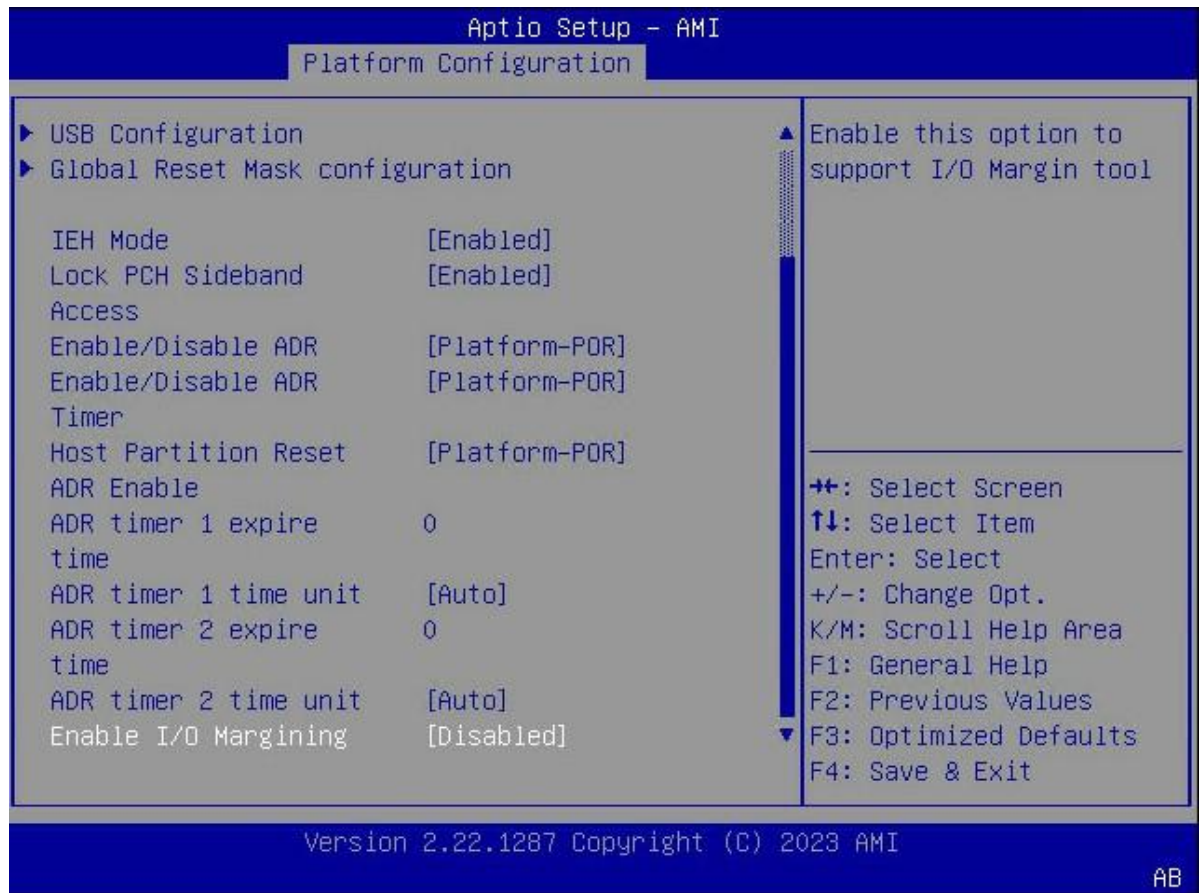
Figure 3-37 PCH-IO Configuration Screen—1

Figure 3-38 PCH-IO Configuration Screen—2



For a description of the parameters on the **PCH-IO Configuration** screen, refer to [Table 3-31](#).

Table 3-31 Parameter Descriptions for the PCH-IO Configuration Screen

Parameter	Description	Default
PCI Express Configuration	Sets PCIe parameters. For details, refer to 3.3.1.1 PCI Express Configuration .	-
SATA And RST Configuration	Sets SATA and RST parameters. For details, refer to 3.3.1.2 SATA And RST Configuration .	-
USB Configuration	Sets USB parameters. For details, refer to 3.3.1.3 USB Configuration .	-
Global Reset Mask configuration	Sets global reset mask parameters. For details, refer to 3.3.1.4 Global Reset Mask configuration .	-
IEH Mode	Enables or bypasses IEH mode. Options: Enabled: enables IEH mode.	Enabled

Parameter	Description	Default
	When this parameter is set to Enabled, errors from various sources are centralized to the same location and then sent to the CPU. ● Bypass Mode: bypasses IEH mode.	
Lock PCH Sideband Access	Locks or unlocks PCH sideband access, including sideband interfaces and sideband PortID masks for some endpoints such as PSFx. If POSTBOOT SAI is set, this parameter is invalid. Options: ● Enabled: locks PCH sideband access. ● Disabled: unlocks PCH sideband access.	Enabled
Enable/Disable ADR	Enables or disables the ADR feature. This feature is not available if eADR is enabled. Options: ● Platform-POR: The ADR feature is disabled. ● Disabled: disables the ADR feature. When this parameter is set to Disabled, some of the parameters below are hidden. ● Enabled: enables the ADR feature.	Platform-POR
Enable/Disable ADR Timer	Enables or disables the ADR timer. Options: ● Platform-POR: The ADR feature is disabled. ● Disabled: disables the ADR timer. When this parameter is set to Disabled, some of the parameters below are hidden. ● Enabled: enables the ADR timer.	Platform-POR
Host Partition Reset ADR Enabled	Enables or disables the ADR feature during host partition reset. Options: ● Platform-POR: disables the ADR feature. ● Disabled: disables the ADR feature. ● Enabled: enables the ADR feature.	Platform-POR
ADR timer 1 expire time	Enter the desired expiration time for the ADR1 timer 1. Value 0 indicates the automatic mode. Valid value range: 1–256. The time unit is specified in ADR timer 1 expire time unit.	0
ADR timer 1 time unit	Select the unit for ADR timer 1. Options: ● 1 us	Auto

Parameter	Description	Default
	● 10 us ● 100 us ● 1 ms ● 10 ms ● 100 ms ● 1s ● 10s ● Automatic	
ADR timer 2 expire time	Enter the desired expiration time for the ADR timer 2. Value 0 indicates the automatic mode. Valid value range: 1–256. The time unit is specified in ADR timer 2 expire time unit.	0
ADR timer 2 time unit	Select the unit for ADR timer 2. Options: ● 1 us ● 10 us ● 100 us ● 1 ms ● 10 ms ● 100 ms ● 1s ● 10s ● Auto	Auto
Enabled I/O Margining	Enables the I/O Margining feature to support the I/O Margining tool. Options: ● Enabled: supports the I/O Margining tool. ● Disabled: does not support the I/O Margining tool.	Disabled

3.3.1.1 PCI Express Configuration

Figure 3-39 shows the **PCI Express Configuration** screen.

Figure 3-39 PCI Express Configuration Screen



For a description of the parameters on the **PCI Express Configuration** screen, refer to [Table 3-32](#).

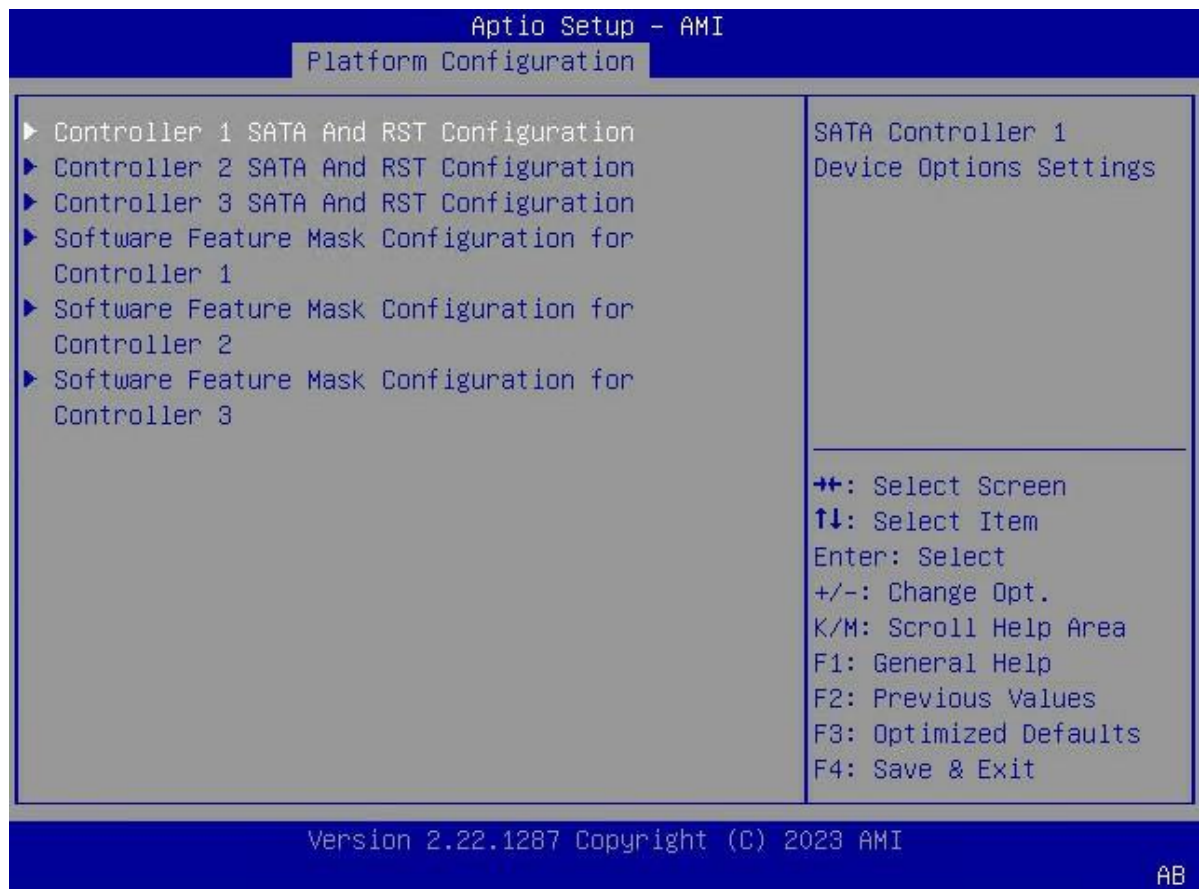
Table 3-32 Parameter Descriptions for the PCI Express Configuration Screen

Parameter	Description	Default
PCH PCI-E ASPM Support (Global)	Disables ASPM support on all PCIe ports. Options: ● Disabled: disables ASPM support on all PCIe ports. ● L1 Only: supports ASPM only by L1.	Disabled

3.3.1.2 SATA And RST Configuration

[Figure 3-40](#) shows the **SATA And RST Configuration** screen.

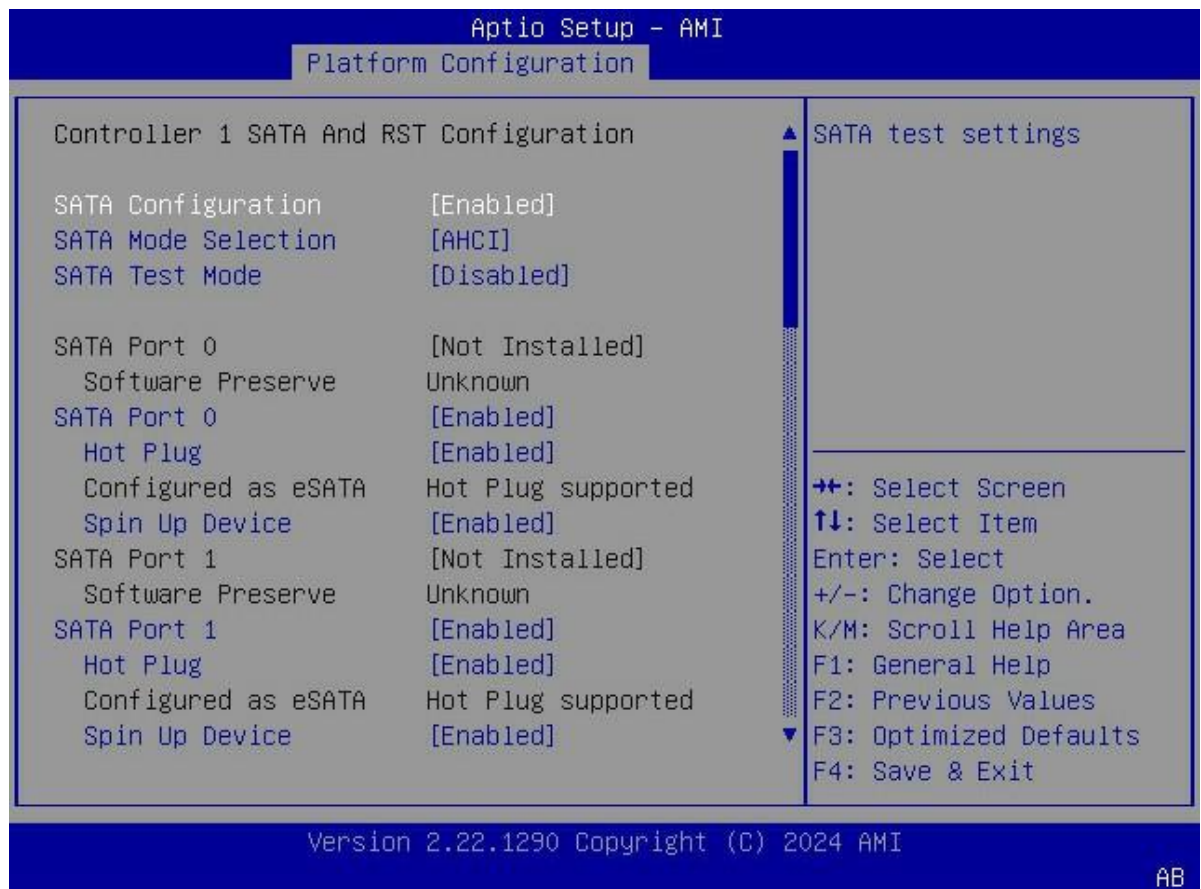
Figure 3-40 SATA And RST Configuration Screen



Note

The parameters on the **SATA And RST Configuration** screen vary with the server models. For different controllers, the parameters displayed on the **Controller SATA And RST Configuration** screen are different, but their principles are the same. This procedure uses the **Controller 1 SATA And RST Configuration** screen as an example.

Figure 3-41 shows the **Controller 1 SATA And RST Configuration** screen.

Figure 3-41 Controller 1 SATA And RST Configuration Screen

For a description of the parameters on the **Controller 1 SATA And RST Configuration** screen, refer to [Table 3-33](#).

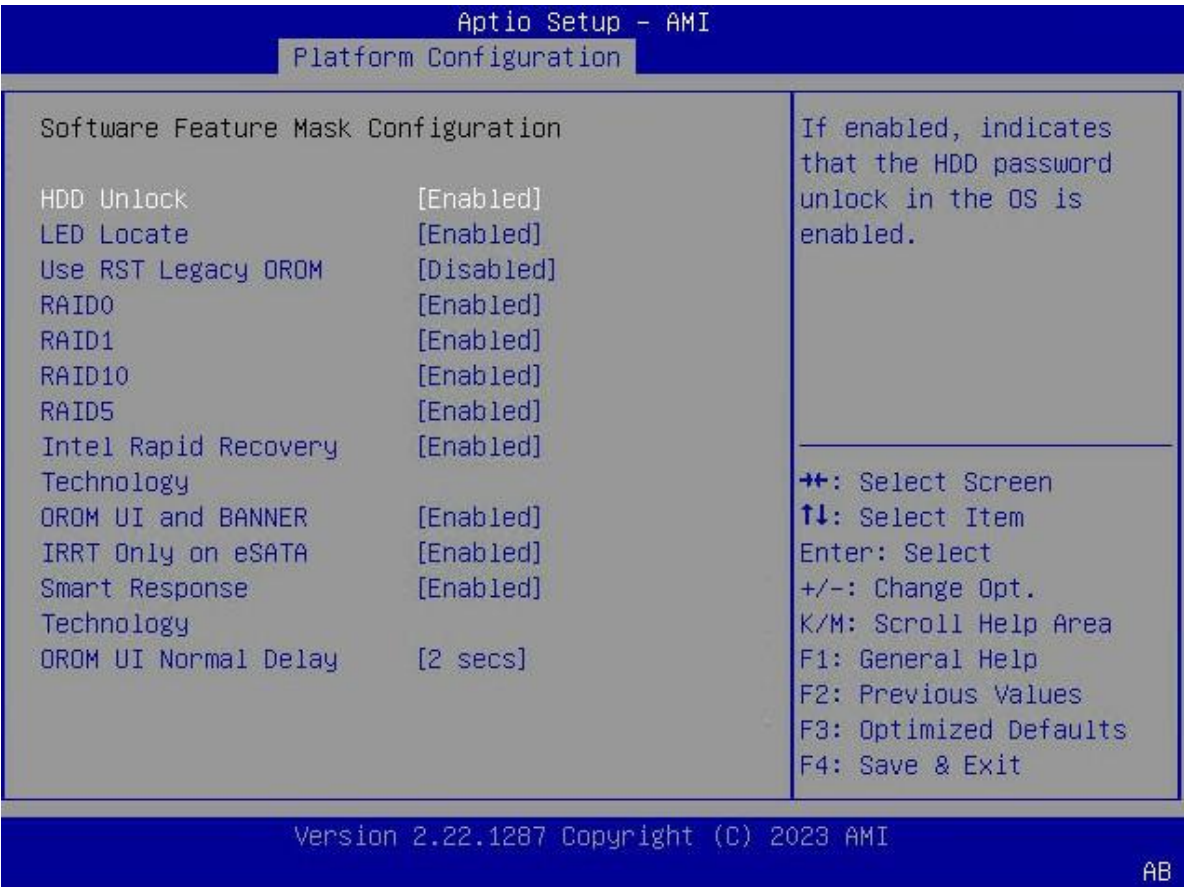
Table 3-33 Controller 1 SATA And RST Configuration Parameter Descriptions

Parameter	Description	Default
SATA Configuration	Enables or disables the SATA configuration feature. Options: - Enabled: enables the SATA configuration feature. - Disabled: disables the SATA configuration feature. After the feature is disabled, the parameters below are hidden.	Enabled
SATA Mode Selection	Select a SATA mode. Options: - AHCI: AHCI mode. When AHCI mode is selected, the SATA Interrupt Selection and RAID Device ID parameters are hidden. - RAID: RAID mode.	AHCI

Parameter	Description	Default
SATA Interrupt Selection	Select the interrupt that the OS will use. This parameter takes effect only when the SAT controller is in RAID mode. Options: ● Msix ● Msi ● Legacy	Msix
SATA Test Mode	Enables or disables SATA Test mode. Options: ● Enabled: enables SATA Test mode. ● Disabled: disables SATA Test mode.	Disabled
RAID Device ID	Select the ID of the RAID device. This parameter takes effect only when the SATA controller is in RAID mode. Options: ● Client ● Alternate ● Server	Server
SATA Port 0	Name of the device installed in SATA port 0. If the device is present, the device information is displayed. If the device is not present, the information shows that the device is not installed.	-
Software Preserve	Software preservation.	Unknown
SATA Port 0	Enables or disables the SATA port. Options: ● Enabled ● Disabled	Enabled
Hot Plug	Whether the port is hot swappable. Options: ● Enabled: The port is hot swappable. ● Disabled: The port is not hot swappable.	Enabled
Configured as eSATA	Configured as eSATA.	Hot Plug supported
Spin Up Device	If interleaving boot for any port is enabled, interleaving boot is performed only on the ports with the driver enabled. Options: ● Enabled ● Disabled	Disabled

Figure 3-42 shows the **Software Feature Mask Configuration** screen.

Figure 3-42 Software Feature Mask Configuration



For a description of the parameters on the **Software Feature Mask Configuration** screen, refer to [Table 3-34](#).

Table 3-34 Parameter Descriptions for the Software Feature Mask Configuration Screen

Parameter	Description	Default
HDD Unlock	Enables or disables the HDD password unlocking feature in the OS. Options: - Enabled: enables the HDD password unlocking feature in the OS. - Disabled: disables the HDD password unlocking feature in the OS.	Enabled
LED Locate	Enables or disables the LED location feature. Options: Enabled: enables the LED location feature. After this feature is enabled, the LED/SGPIO hardware is connected and the ping feature is enabled in the OS.	Enabled

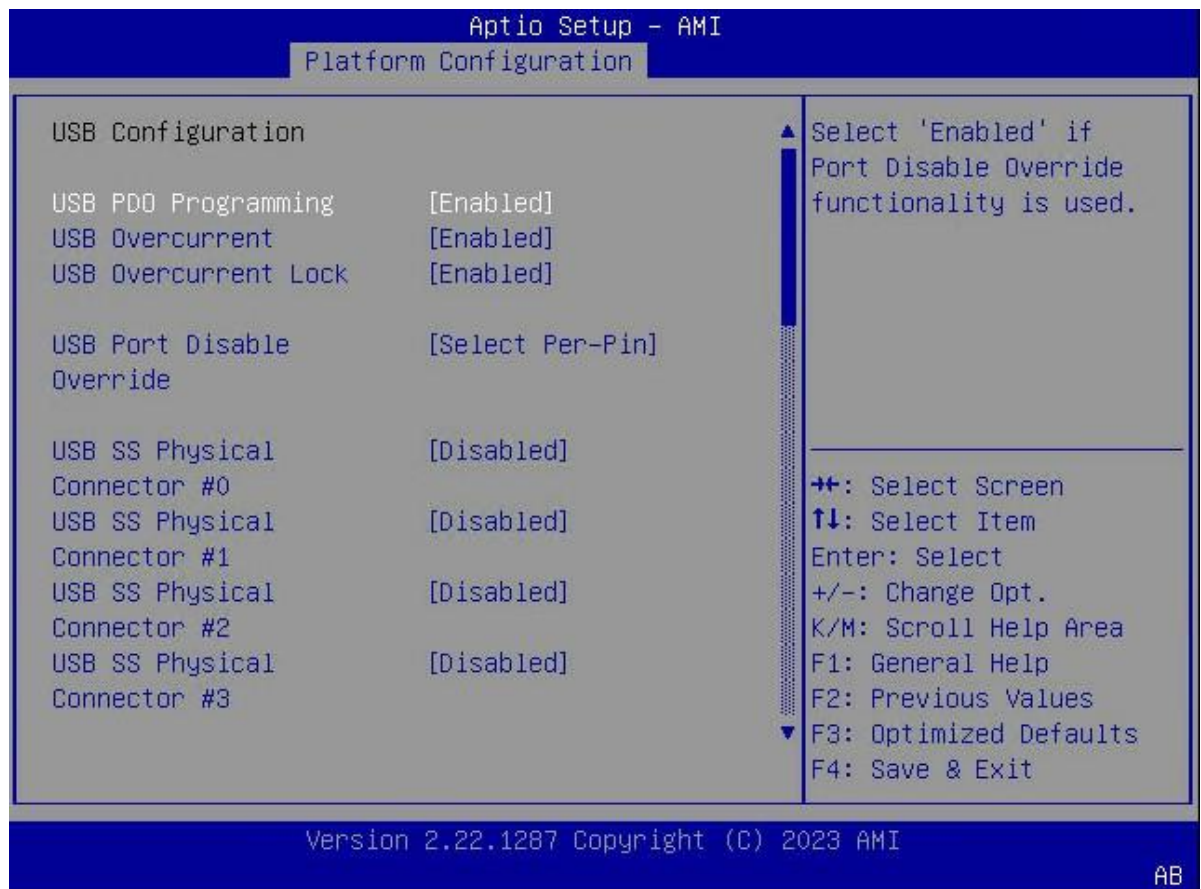
Parameter	Description	Default
	Disabled: disables the LED location feature.	
The following parameters are displayed only when the SATA controller is in RAID1 mode. Otherwise, they are hidden.		
Use RST Legacy OROM	Enables or disables RST Legacy OROM when CSM is enabled. Options: - Enabled: enables RST Legacy OROM. - Disabled: disables RST Legacy OROM.	Disabled
RAID0	Enables or disables the RAID0 feature. Options: - Enabled: enables the RAID0 feature. - Disabled: disables the RAID0 feature.	Enabled
RAID1	Enables or disables the RAID1 feature. Options: - Enabled: enables the RAID1 feature. - Disabled: disables the RAID1 feature.	Enabled
RAID10	Enables or disables the RAID10 feature. Options: - Enabled: enables the RAID10 feature. - Disabled: disables the RAID10 feature.	Enabled
RAID5	Enables or disables the RAID5 feature. Options: - Enabled: enables the RAID5 feature. - Disabled: disables the RAID5 feature.	Enabled
Intel Rapid Recovery Technology	Enables or disables Intel's rapid recovery technology. Options: - Enabled: enables Intel's rapid recovery technology. - Disabled: disables Intel's rapid recovery technology.	Enabled
OROM UI and BANNER	Enables or disables the OROM UI and banner. Options: - Enabled: enables the OROM UI and banner. When this parameter is set to Enabled, the OROM UI is displayed. - Disabled: disables the OROM UI and banner. When this parameter is set to Disabled, no OROM banner or information is displayed if all disks and RAID volumes are normal.	Enabled

Parameter	Description	Default
IRRT Only on eSATA	Enables or disables the use of only the IRRT feature on the eSATA. Options: ● Enabled: enables the use of only the IRRT feature on the eSATA. When this parameter is set to Enabled, only IRRT volumes can span internal and eSATA drivers. ● Disabled: disables the use of only the IRRT feature on the eSATA. When this parameter is set to Disabled, any RAID volumes can span internal and eSATA drivers.	Enabled
Smart Response Technology	Enables or disables the smart response technology. Options: ● Enabled: enables the smart response technology. ● Disabled: disables the smart response technology.	Enabled
OROM UI Normal Delay	Select the delay of the OROM UI Splash screen in normal state. Options: ● 2 secs ● 4 secs ● 6 secs ● 8 secs	2 secs

3.3.1.3 USB Configuration

Figure 3-43 shows the **USB Configuration** screen.

Figure 3-43 USB Configuration Screen



For a description of the parameters on the **USB Configuration** screen, refer to [Table 3-35](#).

Table 3-35 Parameter Descriptions for the USB Configuration Screen

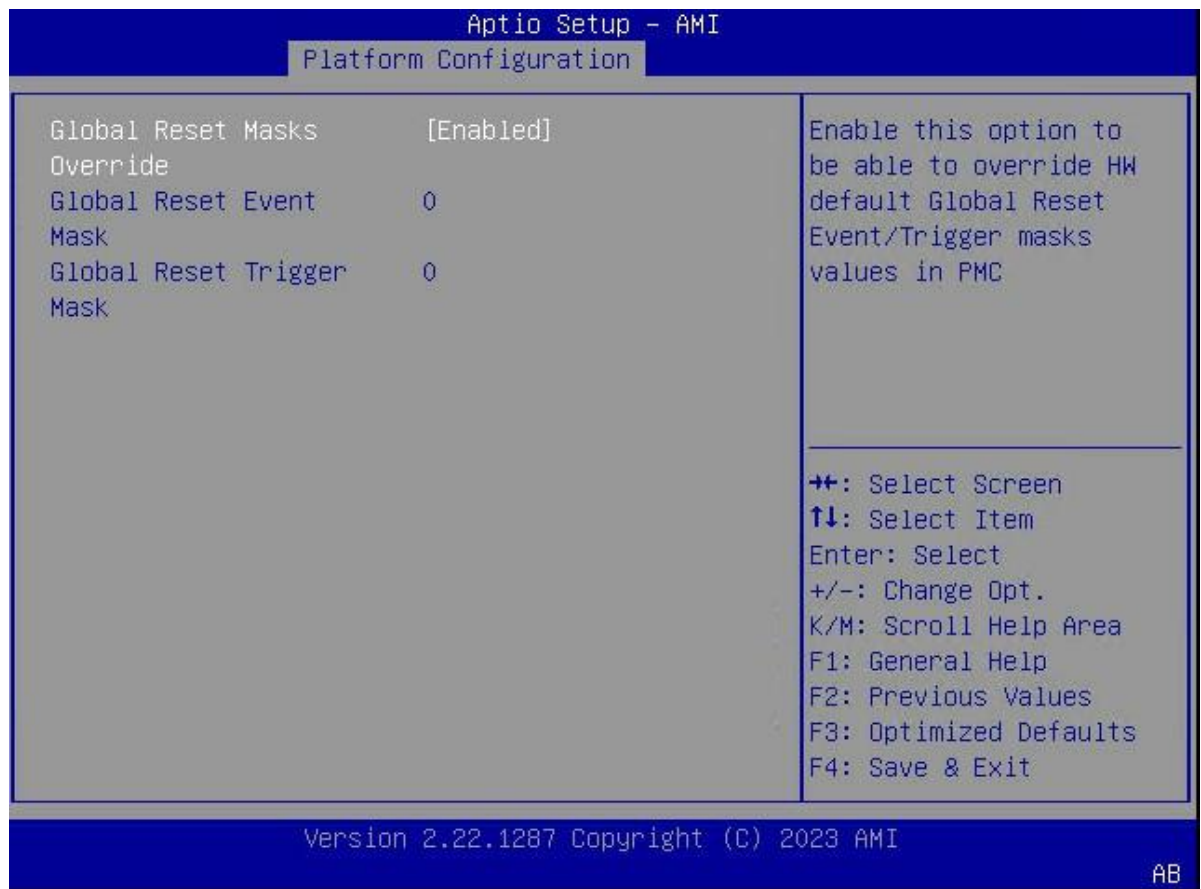
Parameter	Description	Default
USB PDO Programming	Enables or disables USB PDO programming. Options: ● Enabled: enables USB PDO programming. ● Disabled: disables USB PDO programming. If the USB Port Disable Override feature is used, select Enabled .	Enabled
USB Overcurrent	Enables or disables the USB overcurrent feature. Options: ● Enabled: enables USB overcurrent. ● Disabled: disables USB overcurrent. Select Disabled in pin-based debugging state. If the pin-based debugging state is enabled but USB Overcurrent is not disabled, USB DbC does not take effect.	Enabled
USB Overcurrent Lock	Enables or disables the USB overcurrent lock.	Enabled

Parameter	Description	Default
	Options: - Enabled: enables the USB overcurrent lock. - Disabled: disables the USB overcurrent lock. If USB Overcurrent is enabled, select Enabled to allow the XHCI controller to consume overcurrent mapping data.	
USB Port Disable Override	Enables or disables the overriding of USB port disabling settings. Options: - Disabled: disables each USB port. When this parameter is set to Disabled, the physical port parameters below are hidden. - Select Per-Pin: Select each pin to display the following physical port parameters. You can enable or disable each pin (port) separately.	Select Per-Pin
USB SS Physical Connector #0	Enables or disables the USB physical connector (physical port). Options: - Enabled: enables the USB physical port. - Disabled: disables the USB physical port. When this parameter is set to Disabled, any USB device inserted into the connector is not detected by the BIOS or the OS.	Disabled

3.3.1.4 Global Reset Mask configuration

Figure 3-44 shows the **Global Reset Mask Configuration** screen.

Figure 3-44 Global Reset Mask Configuration Screen



For a description of the parameters on the **Global Reset Mask Configuration** screen, refer to [Table 3-36](#).

Table 3-36 Parameter Descriptions for the Global Reset Mask Configuration Screen

Parameter	Description	Default
Global Reset Masks Override	Enables or disables the global reset mask overwriting feature. Options: - Enabled: enables the global reset mask overwriting feature. When this parameter is set to Enabled, the default global hardware reset event and trigger mask values in the PMC are overwritten. - Disabled: disables the global reset mask overwriting feature.	Enabled
Global Reset Event Mask	Enter the global reset event mask.	0
Global Reset Tigger Mask	Enter the global reset trigger mask.	0

3.3.2 Miscellaneous Configuration

Figure 3-45 shows the **Miscellaneous Configuration** screen.

Figure 3-45 Miscellaneous Configuration Screen



For a description of the parameters on the **Miscellaneous Configuration** screen, refer to [Table 3-37](#).

Table 3-37 Parameter Descriptions for the Miscellaneous Configuration Screen

Parameter	Description	Default
KCS Access Control Policy	Sets when to send IPMI commands through the KCS interface. Options: - Allow All: anytime. - Restricted: until the BIOS sends the DONE signal. - Deny All: never.	Allow All
Wake On Lan Support	Enables or disables the Wake On Lan Support feature. Options: Enabled: Enables the Wake On Lan Support feature.	Disabled

Parameter	Description	Default
	● Disabled: Disables the Wake On Lan Support feature.	
Serial Debug Message Level	Sets the level of the debugging messages output through the serial port. Options: ● Disabled: The serial port does not output system debugging messages. ● Minimum: Only critical debugging messages are output. ● Normal: Only critical and informational debugging messages are output. ● Minimum: All debugging messages are output. ● Auto: Minimum (default) or Medium (advanced debugging mode). ● Fixed PCD.	Disabled
Video Card Selected	Sets the VGA device type. Options: ● Auto ● Onboard Device ● PCIe Device	Onboard Device
External SSC - CK440	Sets the SSC feature, which affects only the external clock generator. Options: ● SSC Off ● SSC = -0.3% ● SSC = -0.5% ● Hardware	Hardware

3.3.3 Server ME Configuration

Figure 3-46 through Figure 3-48 show the **Server ME Configuration** screen.

Figure 3-46 Server ME Configuration Screen—1

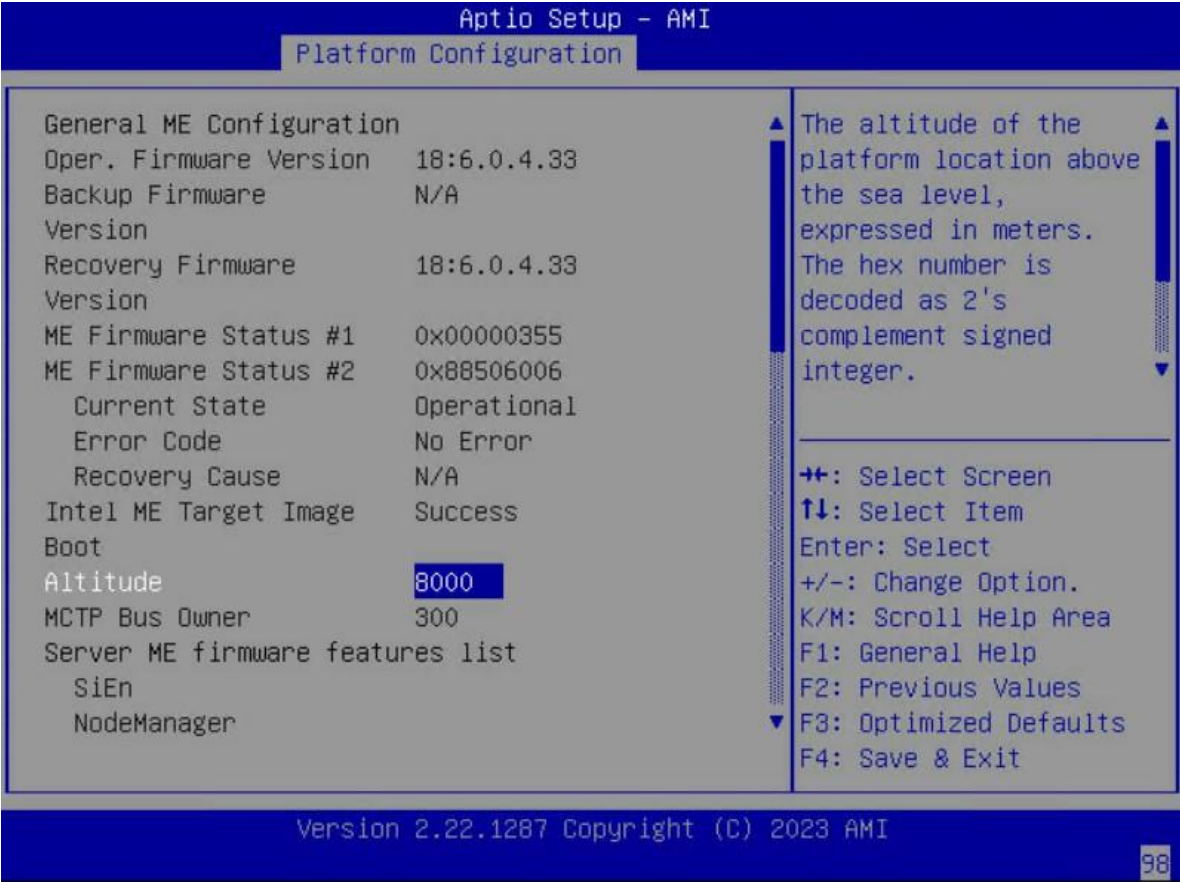


Figure 3-47 Server ME Configuration Screen—2

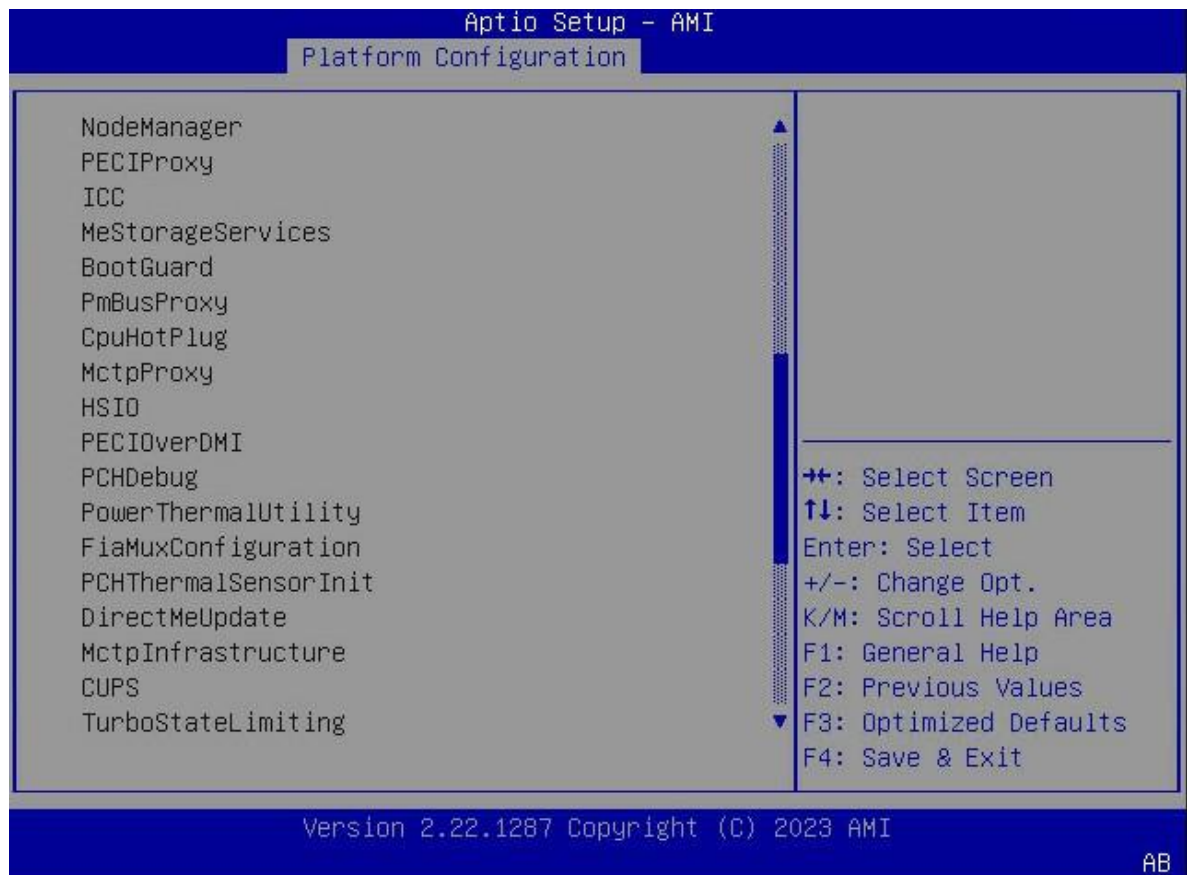
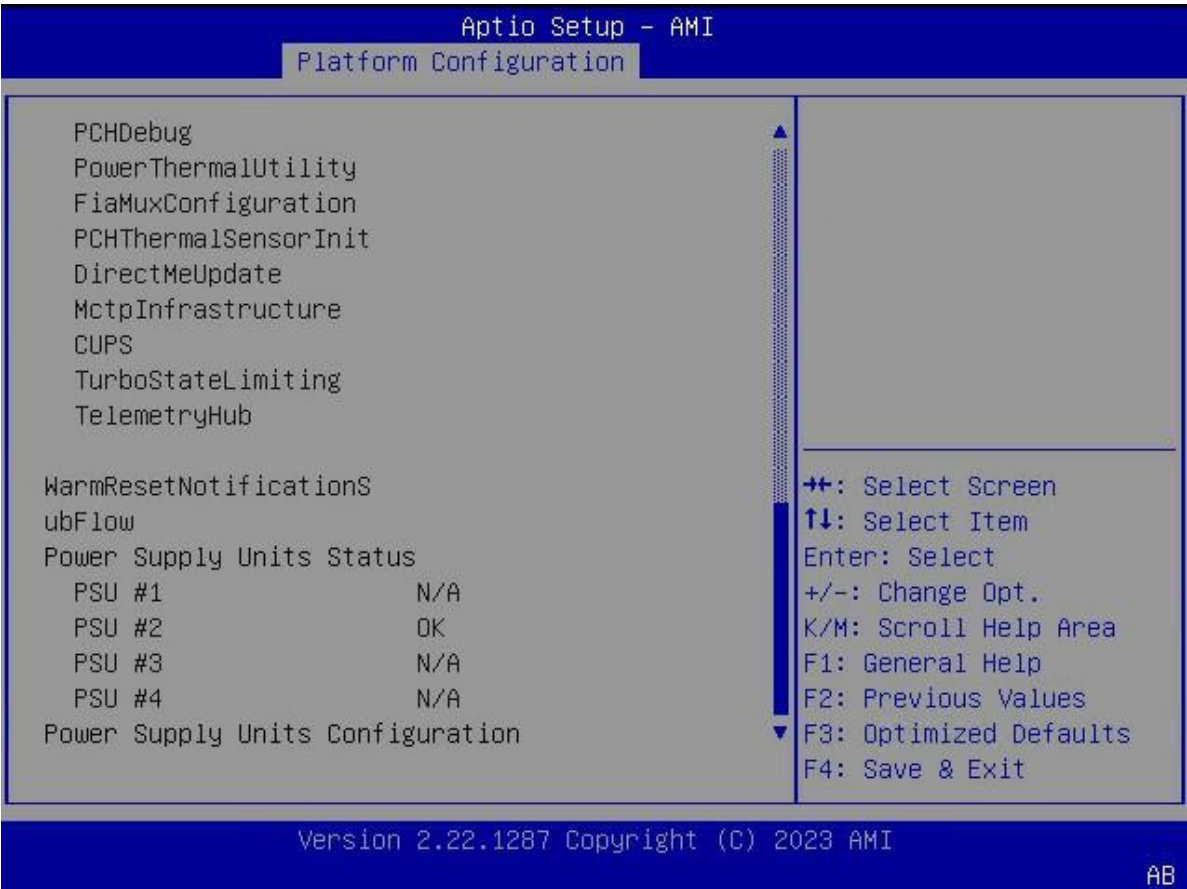


Figure 3-48 Server ME Configuration Screen—3



For a description of the parameters on the **Server ME Configuration** screen, refer to [Table 3-38](#).

Table 3-38 Parameter Descriptions for the Server ME Configuration Screen

Parameter	Description	Default
Oper.Firmware Version	Valid firmware version number.	-
Backup Firmware Version	Backup firmware version number.	-
Recovery Firmware Version	Firmware version number in recovery mode.	-
ME Firmware Status #1	ME firmware status #1.	-
ME Firmware Status #2	ME firmware status #2.	-
Current State	Current ME state.	-
Error Code	Error code information.	-
Recovery Cause	Recovery cause.	-
Intel ME Target Image Boot	Booted from the Intel ME target image.	-
Altitude	Enter the platform height (in meters) above the sea level.	8000

Parameter	Description	Default
	The hexadecimal number is decoded into the signed integer of the complementary code of two. If the value is 8000 , the altitude is unknown.	
MCTP Bus Owner	The position of the MCTP bus owner on the PCIe.	-
Server ME firmware features list	The server ME firmware features are listed below.	-
Power Supply Units Status	The state of each power supply is displayed below.	-
Power Supply Units Configuration	Adds a power supply device.	-

3.3.4 Runtime Error Logging

Figure 3-49 through Figure 3-50 show the **Runtime Error Logging** screen.

Figure 3-49 Runtime Error Logging Screen—1

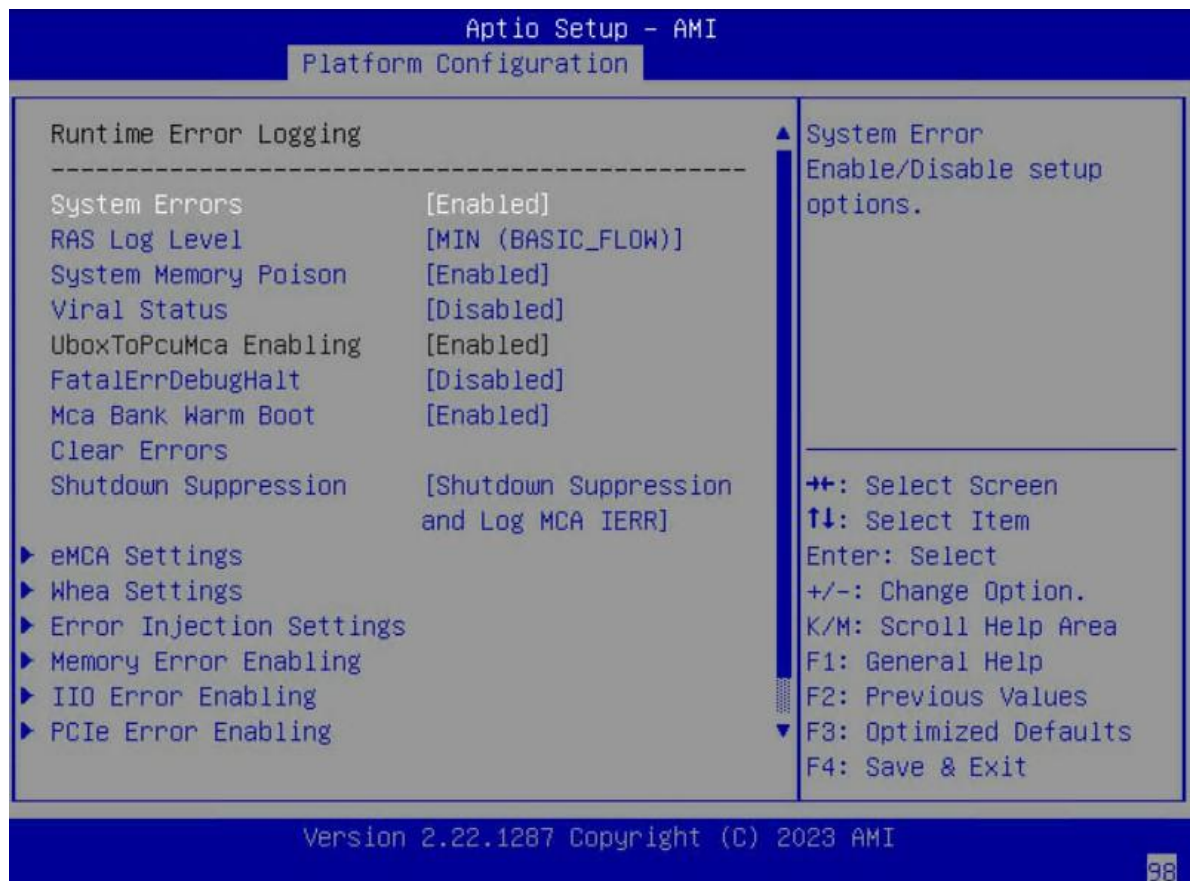
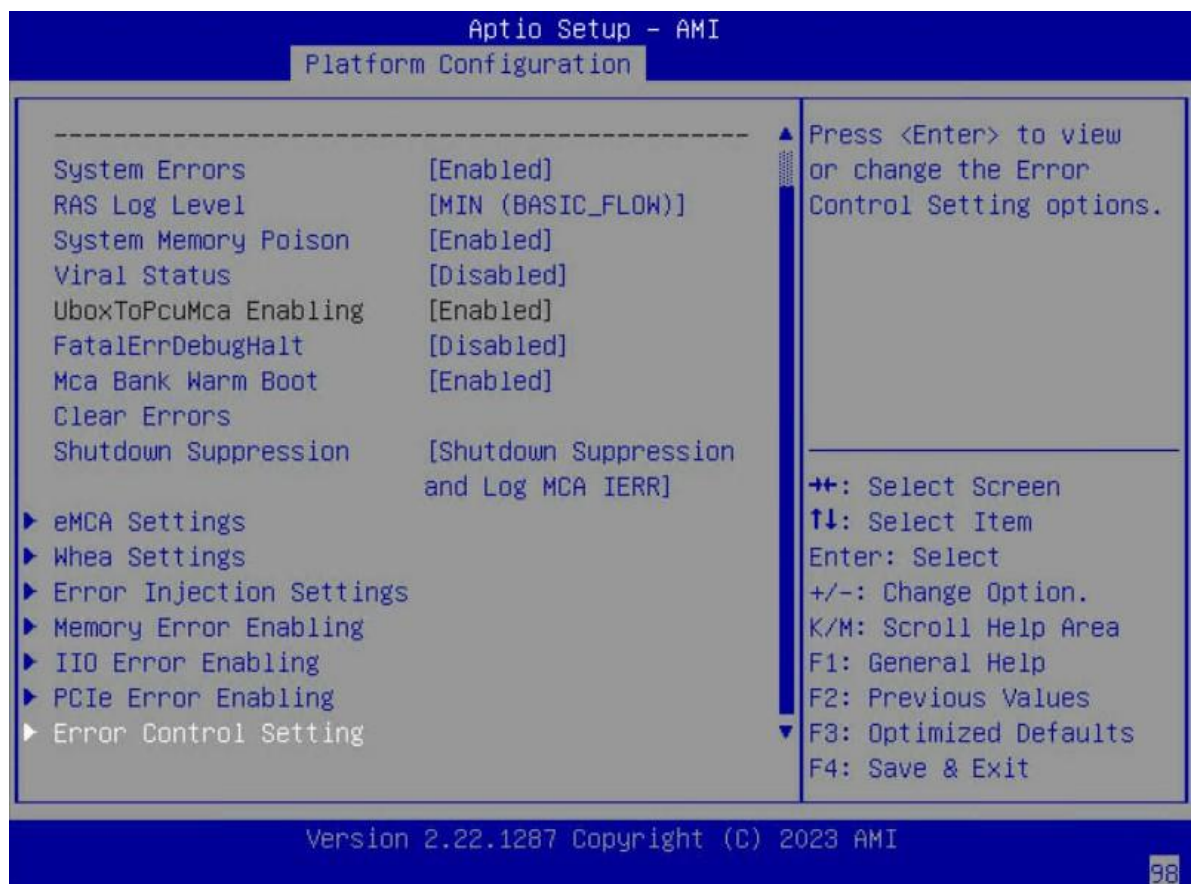


Figure 3-50 Runtime Error Logging Screen—2



For a description of the parameters on the **Runtime Error Logging** screen, refer to [Table 3-39](#).

Table 3-39 Parameter Descriptions for the Runtime Error Logging Screen

Parameter	Description	Default
System Errors	Enables or disables system error collection. Options: ● Enabled: enables system error collection. ● Disabled: disables system error collection. When this parameter is set to Disabled , some parameters below are hidden or grayed out.	Enabled
RAS Log Level	Select a RAS log level. Options: ● None: none. ● Min (BASIC_FLOW): minimum. ● Mid (BASIC_FLOW, FUNC_FLOW): medium ● Max (BASIC_FLOW, FUNC_FLOW, REG): maximum	MIN (BASIC_FLOW)
System Memory Poison	Enables or disables system memory poison mode. Options:	Enabled

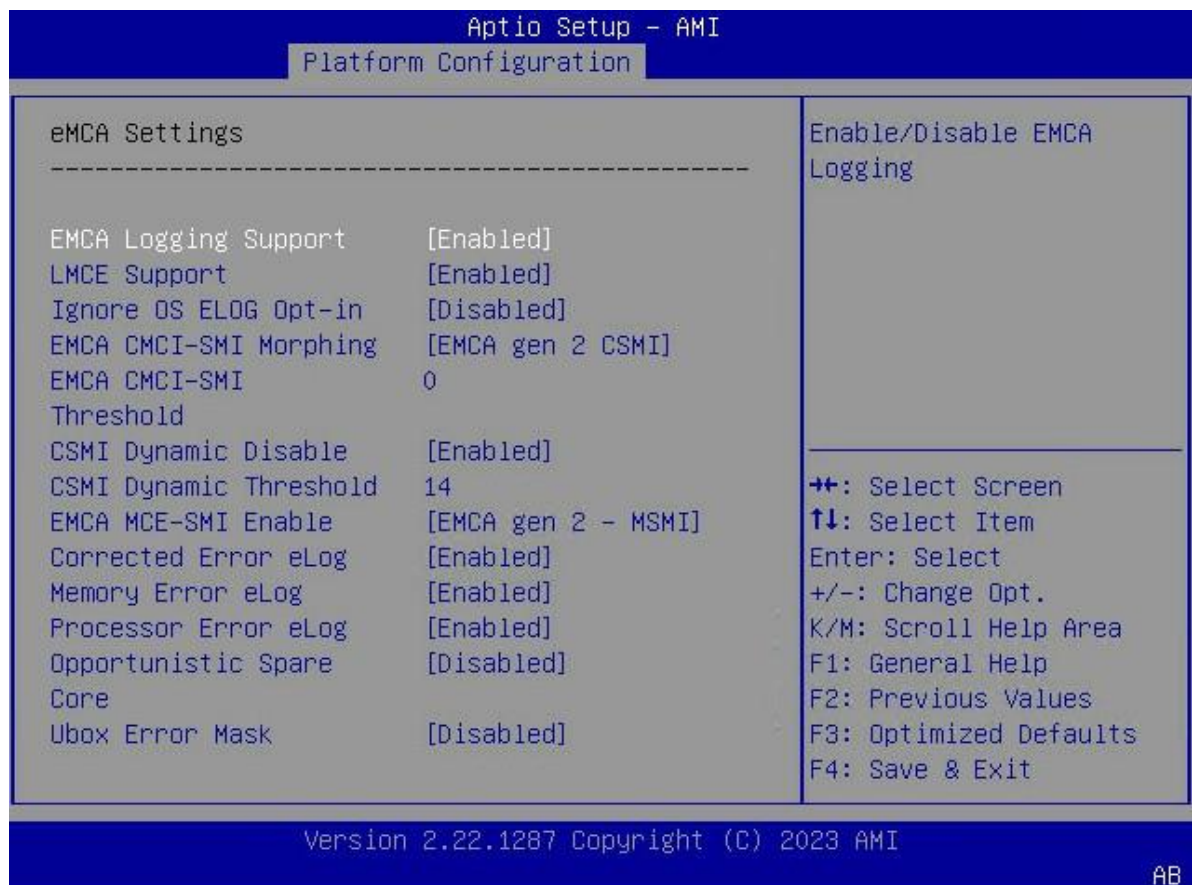
Parameter	Description	Default
	- Enabled: enables system memory poison mode. - Disabled: disables system memory poison mode.	
Viral Status	This parameter is displayed when System Memory Poison is set to Enabled. Enables or disables the Viral status. Options: - Enabled: enables the Viral status. - Disabled: disables the Viral status.	Disabled
Clear Viral Status	This parameter is displayed when Viral Status is set to Enabled. Enables or disables the clearing of Viral status. Options: - Enabled: enables the clearing of Viral status. - Disabled: disables the clearing of Viral status.	Disabled
UboxToPcuMca Enabling	Enables the UboxToPcuMca feature.	Enabled
FatalErrDebugHalt	Enables or disables the fatal error debug feature. Options: - Enabled: enables the fatal error debug feature. - Disabled: disables the fatal error debug feature.	Disabled
Mca Bank Warm Boot Clear Errors	Enables or disables error information clearing during MCA warm boot. Options: - Enabled: enables error information clearing during MCA warm boot. - Disabled: disables error information clearing during MCA warm boot.	Enabled
Shutdown Suppression	Sets the support for shutdown suppression and MCA IERR logging. Options: - Disabled: disables the support. - Shutdown Suppression and Log MCA IERR: shuts down suppression and MCA IERR error logging. - Shutdown Log MCA IERR: shuts down MCA IERR error logging.	Shutdown Suppression and Log MCA IERR
eMCA Settings	Sets eMCA parameters. For details, refer to 3.3.4.1 eMCA Settings.	-
Whea Settings	Sets Whea parameters. For details, refer to 3.3.4.2 Whea Settings.	-
Error Injection Settings	Sets error injection parameters.	-

Parameter	Description	Default
	For details, refer to 3.3.4.3 Error Injection Settings .	
Memory Error Enabling	Sets memory error enabling parameters. For details, refer to 3.3.4.4 Memory Error Enabling .	-
I/O Error Enabling	Sets I/O error enabling parameters. For details, refer to 3.3.4.5 I/O Error Enabling .	-
PCIe Error Enabling	Sets PCIe error enabling parameters. For details, refer to 3.3.4.6 PCIe Error Enabling .	-
Error Control Setting	Sets error control parameters. For details, refer to 3.3.4.7 Error Control Setting .	-

3.3.4.1 eMCA Settings

Figure 3-51 shows the **eMCA Settings** screen.

Figure 3-51 EMCA Settings Screen



For a description of the parameters on the **eMCA Settings** screen, refer to [Table 3-40](#).

Table 3-40 Parameter Descriptions for the eMCA Settings Screen

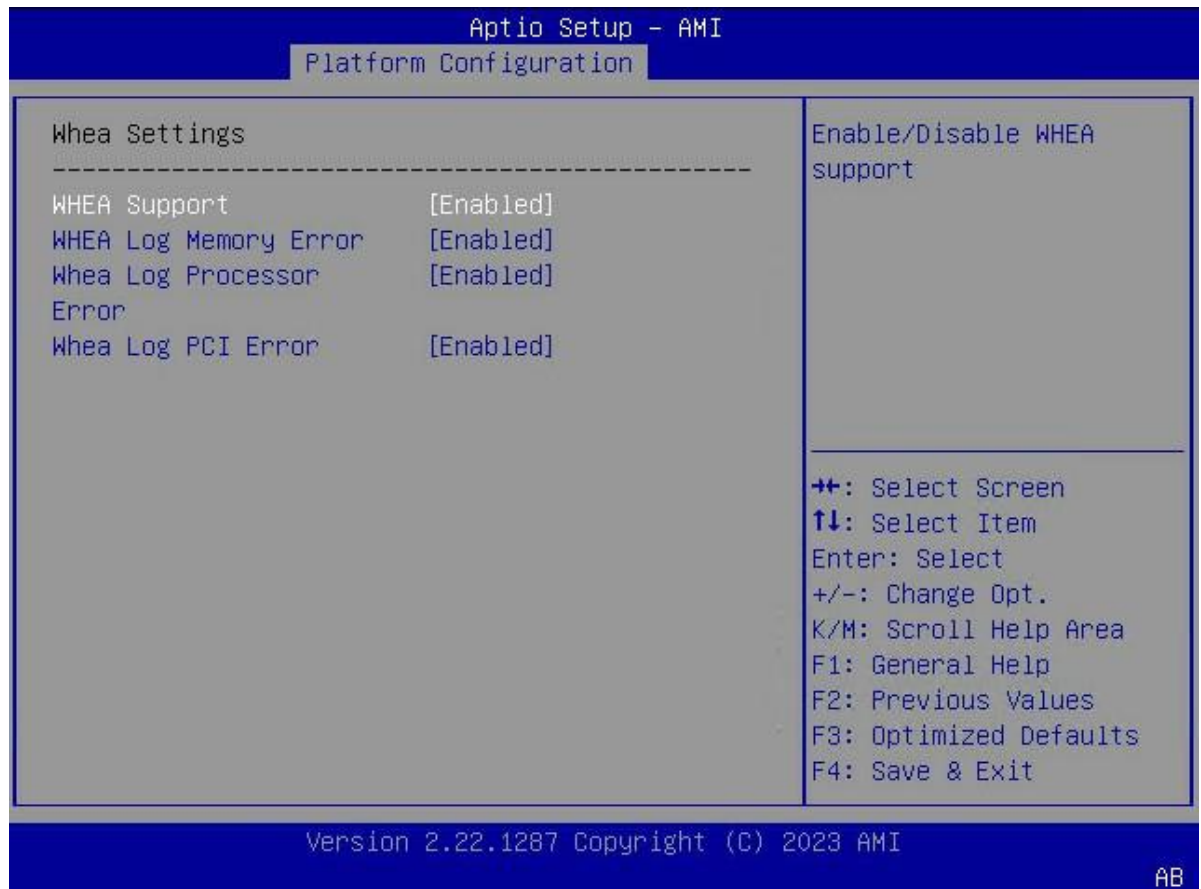
Parameter	Description	Default
EMCA Logging Support	Enables or disables eMCA Logging Support. When this parameter is set to Disabled , some of the parameters below are hidden.	Enabled
LMCE Support	Enables or disables LMCE Support. When this parameter is set to Disabled , some of the parameters below are hidden.	Enabled
Ignore OS ELOG Opt-in	Indicates whether to ignore OS ELOG Opt-in and log the behavior. Options: - Enabled: ignores OS ELOG Opt-in and logs the behavior. - Disabled: neither ignores OS ELOG Opt-in nor logs the behavior.	Disabled
EMCA CMCI-SMI Morphing	Sets the eMCA CMCI-SMI morphing feature. Options: - EMCA gen 2 CSMI - Disabled When this parameter is set to Disabled , some of the parameters below are hidden.	EMCA gen 2 CSMI
EMCA CMCI-SMI Threshold	Sets the threshold for correctable errors for CMCI-SMI.	0
CSMI Dynamic Disable	Indicates whether to dynamically disable CSMI. Options: - Enabled: disables CSMI when the error threshold is reached. - Disabled: always enables CSMI. When set to Disabled , the CSMI Dynamic Threshold parameter is hidden.	Disabled
CSMI Dynamic Threshold	Sets the threshold for dynamically disabling CSMI. When the error threshold is reached, CSMI is disabled.	14
EMCA MCE-SMI Enable	Enables or disables EMCA MCE-SMI. Options: - EMCA gen 2 - MSMI: enables EMCA MCE-SMI in EMCA gen 2 MSMI mode. - Disabled: disables EMCA MCE-SMI.	EMCA gen 2 - MSMI
Corrected Error eLog	Enables or disables corrected error eLogs. Options:	Enabled

Parameter	Description	Default	
	● Enabled: enables corrected error elogs. ● Disabled: disables corrected error elogs.		
Memory Error eLog	Enables or disables memory error elogs. Options: ● Enabled: enables memory error elogs. ● Disabled: disables memory error elogs.	Enabled	
Processor Error eLog	Enables or disables processor error elogs. Options: ● Enabled: enables processor error elogs. ● Disabled: disables processor error elogs.	Enabled	
Opportunistic Spare Core	Enables or disables the opportunistic spare core. Options: ● Enabled: enables the opportunistic spare core. ● Disabled: disables the opportunistic spare core.	Disabled	
Ubox Error Mask	Enables or disables the Ubox error mask. Options: ● Enabled: enables the Ubox error mask. ● Disabled: disables the Ubox error mask.	Disabled	

3.3.4.2 Whea Settings

Figure 3-52 shows the **Whea Settings** screen.

Figure 3-52 Whea Settings Screen



For a description of the parameters on the **WHEA Settings** screen, refer to [Table 3-41](#).

Table 3-41 Parameter Descriptions for the Whea Settings Screen

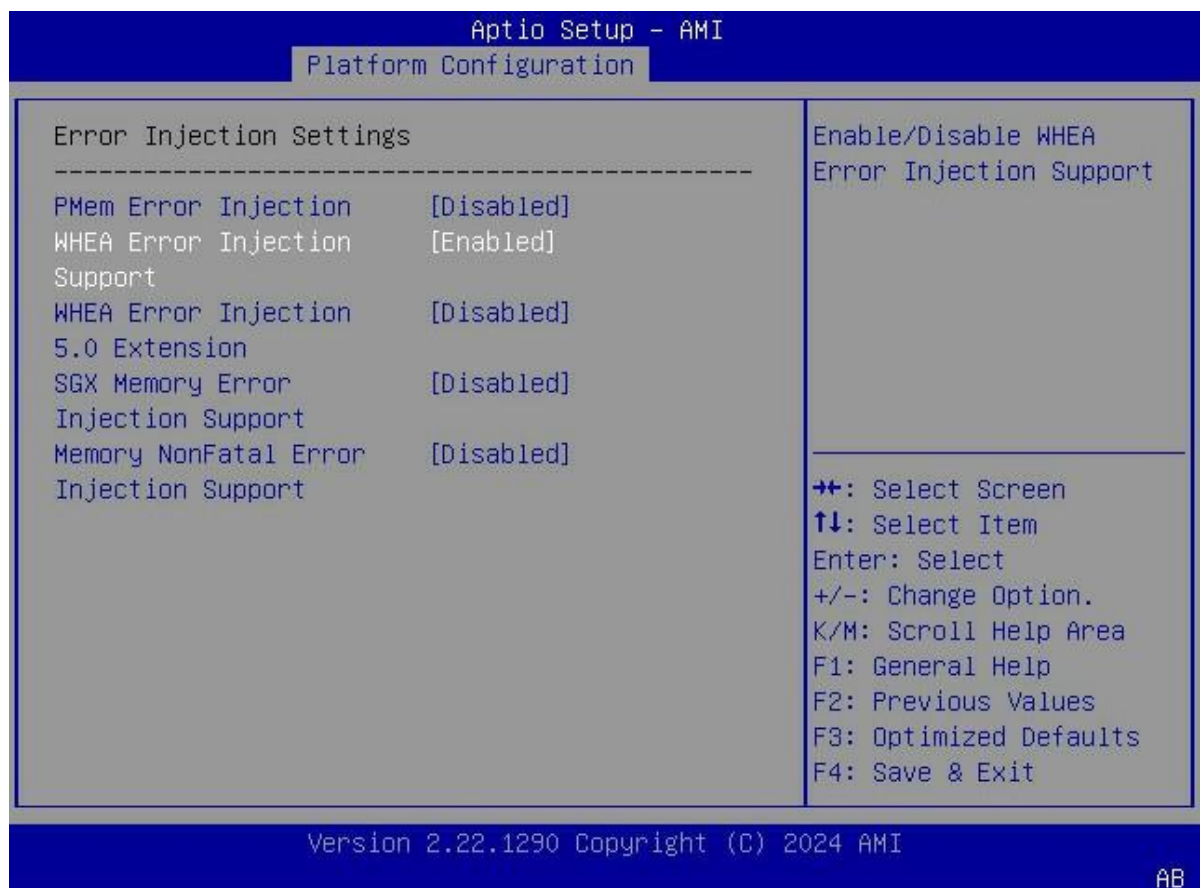
Parameter	Description	Default
WHEA Support	Enables or disables the support for WHEA Options: ● Enable: enables WHEA support. ● Disable: disables WHEA support. When this parameter is set to Disabled , the parameters below are hidden.	Enabled
WHEA Log Memory Error	Enables or disables the support for WHEA in logging memory errors. Options: ● Enable: enables the support for WHEA in logging memory errors. ● Disable: disables the support for WHEA in logging memory errors.	Enabled
WHEA Log Processor Error	Enables or disables the support for WHEA in logging processor errors.	Enabled

Parameter	Description	Default
	Options: ● Enable: enables the support for WHEA in logging processor errors. ● Disabled: disables the support for WHEA in logging processor errors.	
WHEA Log PCI Error	Enables or disables the support for WHEA in logging PCI errors. Options: ● Enable: enables the support for WHEA in logging PCI errors. ● Disable: disables the support for WHEA in logging PCI errors.	Enabled

3.3.4.3 Error Injection Settings

Figure 3-53 shows the **Error Injection Settings** screen.

Figure 3-53 Error Injection Settings Screen



For a description of the parameters on the **Error Injection Settings** screen, refer to [Table 3-42](#).

Table 3-42 Parameter Descriptions for the Error Injection Settings Screen

Parameter	Description	Default
PMem Error Injection	Enables or disables the PMem error injection feature. Options: ● Enabled: enables the PMem error injection feature. ● Disabled: disables the PMem error injection feature.	Disabled
WHEA Error Injection Support	Enables or disables WHEA error injection support. Options: ● Enabled: enables WHEA error injection support. ● Disabled: disables WHEA error injection support. When this parameter is set to Disabled , the parameters below are hidden.	Disabled
WHEA Error Injection 5.0 Extension	Enables or disables WHEA error injection 5.0 extension. Options: ● Enabled: enables WHEA error injection 5.0 extension. ● Disabled: disables WHEA error injection 5.0 extension.	Disabled
SGX Memory Error Injection Support	Enables or disables SGX memory error injection support. Options: ● Enabled: enables SGX memory error injection support. ● Disabled: disables SGX memory error injection support.	Disabled
Memory NonFatal Error Injection Support	Enables or disables memory non-fatal error injection support. Options: ● Enabled: enables memory non-fatal error injection support. ● Disabled: disables memory non-fatal error injection support.	Disabled

3.3.4.4 Memory Error Enabling

Figure 3-54 through Figure 3-55 show the **Memory Error Enabling** screen.

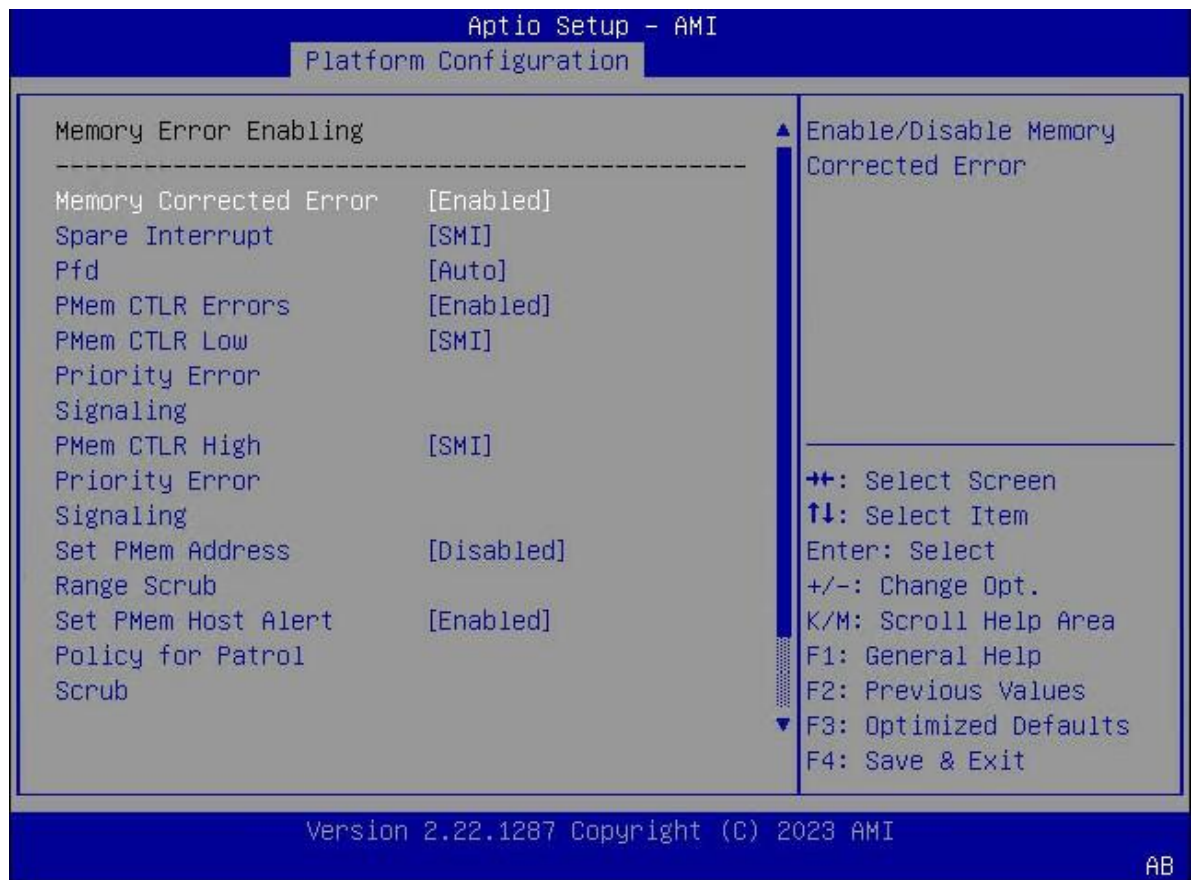
Figure 3-54 Memory Error Enabling Screen—1

Figure 3-55 Memory Error Enabling Screen—2



For a description of the parameters on the **Memory Error Enabling** screen, refer to [Table 3-43](#).

Table 3-43 Parameter Descriptions for the Memory Error Enabling Screen

Parameter	Description	Default
Memory Corrected Error	Enables or disables correctable memory error reporting. Options: - Enabled: enables correctable memory error reporting. - Disabled: disables correctable memory error reporting. When this parameter is set to Disabled , the Spare Interrupt parameter is hidden.	Enabled
Spare Interrupt	Sets the spare interrupt. Options: - Disabled - SMI - Error Pin - CMCI	SMI

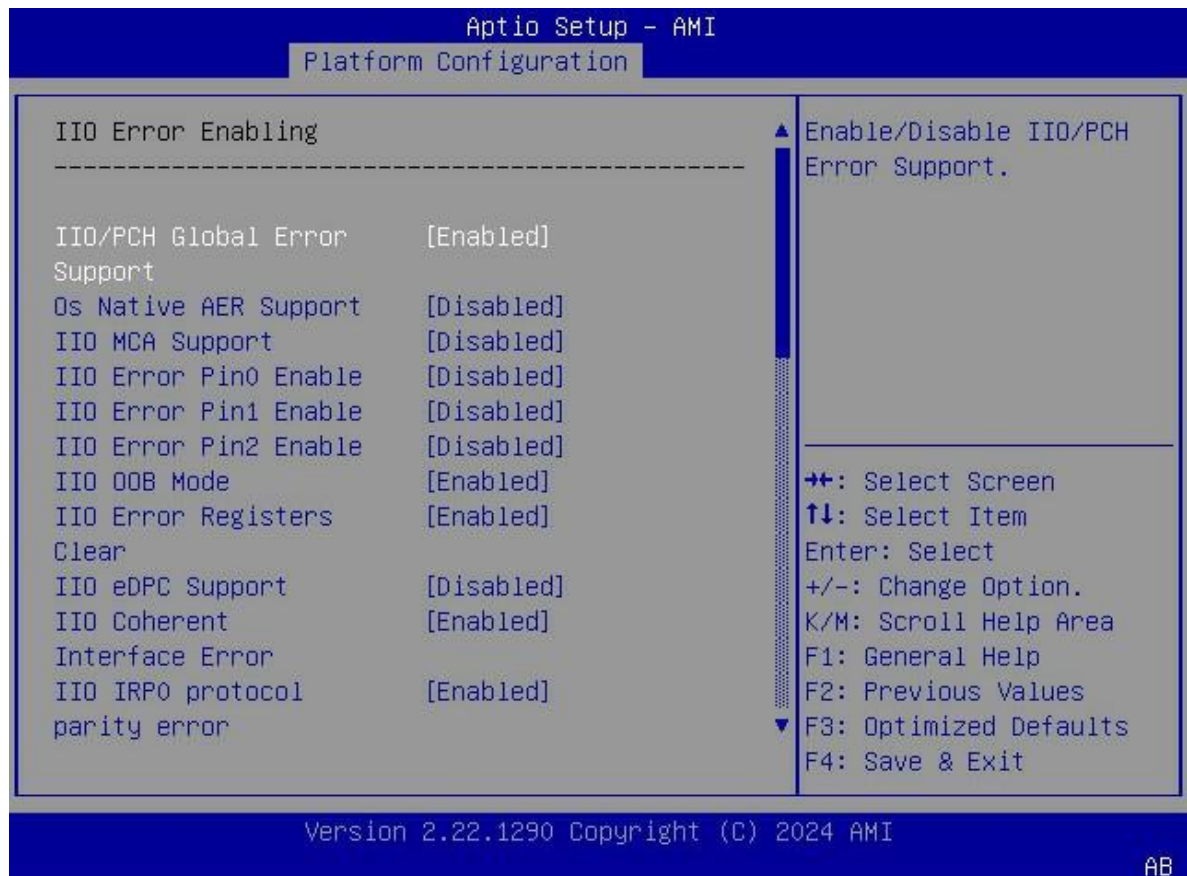
Parameter	Description	Default
Pfd	The PFD is used to identify hard faults from errors. Enables or disables the PFD feature. Options: ● Enabled: enables the PFD feature. ● Disabled: disables the PFD feature. ● Auto: dynamically enables PFD based on the system configuration.	Auto
PMem CTLR Errors	Enables or disables PMem CTLR error reporting and logging. Options: ● Enabled: enables PMem CTLR error reporting and logging. ● Disabled: disables PMem CTLR error reporting and logging.	Enabled
PMem CTLR Low Priority Error Signaling	Sets PMem CTLR low priority error signaling. Options: ● Disabled ● SMI ● Erro# Pin	SMI
PMem CTLR High Priority Error Signaling	Sets PMem CTLR high priority error signaling. Options: ● Disabled ● SMI ● Erro# Pin	SMI
Set PMem Address Range Scrub	Enables or disables PMem DIMM physical address range scrubbing. Options: ● Enabled: enables PMem DIMM physical address range scrubbing. ● Disabled: disables PMem DIMM physical address range scrubbing.	Disabled
Set PMem Host Alert Policy for Patrol Scrub	Enables or disables the triggering of PMem interrupts based on uncorrectable errors detected by NGN patrol scrubbing. Options: ● Enabled: enables the triggering of PMem interrupts. ● Disabled: disables the triggering of PMem interrupts.	Enabled
Enable Reporting SPA to OS	Enables or disables SPA reporting to the OS.	Enabled

Parameter	Description	Default
	Options: - Enabled: enables SPA reporting to the OS. - Disabled: disables SPA reporting to the OS.	
Set PMem Host Alert Policy for DPA Error	Sends signals to Poison or Viral when a DIMM physical address error is received. Options: - Poison: sends signals to Poison. - Viral: sends signals to Viral.	Poison

3.3.4.5 IIO Error Enabling

Figure 3-56 through Figure 3-58 show the **IIO Error Enabling** screen.

Figure 3-56 IIO Error Enabling Screen—1



AB

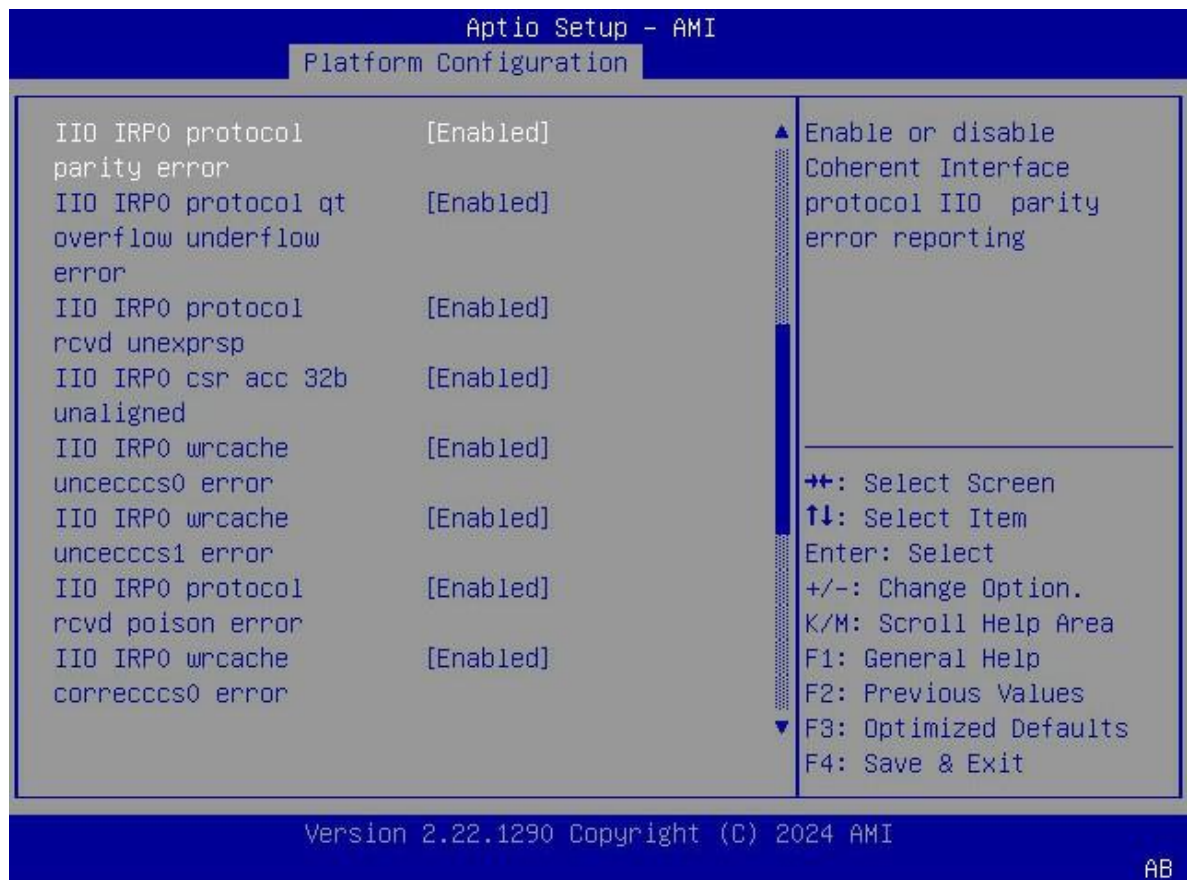
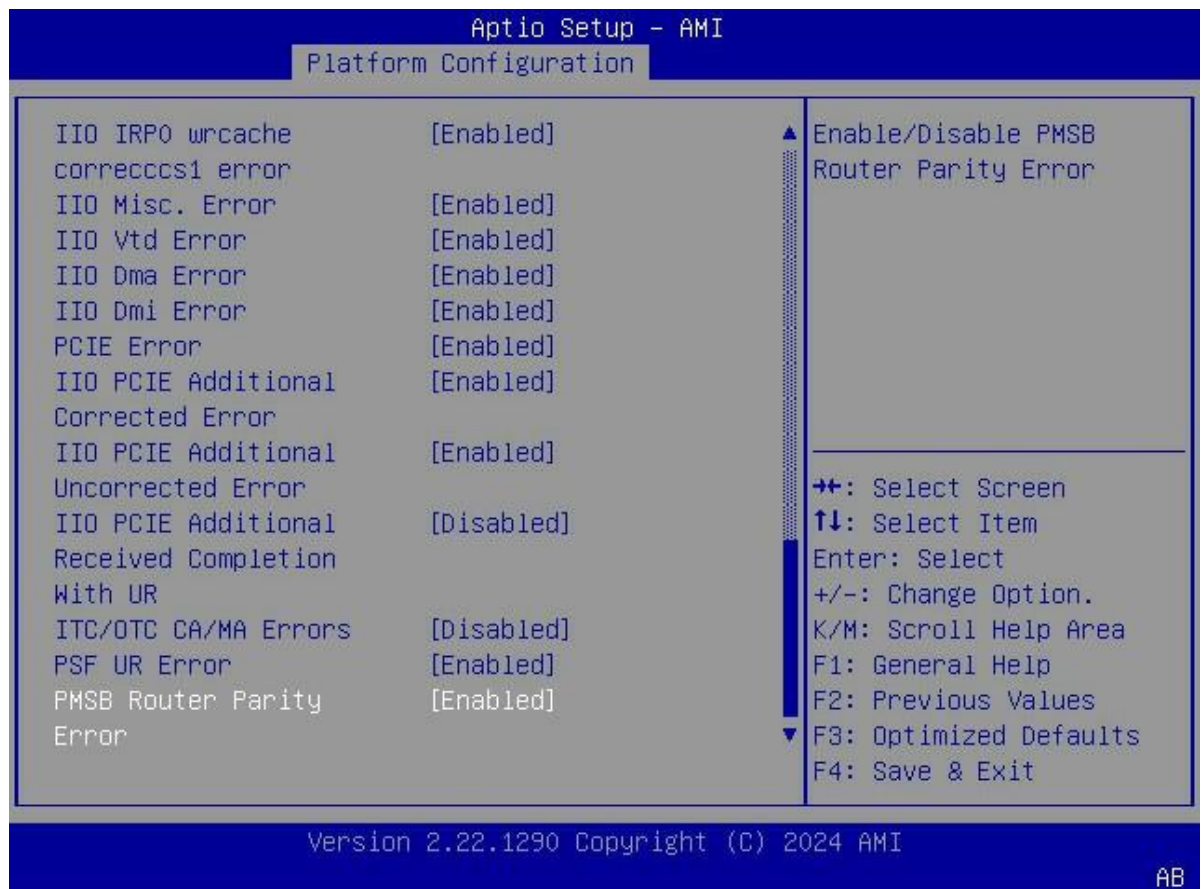
Figure 3-57 IIO Error Enabling Screen—2

Figure 3-58 IIO Error Enabling Screen—3



For a description of the parameters on the **IIO Error Enabling** screen, refer to [Table 3-44](#).

Table 3-44 Parameter Descriptions for the IIO Error Enabling Screen

Parameter	Description	Default
IIO/PCH Global Error Support	Enables or disables IIO/PCH global error support. Options: ● Enabled: enables IIO/PCH global error support. ● Disabled: disables IIO/PCH global error support. When this parameter is set to Disabled , the parameters below are hidden.	Enabled
OS Native AER Support	Enables or disables OS native AER support. Options: ● Enabled: enables OS native AER support. ● Disabled: disables OS native AER support.	Disabled
IIO MCA Support	Enables or disables the IIO MCA feature. Options: ● Enabled: enables the IIO MCA feature. ● Disabled: disables the IIO MCA feature.	Disabled

Parameter	Description	Default
	When this parameter is set to Disabled , the Clear PCC for IIO Non-Fatal Error parameter is hidden and the IIO Error Pin1 Enable and IIO Error Pin2 Enable parameters are activated.	
Clear PCC for IIO Non-Fatal Error	Enables or disables the clearing of the PCC register if an IIO non-fatal error occurs, that is, setting it to 0. Options: ● Enabled: PCC is cleared. ● Disabled: PCC is not cleared.	Disabled
IIO Error Pin0 Enable	Enables or disables IIO error pin0. Options: ● Enabled: enables IIO error Pin0. ● Disabled: disables IIO error Pin0.	Disabled
IIO Error Pin1 Enable	Enables or disables IIO error pin1. Options: ● Enabled: enables IIO error Pin1. ● Disabled: disables IIO error Pin1.	Disabled
IIO Error Pin2 Enable	Enables or disables IIO error pin2. Options: ● Enabled: enables IIO error Pin2. ● Disabled: disables IIO error Pin2.	Disabled
IIO OOB Mode	Enables or disables IIO OOB mode. Options: ● Enabled: enables IIO OOB mode. ● Disabled: disables IIO OOB mode.	Enabled
IIO Error Registers Clear	Enables or disables the clearing of IIO error registers. Options: ● Enabled: enables the clearing of IIO error registers. ● Disabled: disables the clearing of IIO error registers.	Enabled
IIO eDPC Support	Sets the IIO eDPC feature. Options: ● Disabled: disables the IO eDPC feature. After this feature is disabled, some of the parameters below are hidden. ● On Fatal Error ● On Fatal and Non-Fatal Errors	On Fatal and Non-Fatal Errors
IIO eDPC Interrupt	Enables or disables the IIO eDPC interrupt.	Enabled

Parameter	Description	Default
	Options: ● Enabled: enables the IIO eDPC interrupt. ● Disabled: disables the IIO eDPC interrupt.	
IIO eDPC ERR_COR Message	Enables or disables the IIO eDPC ERR_COR information. Options: ● Enabled: enables the IIO eDPC ERR_COR information. ● Disabled: disables the IIO eDPC ERR_COR information.	Enabled
PCIe Poison TLP Egress Blocking	Enables or disables PCIe Poison TLP egress blocking. Options: ● Enabled: enables PCIe Poison TLP egress blocking. ● Disabled: disables PCIe Poison TLP egress blocking.	Enabled
IIO Coherent Interface Error	Enables or disables the detection of IIO coherent interface errors. Options: ● Enabled: enables the detection of IIO coherent interface errors. ● Disabled: disables the detection of IIO coherent interface errors.	Enabled
IIO IRP0 protocol parity error	Enables or disables the parity error detection for the IIO coherent interface protocol. Options: ● Enabled: enables the parity error detection for the IIO coherent interface protocol. ● Disabled: disables the parity error detection for the IIO coherent interface protocol.	Enabled
IIO IRP0 protocol qt overflow underflow error	Enables or disables the reporting of overflow or underflow errors of protocol layer queue tables of the IIO coherent interface. Options: ● Enabled: enables the reporting of overflow or underflow errors of protocol layer queue tables of the IIO coherent interface.	Enabled

Parameter	Description	Default
	Disabled: disables the reporting of overflow or underflow errors of protocol layer queue tables of the IIO coherent interface.	
IIO IRP0 protocol rcvd unexprsp	Enables or disables the receiving of unexpected responses by the Coherent interface protocol layer and the reporting of errors. Options: - Enabled: enables the receiving of unexpected responses by the Coherent interface protocol layer and the reporting of errors. - Disabled: disables the receiving of unexpected responses by the Coherent interface protocol layer and the reporting of errors.	Enabled
IIO IRP0 csr acc 32b unaligned	Enables or disables the reporting of 32-bit boundary crossing errors for IIO coherent interface CSR access. Options: - Enabled: enables the reporting of 32-bit boundary crossing errors for IIO coherent interface CSR access. - Disabled: disables the reporting of 32-bit boundary crossing errors for IIO coherent interface CSR access.	Enabled
IIO IRP0 wrccache uncecccs0 error	Enables or disables the reporting of uncorrectable cache write ECC errors of the Coherent interface. Options: - Enabled: enables the reporting of uncorrectable cache write ECC errors of the Coherent interface. - Disabled: disables the reporting of uncorrectable cache write ECC errors of the Coherent interface.	Enabled
IIO IRP0 wrccache uncecccs1 error	Enables or disables the reporting of uncorrectable cache write ECC errors of the Coherent interface. Options: - Enabled: enables the reporting of uncorrectable cache write ECC errors of the Coherent interface. - Disabled: disables the reporting of uncorrectable cache write ECC errors of the Coherent interface.	Enabled
IIO IRP0 protocol rcvd poison error	Enables or disables the reporting of poisoned packet errors received at the protocol layer of the IIO coherent interface. Options:	Enabled

Parameter	Description	Default
	● Enabled: enables the reporting of poisoned packet errors received at the protocol layer of the IIO coherent interface. ● Disabled: disables the reporting of poisoned packet errors received at the protocol layer of the IIO coherent interface.	
IIO IRP0 wrcache correcccs0 error	Enables or disables the reporting of correctable cache write ECC errors of the Coherent interface. Options: ● Enabled: enables the reporting of correctable cache write ECC errors of the Coherent interface. ● Disabled: disables the reporting of correctable cache write ECC errors of the Coherent interface.	Enabled
IIO IRP0 wrcache correcccs1 error	Enables or disables the reporting of correctable cache write ECC errors of the Coherent interface. Options: ● Enabled: enables the reporting of correctable cache write ECC errors of the Coherent interface. ● Disabled: disables the reporting of correctable cache write ECC errors of the Coherent interface.	Enabled
IIO Misc. Error	Enables or disables the reporting of IIO Misc. errors. Options: ● Enabled: enables the reporting of IIO Misc. errors. ● Disabled: disables the reporting of IIO Misc. errors.	Enabled
IIO Vtd Error	Enables or disables the reporting of IIO Vtd errors. Options: ● Enabled: enables the reporting of IIO Vtd errors. ● Disabled: disables the reporting of IIO Vtd errors.	Enabled
IIO Dma Error	Enables or disables the reporting of IIO Dma errors. Options: ● Enabled: enables the reporting of IIO Dma errors. ● Disabled: disables the reporting of IIO Dma errors.	Enabled
IIO Dmi Error	Enables or disables the reporting of IIO Dmi errors. Options: ● Enabled: enables the reporting of IIO Dmi errors. ● Disabled: disables the reporting of IIO Dmi errors.	Enabled
PCIE Error	Enables or disables the reporting of PCIe errors. Options: ● Enabled: enables the reporting of PCIe errors.	Enabled

Parameter	Description	Default
	Disabled: disables the reporting of PCIe errors.	
IIO PCIe Additional Corrected Error	Enables or disables the reporting of IIO PCIe additional correctable errors. Options: - Enabled: enables the reporting of IIO PCIe additional correctable errors. - Disabled: disables the reporting of IIO PCIe additional correctable errors.	Enabled
IIO PCIe Additional Uncorrected Error	Enables or disables the reporting of IIO PCIe additional uncorrectable errors. Options: - Enabled: enables the reporting of IIO PCIe additional uncorrectable errors. - Disabled: disables the reporting of IIO PCIe additional uncorrectable errors.	Enabled
IIO PCIe Additional Received Completion With UR	Enables or disables IIO PCIe's additional receiving feature when URs are used. Options: - Enabled: enables IIO PCIe's additional receiving feature when URs are used. - Disabled: disables IIO PCIe's additional receiving feature when URs are used.	Disabled
ITC/OTC CA/MA Errors	Enables or disables the reporting of complete abort and master abort errors on ITC and OTC. Options: - Enabled: enables the reporting of complete abort and master abort errors on ITC and OTC. - Disabled: disables the reporting of complete abort and master abort errors on ITC and OTC.	Disabled
PSF UR Error	Enables or disables the reporting of UR errors on the PSF. Options: - Enabled: enables the reporting of UR errors on the PSF. - Disabled: disables the reporting of UR errors on the PSF.	Enabled
PMSB Router Parity Error	Enables or disables the reporting of PMSB Router parity errors. Options:	Enabled

Parameter	Description	Default
	- Enabled: enables the reporting of PMSB Router parity errors. - Disabled: disables the reporting of PMSB Router parity errors.	

3.3.4.6 PCIe Error Enabling

Figure 3-59 through Figure 3-61 show the **PCIe Error Enabling** screen.

Figure 3-59 PCIe Error Enabling Screen—1

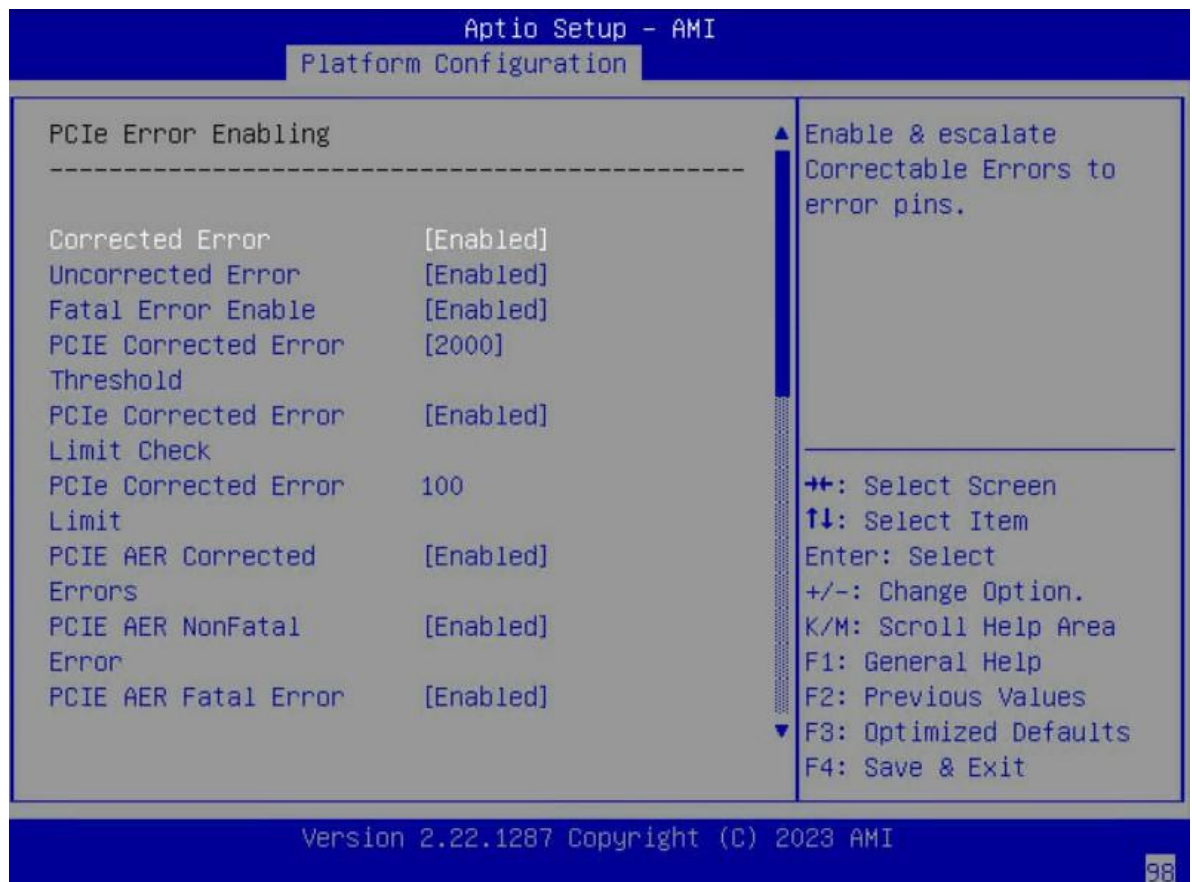


Figure 3-60 PCIe Error Enabling Screen—2

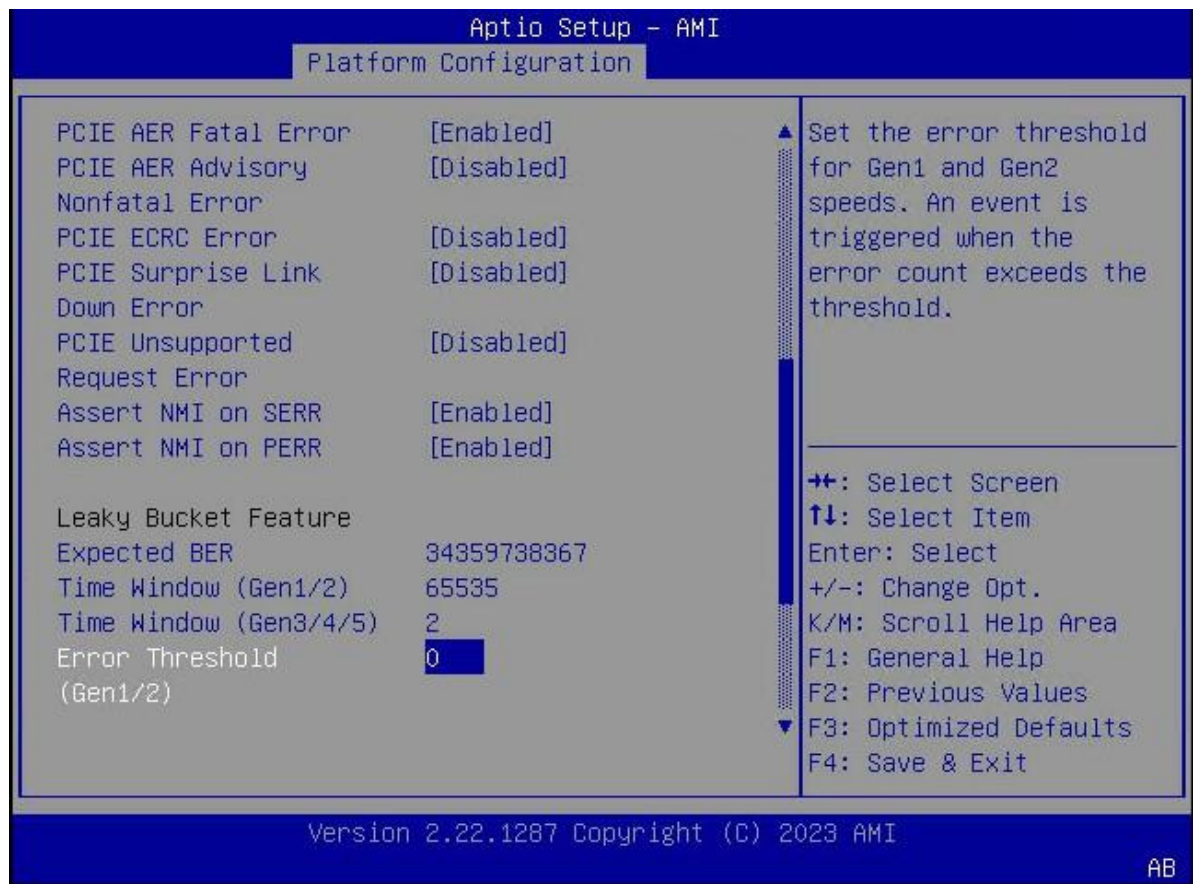
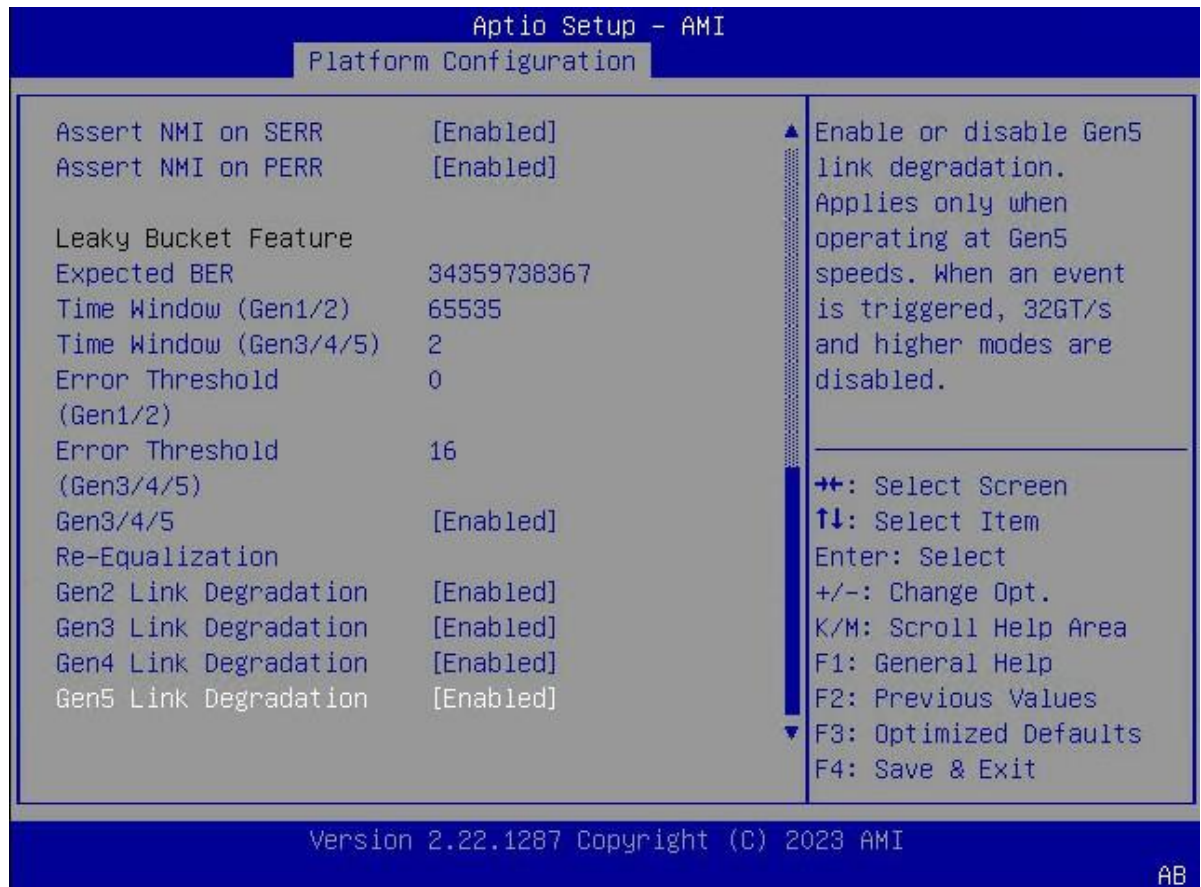


Figure 3-61 PCIe Error Enabling Screen—3



For a description of the parameters on the **PCIe Error Enabling** screen, refer to [Table 3-45](#).

Table 3-45 Parameter Descriptions for the PCIe Error Enabling Screen

Parameter	Description	Default
Corrected Error	Enables or disables PCIe correctable error logging. Options: ● Enabled: enables PCIe correctable error logging. ● Disabled: disables PCIe correctable error logging. After this feature is disabled, some of the parameters below are hidden.	Enabled
Uncorrected Error	Enables or disables PCIe uncorrectable error logging. Options: ● Enabled: enables PCIe uncorrectable error logging. ● Disabled: disables PCIe uncorrectable error logging.	Enabled
Fatal Error Enable	Enables or disables fatal error logging. Options: ● Enabled: enables fatal error logging.	Enabled

Parameter	Description	Default
	Disabled: disables fatal error logging.	
PCIE Corrected Error Threshold	Select the threshold for logging PCle correctable errors. Options: - Disable 2000 4000 8000	2000
PCIE Corrected Error Limit Check	Enables or disables the limit check on PCle correctable errors. Options: - Enabled: enables the limit check on PCle correctable errors. After this feature is enabled, the logging of PCle correctable errors is disabled if the limit is exceeded. - Disabled: disables the limit check on PCle correctable errors.	Disabled
PCIE Corrected Error Limit	Enter the maximum number of PCle correctable errors.	100
PCIE AER Corrected Errors	Enables or disables PCle AER correctable error logging. Options: - Enabled: enables PCle AER correctable error logging. - Disabled: disables PCle AER correctable error logging.	Enabled
PCIE AER NonFatal Error	Enables or disables PCle AER non-fatal error logging. Options: - Enabled: enables PCle AER non-fatal error logging. - Disabled: disables PCle AER non-fatal error logging.	Enabled
PCIE AER Fatal Error	Enables or disables PCle AER fatal error logging. Options: - Enabled: enables PCle AER fatal error logging. - Disabled: disables PCle AER fatal error logging.	Enabled
PCIE AER Advisory Nonfatal Error	Enables or disables PCle AER Advisory non-fatal error logging. Options:	Disabled

Parameter	Description	Default
	● Enabled: enables PCIe AER Advisory non-fatal error logging. ● Disabled: disables PCIe AER Advisory non-fatal error logging.	
PCIe ECRC Error	Enables or disables PCIe ECRC error logging. Options: ● Enabled: enables PCIe ECRC error logging. ● Disabled: disables PCIe ECRC error logging.	Disabled
PCIe Surprise Link Down Error	Enables or disables the PCIe Surprise Link Down error detection. Options: ● Enabled: enables the PCIe Surprise Link Down error detection. ● Disabled: disables the sPCIe Surprise Link Down error detection.	Disabled
PCIe Unsupported Request Error	Enables or disables the PCIe Unsupported Request Error detection. Options: ● Enabled: enables the PCIe Unsupported Request Error detection. ● Disabled: disables the PCIe Unsupported Request Error detection.	Disabled
Assert NMI on SERR	Enables or disables the generation of an NMI and logging of an error upon an SERR. Options: ● Enabled: enables the generation of an NMI and logging of an error upon an SERR. ● Disabled: disables the generation of an NMI and logging of an error upon an SERR. After this feature is disabled, Assert NMI on PERR is not configurable.	Enabled
Assert NMI on PERR	Enables or disables the generation of an NMI and logging of an error upon a PERR. Options: ● Enabled: enables the generation of an NMI and logging of an error upon a PERR. ● Disabled: disables the generation of an NMI and logging of an error upon a PERR.	Enabled
Expected BER	Enter the expected bit error rate for all speeds.	34359738367

Parameter	Description	Default
Time Window (Gen1/2)	Enter the error string protection time window for Gen1 and Gen2. The error string count in the window is 1.	65535
Time Window (Gen3/4/5)	Enter the error string protection time window for Gen3, Gen4, and Gen5. The error string count in the window is 1.	2
Error Threshold (Gen1/2)	Enter the error threshold for Gen1 and Gen2. An event is triggered when the number of errors exceeds the threshold.	0
Error Threshold (Gen3/4/5)	Enter the error threshold for Gen3, Gen4, and Gen5. An event is triggered when the number of errors exceeds the threshold.	16
Gen3/4/5 Re- Equalization	Enables or disables the re-equalization feature for Gen3, Gen4, or Gen5. Only available at Gen3, Gen4, or Gen5. Re-equalization occurs when an event is triggered. Options: ● Enabled: enables the re-equalization feature for Gen3, Gen4, or Gen5. ● Disabled: disables the re-equalization feature for Gen3, Gen4, or Gen5.	Enabled
Gen2 Link Degradation	Enables or disables Gen2 link degradation. Only available at Gen2. When an event is triggered, 5 GT/s and higher mode are disabled. Options: ● Enabled: enables Gen2 link degradation. ● Disabled: disables Gen2 link degradation.	Enabled
Gen3 Link Degradation	Enables or disables Gen3 link degradation. Only available at Gen3. When an event is triggered, 8 GT/s and higher mode are disabled. Options: ● Enabled: enables Gen3 link degradation. ● Disabled: disables Gen3 link degradation.	Enabled
Gen4 Link Degradation	Enables or disables Gen4 link degradation. Only available at Gen4. When an event is triggered, 16 GT/s and higher mode are disabled. Options: ● Enabled: enables Gen4 link degradation. ● Disabled: disables Gen4 link degradation.	Enabled
Gen5 Link Degradation	Enables or disables Gen5 link degradation.	Enabled

Parameter	Description	Default
	Only available at Gen5. When an event is triggered, 32 GT/s and higher mode are disabled. Options: • Enabled: enables Gen5 link degradation. • Disabled: disables Gen5 link degradation.	

3.3.4.7 Error Control Setting

Figure 3-62 shows the **Error Control Setting** screen.

Figure 3-62 Error Control Setting Screen



For a description of the parameters on the **Error Control Setting** screen, refer to [Table 3-46](#).

Table 3-46 Parameter Descriptions for the Error Control Setting Screen

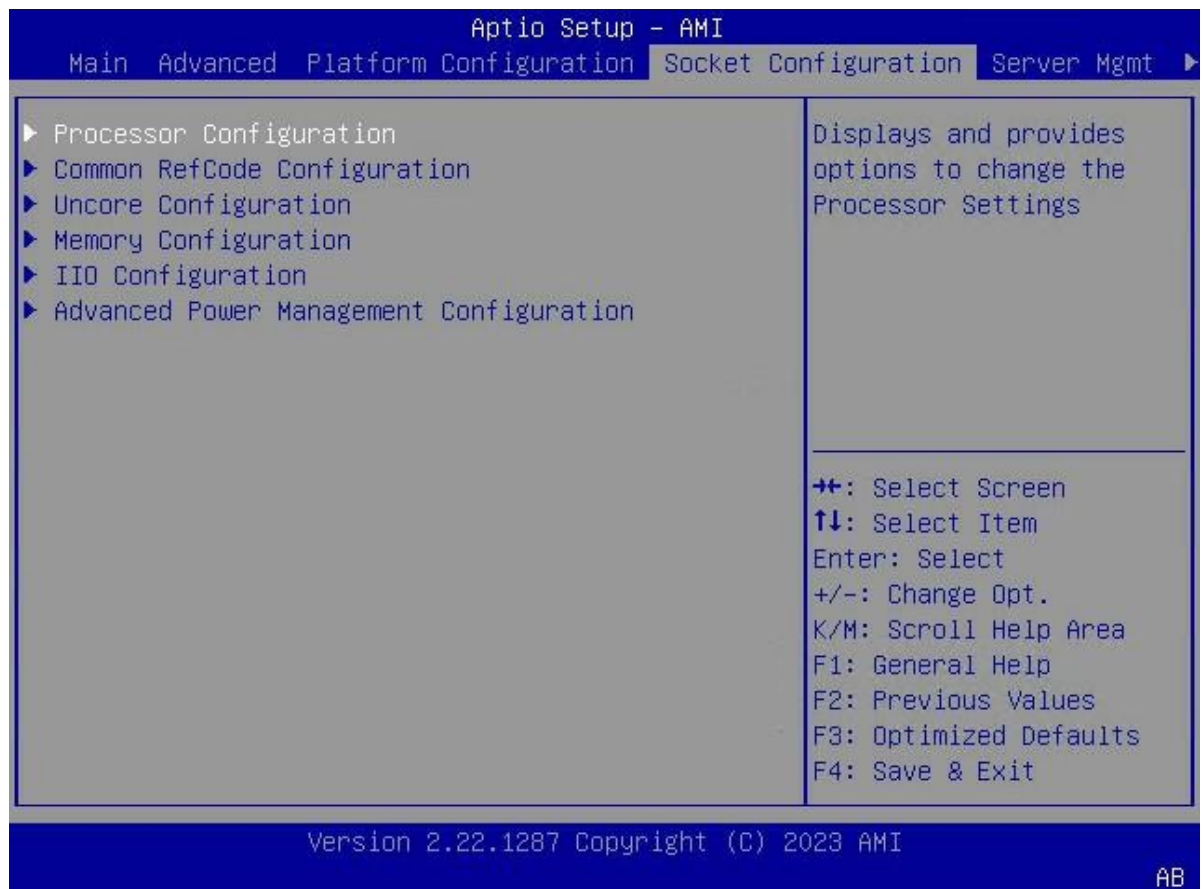
Parameter	Description	Default
2LM Correctable Error Logging in m2mem	Enables or disables the 2LM correctable error logging in m2mem. Options: • Enabled: enables the logging of the 2LM correctable errors in m2mem.	Enabled

Parameter	Description	Default
	● Disabled: disables the logging of the 2LM correctable errors in m2mem.	
Latch First Corrected Error in KTI	Enables or disables the locking of the first corrected error in KTI. Options: ● Enabled: enables the locking of the first corrected error in KTI. ● Disabled: disables the locking of the first corrected error in KTI.	Disabled
Patrol Scrub Error Reporting	Select the type of error reported during preventive maintenance. Options: UCNA: uncorrectable but recoverable errors.	UCNA
LLC EWB Error Control	Select the type of EWB error notification. Options: ● UCNA ● SRAO	UCNA

3.4 Socket Configuration

Figure 3-63 shows the **Socket Configuration** screen.

Figure 3-63 Socket Configuration Screen



For a description of the parameters on the **Socket Configuration** screen, refer to [Table 3-47](#).

Table 3-47 Parameter Descriptions for the Socket Configuration Screen

Parameter	Description
Processor Configuration	Sets processor parameters. For details, refer to 3.4.1 Processor Configuration .
Common RefCode Configuration	Sets general RefCode parameters. For details, refer to 3.4.2 Common RefCode Configuration .
Uncore Configuration	Sets UPI parameters. For details, refer to 3.4.3 Uncore Configuration .
Memory Configuration	Sets memory parameters. For details, refer to 3.4.4 Memory Configuration .
IIO Configuration	Sets IIO parameters. For details, refer to 3.4.5 IIO Configuration .
Advanced Power Management Configuration	Sets advanced power management parameters. For details, refer to 3.4.6 Advanced Power Management Configuration .

3.4.1 Processor Configuration

Figure 3-64 through Figure 3-68 show the **Processor Configuration** screen.

Figure 3-64 Processor Configuration Screen—1

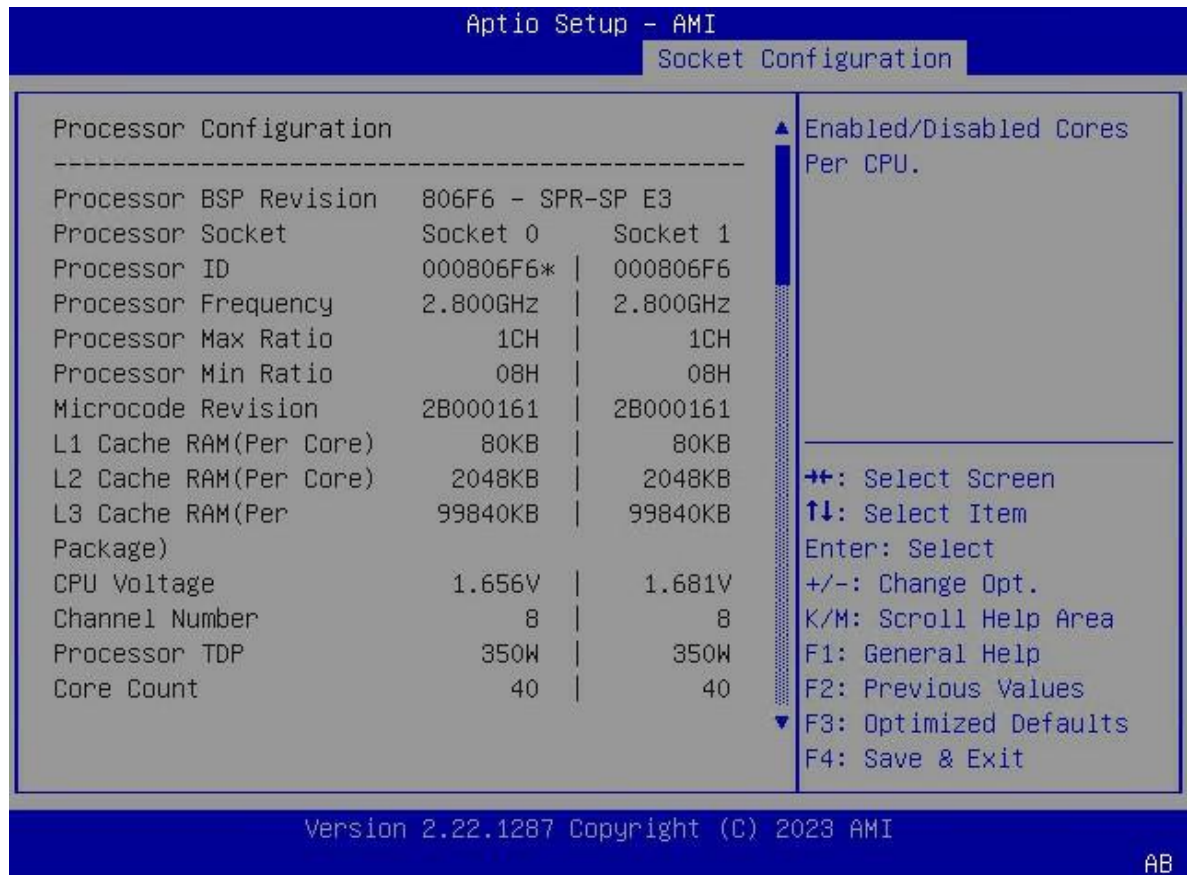


Figure 3-65 Processor Configuration Screen—2

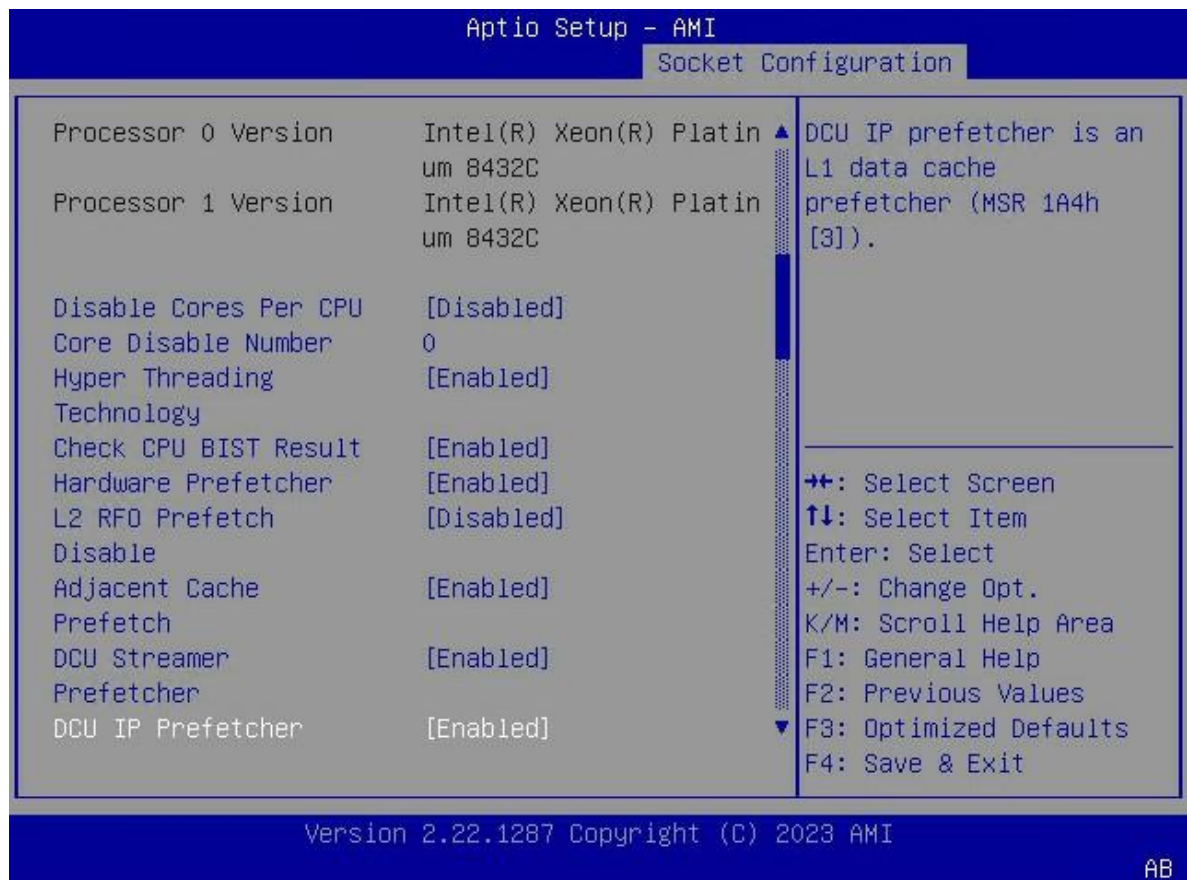


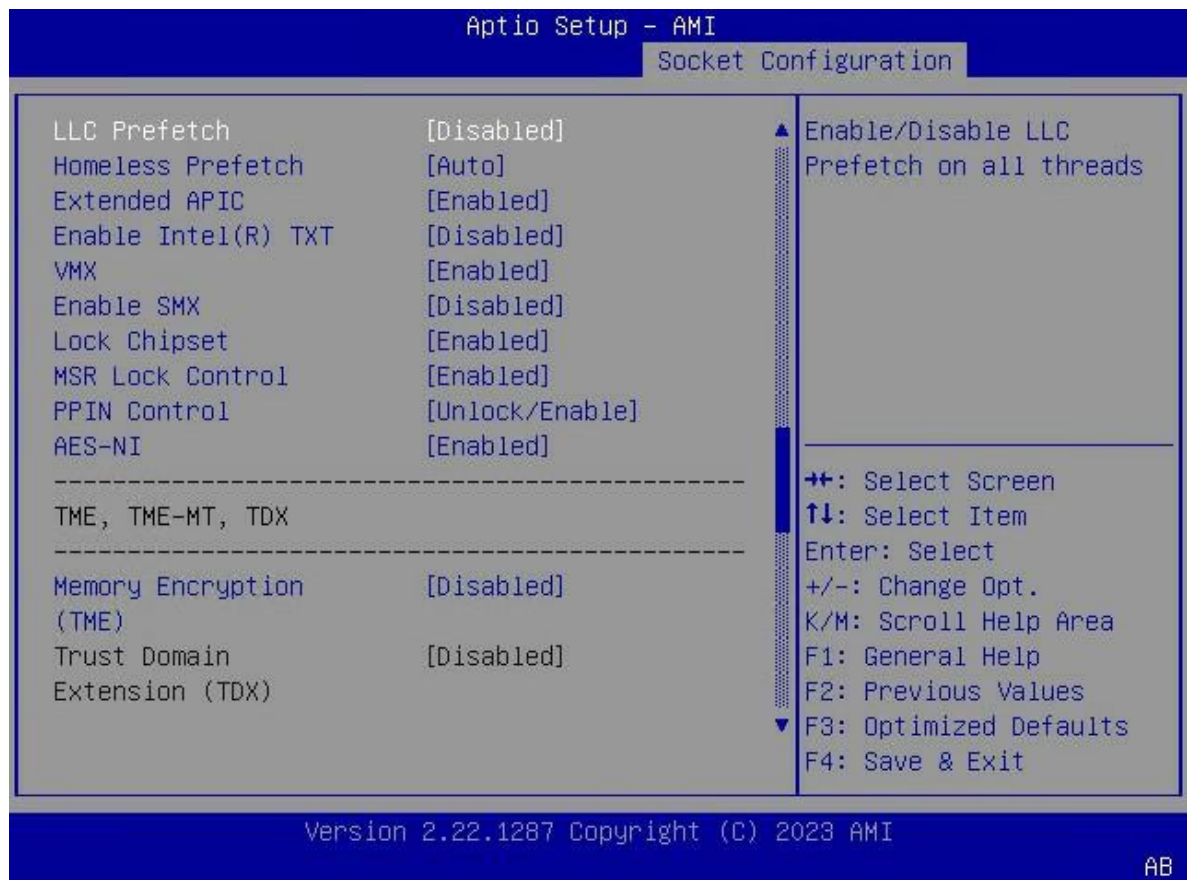
Figure 3-66 Processor Configuration Screen—3

Figure 3-67 Processor Configuration Screen—4

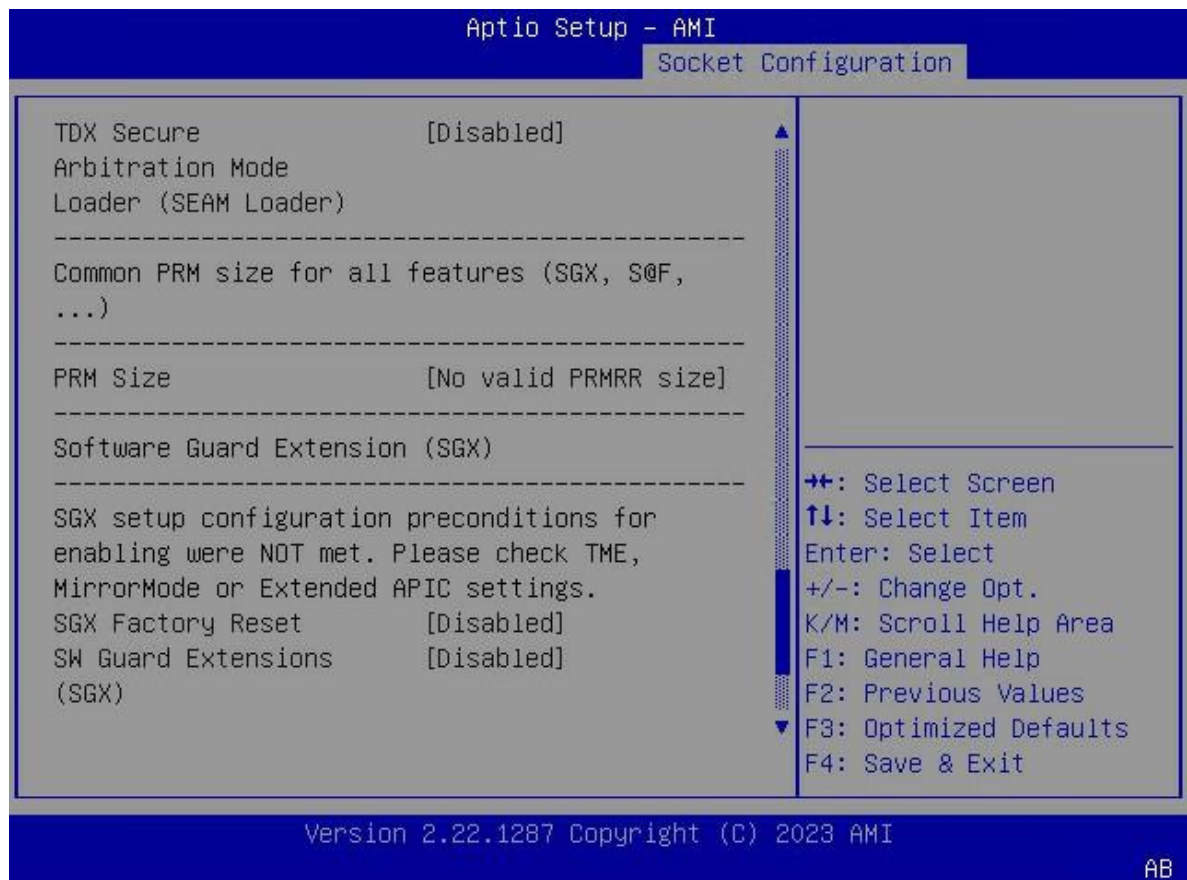
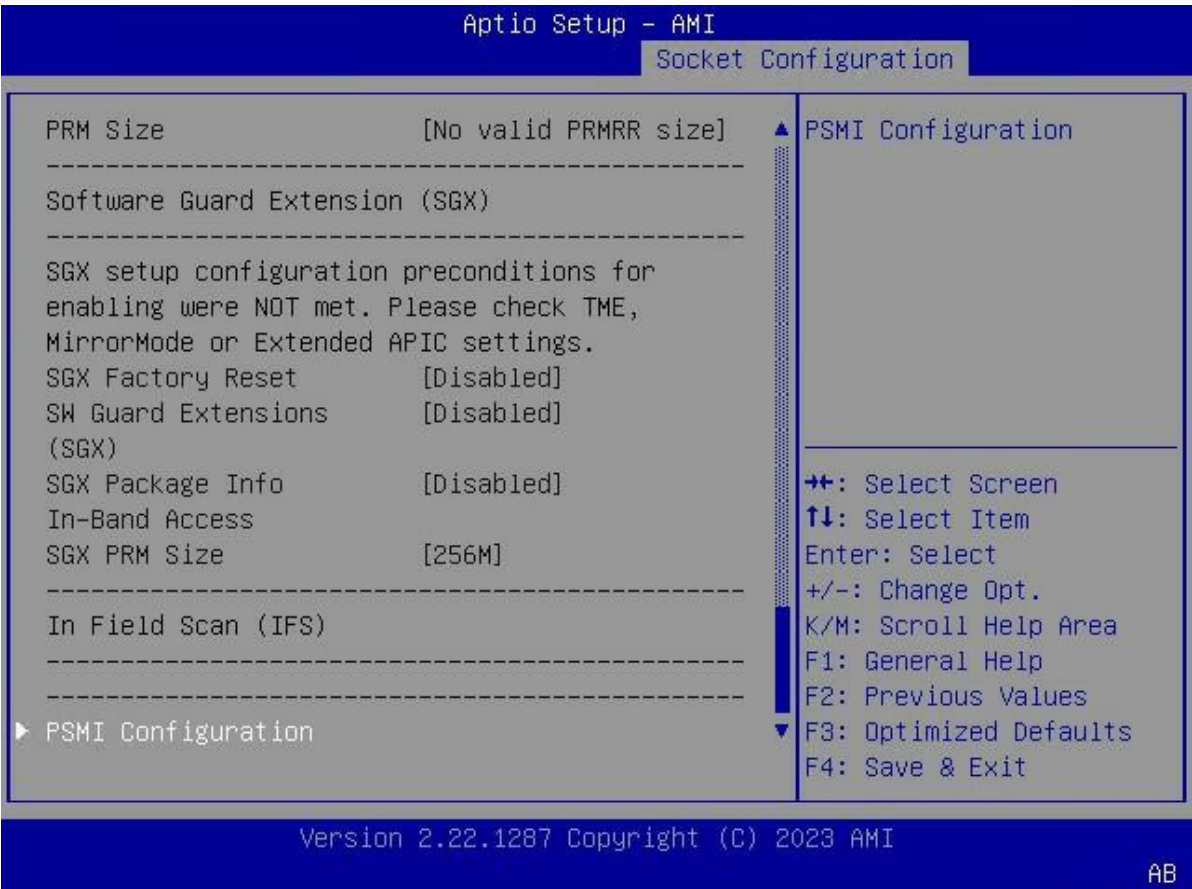


Figure 3-68 Processor Configuration Screen—5



For a description of the parameters on the **Processor Configuration** screen, refer to [Table 3-48](#).

Table 3-48 Parameter Descriptions for the Processor Configuration Screen

Parameter	Description	Default
Processor BSP Revision	Revision number of the processor BSP .	806F6-SPR-SP E3
Processor Socket	Processor socket number.	Socket 0 Socket 1
Processor ID	Processor ID.	000806F6*
Processor Frequency	Nominal frequency of the processor.	2.800GHz
Processor Max Ratio	Maximum multiplier of the processor.	1CH
Processor Min Ratio	Minimum multiplier of the processor.	08H
Microcode Revision	Microcode version number of the processor.	2B000161
L1 Cache RAM (Per Core)	L1 cache capacity.	80KB
L2 Cache RAM(Per Core)	L2 cache capacity.	2048KB
L3 Cache RAM(Per Package)	L3 cache capacity.	99840KB

Parameter	Description	Default
CPU Voltage	CPU voltage.	1.656V
Channel Number	Number of channels.	8
Processor TDP	Processor TDP.	350W
Core Count	Number of cores.	40
Processor 0 Version	Version of processor 0.	Intel(R) Xeon(R) Platinum 8432C
Processor 1 Version	Version of processor 1.	Intel(R) Xeon(R) Platinum 8432C
Disable Cores Per CPU	Enables or disables cores per CPU. Options: ● Enabled: disables cores per CPU. ● Disabled: enables cores per CPU.	Disabled
Socket0 Core Disable Number	This parameter is displayed when Disable Cores Per CPU is set to Enabled . Enter the number of disabled cores. Value 0 indicates that no cores are disabled.	0
Socket1 Core Disable Number	This parameter is displayed when Disable Cores Per CPU is set to Enabled . Enter the number of disabled cores. Value 0 indicates that no cores are disabled.	0
Hyper Threading Technology	Enables or disables the Hyper-Threading feature. Options: ● Enabled: enables the Hyper-Threading feature. ● Disabled: disables the Hyper-Threading feature.	Enabled
Check CPU BIST Result	Sets whether to use the CPU BIST check result. Options: ● Enabled: disables the CPU cores with BIST failures. ● Disabled: ignores the BIST result.	Enabled
Hardware Prefetcher	Before a CPU processes data or instructions, the hardware prefetcher prefetches the data and instructions from the memory to the L2 cache to reduce time required by the CPU for reading data from the memory, thus improving CPU performance. Enables or disables the hardware prefetch feature. Options: ● Enabled: enables the hardware prefetch feature.	Enabled

Parameter	Description	Default
	Disabled: disables the hardware prefetch feature.	
L2 RFO Prefetch Disable	Sets whether to disable the L2 RFO prefetch feature. Options: - Enabled: disables the L2 RFO prefetch feature. - Disabled: enables the L2 RFO prefetch feature.	Disabled
Adjacent Cache Prefetcher	Before processing an instruction or data, the CPU reads the data from the adjacent memory in advance to accelerate the reading speed. Enables or disables the adjacent cache prefetch feature. Options: - Enabled: enables the adjacent cache prefetch feature. - Disabled: disables the adjacent cache prefetch feature.	Enabled
DCU Streamer Prefetcher	Enables or disables the DCU stream prefetch feature. Options: - Enabled: enables the DCU stream prefetch feature. - Disabled: disables the DCU stream prefetch feature.	Enabled
DCU IP Prefetcher	Enables or disables the DCU IP prefetch feature. Options: - Enabled: enables the DCU IP prefetch feature. - Disabled: disables the DCU IP prefetch feature.	Enabled
LLC Prefetch	Enables or disables the LLC prefetch feature. Options: - Enabled: enables the LLC prefetch feature. - Disabled: disables the LLC prefetch feature.	Enabled
Homeless Prefetch	Enable or disable the Homeless prefetch feature on all threads. Options: - Enabled: enables the Homeless prefetch feature. - Disabled: disables the Homeless prefetch feature. - Auto: automatic mode.	Auto
FB Thread Slicing	Enables or disables FB thread slicing per thread. Options: - Enabled: enables FB thread slicing per thread. - Disabled: disables FB thread slicing per thread.	Disabled

Parameter	Description	Default
AMP Prefetch	Enables or disables the AMP prefetch feature. Options: ● Enabled: enables the AMP prefetch feature. ● Disabled: disables the AMP prefetch feature. ● Auto: automatically sets this parameter based on the CPU configuration: ➔ EMR XCC and MCC CPU: enables the AMP prefetch feature. ➔ Other CPUs: disables the AMP prefetch feature.	Auto
Extended APIC	Enables or disables the extended APIC. Options: ● Enabled: enables the extended APIC. ● Disabled: disables the extended APIC.	Enabled
Enable Intel (R) TXT	Enables or disables the Intel TXT security feature. Options: ● Enabled: enables the Intel TXT security feature. If this feature is enabled, VMX, Enabled SMX, and Lock Chipset are greyed out. ● Disabled: disables the Intel TXT security feature.	Disabled
VMX	Enables or disables the Vanderpool technology. Options: ● Enabled: enables the Vanderpool technology. ● Disabled: disables the Vanderpool technology.	Enabled
Enable SMX	Enables or disables SMX. Options: ● Enabled: enables SMX. ● Disabled: disables SMX.	Disabled
Lock Chipset	Sets whether to lock the chipset. Options: ● Enabled: locks the chipset. ● Disabled: Unlocks the chipset.	Enabled
MSR Lock Control	Sets whether to enable MSR Lock control. Options: ● Enabled: enables MSR Lock control. When this parameter is set to Enabled, MSR 3Ah and CSR 80 h are locked. ● Disabled: disables MSR Lock control.	Enabled
PPIN Control	Sets whether to lock PPIN control.	Unlock/Enable

Parameter	Description	Default
	Options: ● Unlock/Enable: unlocks PPIN control. ● Lock/Disable: locks PPIN control.	
AES-NI	Enables or disables the AES-NI feature. Options: ● Enabled: enables the AES-NI feature. ● Disabled: disables the AES-NI feature.	Enabled
Memory Encryption (TME)	Enables or disables full memory encryption. Options: ● Enabled: enables full memory encryption. ● Disabled: disables full memory encryption.	Disabled
Total Memory Encryption (TME) Bypass	This parameter is displayed when Memory Encryption (TME) is set to Enabled . Enables or disables the TME feature. Options: ● Enabled: enables the TME feature. ● Disabled: disables the TME feature. ● Auto: automatic mode.	Auto
Total Memory Encryption Multi-Tenant (TME-MT)	This parameter is displayed when Memory Encryption (TME) is set to Enabled . Enables or disables the TME-MT feature. Options: ● Enabled: enables the TME-MT feature. ● Disabled: disables the TME-MT feature.	Disabled
Memory integrity	This parameter is displayed when Memory Encryption (TME) is set to Enabled . Enables or disables memory consistency check. Options: ● Enabled: enables memory consistency check. ● Disabled: disables memory consistency check.	Disabled
Trust Domain Extension (TDX)	Enables or disables the TDX feature. Options: ● Enabled: enables the TDX feature. ● Disabled: disables the TDX feature.	Disabled
TDX Secure Arbitration Mode Loader (SEAM Loader)	Enables or disables the SEAM Loader. Options: ● Enabled: enables the SEAM Loader. ● Disabled: disables the SEAM Loader.	Disabled

Parameter	Description	Default
SGX Factory Reset	Sets whether to restore SGX to the factory default settings. Options: ● Enabled: restores SGX to the factory default settings. ● Disabled: disables the restoration of SGX to the factory default settings.	Disabled
SGX	Enables or disables the SGX feature. Options: ● Enabled: enables the SGX feature. ● Disabled: disables the SGX feature.	Disabled
SGX Package Info In-Band Access	Enables or disables the in-band control feature for SGX package information. Options: ● Enabled: enables the in-band control feature for SGX package information. ● Disabled: disables the in-band control feature for SGX package information.	Disabled
SGX PRM Size	This parameter is displayed when SW Guard Extensions(SGX) is set to Enabled . Sets the size of the SGX PRM. Options: ● 256M ● 512M ● 1G ● 2G ● 4G ● 8G ● 16G ● 32G ● 64G ● 128G	256M
SGX QoS	This parameter is displayed when SW Guard Extensions(SGX) is set to Enabled . Enables or disables the SGX QoS feature. Options: ● Enabled: enables the SGX QoS feature. ● Disable: disables the SGX QoS feature.	Enabled

Parameter	Description	Default
Select Owner EPOCH input type	This parameter is displayed when SW Guard Extensions (SGX) is set to Enabled. Select the owner's EPOCH input type. Options: - Manual User Defined Owner EPOCHs: allows the user to manually define the owner's EPOCHs. - Change to New Random Owner EPOCHs: changes the value of EPOCH to a system-generated random number.	Manual User Defined Owner EPOCHs
Software Guard Extensions Epoch 0	This parameter is displayed when SW Guard Extensions (SGX) is set to Enabled. Enter the SGE Epoch value when the SGX period is set to zero. If Select Owner EPOCH input type is set to Change to New Random Owner EPOCHs, the generated random number is displayed.	0
Software Guard Extensions Epoch 1	This parameter is displayed when SW Guard Extensions (SGX) is set to Enabled. Enter the SGE Epoch value when the SGX period is set to one. If Select Owner EPOCH input type is set to Change to New Random Owner EPOCHs, the generated random number is displayed.	0
SGXLEPUBKEYHASHx Write Enable	This parameter is displayed when SW Guard Extensions (SGX) is set to Enabled. Enables or disables the SGXLEPUBKEYHASHx write feature. Options: - Enabled: enables the SGXLEPUBKEYHASHx write feature. - Disabled: disables the SGXLEPUBKEYHASHx write feature.	Enabled
SGXLEPUBKEYHASH0	This parameter is displayed when SGXLEPUBKEYHASHx Write Enable is set to Enabled. Sets bytes 0–7 for SGX to boot the SGX Launch Enclave Public Key Hash.	0
SGXLEPUBKEYHASH1	This parameter is displayed when SGXLEPUBKEYHASHx Write Enable is set to Enabled.	0

Parameter	Description	Default
	Sets bytes 8–15 for SGX to boot the SGX Launch Enclave Public Key Hash.	
SGXLEPUBKEYHASH2	This parameter is displayed when SGXLEPUBKEYHASHx Write Enable is set to Enabled . Sets bytes 16–23 for SGX to boot the SGX Launch Enclave Public Key Hash.	0
SGXLEPUBKEYHASH3	This parameter is displayed when SGXLEPUBKEYHASHx Write Enable is set to Enabled . Sets bytes 24–31 for SGX to boot the SGX Launch Enclave Public Key Hash.	0
SGX Auto MP Registration	This parameter is displayed when SW Guard Extensions (SGX) is set to Enabled . Enables or disables the SGX auto-MP registration agent, which is used by the SGX to register at the platform. Options: ● Enabled: enables the SGX auto-MP registration agent. ● Disabled: disables the SGX auto-MP registration agent.	Disabled
PSMI Configuration	Sets PSMI parameters. For details, refer to 3.4.1.1 PSMI Configuration .	-

3.4.1.1 PSMI Configuration

[Figure 3-69](#) shows the **PSMI Configuration** screen.

Figure 3-69 PSMI Configuration Screen

For a description of the parameters on the **PSMI Configuration** screen, refer to [Table 3-49](#).

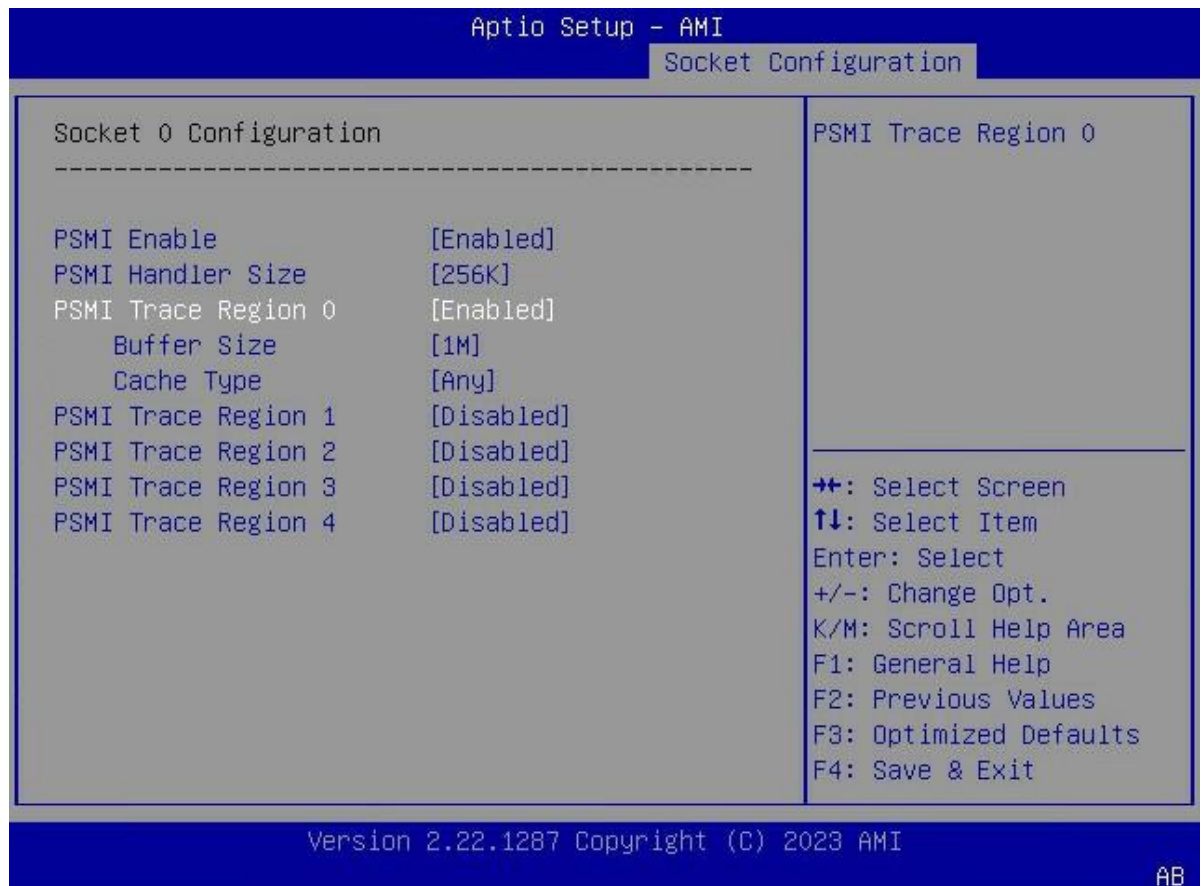
Table 3-49 Parameter Descriptions for the PSMI Configuration Screen

Parameter	Description	Default
Global PSMI Enable	Enables or disables global PSMI. Options: - Enabled: enables global PSMI. After this parameter is set to Enabled, the following parameters are displayed. - Disabled: disables global PSMI. - Force setup: forced setting.	Enabled
Socket 0 Configuration	Sets the PSMI parameters of Socket 0, see Figure 3-70 .	-
Socket 1 Configuration	Sets the PSMI parameters of Socket 1, see Figure 3-70 .	-

**Note**

The items on the **Socket 0 Configuration** screen are the same as those on the **Socket 1 Configuration** screen. This manual uses the **Socket 0 Configuration** screen as an example.

Figure 3-70 Socket 0 Configuration Screen



For a description of the parameters on the **Socket 0 Configuration** screen, refer to [Table 3-50](#).

Table 3-50 Parameter Descriptions for the Socket 0 Configuration Screen

Parameter	Description	Default
PSMI Enable	Enables or disables PSMI. Options: - Enabled: enables PSMI. After this parameter is set to Enabled, the following parameters are displayed. - Disabled: disables PSMI.	Enabled
PSMI Handler Size	Sets the size of the PSMI handler. Options: 256K 512K 1M	256K

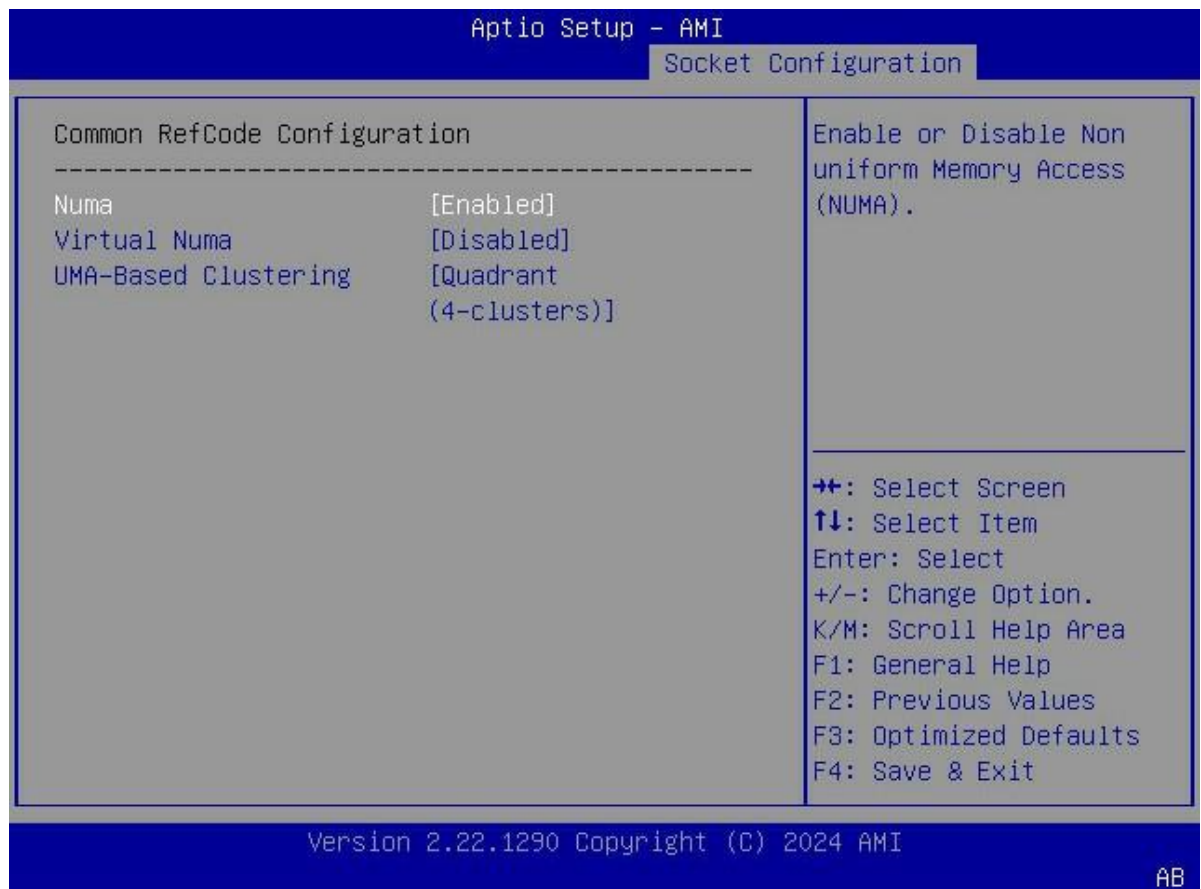
Parameter	Description	Default
PSMI Trace Region 0	Enables or disables PSMI trace region 0. Options: ● Enabled: enables PSMI trace region 0. After this parameter is set to Enabled, the following parameters are displayed. ● Disabled: disables PSMI trace region 0.	Disabled
Buffer Size	Sets the buffer size. Options: 1M–16G.	1M
Cache Type	Sets the cache type. Options: ● Any ● Uncached ● Write Combine	Any

**Note**

The configuration method for **PSMI Trace Region 0** is the same as that for other regions. In this guide, **PSMI Trace Region 0** is used as an example.

3.4.2 Common RefCode Configuration

Figure 3-71 shows the **Common RefCode Configuration** screen.

Figure 3-71 Common RefCode Configuration Screen

For a description of the parameters on the **Common RefCode Configuration** screen, refer to [Table 3-51](#).

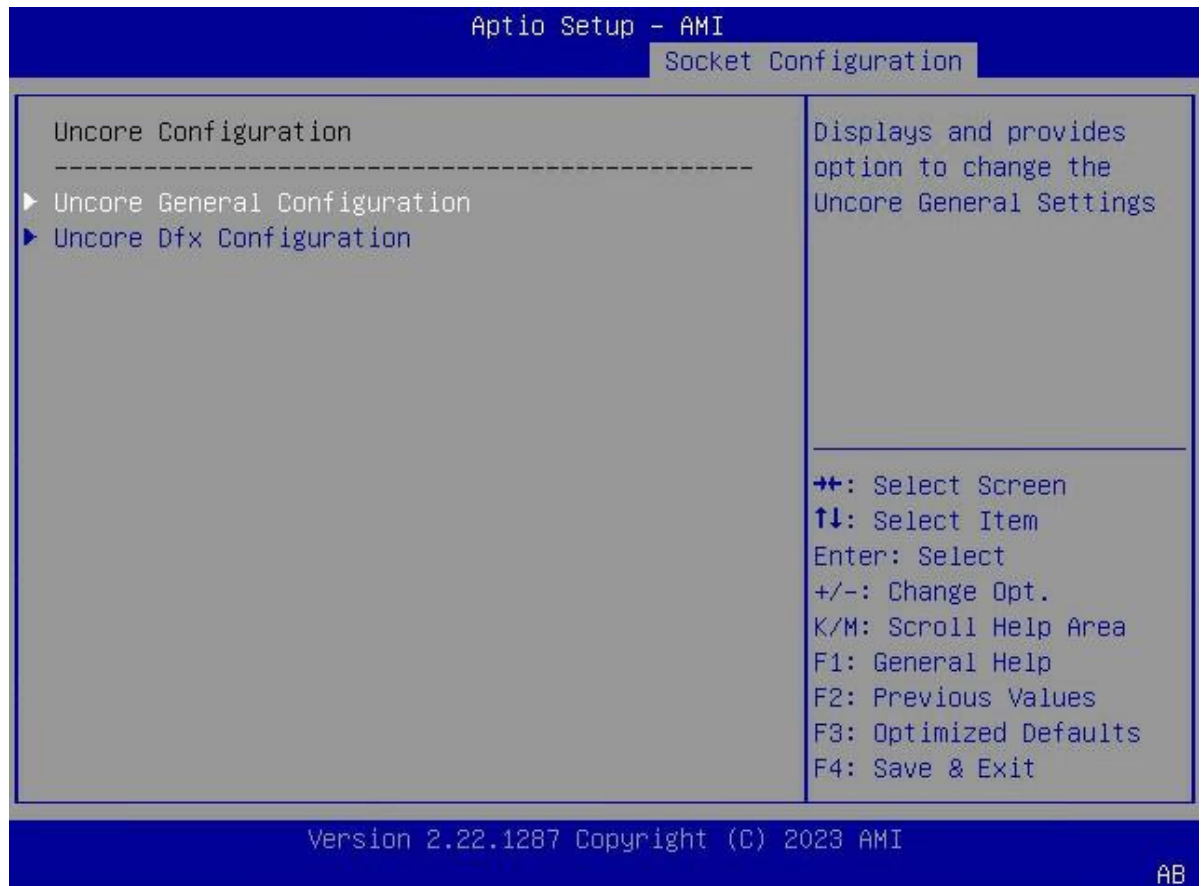
Table 3-51 Parameter Descriptions for the Common RefCode Configuration Screen

Parameter	Description	Default
Numa	Enables or disables Numa. Options: ● Enabled: enables Numa. ● Disabled: disables Numa.	Enabled
Virtual Numa	Enables or disables virtual Numa. Options: ● Enabled: enables virtual Numa. ● Disabled: disables virtual Numa.	Disabled
UMA-Based Clustering	UBC mode is a UMA -based cluster configuration. Select the UBC mode. Options: ● Hemisphere(2-clusters) ● Quadrant(4-clusters)	Quadrant(4-clusters)

3.4.3 Uncore Configuration

Figure 3-72 shows the **Uncore Configuration** screen.

Figure 3-72 Uncore Configuration Screen



For a description of the parameters on the **Uncore Configuration** screen, refer to [Table 3-52](#).

Table 3-52 Parameter Descriptions for the Uncore Configuration Screen

Parameter	Description
Uncore General Configuration	Sets Uncore general parameters. For details, refer to 3.4.3.1 Uncore General Configuration .
Uncore Dfx Configuration	Sets Uncore Dfx parameters. For details, refer to 3.4.3.2 Uncore Dfx Configuration .

3.4.3.1 Uncore General Configuration

Figure 3-73 through Figure 3-74 show the **Uncore General Configuration** screen.

Figure 3-73 Uncore General Configuration Screen—1

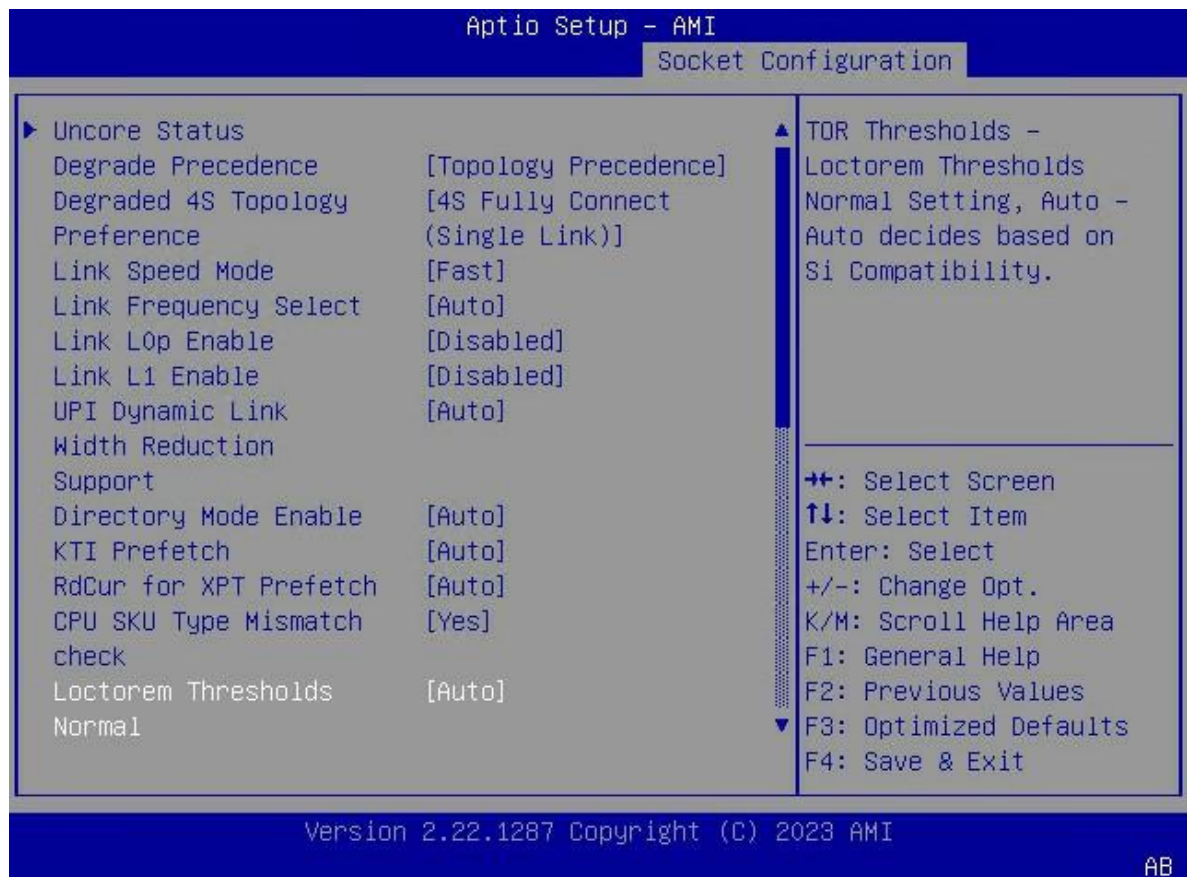
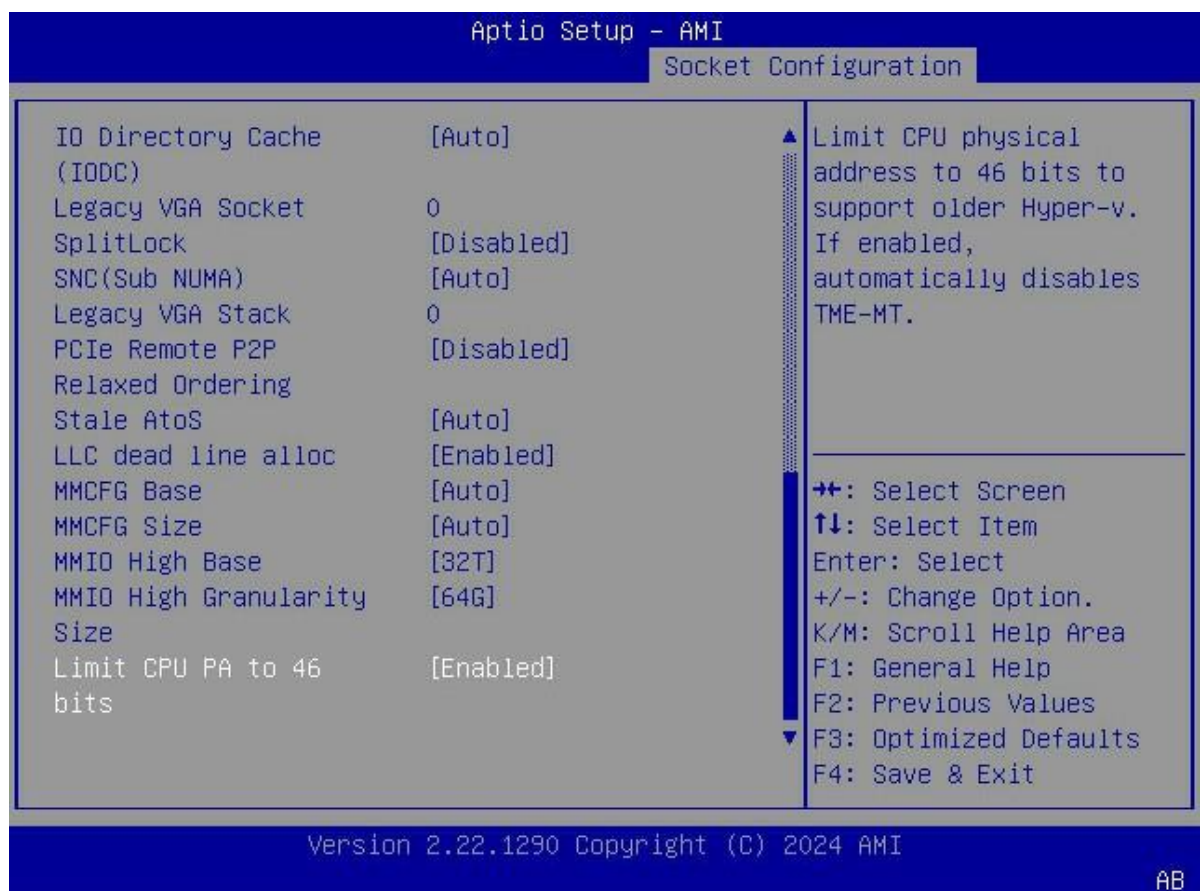


Figure 3-74 Uncore General Configuration Screen—2

For a description of the parameters on the **Uncore General Configuration** screen, refer to [Table 3-53](#).

Table 3-53 Parameter Descriptions for the Uncore General Configuration Screen

Parameter	Description	Default
Uncore Status	Press the Enter key to expand the Uncore Status area, see Figure 3-75 .	-
Degrade Precedence	Select a priority decrease method. Options: - Topology Precedence: decreases the topology priority when system options conflict. - Feature Precedence: decreases the feature priority when system options conflict.	Topology Precedence
Degrade 4S Topology Preference	When the system can be degraded, select 4S topology preference. Options: 4S Fully Connect (Single Link) 4S Ring (Dual Link)	4S Fully Connect (Single Link)
Link Speed Mode	Select the link speed mode.	Fast

Parameter	Description	Default
	Options: ● Fast ● Slow	
Link Frequency Select	Select the link speed. Options: ● 12.8 GT/s ● 14.4 GT/s ● 16.0 GT/s ● Auto: uses the maximum UPI rate that is supported.	Auto
Link L0p Enable	Enables or disables L0p. Options: ● Enabled: enables L0p. ● Disabled: disables L0p. ● Auto: enables L0p.	Disabled
Link L1 Enable	Enables or disables L1. Options: ● Enabled: enables L1. ● Disabled: disables L1. ● Auto: enables L1.	Disabled
UPI Dynamic Link Width Reduction Support	Enables or disables the support for UPI dynamic link width reduction. Options: ● Enabled: enables the support for UPI dynamic link width reduction. After this feature is enabled, when a hard fault of one or more UPI data channels is removed, the link size is dynamically adjusted to half the width. ● Disabled: disables the support for UPI dynamic link width reduction. ● Auto: enables the support for UPI dynamic link width reduction.	Auto
Directory Mode Enable	Enables or disables directory mode. Options: ● enabled: enables directory mode. ● Disabled: disables directory mode. ● Auto: enables directory mode.	Auto
KTI Prefetch	Enables or disables the KTI prefetch feature. Options: ● Enabled: enables the KTI prefetch feature.	Auto

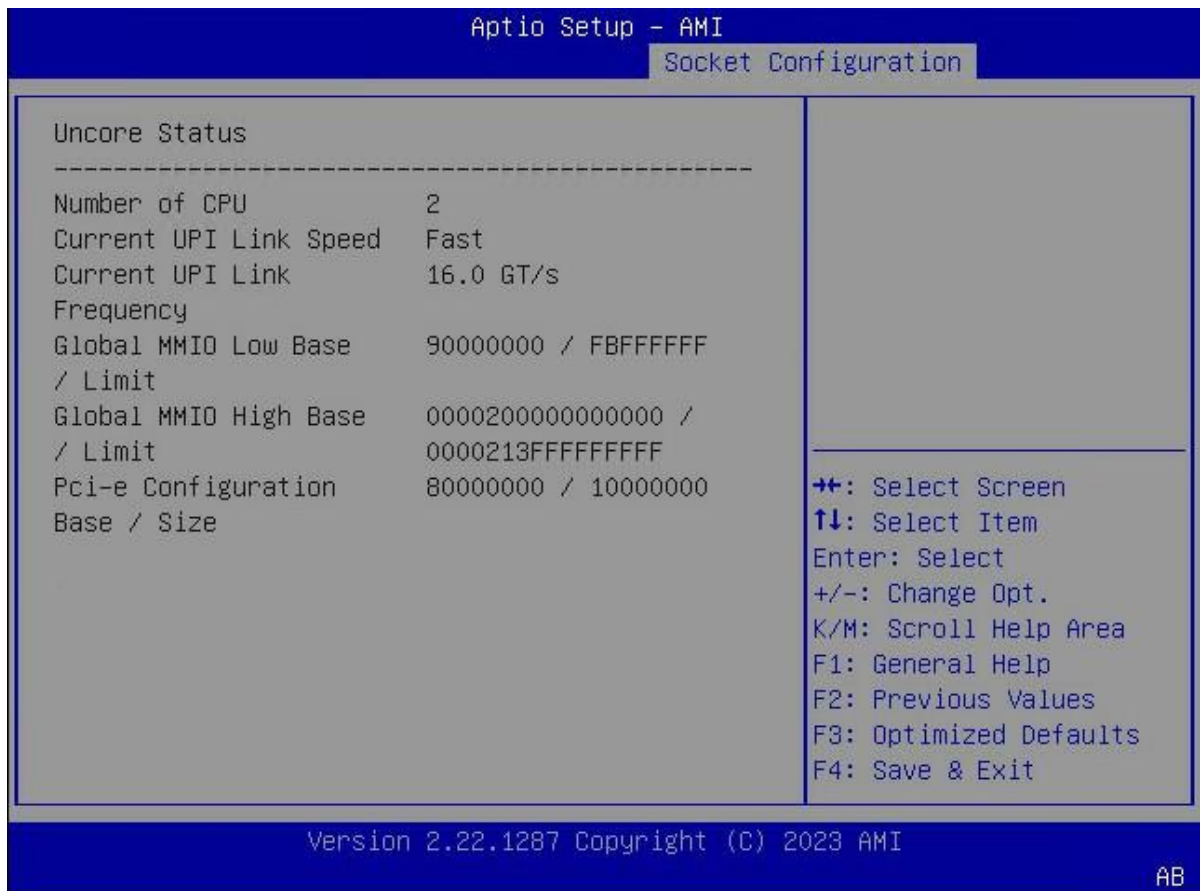
Parameter	Description	Default
	- Disabled: disables the KTI prefetch feature. - Auto: enables the KTI prefetch feature.	
RdCur for XPT Prefetch	Enables or disables RdCur for XPT preprocessing. Options: - Enabled: enables RdCur. - Disabled: disables RdCur. - Auto: same as the previous setting.	Auto
CPU SKU Type Mismatch check	Indicates whether to check CPU SKU type mismatches. Options: - Yes: performs the check. - No: performs no check.	Yes
Loctorem Thresholds Normal	Sets the normal setting of the Loctorem threshold in TDR thresholds. Options: - Disabled - Auto - Low - Medium - High	Auto
Loctorem Thresholds Empty	Sets the empty setting of the Loctorem threshold in TDR thresholds. Options: - Disable - Auto - Low - Medium - High	Auto
IO Directory Cache (IODC)	Monitor generation for remote InvItom (IIO), WCILF (cores), not memory lookup. Options: - Disabled - Auto - Enable for Remote InvItom Hybrid Push - InvItom AllocFlow - Enable for Remote InvItom Hybrid AllocNonAlloc - Enable for Remote InvItom and Remote WCILF	Auto
Legacy VGA Socket	Enter the slot number of the Legacy VGA. Range: 0–N. N=MAX_SOCKET-1	0

Parameter	Description	Default
SplitLock	Enables or disables SplitLock. Options: ● Enabled: enables SplitLock. ● Disabled: disables SplitLock. ● Auto: disables SplitLock.	Disabled
SNC (Sub NUMA)	Options: ● Disabled: supports 1-cluster and 4-IMC interleaving. ● Enabled SNC2 (2-clusters): supports 2-clusters SNC and 2-IMC way interleaving. ● Enabled SNC4 (4-clusters): supports 4-clusters SNC and 1-IMC way interleaving. ● Auto: automatically sets this parameter based on the CPU configuration: → HBM CPU: sets this parameter to Enabled SNC4 (4-clusters). → EMR CPU: sets this parameter to Enabled SNC2 (2-clusters). → SPR CPU: sets this parameter to Disabled.	Auto
Legacy VGA Stack	Enter the Legacy VGA IIO device. Range: 0–7.	0
PCIe Remote P2P Relaxed Ordering	Options: ● Enabled: enables P2P relaxed ordering. ● Disabled: forcibly implements P2P writes.	Disabled
Stale AtoS	Sets whether to enable transition between the following memory states: ● Snoop All Status ● Shared (S) Status Options: ● Enabled: enables transition. ● Disabled: disables transition. ● Auto: sets this parameter to Enabled when Optane memory is installed, and to Disabled when Optane memory is not installed.	Auto
LLC dead line alloc	Enables or disables LLC dead line allocation. Options: ● Enabled: enables LLC dead line allocation. ● Disabled: disables LLC dead line allocation. ● Auto: enables LLC dead line allocation.	Enabled
MMCFG Base	Select the MMCFG base. Options:	Auto

Parameter	Description	Default
	• 1G • 1.5G • 1.75G • 2G • 2.25G • 3G • Auto: sets this parameter in accordance with the number and type of identified CPUs.	
MMCFG Size	Select the MMCFG size. Options: • 128M • 256M • 512M • 1G • 2G • Auto: sets this parameter in accordance with the number and type of identified CPUs.	Auto
MMIO High Base	Select the high base of the MMIO. Options: • 56T • 40T • 32T • 24T • 16T • 4T • 2T • 1T • 512G • 3584T	32T
MMIO High Granularity Size	Select the MMIO high granularity size. The MMIO High space has a maximum of thirty-two granularities. The MMIO High resources of each stack are allocated as a multiple of the granularity. By default, one granularity is allocated to each stack. Options: • 1G • 4G • 16G • 64G • 256G • 1024G	64G

Parameter	Description	Default
Limit CPU PA to 46 bits	Enables or disables the restriction on the CPU PA to 46 bits to support the legacy Hyper-v feature. Options: - Enabled: enables the restriction and automatically disables TME-MT. - Disabled: disables the restriction.	Disabled

Figure 3-75 Uncore Status Screen



3.4.3.2 Uncore Dfx Configuration

Figure 3-76 shows the **Uncore Dfx Configuration** screen.

Figure 3-76 Uncore Dfx Configuration Screen

For a description of the parameters on the **Uncore Dfx Configuration** screen, refer to [Table 3-54](#).

Table 3-54 Parameter Descriptions for the Uncore Dfx Configuration Screen

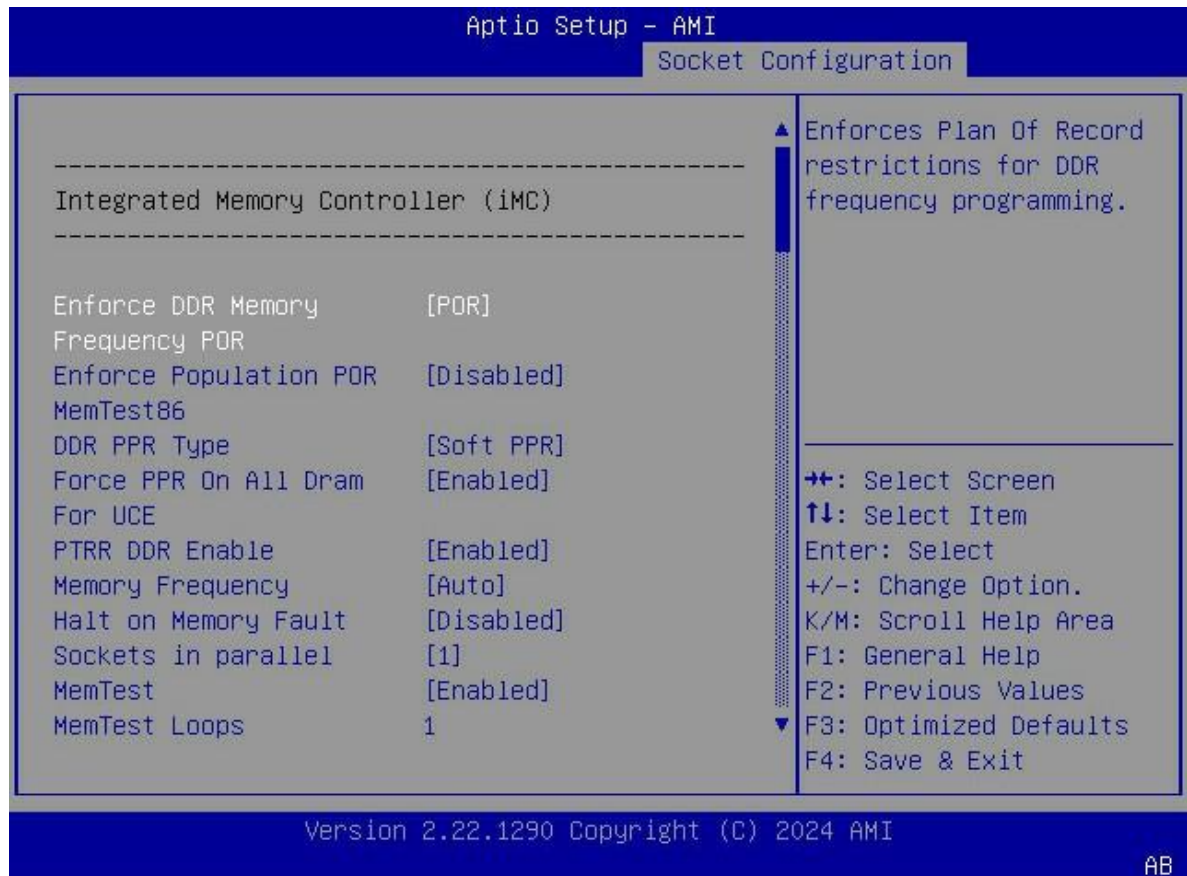
Parameter	Description	Default
CXL Security Level	Specifies the CXL security level. Options: - Fully Trusted: allows CXL devices to access CXL.\$ for both host-attached and device-attached memory ranges in the write-back (WB) address space. - Partially Trusted: allows CXL devices to access CXL.\$ for device-attached memory ranges only. - Untrusted: The host stops all requests on CXL.\$. - Auto: determined automatically in accordance with SI compatibility.	Auto
XPT Prefetch	Enables or disables the XPT prefetch feature. - Enabled: enables the XPT prefetch feature. - Disabled: disables the XPT prefetch feature.	Auto

Parameter	Description	Default
	Auto: automatic mode.	

3.4.4 Memory Configuration

Figure 3-77 through Figure 3-81 show the **Memory Configuration** screen.

Figure 3-77 Memory Configuration Screen—1



AB

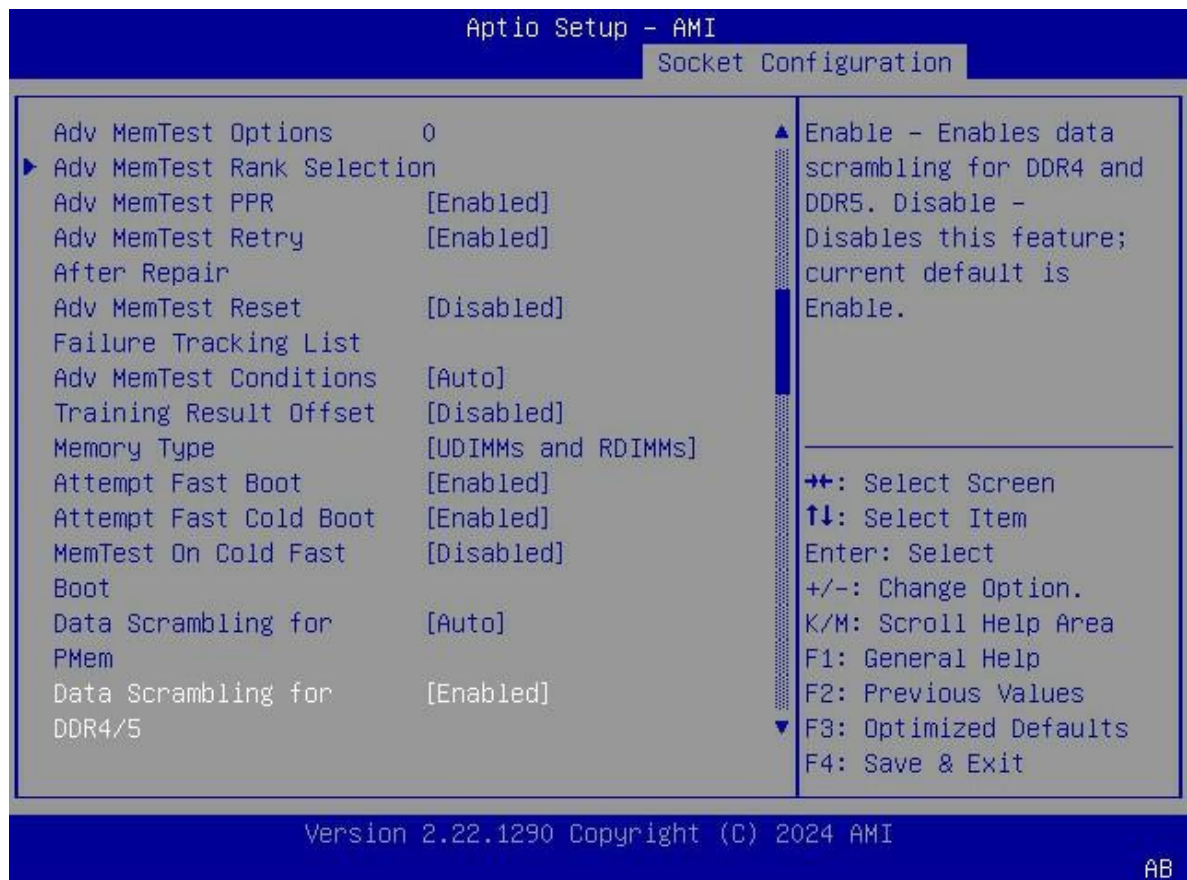
Figure 3-78 Memory Configuration Screen—2

Figure 3-79 Memory Configuration Screen—3

Aptio Setup - AMI		Socket Configuration
Allow Memory Test	[Enabled]	▲ Set normal operation duration interval (0 - 65535)
Correctable Error		
Scrambling Seed Low	41003	
Scrambling Seed High	54165	
Enable fADR	[Disabled]	
Enable ADR	[Enabled]	
Legacy ADR Mode	[Auto]	
Minimum System Memory Size	[2GB]	
NVDIMM Energy Policy	[Device-Managed]	
ADR Data Save Mode	[NVDIMMs]	
Custom Refresh Enable	[Disabled]	
DDR 2x Refresh Enable	[Auto]	
Adaptive Refresh	[Default]	
Management Level		
Opp read during WMM	[Enabled]	
Normal Operation	400	
Duration		
Version 2.22.1290 Copyright (C) 2024 AMI		
AB		

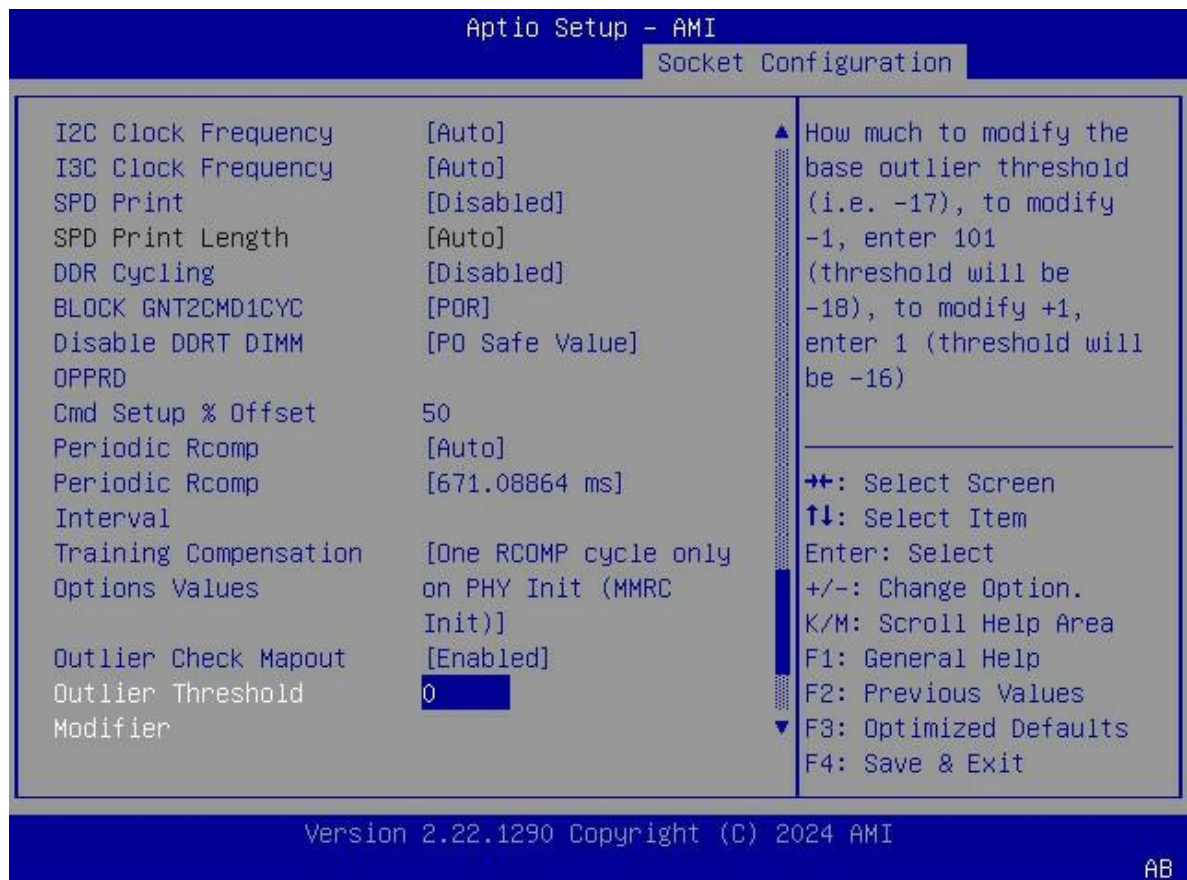
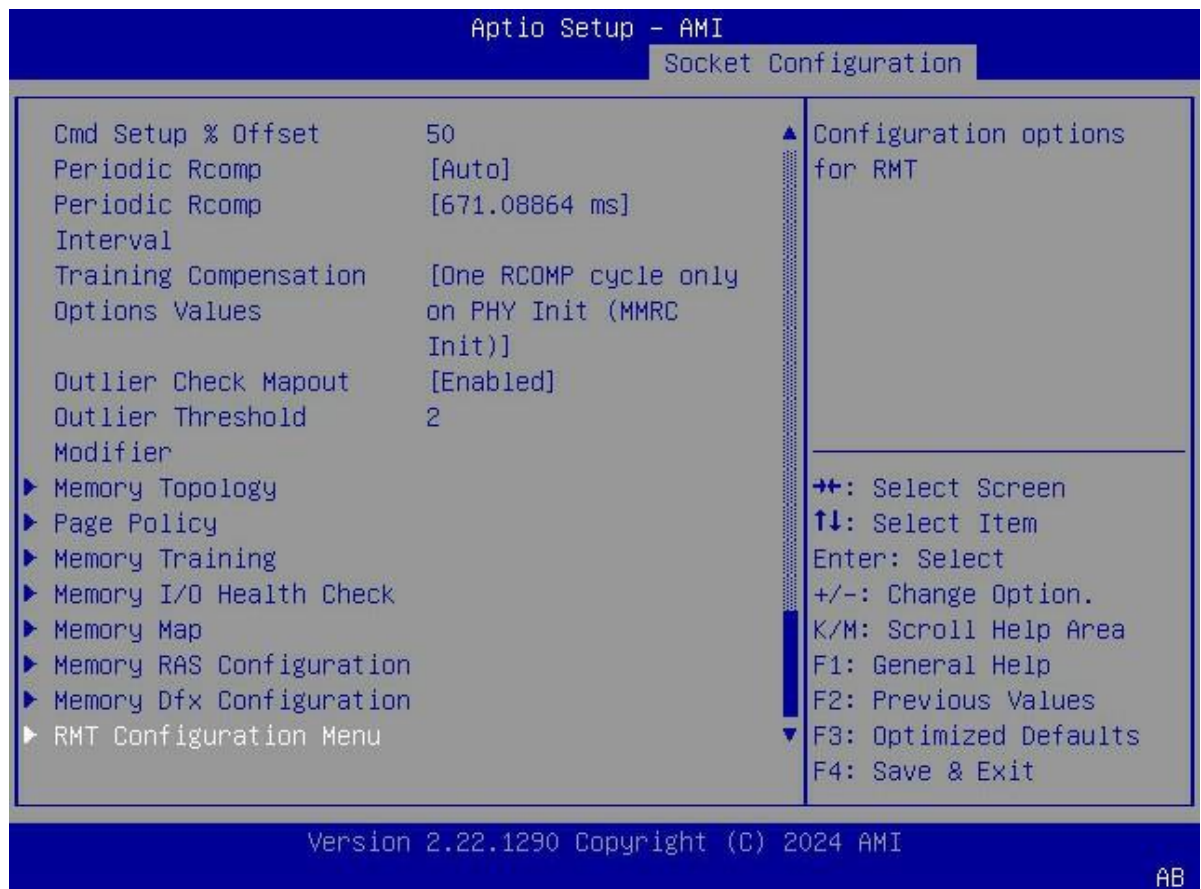
Figure 3-80 Memory Configuration Screen—4

Figure 3-81 Memory Configuration Screen—5



For a description of the parameters on the **Memory Configuration** screen, refer to [Table 3-55](#).

Table 3-55 Parameter Descriptions for the Memory Configuration Screen

Parameter	Description	Default
Enforce DDR Memory Frequency POR	Sets whether to apply POR rules for the DDR memory. Options: ● POR: enables POR rules. ● Disabled: disables POR rules.	POR
Enforce Population POR	Enables or disables POR rules. Options: ● Enabled: enables POR rules. When this parameter is set to Enabled, memory must be installed based on POR rules. ● Disabled: disable POR rules.	Disabled
MemTest86	After the MemTest86 (v9.4) is started, the Aptio Setup screen cannot be returned.	-
DDR PPR Type	Select a PPR type. Options:	Soft PPR

Parameter	Description	Default
	● Hard PPR ● Soft PPR ● PPR Disabled: disables PPR.	
Force PPR On All Dram For UCE	Sets whether to force all PPRs on the DRAM to be used for the UCE . Options: ● Enabled: yes. ● Disabled: no.	Disabled
PTRR DDR Enable	Enables or disables the PTRR DDR. ● Enabled: enables the PTRR DDR. The default value is Enabled, which is used only when the RDIMM configuration is independent of the VolMemMode configuration and mixed with the DDRT configuration, and the VolMeMode=1 LM is used for the mixed configuration. ● Disabled: disables PTRR DDR. When VolMemMode is equal to 2LM, the BIOS forcibly disables the PTRR DDR.	Enabled
Memory Frequency	Select the memory frequency. Options: ● Auto: automatically sets this parameter in accordance with the memory and CPU capability, and actual training status. ● 3200 ● 3600 ● 4000 ● 4400 ● 4800 ● 5200 ● 5600	Auto
Halt on Memory Fault	Enables or disables a halt when a memory fault occurs. Options: ● Enabled: enables the halt. ● Disabled: disables the halt.	Disabled
Sockets in parallel	Configures parallel CPU operation mode. ● ALL: All CPUs operate in parallel. ● 1: Only one CPU operates at a time. ● 2: Only two CPUs operate in parallel at a time. ● 4: Only four CPUs operate in parallel at a time.	ALL

Parameter	Description	Default
MemTest	Enables or disables the memory test during normal boot. Options: ● Enabled: enables the memory test. ● Disabled: disables the memory test.	Enabled
MemTest Loops	Enter the number of memory test cycles during normal boot. 0: unlimited number of times.	1
Adv MemTest Options	Provides advanced memory test options.	0
Adv MemTest Rank Selection	Sets the level of the advanced memory test. For details, refer to 3.4.4.1 Adv MemTest Rank Selection .	-
Adv MemTest PPR	Enables or disables advanced memory test PPR. Options: ● Enabled: enables advanced memory test PPR. ● Disabled: disables advanced memory test PPR.	Enabled
Adv MemTest Retry After Repair	Sets whether to perform a memory test again after repair. Options: ● Enabled: yes. ● Disabled: no.	Enabled
Adv MemTest Reset Failure Tracking List	Enables or disables failure tracking list reset after each memory test for multi-option performance tests. Options: ● Enabled: enables failure tracking list reset. ● Disabled: disables failure tracking list reset.	Disabled
Adv MemTest Conditions	Select a method for setting memory test conditions. Options: ● Disabled: No test conditions are set. ● Auto: sets the test conditions by test type. ● Manual: sets global test conditions.	Auto
Adv MemTest PMIC VDD Level	This parameter is displayed when Adv MemTest Conditions is set to Manual . Specifies the PMIC VDD and VDDQ levels in millivolts.	1100
Adv MemTest tWR	This parameter is displayed when Adv MemTest Conditions is set to Manual .	48

Parameter	Description	Default
	Specifies the tWR time between 48 tCKs and 96 tCKs.	
Adv MemTest tREFI	This parameter is displayed when Adv MemTest Conditions is set to Manual . Specifies the tREFI (refresh rate) time between 1850 ns and 7800 ns.	3900
Adv MemTest Pause	This parameter is displayed when Adv MemTest Conditions is set to Manual . Specifies a pause delay between 0 us and 256000 us. This is the time period during which refresh is disabled between the write sequence and the read sequence.	64000
Training Result Offset	Enables or disables training result offset. Options: ● Enabled: enables training result offset. ● Disabled: disables training result offset.	Disabled
Offset RecEnDelay	This parameter is displayed when Training Result Offset is set to Enabled . Enter the offset of the final RecEnDelay memory training result.	100
Offset TxDq	This parameter is displayed when Training Result Offset is set to Enabled . Enter the offset for the final TxDq memory training result.	100
Offset RxDq	This parameter is displayed when Training Result Offset is set to Enabled . Enter the offset of the final RxDq memory training result.	100
Offset TxVref	This parameter is displayed when Training Result Offset is set to Enabled . Enter the offset of the final TxVref memory training result.	100
Offset RxVref	This parameter is displayed when Training Result Offset is set to Enabled . Enter the offset of the final RxVref memory training result.	100
Offset RxSampler	This parameter is displayed when Training Result Offset is set to Enabled .	100

Parameter	Description	Default
	Enter the offset of the final RxSampler memory training result.	
Offset CmdAll	This parameter is displayed when Training Result Offset is set to Enabled . Enter the offset of the CmdAll final memory training result.	100
Offset CmdRxVref	This parameter is displayed when Training Result Offset is set to Enabled . Enter the offset of the final CmdRxVref memory training result.	100
Offset CmdRxSampler	This parameter is displayed when Training Result Offset is set to Enabled . Enter the offset of the CmdRxSampler final memory training result.	100
Offset CtlAll	This parameter is displayed when Training Result Offset is set to Enabled . Enter the offset of the final Ctlall memory training result.	100
Offset CtlVref	This parameter is displayed when Training Result Offset is set to Enabled . Enter the offset of the final CtlVref memory training result.	100
Memory Type	Select the supported DIMM type. Options: ● RDIMMs only: supports only RDIMMs. ● UDIMMs only: supports only UDIMMs. ● UDIMMs and RDIMMs: supports UDIMMs and RDIMMs.	UDIMMs and RDIMMs
Attempt Fast Boot	Enables or disables the attempt to use fast boot. Options: ● Enabled: enables the attempt to use fast boot. ● Disabled: disables the attempt to use fast boot.	Enabled
Attempt Fast Cold Boot	Enables or disables the attempt to use fast cold boot. Options: ● Enabled: enables the attempt to use fast cold boot. ● Disabled: disables the attempt to use fast cold boot.	Enabled
MemTest On Cold Fast Boot	Enables or disables the memory test during fast boot.	Disabled

Parameter	Description	Default
	Options: ● Enabled: enables the memory test. ● Disabled: disables the memory test.	
Data Scrambling for PMem	Enables or disables data scrambling for the PMem. Options: ● Enabled: enables data scrambling for the PMem. ● Disabled: disables data scrambling for the PMem. ● Auto: sets this parameter based on the stepping configuration.	Auto
Data Scrambling for DDR4/5	Enables or disables data scrambling for DDR4/5. Options: ● Enabled: enables data scrambling for DDR4/5. ● Disabled: disables data scrambling for DDR4/5.	Enabled
Allow Memory Test Correctable Error	Enables or disables the correctable error feature during a memory test. Options: ● Enabled: logs errors and enables the correctable error feature (DIMM level is not removed). ● Disabled: logs errors and disables the correctable error feature (DIMM level is removed).	Enabled
Scrambling Seed Low	Lower 32 bits of the scrambling seed.	41003
Scrambling Seed High	Upper 32 bits of the scrambling seed.	54165
Enable fADR	Enables or disables the fADR feature. Options: ● Enabled: enables the fADR feature. ● Disabled: disables the fADR feature.	Disabled
Enable ADR	This parameter is displayed when Enable fADR is set to Disabled . Enables or disables the storage of memory information upon a power failure. Options: ● Enabled: enables the storage of memory information upon a power failure. ● Disabled: disables the storage of memory information upon a power failure.	Enabled
Legacy ADR Mode	This parameter is displayed when Enable fADR is set to Disabled . Enables or disables the storage of memory information upon a power failure in legacy mode.	Auto

Parameter	Description	Default
	Options: ● Enabled: enables the storage of memory information upon a power failure in legacy mode. ● Disabled: disables the storage of memory information upon a power failure in legacy mode. ● Auto: dynamically checks whether the conditions for enabling the storage of memory information upon a power failure in legacy mode are met, based on the environment. If yes, the system enables the function. If no, the system disables the function.	
Minimum System Memory Size	This parameter is displayed when Enable fADR is set to Disabled . Minimum memory size allocated to system memory when only JEDEC NVDIMM is present. Options: ● 2GB ● 4GB ● 6GB ● 8GB	2GB
fADR Configuration	This parameter is displayed when EnabledfADR is set to Enabled . For details, refer to 3.4.4.2 fADR Configuration .	-
NVDIMM Energy Policy	Sets the NVDIMM energy policy. Options: ● Device-Managed ● Host-Managed	Device-Managed
ADR Data Save Mode	Sets ADR data storage mode. Options: ● Disabled: disables ADR data storage mode. ● Batterybacked DIMMS ● NVDIMMs ● Copy to Flash: copies data to the flash.	NVDIMMs
Check PCH_PM_STS	This parameter is hidden when ADR Data Save Mode is set to NVDIMMs . This parameter is displayed in other modes. Sets whether to use the PCH_PM_STS register as a recovery metric. Options: ● Enabled: uses the PCH_PM_STS register as a recovery metric.	Disabled

Parameter	Description	Default
	Disabled: disables the use of the PCH_PM_STS register as a recovery metric.	
Check PlatformDetectADR	This parameter is hidden when ADR Data Save Mode is set to NVDIMMs. This parameter is displayed in other modes. Sets whether to use the PlatformDetectADR feature as a recovery metric. Options: - Enabled: uses the PlatformDetectADR feature as a recovery metric. - Disabled: disables the use of the PlatformDetectADR feature as a recovery metric.	Disabled
Custom Refresh Enable	Enables or disables the custom memory refresh rate. Options: - Enabled: enables the custom memory refresh rate. - Disabled: disables the custom memory refresh rate.	Disabled
Custom Refresh Rate	This parameter is displayed when Custom Refresh Enable is set to Enabled. Enter the custom memory refresh rate.	20
DDR 2x Refresh Enable	Enables or disables the DDR 2x refresh feature. Options: - Enabled: enables the DDR 2x refresh feature. - Disabled: disables the DDR 2x refresh feature. - Auto: automatic mode.	Auto
Adaptive Refresh Management Level	Sets the adaptive refresh management level when refresh management is required. Options: - Default: default. - Level A - Level B - Level C	Default
Opp read during WMM	Enables or disables issuing read commands opportunistically during WMM. Options: - Enabled: enables issuing read commands opportunistically during WMM. - Disabled: disables issuing read commands opportunistically during WMM.	Enabled

Parameter	Description	Default
Normal Operation Duration	Enter the normal operation duration, range: 0–65535, unit: seconds.	400
I2C Clock Frequency	Select the DDR5 I2C clock frequency for SPD-based access. Options: ● Auto ● 400 kHz in I2C mode ● 700 kHz in I2C mode ● 1 MHz in I2C mode	Auto
I3C Clock Frequency	Select the DDR5 I3C clock frequency for SPD-based access. Options: ● Auto: dynamically adjusts the frequency based on the CPU status. ● 4 MHz in I3C mode ● 6 MHz in I3C mode ● 8 MHz in I3C mode ● 10 MHz in I3C mode	Auto
SPD Print	Enables or disables SPD-based printing. Options: ● Enabled: enables SPD-based printing. ● Disabled: disables SPD-based printing.	Disabled
SPD Print Length	This parameter is displayed when SPD Print is set to Enabled . Select the length for SPD-based printing. Options: ● Auto: prints all SPD bytes. ● 256 Bytes ● 512 Bytes	Auto
DDR Cycling	Enables or disables the DDR cycling feature. Options: ● Enabled: enables the DDR cycling feature. When this parameter is set to Enabled, the MRC will bear pressure. ● Disabled: disables the DDR cycling feature.	Disabled
BLOCK GNT2CMD1CYC	Enables or disables the BLOCK GNT2CMD1CYC feature. Options: ● POR: enables the BLOCK GNT2CMD1CYC feature.	POR

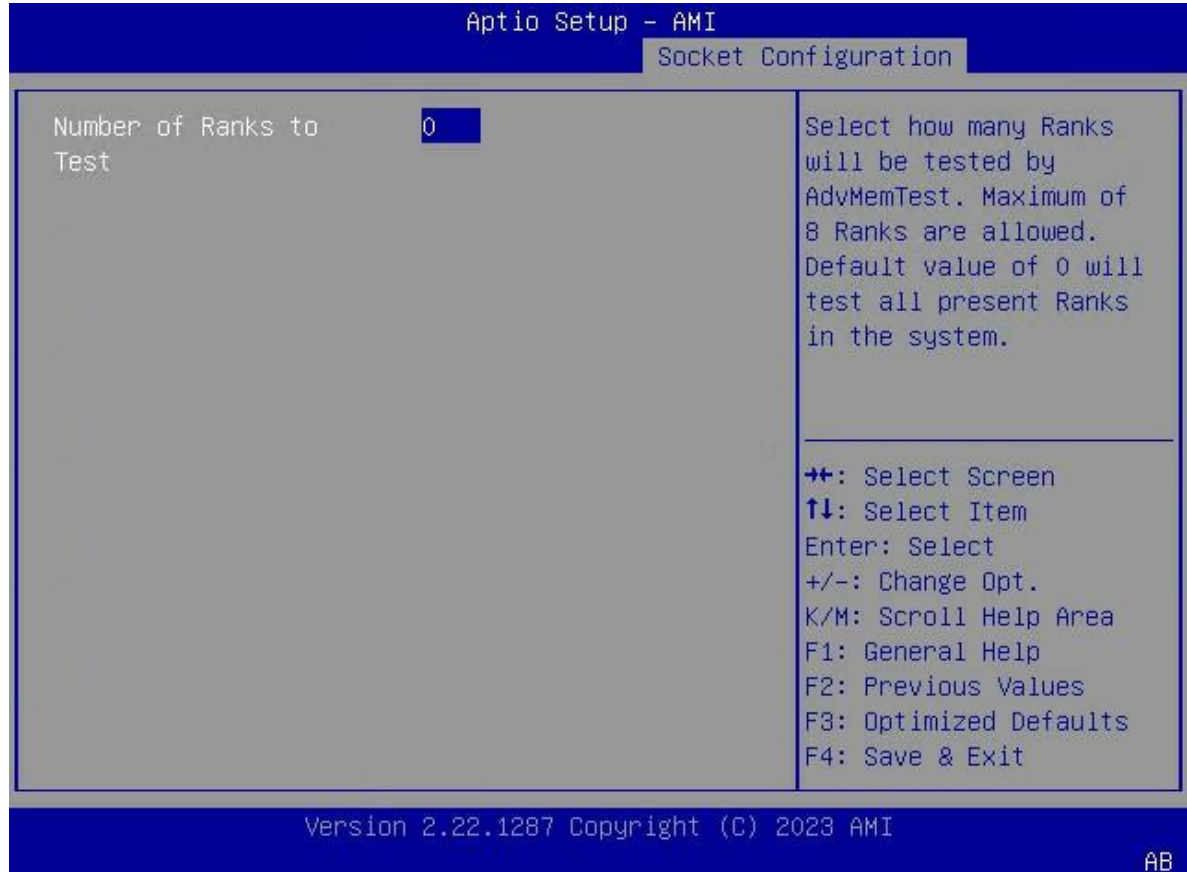
Parameter	Description	Default
	PO Safe Value: disables the BLOCK GNT2CMD1 CYC feature.	
Disabled DDRT DIMM OPPRD	Enables or disables the DDRT DIMM OPPRD feature. Options: - POR: enables the DDRT DIMM OPPRDC feature. - PO Safe Value: disables the DDRT DIMM OPPRD feature.	PO Safe Value
Cmd Setup % Offset	The ratio of "Cmd Setup" to "hold" in percentage is used as the offset of the latest command training result. Range: 0–100.	50
Periodic Rcomp	Enables or disables the periodic memory Rcomp. Options: - Enabled: enables the periodic memory Rcomp. - Disabled: disables the periodic memory Rcomp. - Auto: keeps the current setting.	Auto
Periodic Rcomp Interval	This parameter is hidden when Periodic Rcomp is set to Disabled . Select the interval for the periodic Rcomp.	671.08864 ms
Training Compensation Options Values	This parameter is displayed when Periodic Rcomp is set to Enabled . Select a training compensation option. Options: - One RCOMP cycle only on PHY Init (MMRC Init) - One RCOMP cycle after every JEDEC Init - One RCOMP cycle right before every training step	One RCOMP cycle only on PHY Init (MMRC Init)
Outlier Check Mapout	Enables or disables vendor-specific external detection and mapping of DIMMs. Options: - Enabled: enables vendor-specific external detection and mapping of DIMMs. - Disabled: disables vendor-specific external detection and mapping of DIMMs.	Enabled
Outlier Threshold Modifier	Modifies the basic threshold.	0
Memory Topology	Displays the memory information. For details, refer to 3.4.4.3 Memory Topology .	-
Page Policy	Sets page policies for memory. For details, refer to 3.4.4.4 Page Policy .	-
Memory Training	Sets memory training parameters.	-

Parameter	Description	Default
	For details, refer to 3.4.4.5 Memory Training .	
Memory I/O Health Check	Sets memory I/O status check parameters. For details, refer to 3.4.4.6 Memory I/O Health Check .	-
Memory Map	Sets memory mapping parameters. For details, refer to 3.4.4.7 Memory Map .	-
Memory RAS Configuration	Sets memory RAS parameters. For details, refer to 3.4.4.8 Memory RAS Configuration .	-
Memory Dfx Configuration	Sets memory Dfx parameters. For details, refer to 3.4.4.9 Memory Dfx Configuration .	-
RMT Configuration Menu	Sets RMT parameters. For details, refer to 3.4.4.10 RMT Configuration Menu .	-

3.4.4.1 Adv MemTest Rank Selection

Figure 3-82 shows the **Adv MemTest Rank Selection** screen.

Figure 3-82 Adv MemTest Rank Selection Screen



For a description of the parameters on the **Adv MemTest Rank Selection** screen, refer to [Table 3-56](#).

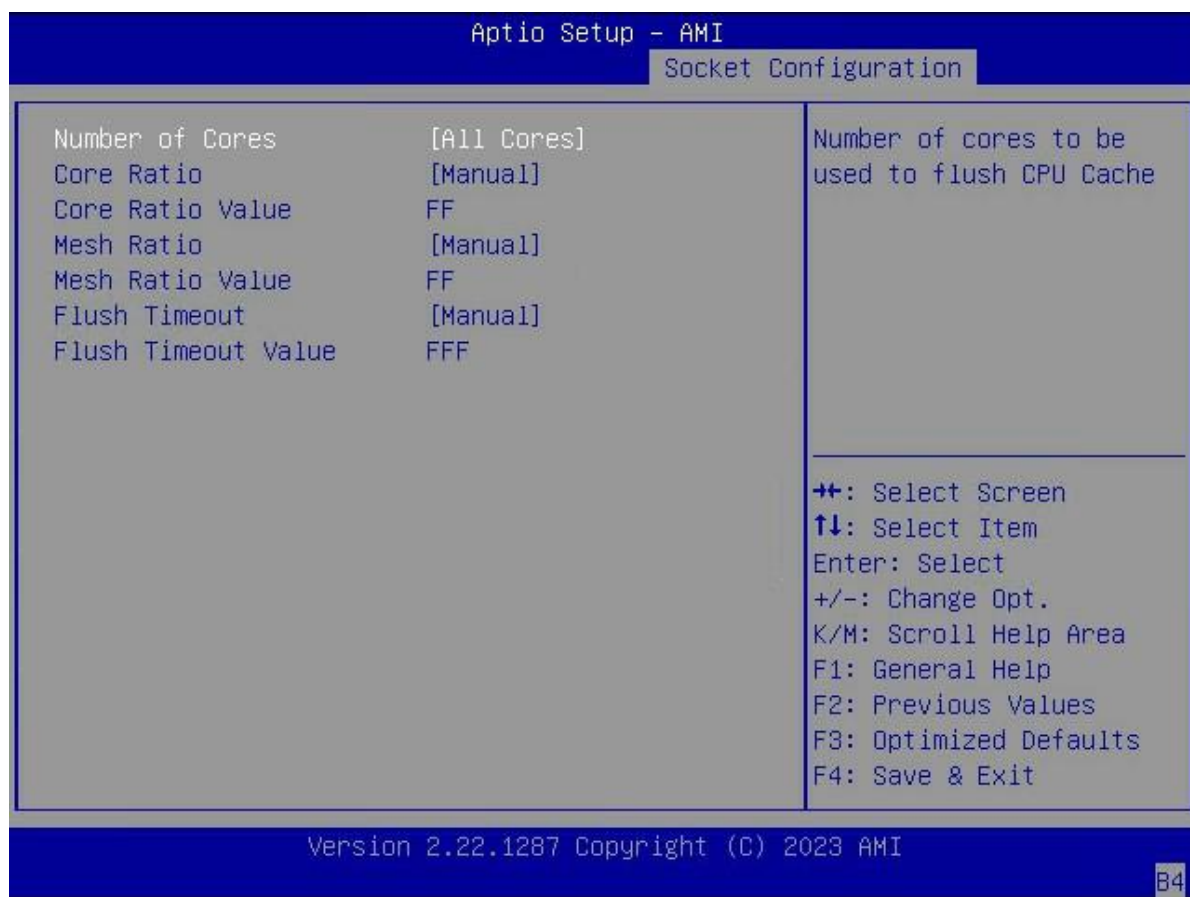
Table 3-56 Parameter Descriptions for the Adv MemTest Rank Selection Screen

Parameter	Description	Default
Number of Ranks to Test	Select the number of ranks to be tested by AdvMemTest. A maximum of eight ranks are allowed. The default value, which is 0, indicates that all present ranks in the test system will be tested.	0

3.4.4.2 fADR Configuration

[Figure 3-83](#) shows the **fADR Configuration** screen.

Figure 3-83 fADR Configuration Screen



For a description of the parameters on the **fADR Configuration** screen, refer to [Table 3-57](#).

Table 3-57 Parameter Descriptions for the fADR Configuration Screen

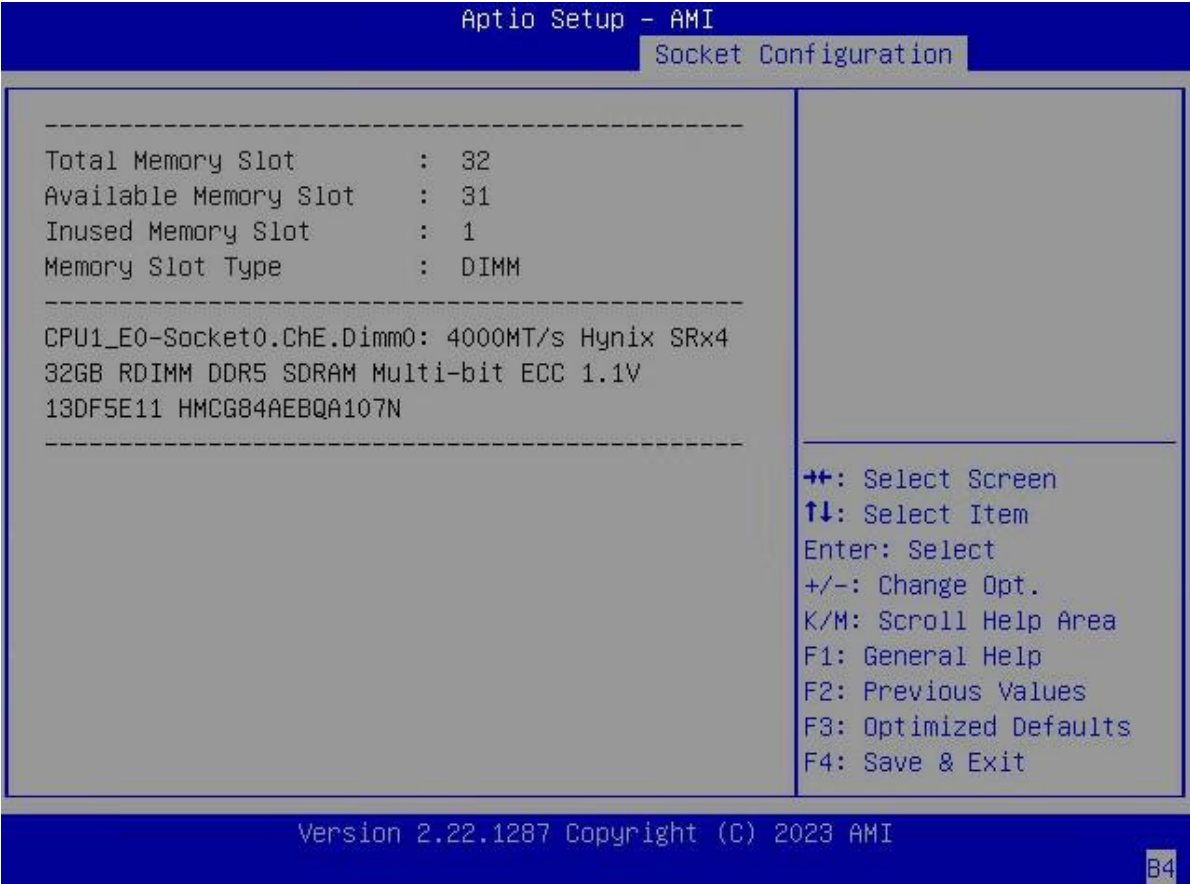
Parameter	Description	Default
Number of Cores	Select the number of cores to refresh the CPU cache.	All Cores

Parameter	Description	Default
	Options: ● 1 Core: one core. ● 4 Cores: four cores. ● All Cores: all cores.	
Core Ratio	Select the core ratio used during ADR . Options: ● Auto: The core ratio is set to Core/IA P1 Ratio. ● Manual: The core ratio is set to the value requested by the user.	Auto
Core Ratio Value	This parameter is displayed when Core Ratio is set to Manual . Enter the core ratio used during ADR.	FF
Mesh Ratio	Select the mesh ratio used during ADR. Options: ● Auto: The mesh ratio is set to Mesh/CLM P1 Ratio. ● Manual: The mesh ratio is set to the value requested by the user.	Auto
Mesh Ratio Value	This parameter is displayed when Mesh Ratio is set to Manual . Enter the mesh ratio used during ADR.	FF
Flush Timeout	Select the refresh timeout used during ADR. Options: ● Auto: The fresh timeout grows linearly with each enabled socket. ● Manual: The fresh timeout is set to the value requested by the user.	Auto
Flush Timeout Value	This parameter is displayed when Flush Timeout is set to Manual . Enter the refresh timeout used during ADR.	FFF

3.4.4.3 Memory Topology

[Figure 3-84](#) shows the **Memory Topology** screen.

Figure 3-84 Memory Topology Screen



For a description of the parameters on the **Memory Topology** screen, refer to [Table 3-58](#).

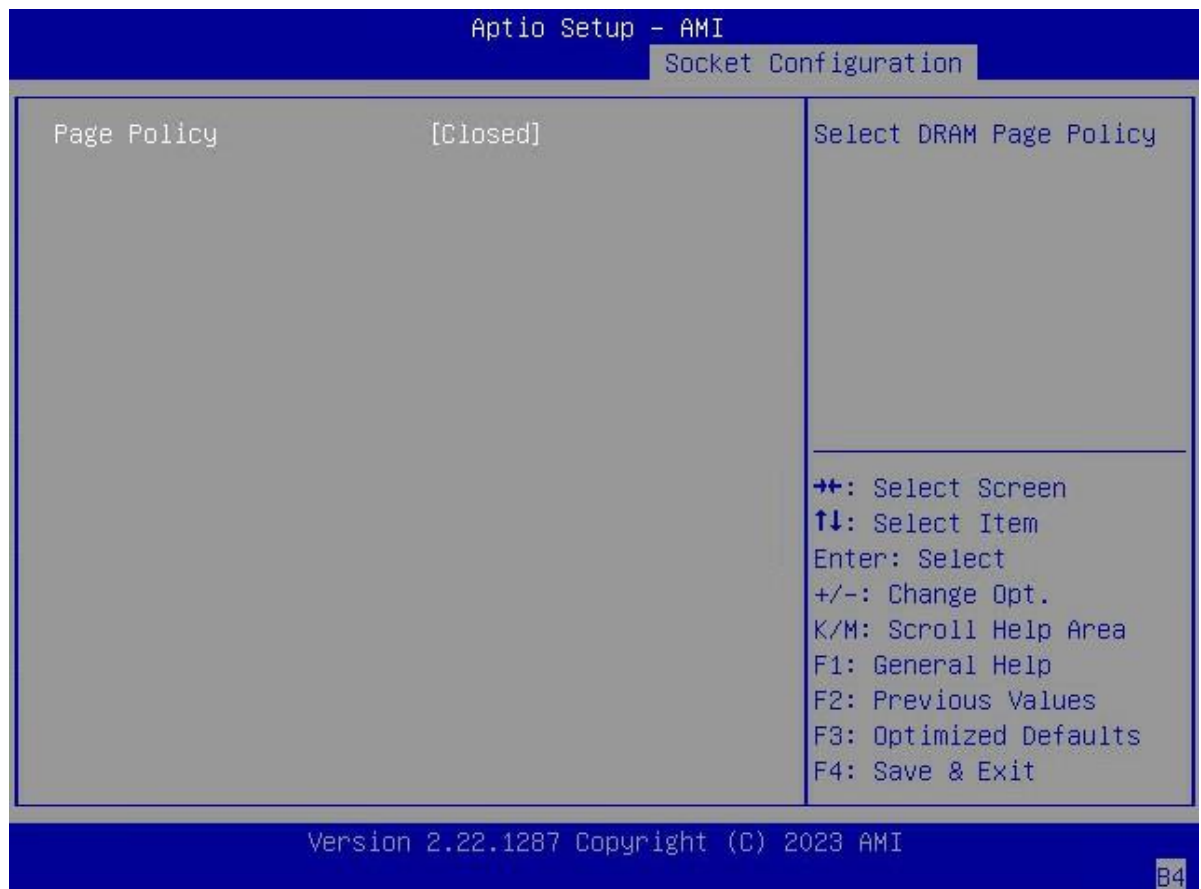
Table 3-58 Parameter Descriptions for the Memory Topology Screen

Parameter	Description
Total Memory Slot	Total number of memory slots.
Available Memory Slot	Number of available memory slots.
Inused Memory Slot	Number of memory slots being used.
Memory Slot Type	Type of memory slot.

3.4.4.4 Page Policy

[Figure 3-85](#) shows the **Page Policy** screen.

Figure 3-85 Page Policy Screen



For a description of the parameters on the **Page Policy** screen, refer to [Table 3-59](#).

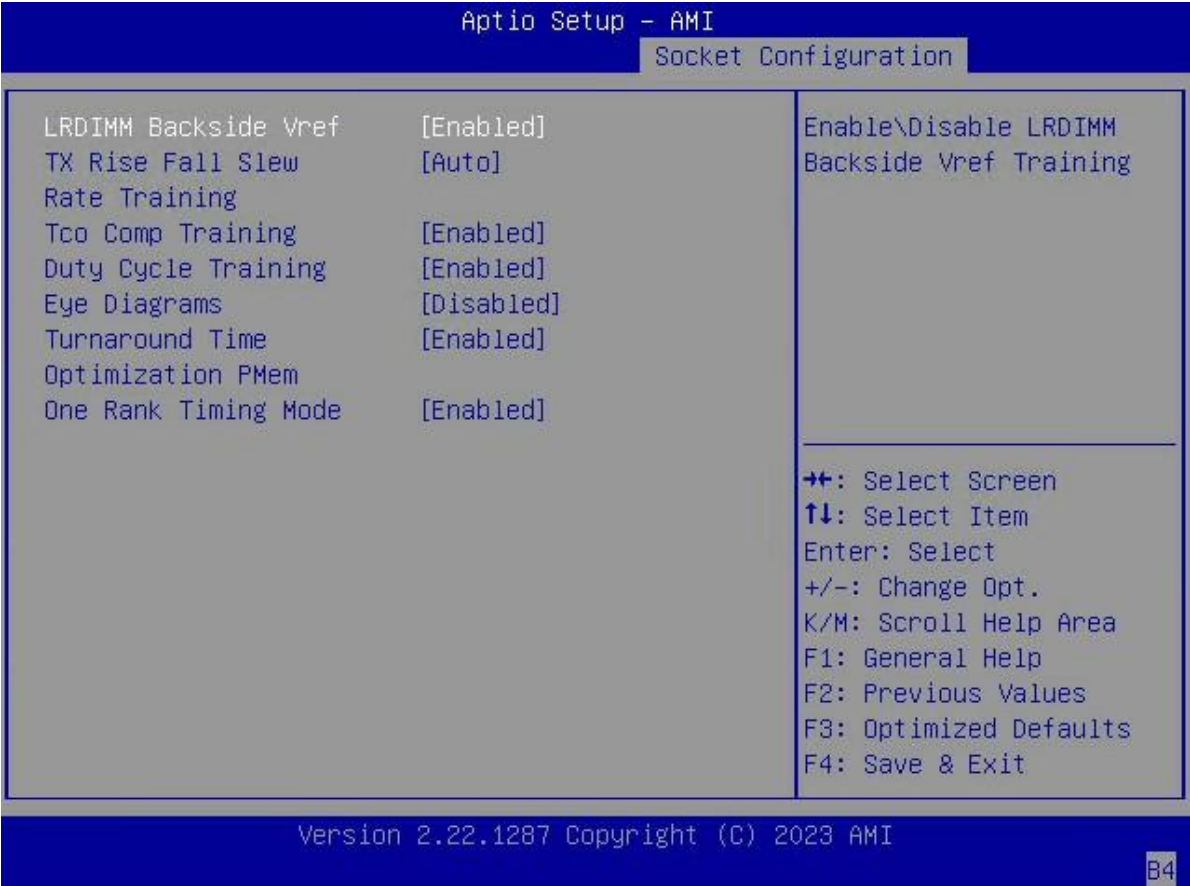
Table 3-59 Parameter Descriptions for the Page Policy Screen

Parameter	Description	Default
Page Policy	Enables or disables the memory page management policy. Options: ● Closed: disables the memory page management policy. ● Adaptive: adaptive.	Closed

3.4.4.5 Memory Training

[Figure 3-86](#) shows the **Memory Training** screen.

Figure 3-86 Memory Training Screen



For a description of the parameters on the **Memory Training** screen, refer to [Table 3-60](#).

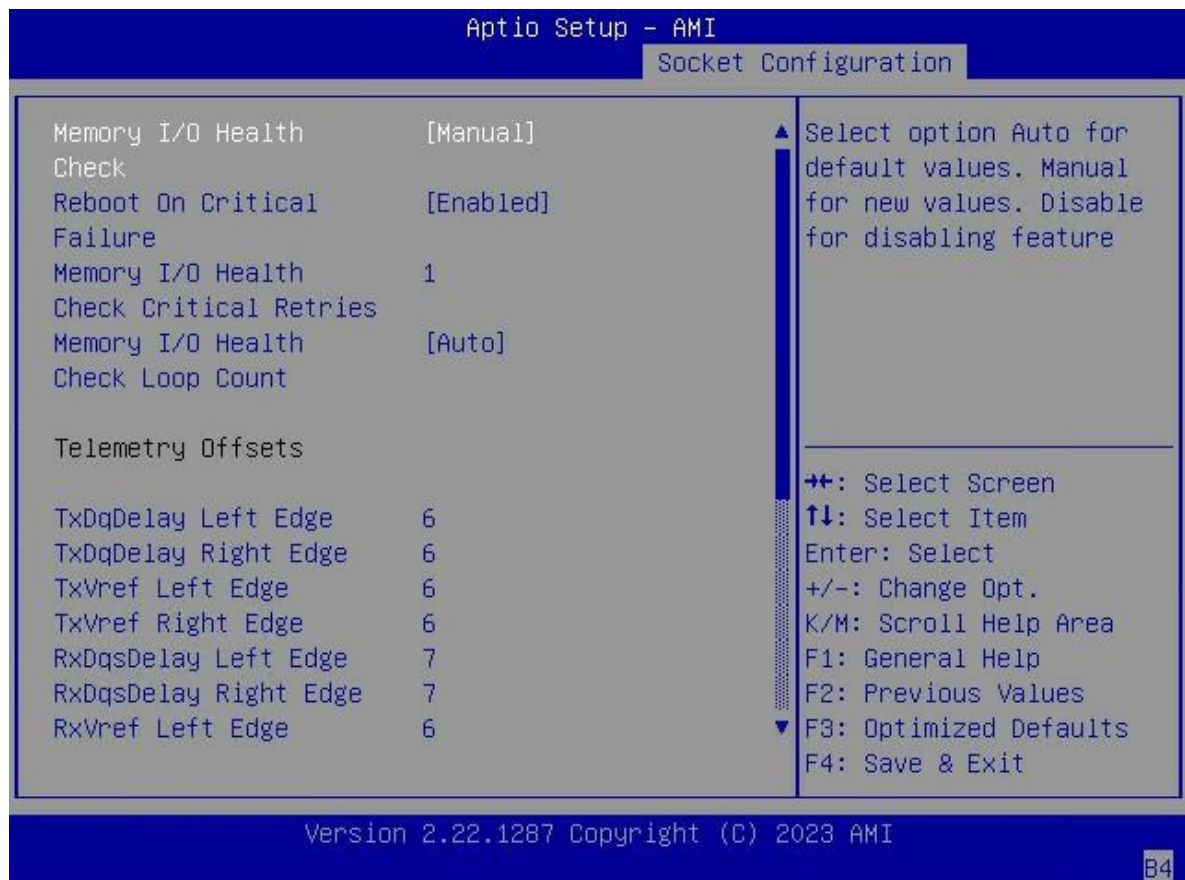
Table 3-60 Parameter Descriptions for the Memory Training Screen

Parameter	Description	Default
LRDIMM Backside Vref	Enables or disables LRDIMM Backside Vref training. Options: ● Enabled: enables LRDIMM Backside Vref training. ● Disabled: disables LRDIMM Backside Vref training.	Enabled
TX Rise Fall Slew Rate Training	Enables or disables TX Rise Fall Slew Rate training. Options: ● Enabled: enables TX Rise Fall Slew Rate training. ● Disabled: disables TX Rise Fall Slew Rate training. ● Auto: enables TX Rise Fall Slew Rate training when DDR Freq is equal to or greater than 2933.	Auto
Tco Comp Training	Enables or disables Tco Comp training. Options: ● Enabled: enables Tco Comp training.	Enabled

Parameter	Description	Default
	● Disabled: disables Tco Comp training.	
Duty Cycle Training	Enables or disables Duty Cycle training. Options: ● Enabled: enables Duty Cycle training. ● Disabled: disable Duty Cycle training.	Enabled
Eye Diagrams	Enables or disables Eye Diagrams for each level of Rx and TxDq. Options: ● Enabled: enables Eye Diagrams for each level of Rx and TxDq. ● Disabled: disables Eye Diagrams for each level of Rx and TxDq.	Disabled
Turnaround Time Optimization PMem	Enables or disables Turnaround Time optimization for PMem. Options: ● Enabled: enables Turnaround Time optimization for PMem. ● Disabled: disables Turnaround Time optimization for PMem.	Enabled
One Rank Timing Mode	Enables or disables One Rank Timing mode. Options: ● Enabled: enables One Rank Timing mode. ● Disabled: disables One Rank Timing mode.	Enabled

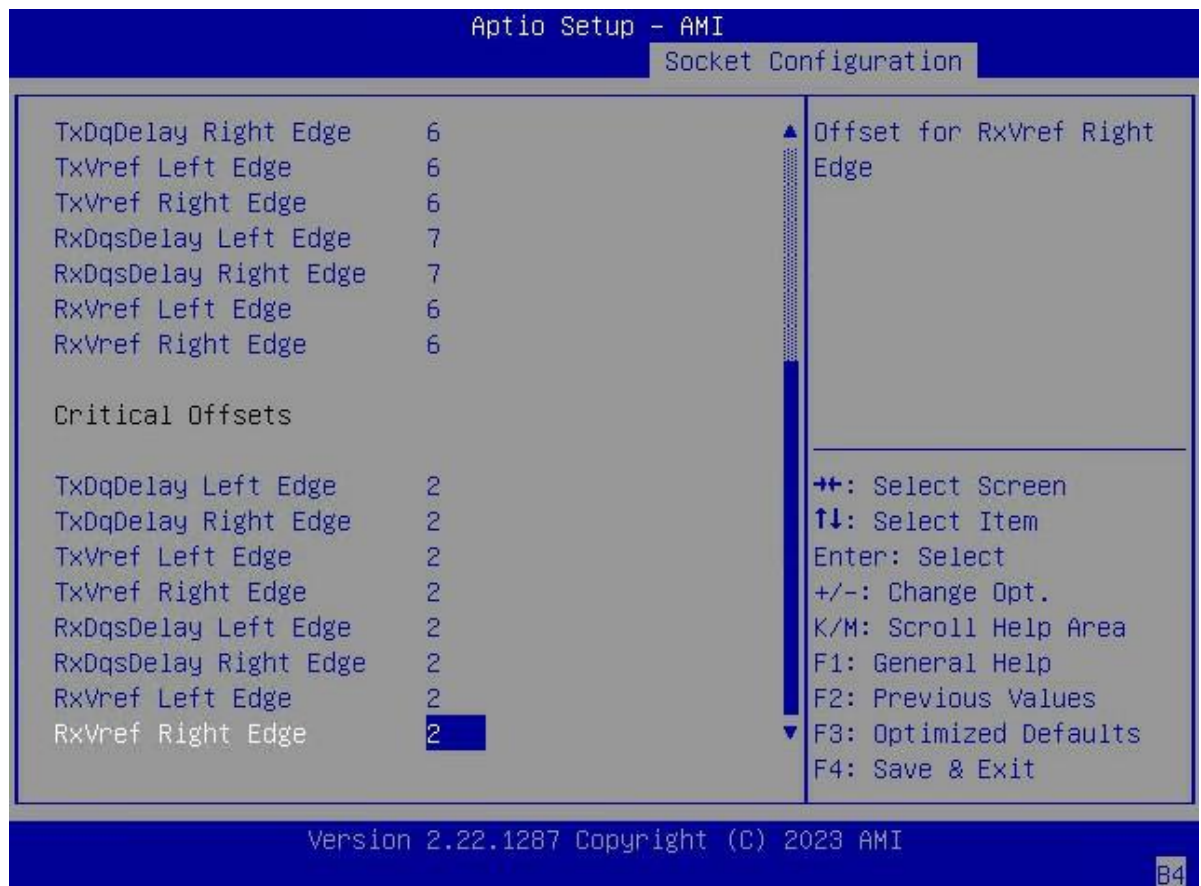
3.4.4.6 Memory I/O Health Check

Figure 3-87 through Figure 3-88 show the **Memory I/O Health Check** screen.

Figure 3-87 Memory I/O Health Check Screen—1

B4

Figure 3-88 Memory I/O Health Check Screen—2



For a description of the parameters on the **Memory I/O Health Check** screen, refer to [Table 3-61](#).

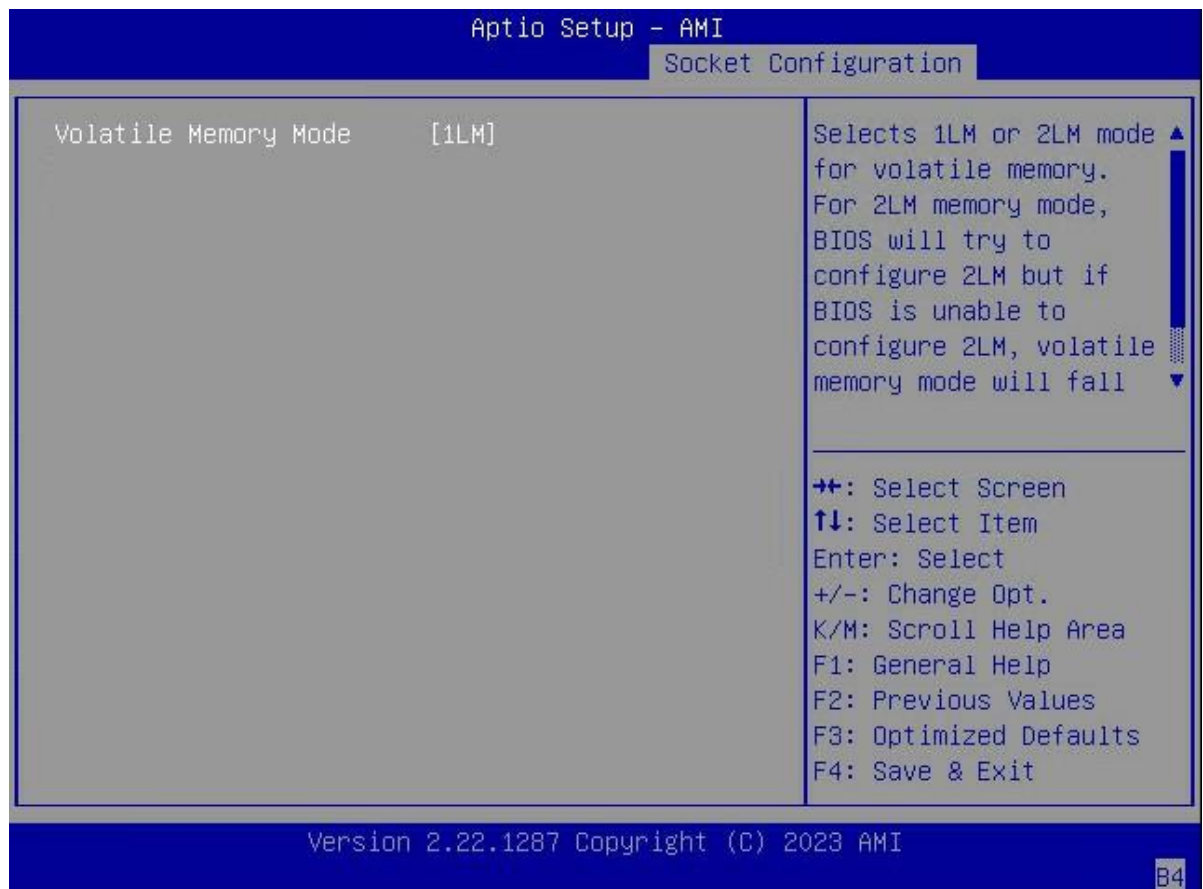
Table 3-61 Parameter Descriptions for the Memory I/O Health Check Screen

Parameter	Description	Default
Memory I/O Health Check	Enables or disables memory I/O health check. Options: ● Auto: enables the default check. ● Manual: enables the self-defined check. ● Disabled: disables memory I/O health check.	Auto
Reboot On Critical Failure	This parameter is displayed when Memory I/O Health Check is set to Manual . This feature determines whether to restart the system when a serious I/O error occurs. Options: ● Enabled: restarts the system. ● Disabled: does not restart the system.	Enabled

Parameter	Description	Default
Memory I/O Health Check Critical Retries	This parameter is displayed when Memory I/O Health Check is set to Manual and Reboot On Critical Failure is set to Enabled . Enter the number of system restart times, range: 0–7.	1
Memory I/O Health Check Loop Count	Sets the statistical method for collecting the number of CPGC test cycles for checking I/O status.	Auto
Telemetry Offsets		
TxDqDelay Left Edge	Enter the offset of the left edge of the TxDqDelay.	6
TxDqDelay Right Edge	Enter the offset of the right edge of the TxDqDelay.	6
TxVref Left Edge	Enter the offset of the left edge of the TxVref.	6
TxVref Right Edge	Enter an offset for the right edge of TxVref.	6
RxDqsDelay Left Edge	Enter the offset of the left edge of the RxDqsDelay.	7
RxDqsDelay Right Edge	Enter the offset of the right edge of the RxDqsDelay.	7
RxVref Left Edge	Enter the offset of the left edge of the RxVref.	6
RxVref Right Edge	Enter the offset of the right edge of the RxVref.	6
Critical Offsets		
TxDqDelay Left Edge	Enter the offset of the left edge of the TxDqDelay.	2
TxDqDelay Right Edge	Enter the offset of the right edge of the TxDqDelay.	2
TxVref Left Edge	Enter the offset of the left edge of the TxVref.	2
TxVref Right Edge	Enter an offset for the right edge of the TxVref.	2
RxDqsDelay Left Edge	Enter the offset of the left edge of the RxDqsDelay.	2
RxDqsDelay Right Edge	Enter the offset of the right edge of the RxDqsDelay.	2
RxVref Left Edge	Enter the offset of the left edge of the RxVref.	2
RxVref Right Edge	Enter the offset of the right edge of the RxVref.	2

3.4.4.7 Memory Map

Figure 3-89 shows the **Memory Map** screen.

Figure 3-89 Memory Map Screen

For a description of the parameters on the **Memory Map** screen, refer to [Table 3-62](#).

Table 3-62 Parameter Descriptions for the Memory Map Screen

Parameter	Description	Default
Volatile Memory Mode	Sets the volatile memory mode. Options: 1LM	1LM

3.4.4.8 Memory RAS Configuration

[Figure 3-90](#) through [Figure 3-91](#) show the **Memory RAS Configuration** screen.

Figure 3-90 Memory RAS Configuration Screen—1

Figure 3-91 Memory RAS Configuration Screen—2



For a description of the parameters on the **Memory RAS Configuration** screen, refer to [Table 3-63](#).

Table 3-63 Parameter Descriptions for the Memory RAS Configuration Screen

Parameter	Description	Default
Dynamic ECC Mode Selection	Enables or disables dynamic ECC mode selection. Options: - Enabled: enables dynamic ECC mode selection. - Disabled: disables dynamic ECC mode selection. - Enabled + Allow Partial Poison Mode: enables dynamic ECC mode selection and allows Partial Poison mode.	Enabled
Enable Pcode WA for SAI PG	Enables or disables the Pcode WA feature of the SAI PG. Options: - Enabled: enables the Pcode WA feature of the SAI PG. - Disabled: disables the Pcode WA feature of the SAI PG.	Disabled

Parameter	Description	Default
Mirror Mode	Sets the memory mirroring mode. Options: ● Full Mirror Mode: full mirroring mode. ● Partial Mirror Mode: partial mirroring mode. ● Disabled: disables mirroring mode.	Disabled
Mirror TAD0	Enables or disables mirroring on the entire memory for TAD0. Options: ● Enabled: enables mirroring on the entire memory for TAD0. After this feature is enabled, mirroring is enabled on the entire memory for TAD0. ● Disabled: disables mirroring for TAD0.	Disabled
UEFI ARM Mirror	Enables or disables UEFI ARM mirroring. Options: ● Enabled: enables UEFI ARM mirroring. ● Disabled: disables UEFI ARM mirroring.	Disabled
Memory Correctable Error Flood Policy	Select a memory correctable error flood policy. Options: ● Disabled: disables the support. ● Once ● Frequency	Frequency
Trigger SW Error Threshold	Enables or disables the sparing trigger SW error match threshold. Options: ● Enabled: enables the sparing trigger SW error match threshold. ● Disabled: disables the sparing trigger SW error match threshold.	Disabled
SW Per Bank Threshold	This parameter is displayed when Trigger SW Error Threshold is set to Enabled . Enter the sparing trigger SW error match threshold, range:1–0x7fff.	3
SW Correctable Error Time Window	This parameter is displayed when Trigger SW Error Threshold is set to Enabled . Enter the time window for correctable memory errors, range: 1–24.	24
Memory CE Accumulation Threshold	Select a memory correctable error accumulation threshold.	1200

Parameter	Description	Default
	Options: ● Disabled ● 960 ● 1200 ● 2400 ● 4800 ● 9600 ● 12000 ● 15000 ● 18000 ● 24000 ● 30000	
Memory CE Accumulation Time Window	This parameter is hidden when Memory CE Accumulation Threshold is set to Disabled . Enter the time window for memory correctable error accumulation, range: 1–24.	24
Memory CE Strom Threshold	Select the memory correctable error storm threshold. Options: ● Disabled ● 60 ● 120 ● 240 ● 480 ● 960 ● 1200	120
Memory CE Strom Time Window	This parameter is hidden when Memory CE Strom Threshold is set to Disabled . Enter the time window for correctable memory error storms. Range: 1–60.	1
Leaky bucket time window based interface	Enables or disables the interface based on the leaky bucket time window. Options: ● Enabled: enables the interface based on the leaky bucket time window. ● Disabled: disables the interface based on the leaky bucket time window.	Disabled
Leaky bucket time window based interface Hour	This parameter is displayed when Leaky bucket time window based interface is set to Enabled . Enter the number of hours as the size of the leaky bucket time window. Range: 0–3744.	24

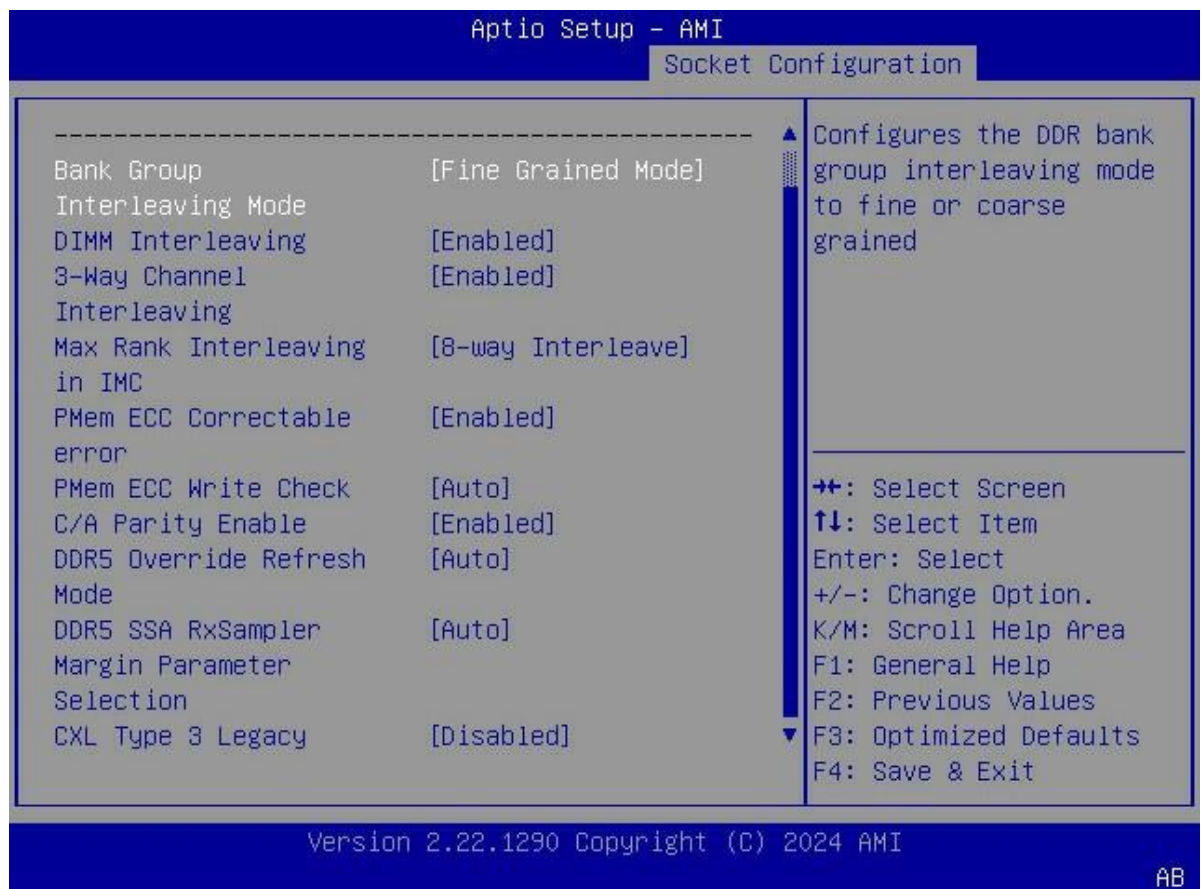
Parameter	Description	Default
Leaky bucket time window based interface Minute	This parameter is displayed when Leaky bucket time window based interface is set to Enabled . Enter the number of minutes as the size of the leaky bucket time window. Range: 0–60.	0
Leaky bucket low bit	This parameter is displayed when Leaky bucket time window based interface is set to Disabled . Enter the leaky bucket low bit, range: 1–41.	20
Leaky bucket high bit	This parameter is displayed when Leaky bucket time window based interface is set to Disabled . Enter the leaky bucket high bit, range: 1–41.	23
Partial Cache Line Sparing PCLS	Enables or disables the PCLS feature. Options: ● Enabled: enables the PCLS feature. ● Disabled: disables the PCLS feature.	Enabled
ADDDC Sparing	Enables or disables the sparing ADDDC feature. Options: ● Enabled: enables the sparing ADDDC feature. ● Disabled: disables the sparing ADDDC feature.	Disabled
Enable ADDDC Error Injection	This parameter is displayed when ADDDC Sparing is set to Enabled . Enables or disables ADDDC error injection. Options: ● Enabled: enables sparing ADDDC error injection. ● Disabled: disables sparing ADDDC error injection.	Enabled
Patrol Scrub	Enables or disables regular memory preventive maintenance. Options: ● Disabled: disables regular memory preventive maintenance. ● Enable at End of POST: enables regular memory preventive maintenance after POST.	Enable at End of POST
Patrol Scrub Interval	This parameter is displayed when Patrol Scrub is set to Enable at End of POST . Enter the time interval for regular memory preventive maintenance. Range: 1–24.	24
DDR5 ECS	Enables or disables ECS and result collection. Options: ● Enabled: enables ECS and disables result collection.	Enabled

Parameter	Description	Default
	- Disabled: disables ECS and result collection. - Enable ECS with Result Collection: enables ECS and result collection.	

3.4.4.9 Memory Dfx Configuration

Figure 3-92 shows the **Memory Dfx Configuration** screen.

Figure 3-92 Memory Dfx Configuration Screen



For a description of the parameters on the **Memory Dfx Configuration** screen, refer to [Table 3-64](#).

Table 3-64 Parameter Descriptions for the Memory Dfx Configuration Screen

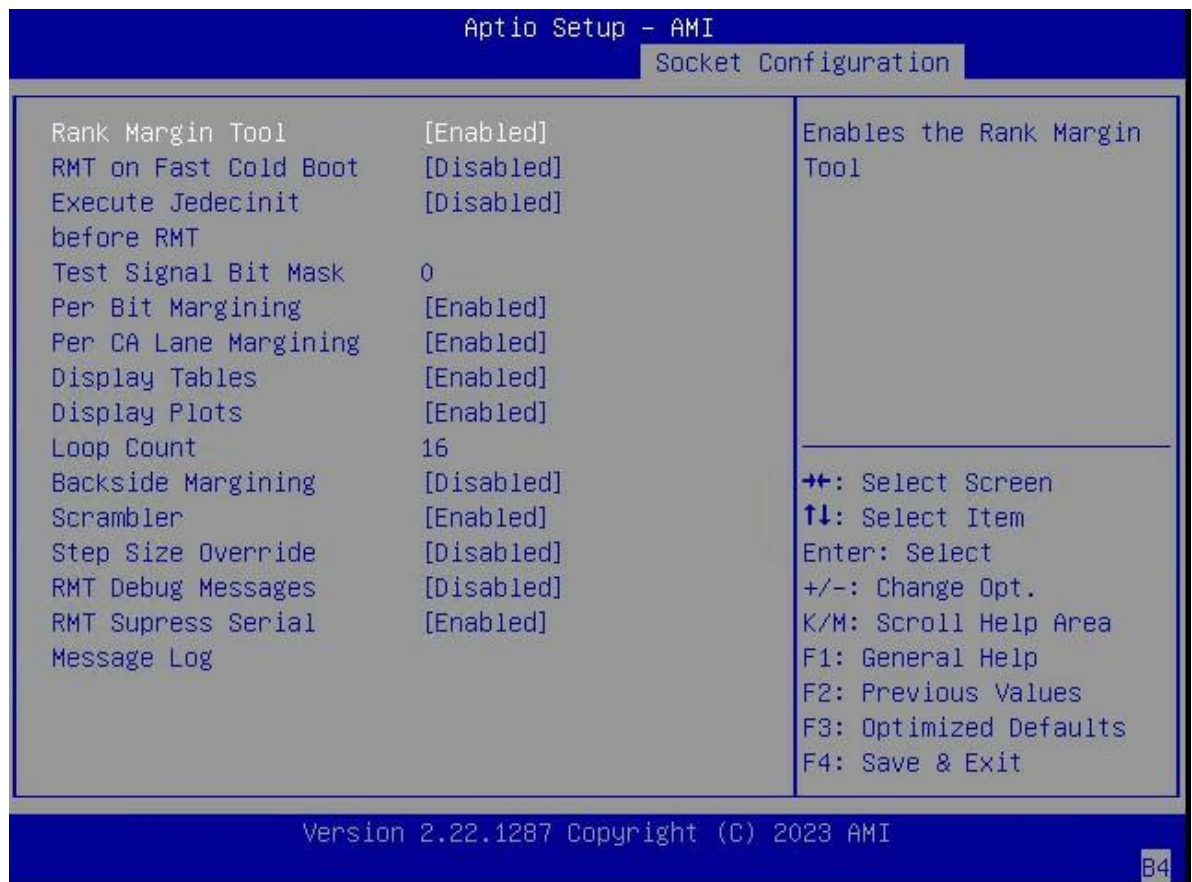
Parameter	Description	Default
Bank Group Interleaving Mode	Sets DDR Bank Group interleaving mode. Options: - Goaese Grained Mode - Fine Grained Mode - Fine Grained Mode (Fine Grained bank group interleave on two bank bits)	Fine Grained Mode

Parameter	Description	Default
DIMM Interleaving	Enables or disables DIMM interleaving. Options: ● Enabled: allows interleaving at the highest level. ● Disabled: restricts interleaving to only 1-way interleaving.	Enabled
3-Way Channel Interleaving	Enables or disables 3-way channel interleaving. Options: ● Enabled: enables 3-way channel interleaving. ● Disabled: restores the number of available channels to the default value when DIMM Interleaving is set to Enabled.	Enabled
Max Rank Interleaving in IMC	Select interleaving mode. Options: ● 1-way Interleave: 1-way interleaving. ● 2-way Interleave: 2-way interleaving. ● 4-way Interleave: 4-way interleaving. ● 8-way Interleave: 8-way interleaving.	8-way Interleave
PMem ECC Correctable error	Enables or disables correctable PMem ECC . Options: ● Enabled: enables correctable PMem ECC. ● Disabled: disables correctable PMem ECC. ● Auto: dynamic selection.	Enabled
PMem ECC Write Check	Enables or disables PMem write ECC. Options: ● Enabled: enables PMem write ECC. ● Disabled: disables PMem write ECC. ● Auto: dynamic selection.	Auto
C/A Parity Enable	Enables or disables DDR4 command address parity. Options: ● Enabled: enables DDR4 command address parity. ● Disabled: disables DDR4 command address parity.	Enabled
DDR5 Override Refresh Mode	Select DDR5 overwriting refresh mode. Options: ● Auto ● All Bank Normal ● All Bank Fine ● Same Bank Fine	Auto

Parameter	Description	Default
DDR5 SSA RxSampler Margin Parameter Selection	Configures DDR5 SSA margin training parameters for the RxSampler. Options: ● Auto: automatic mode. ● RxSampler Even and Odd Offset: even and odd offsets for the RxSampler. ● RxSampler Even Offset: even offset for the RxSampler. ● RxSampler Odd Offset: odd offset for the RxSampler. ● RxVref.	Auto
CXL Type 3 Legacy	Whether to enable CXL type 3 devices to use the procedure for CXL type 2 devices. Options: ● Enabled: allows CXL type 3 devices to use the procedure for CXL type 2 devices. ● Disabled: prevents CXL type 3 devices from using the procedure for CXL type 2 devices.	Disabled

3.4.4.10 RMT Configuration Menu

[Figure 3-93](#) shows the **RMT Configuration Menu** screen.

Figure 3-93 RMT Configuration Menu Screen

For a description of the parameters on the **RMT Configuration Menu** screen, refer to [Table 3-65](#).

Table 3-65 Parameter Descriptions for the RMT Configuration Menu Screen

Parameter	Description	Default
Rank Margin Tool	Enables or disables the Rank Margin tool. Options: - Enabled: enables the Rank Margin tool. When this parameter is set to Enabled, parameters starting with Per Bit Margining are displayed. - Disabled: disables the Rank Margin tool.	Disabled
RMT on Fast Cold Boot	Enables or disables the Rank Margin tool upon fast cold boot. Options: - Enabled: enables the Rank Margin tool upon fast cold boot. - Disabled: disables the Rank Margin tool upon fast cold boot.	Disabled

Parameter	Description	Default
Execute Jedecinit before RMT	Enables or disables Jedecinit execution before the Rank Margin tool runs. Options: ● Enabled: enables Jedecinit execution. ● Disabled: disables Jedecinit execution.	Disabled
Test Signal Bit Mask	Test signal bit mask.	0
Per Bit Margining	This parameter is displayed when Rank Margin Tool is set to Enabled . Enables or disables Per Bit Margining. Options: ● Enabled: enables Per Bit Margining. ● Disabled: disables Per Bit Margining.	Enabled
Per CA Lane Margining	This parameter is displayed when Rank Margin Tool is set to Enabled . Enables or disables Per CA Lane Margining. Options: ● Enabled: enables Per CA Lane Margining. ● Disabled: disables Per CA Lane Margining.	Enabled
Display Tables	This parameter is displayed when Rank Margin Tool is set to Enabled . Select whether to display results in tables. Options: ● Enabled: displays results in tables. ● Disabled: indicates that results are not displayed in tables.	Enabled
Display Plots	This parameter is displayed when Rank Margin Tool is set to Enabled . Select whether to display results with plots. Options: ● Enabled: displays results with plots. ● Disabled: indicates that results are not displayed with plots.	Enabled
Loop Count	This parameter is displayed when Rank Margin Tool is set to Enabled . Enter the number of counts in a statistical period.	16
Backside Margining	This parameter is displayed when Rank Margin Tool is set to Enabled . Enables or disables the margin test at the backup register or buffer.	Disabled

Parameter	Description	Default
	Options: ● Enabled: enables the margin test. ● Disabled: disables the margin test.	
Scrambler	This parameter is displayed when Rank Margin Tool is set to Enabled . Enables or disables the test scrambler of the RMT. Options: ● Enabled: enables the test scrambler of the RMT. ● Disabled: disables the test scrambler of the RMT.	Enabled
Step Size Override	This parameter is displayed when Rank Margin Tool is set to Enabled . Enables or disables step size rewriting. Options: ● Enabled: enables step size rewriting. ● Disabled: disables step size rewriting.	Disabled
RMT Debug Messages	This parameter is displayed when Rank Margin Tool is set to Enabled . Enables or disables RMT debugging. Options: ● Enabled: enables RMT debugging. ● Disabled: disables RMT debugging.	Disabled
RMT Suppress Serial Message Log	This parameter is displayed when Rank Margin Tool is set to Enabled . Sets whether to suppress serial-port-based messages and output only error messages when running the RMT. Options: ● Enabled: suppresses serial-port-based messages and outputs only error messages when running the RMT. ● Disabled: disables the suppression of serial-port-based messages.	Enabled

3.4.5 IIO Configuration

Figure 3-94 through Figure 3-95 show the **IIO Configuration** screen.

Figure 3-94 IIO Configuration Screen—1

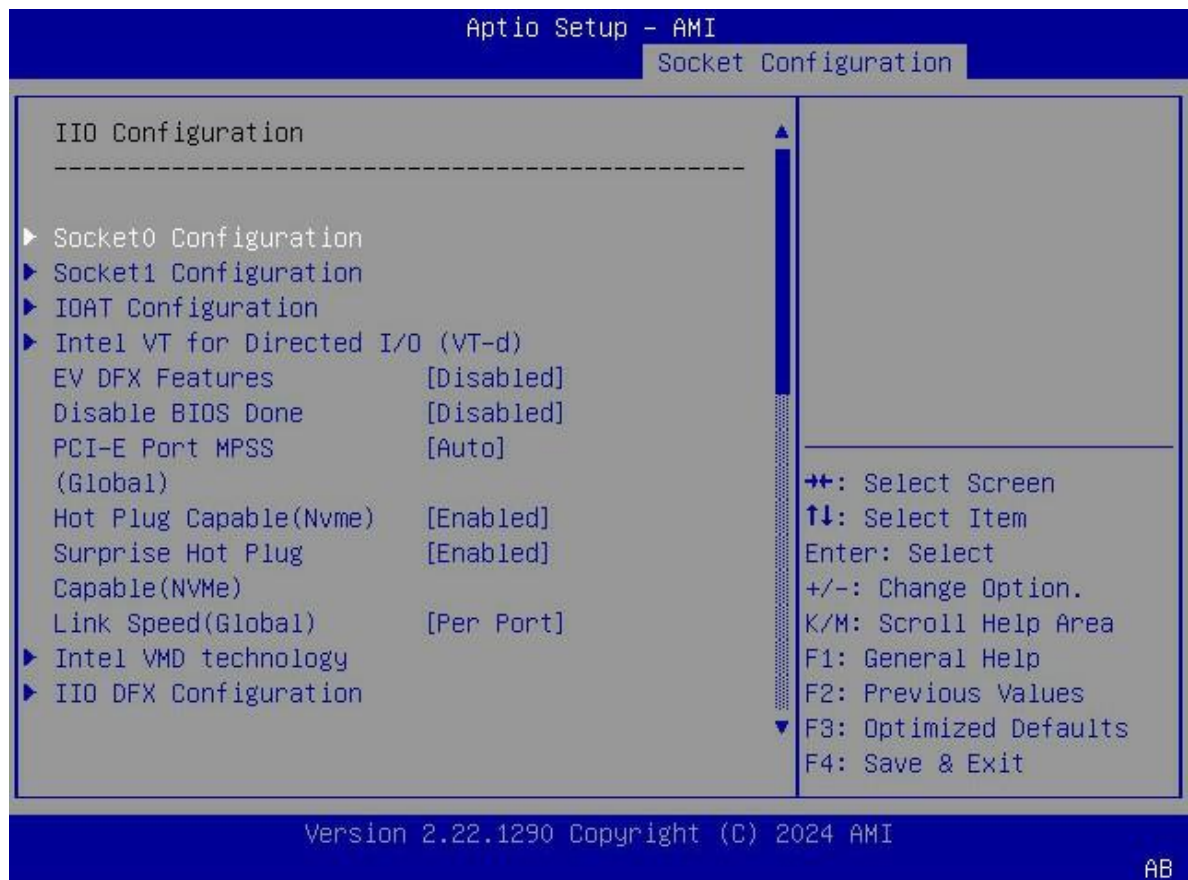


Figure 3-95 IIO Configuration Screen—2



For a description of the parameters on the **IIO Configuration** screen, refer to [Table 3-66](#).

Table 3-66 Parameter Descriptions for the IIO Configuration Screen

Parameter	Description	Default
Socket0 Configuration	Sets socket 0 parameters. For details, refer to 3.4.5.1 Socket0 Configuration .	-
Socket1 Configuration	Sets socket 1 parameters. Socket1 parameters are the same as Socket0 parameters. For details, refer to 3.4.5.1 Socket0 Configuration .	-
IOAT Configuration	Sets IOAT parameters. For details, refer to 3.4.5.2 IOAT Configuration .	-
Intel VT for Directed I/O (VT-d)	Sets VT-d parameters. For details, refer to 3.4.5.3 Intel VT for Directed I/O (VT-d) .	-
EV DFX Features	Enables or disables IIO DFX and other CPU devices (such as PMON). Options:	Disabled

Parameter	Description	Default
	- Enabled: enables IIO DFX and other CPU devices. - Disabled: disables IIO DFX and other CPUs.	
Disable BIOS Done	Enables or disables the boot initialization completion notification sent to processors through MSR 151H. This parameter does not need to be set. Options: - Enabled: enables the boot initialization completion notification sent to processors through MSR 151H. - Disabled: disables the boot initialization completion notification sent to processors through MSR 151H.	Disabled
PCI-E Port MPSS (Global)	Configure the maximum load size supported in all NVMe PCIe device function registers. The "Auto" option retains the default hardware configuration. Options: 128B 256B 512B - Auto	Auto
Hot Plug Capable(Nvme)	Configures the hot swapping capability of the slots where all NVMe devices are located. Options: - Auto: automatic mode. - Enabled: enables the hot swapping capability of the slots where all NVMe devices are located. - Disabled: disables the hot swapping capability of the slots where all NVMe devices are located. - Per Port: The configuration of each NVMe port takes effect separately. If this parameter is set to Auto, Enabled, or Disabled, the NVMe port settings are overwritten.	Enabled
Surprise Hot Plug Capable(NVMe)	Configures the hot swapping capability of the slots where all NVMe devices are located, without any notification. Options: Enabled: enables the hot swapping capability of the slots where all NVMe devices are located, without any notification.	Enabled

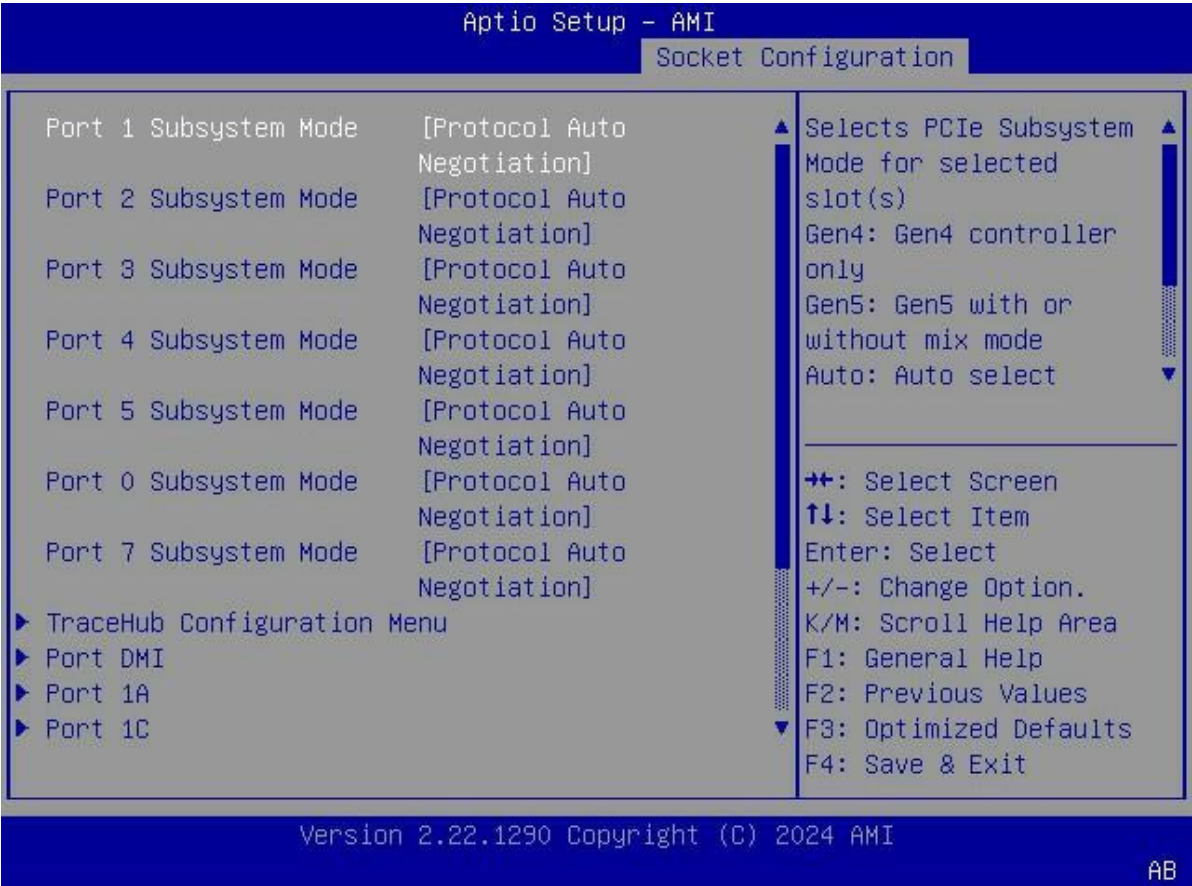
Parameter	Description	Default
	- Disabled: disables the hot swapping capability of the slots where all NVMe devices are located, without any notification. - Per Port: The configuration of each NVMe port takes effect separately. If this parameter is set to Enabled or Disabled, the NVMe port settings are overwritten.	
Link Speed(Global)	Configures the link rate of all PCIe device ports (except the DMI port). Options: - Auto: automatic mode. - Gen 1 (2.5 GT/s) - Gen 2 (5 GT/s) - Gen 3 (8 GT/s) - Gen 4 (16 GT/s) - Gen 5 (32 GT/s) - Per Port: The configuration of each NVMe port takes effect separately. If this parameter is not set to Per Port, the PCIe port settings are overwritten.	Per Port
Intel VMD technology	Sets VMD parameters. For details, refer to 3.4.5.4 Intel VMD technology.	-
IIO DFX Configuration	Configures IIO DFX parameters. For details, refer to 3.4.5.5 IIO DFX Configuration.	-
NTB Link Train by BIOS	Sets whether to enable NTB link training. Options: - Yes: enables NTB link training. - No: disables NTB link training. - Auto: automatic mode.	Yes
Delay before link training	Sets the delay before IIO-port PCIe link training.	No delay
PCIe Hot Plug	Enables or disables PCIe hot swapping. Options: - Enabled: enables PCIe hot swapping. - Disabled: disables PCIe hot swapping.	Enabled
IIO Port Bifurcation Policy	Sets IIO port bifurcation policy. Options: - Auto: automatic mode. - Manual: manual mode.	Auto

Parameter	Description	Default
NVME LED Support	Enables or disables the NVME LED support when the VMD function is disabled. Options: ● Enabled: enables the NVME LED support when the VMD function is disabled. ● Disabled: disables the NVME LED support when the VMD function is disabled.	Enabled
CbDma MultiCast Enable	Enables or disables the CbDma MultiCast feature. Options: ● Yes: enables the CbDma MultiCast feature. ● No: disables the CbDma MultiCast feature.	Yes
PCI-E Completion Timeout	Select the PCIe timeout setting method. Options: ● Per-Port: Each port is set independently. ● Global: All ports are set globally.	Global
PCI-E Completion Timeout Value	This parameter cannot be set if PCI-E Completion Timeout is set to Per-Port . Select the PCIe timeout period.	260ms to 900ms
PCI-E ASPM Support (Global)	Select the PCIe dynamic power management mode. Options: ● Disabled: disables PCIe Dynamic Power Management. ● L1 Only: enters L1 mode only.	Disabled
PCIe 10-bit Tag Support	Enables or disables the PCIe 10-bit tag. Options: ● Disabled: disables the PCIe 10-bit tag in all PCIe root ports. ● Auto: uses the default hardware setting.	Auto
PCIe Max Read Request Size	In the PCI hierarchy, select the maximum read request size and distinguish locations.	4096B
PCIe PTM Support	Enables or disables the PCIe PTM. Options: ● Disabled: disables the PTM feature in the PCI hierarchy. ● Auto: uses the default hardware setting.	Auto
PCIe ENQCMD/ENQCMLS	Enables or disables PCIe enqueue requests. Options: ● No: rejects PCIe enqueue requests. ● Yes: accepts PCIe enqueue requests.	NO

3.4.5.1 Socket0 Configuration

Figure 3-96 shows the **Socket0 Configuration** screen.

Figure 3-96 Socket0 Configuration Screen



For a description of the parameters on the **Socket0 Configuration** screen, refer to [Table 3-67](#).

Table 3-67 Parameter Descriptions for the Socket0 Configuration Screen

Parameter	Description	
Port 1 Subsystem Mode	Configures the PCIe subsystem mode for port 1. Options: ● Gen5: 5th generation controller with or without mix mode. ● Protocol Auto Negotiation: protocol auto-negotiation. ● Gen4 Only: 4th generation controller only. ● Force CXL: forcibly uses CXL mode. There is no training discovery. The attached device must also support this mode.	Protocol Auto Negotiation

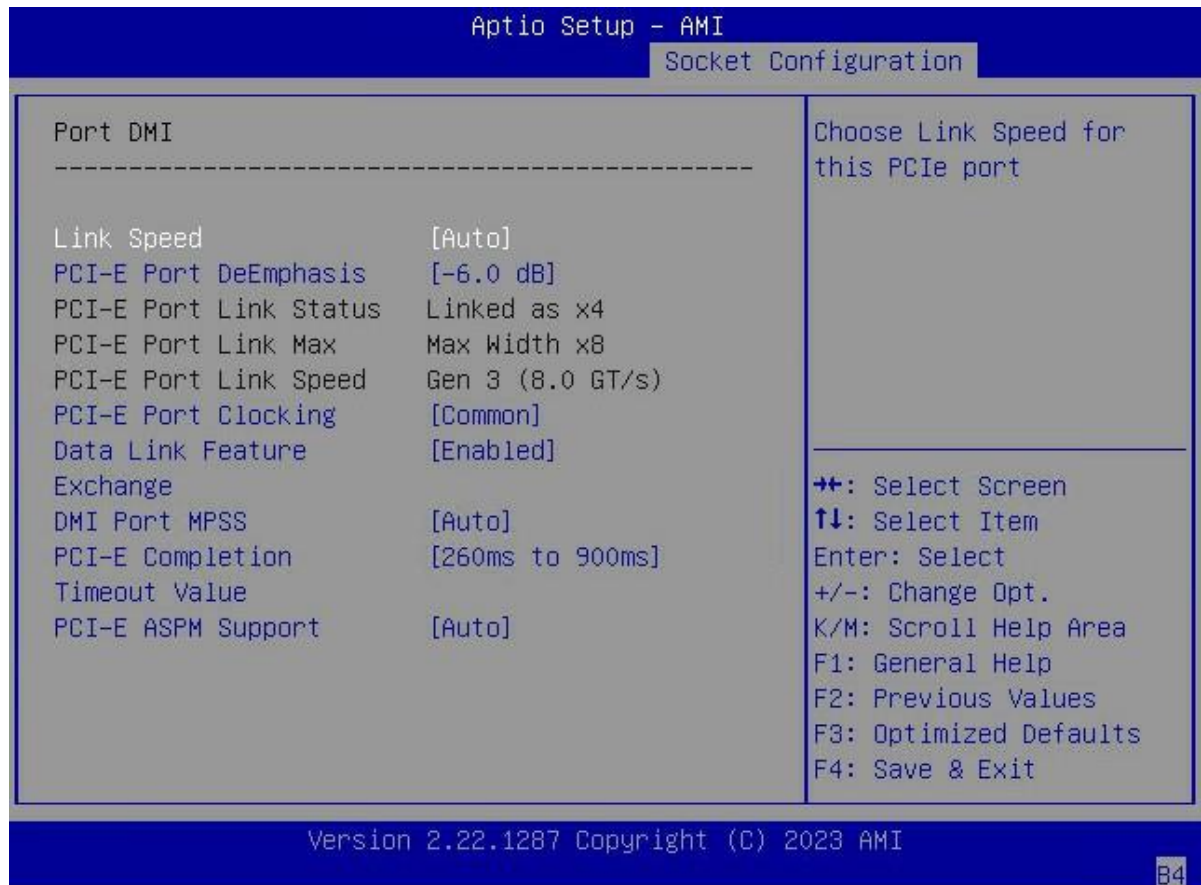
Parameter	Description	
Port 2 Subsystem Mode	Configures the PCIe subsystem mode for port 2. Options: ● Gen5: 5th generation controller with or without mix mode. ● Protocol Auto Negotiation: protocol auto-negotiation. ● Gen4 Only: 4th generation controller only. ● Force CXL: forcibly uses CXL mode. There is no training discovery. The attached device must also support this mode.	Protocol Auto Negotiation
Port 3 Subsystem Mode	Configures the PCIe subsystem mode for port 3. Options: ● Gen5: 5th generation controller with or without mix mode. ● Protocol Auto Negotiation: protocol auto-negotiation. ● Gen4 Only: 4th generation controller only. ● Force CXL: forcibly uses CXL mode. There is no training discovery. The attached device must also support this mode.	Protocol Auto Negotiation
Port 4 Subsystem Mode	Configures the PCIe subsystem mode for port 4. Options: ● Gen5: 5th generation controller with or without mix mode. ● Protocol Auto Negotiation: protocol auto-negotiation. ● Gen4 Only: 4th generation controller only. ● Force CXL: forcibly uses CXL mode. There is no training discovery. The attached device must also support this mode.	Protocol Auto Negotiation
Port 5 Subsystem Mode	Configures the PCIe subsystem mode for port 5.	Protocol Auto Negotiation

Parameter	Description	
	Options: ● Gen5: 5th generation controller with or without mix mode. ● Protocol Auto Negotiation: protocol auto-negotiation. ● Gen4 Only: 4th generation controller only. ● Force CXL: forcibly uses CXL mode. There is no training discovery. The attached device must also support this mode.	
Port 0 Subsystem Mode	Configures the PCIe subsystem mode for port 0. Options: ● Gen5: 5th generation controller with or without mix mode. ● Protocol Auto Negotiation: protocol auto-negotiation. ● Gen4 Only: 4th generation controller only. ● Force CXL: forcibly uses CXL mode. There is no training discovery. The attached device must also support this mode.	Protocol Auto Negotiation
Port 7 Subsystem Mode	Configures the PCIe subsystem mode for port 7. Options: ● Gen5: 5th generation controller with or without mix mode. ● Protocol Auto Negotiation: protocol auto-negotiation. ● Gen4 Only: 4th generation controller only. ● Force CXL: forcibly uses CXL mode. There is no training discovery. The attached device must also support this mode.	Protocol Auto Negotiation
TraceHub Configuration Menu	Sets TraceHub parameters.	-
Port DMI	Provides access to detailed port DMI configurations, see Figure 3-97 .	-

Parameter	Description	
Port 1A	Provides access to detailed port 1A configurations, as shown in Figure 3-98 through Figure 3-99 .	-
Port 2A	Provides access to detailed port 2A configurations, which are similar to detailed port 1A configurations.	-
Port 2E	Provides access to detailed port 2E configurations, which are similar to detailed port 1A configurations.	-
Port 3A	Provides access to detailed port 3A configurations, which are similar to detailed port 1A configurations.	-
Port 3E	Provides access to detailed port 3E configurations, which are similar to detailed port 1A configurations.	-
Port 4A	Provides access to detailed port 4A configurations, which are similar to detailed port 1A configurations.	-
Port 4C	Provides access to detailed port 4C configurations, which are similar to detailed port 1A configurations.	-
Port 4E	Provides access to detailed port 4E configurations, which are similar to detailed port 1A configurations.	-
Port 4G	Provides access to detailed port 4G configurations, which are similar to detailed port 1A configurations.	-
Port 5A	Provides access to detailed port 5A configurations, which are similar to detailed port 1A configurations.	-
Port 5C	Provides access to detailed port 5C configurations, which are similar to detailed port 1A configurations.	-
Port 5E	Provides access to detailed port 5E configurations, which are similar to detailed port 1A configurations.	-

Parameter	Description	
Port 5G	Provides access to detailed port 5G configurations, which are similar to detailed port 1A configurations.	-

Figure 3-97 Port DMI Screen



For a description of the parameters on the **Port DMI** screen, refer to [Table 3-68](#).

Table 3-68 Parameter Descriptions for the Port DMI Screen

Parameter	Description	Default
Link Speed	Select a link speed. Options: ● Auto ● Gen 1 (2.5 GT/s) ● Gen 2 (5 GT/s) ● Gen 3 (8 GT/s) ● Gen 4 (16 GT/s)	Auto
PCI-E Port DeEmphasis	Sets the PCIe port de-emphasis level. Options: ● -6.0 dB	-6.0 dB

Parameter	Description	Default
	● -3.5 dB	
PCI-E Port Link Status	Displays the current PCIe port link status.	-
PCI-E Port Link Max	Displays the maximum bandwidth of the PCIe port link.	-
PCI-E Port Link Speed	Displays the PCIe port link speed.	-
PCI-E Port Clocking	Sets the port clock through LNKCON[6] . Options: ● Distinct ● Common	Common
Data Link Feature Exchange	Enables or disables the data link feature at the DLFCAP register. Options: ● Enabled: enables the data link feature. ● Disabled: disables the data link feature.	Enabled
DMI Port MPSS	Select the DMI Port MPSS. Options: ● 128B ● 256B ● Auto: uses the default hardware setting.	Auto
PCI-E Completion Timeout Value	Select the PCIe timeout period. Options: ● 50us to 50ms ● 16ms to 55ms ● 65ms to 210ms ● 260ms to 900ms ● 1s to 3.5s ● Disabled	260ms to 900ms
PCI-E ASPM Support	Disabled: disables PCIe ASPM support. Options: ● Disabled: disables PCIe ASPM support. ● Auto: uses the default hardware setting.	Auto

Figure 3-98 Port 1A Screen—1

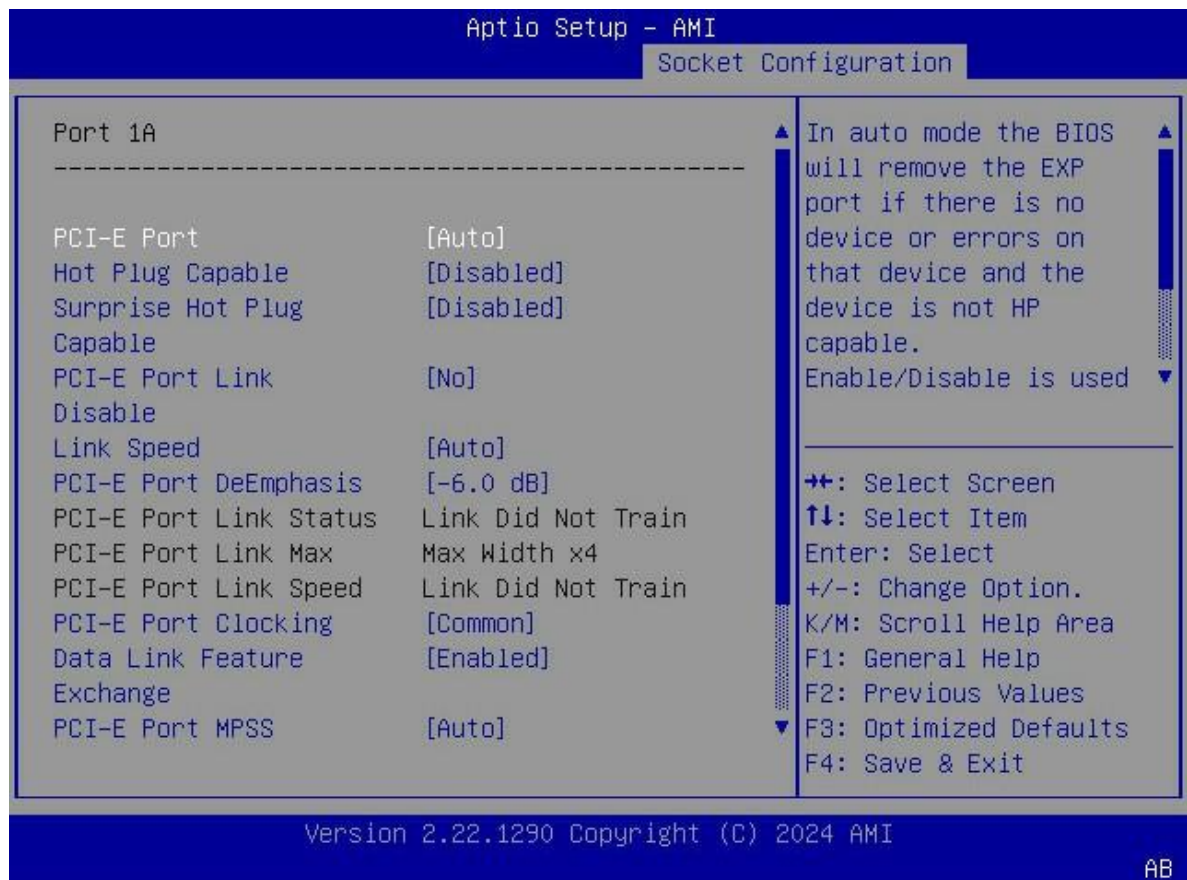
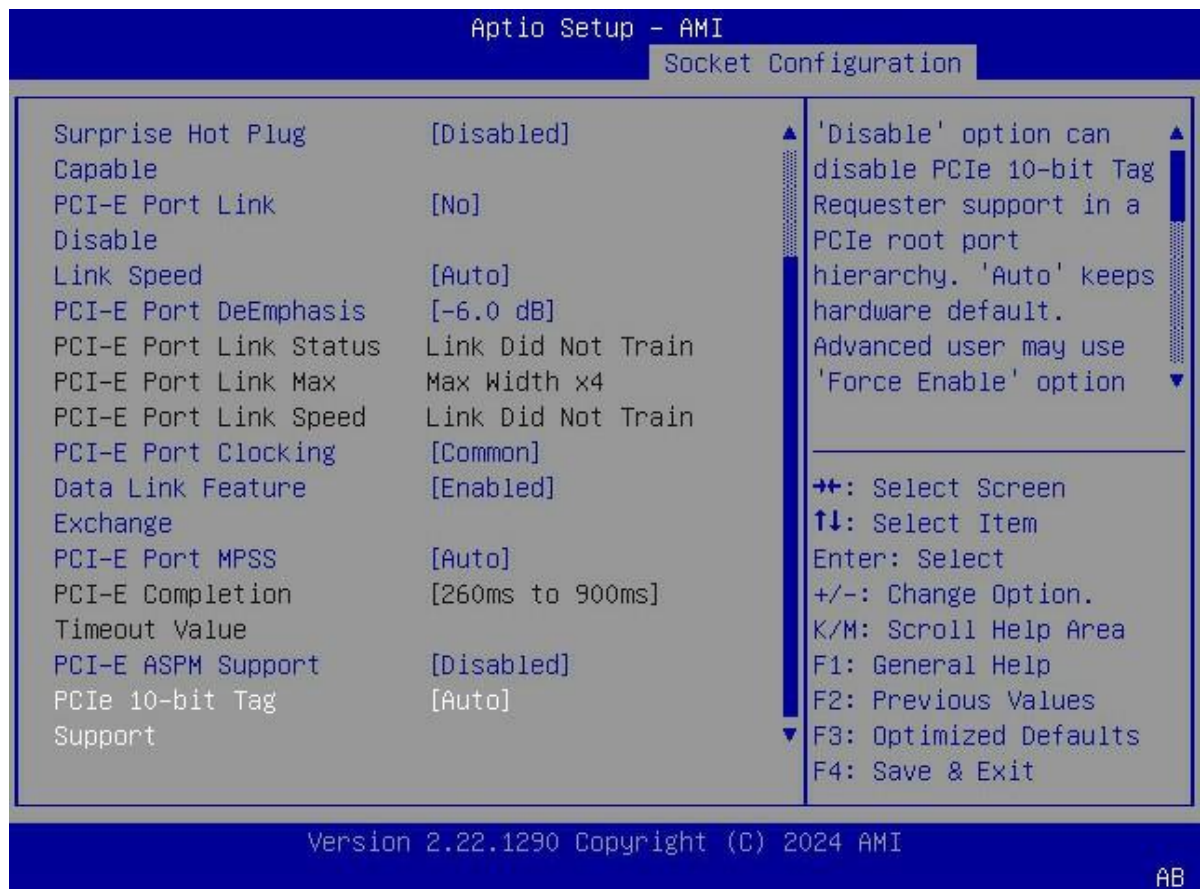


Figure 3-99 Port 1A Screen—2



For a description of the parameters on the **Port 1A** screen, refer to [Table 3-69](#).

Table 3-69 Parameter Descriptions for the Port 1A Screen

Parameter	Description	Default
PCI-E Port	Sets whether to enable the PCIe port. Options: ● Auto: deletes the EXP port. ● Yes: enables the PCIe port. ● No: disables PCIe ports.	Auto
Hot Plug Capable	Enables or disables hot swapping. Options: ● Enabled: enables hot swapping. ● Disabled: disables hot swapping. ● Auto: enables hot swapping.	Disabled
Surprise Hot Plug capable	Enables or disables hot swapping without any notification when the device is being used. Options: ● Enabled: enables hot swapping without any notification when the device is being used.	Disabled

Parameter	Description	Default
	Disabled: disables hot swapping without any notification when the device is being used.	
PCI-E Port Link Disable	Sets whether to enable the shutdown of the PCIe port link. Options: - Yes: enables the shutdown of the PCIe port link. - No: disables the shutdown of the PCIe port link.	No
Link Speed	Sets the link speed. Options: - Auto - Gen 1 (2.5 GT/s) - Gen 2 (5 GT/s) - Gen 3 (8 GT/s) - Gen 4 (16 GT/s) - Gen 5 (32 GT/s)	Auto
PCI-E Port DeEmphasis	Sets the PCIe port de-emphasis level. Options: -6.0 dB -3.5 dB	-6.0 dB
PCI-E Port Link Status	Displays the current PCIe port link status.	-
PCI-E Port Link Max	Displays the maximum bandwidth of the PCIe port link.	-
PCI-E Port Link Speed	Displays the PCIe port link speed.	-
PCI-E Port Clocking	Sets the port clock through LNKCON[6] . Options: - Distinct - Common	Common
Data Link Feature Exchange	Enables or disables data link feature exchange at the DLFCAP register. Options: - Enabled: enables data link feature exchange. - Disabled: disables the data link feature.	Enabled
PCI-E Port MPSS	Sets the PCIe Port MPSS. Options: 128B 256B 512B - Auto: uses the default hardware setting.	Auto

Parameter	Description	Default
PCI-E Completion Timeout Value	Sets the PCIe timeout period.	260ms to 900ms
PCI-E ASPM Support	Configures PCIe ASPM support. Options: ● Disabled: disables PCIe ASPM support. ● Auto: uses the default hardware setting.	Auto
PCIe 10-bit Tag Support	Configures the PCIe 10-bit tag on PCIe root ports. Options: ● Disabled: disables the PCIe 10-bit tag on PCIe root ports. ● Auto: uses the default hardware setting. ● Force Enable: forcibly enables the PCIe 10-bit tag on PCIe root ports.	Auto

3.4.5.2 IOAT Configuration

Figure 3-100 shows the **IOAT Configuration** screen.

Figure 3-100 IOAT Configuration Screen



For a description of the parameters on the **IOAT Configuration** screen, refer to [Table 3-70](#).

Table 3-70 Parameter Descriptions for the IOAT Configuration Screen

Parameter	Description	Default
Relaxed Ordering	Enables or disables the Relaxed Ordering feature. Options: • Yes: enables the Relaxed Ordering feature. • No: disables the Relaxed Ordering feature.	No

3.4.5.3 Intel VT for Directed I/O (VT-d)

Figure 3-101 through Figure 3-102 show the **Intel VT for Directed I/O (VT-d)** screen.

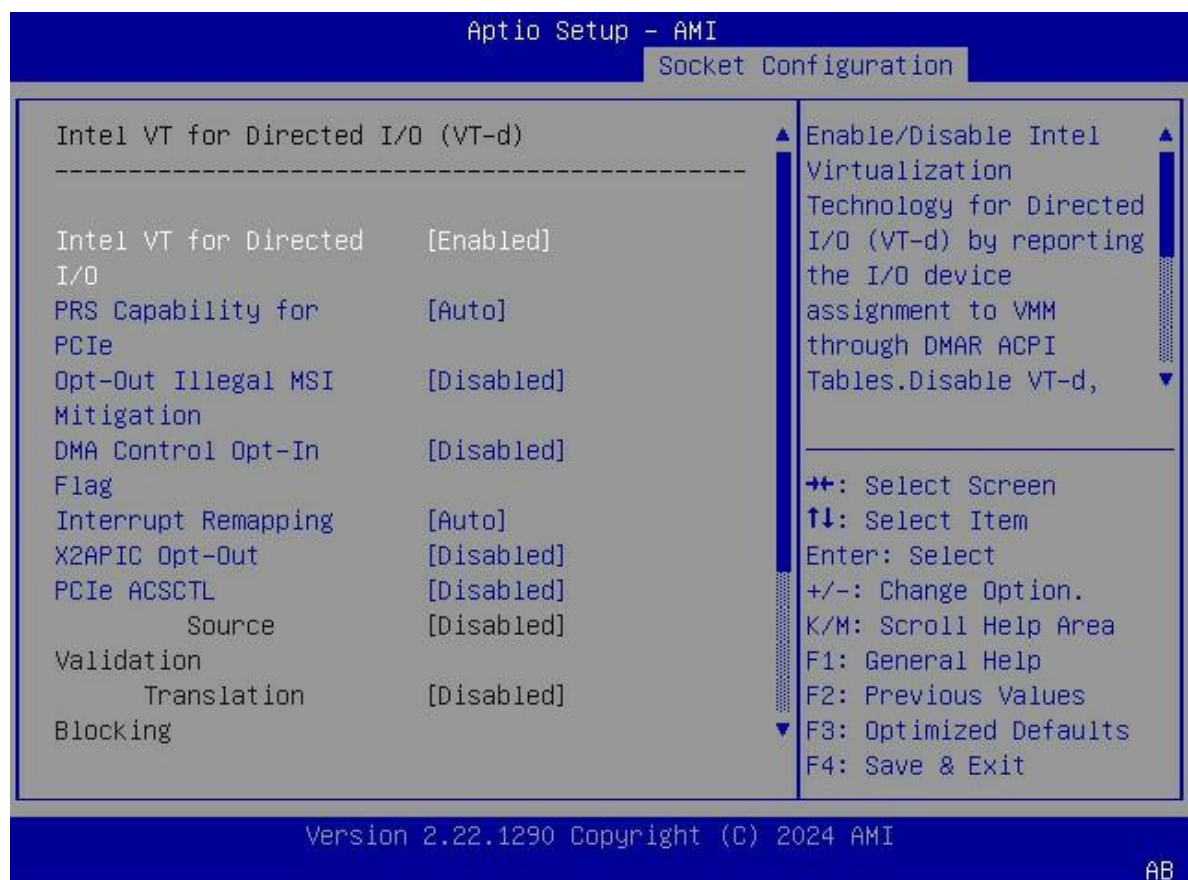
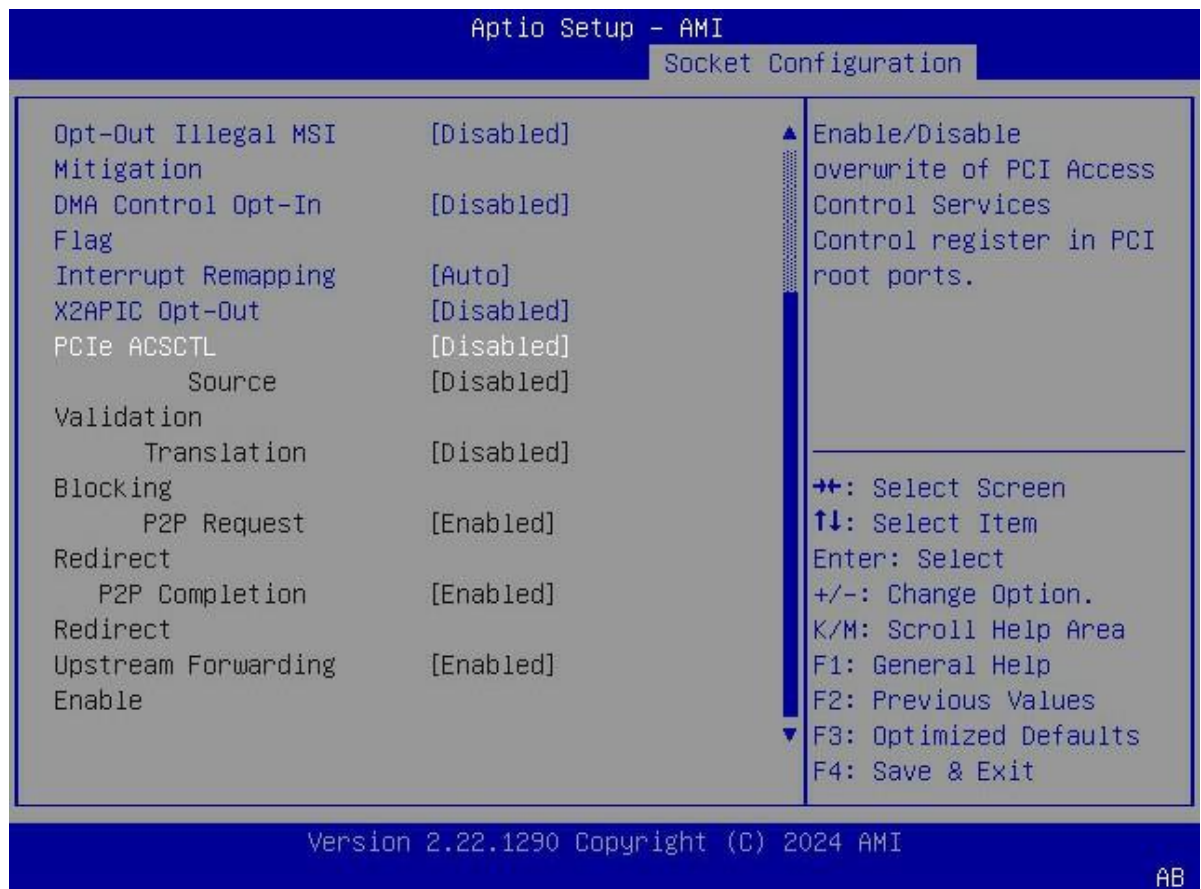
Figure 3-101 Intel VT for Directed I/O (VT-d) Screen—1

Figure 3-102 Intel VT for Directed I/O (VT-d) Screen—2



For a description of the parameters on the **Intel VT for Directed I/O (VT-d)** screen, refer to [Table 3-71](#).

Table 3-71 Parameter Descriptions for the Intel VT for Directed I/O (VT-d) Screen

Parameter	Description	Default
Intel VT for Directed I/O	Enables or disables the Intel virtualization technology for directed I/O. Options: ● Enabled: enables the Intel virtualization technology for directed I/O. ● Disabled: disables the Intel virtualization technology for directed I/O. When this parameter is set to Disabled, the following parameters are not configurable: → DMA Control Opt-In Flag → Interrupt Remapping → X2APIC Opt Out	Enabled
PRS Capability for PCIe	Enables or disables support for the page request service on discrete PCIe devices. This function is only	Auto

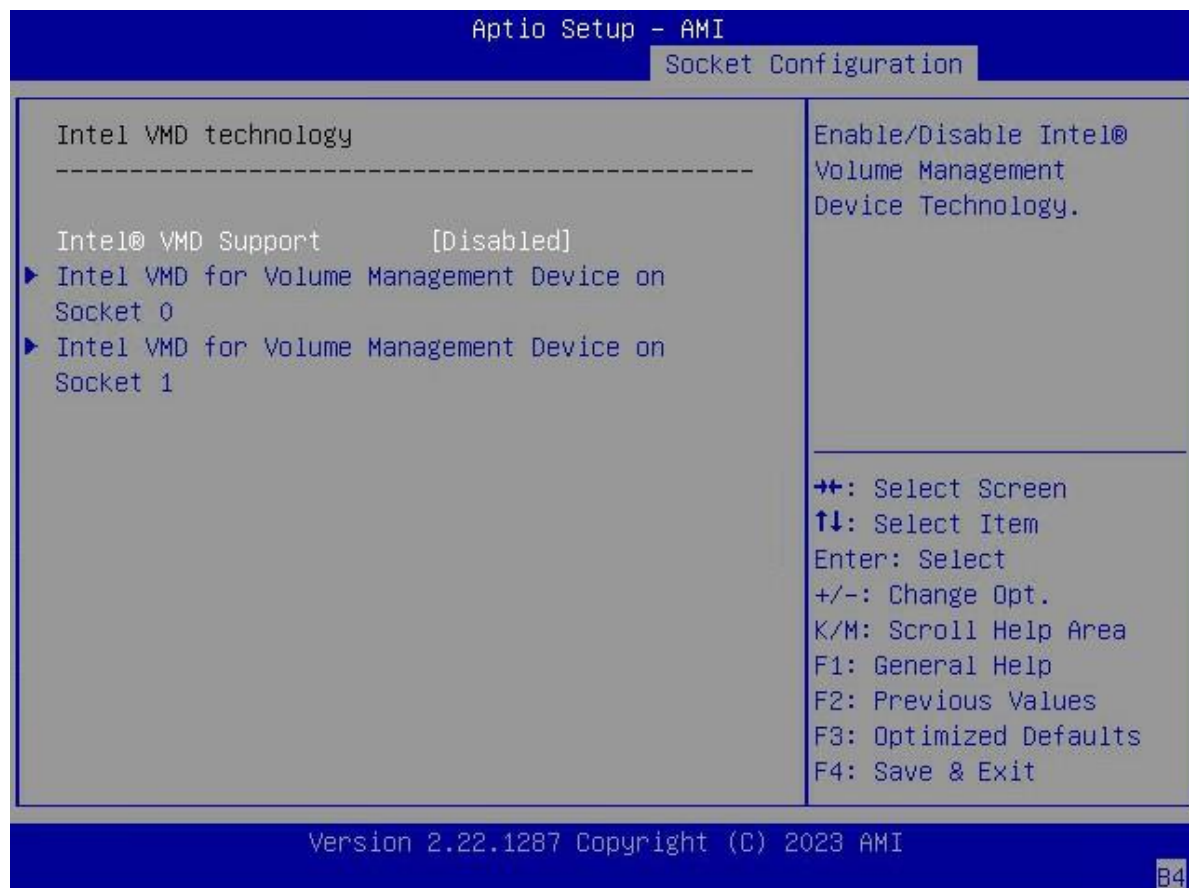
Parameter	Description	Default
	recommended to test whether the PCIe cards of the device supports the PRS. Options: ● Enabled: enables support for the page request service on discrete PCIe devices. When this parameter is set to Enabled, the platform may be suspended. ● Disabled: disables the page request service function on discrete PCIe devices. ● Auto: automatic mode.	
Opt-Out Illegal MSI Mitigation	Enables or disables the optional exit of the illegal 0x FEE platform mitigation policy. ● Enabled: enables the optional exit of the illegal 0x FEE platform mitigation policy. ● Disabled: disables the optional exit of the illegal 0x FEE platform mitigation policy.	Disabled
DMA Control Opt-In Flag	Enables or disables the DMA control Opt-In flag. Options: ● Enabled: enables the DMA control Opt-In flag. ● Disabled: disables the DMA control Opt-In flag.	Disabled
Interrupt Remapping	Enables or disables interrupt remapping. Options: ● Enabled: enables interrupt remapping. After this feature is enabled, the management programs and OSs can use the Intel virtualization technology to provide interrupt remapping for the directed I/O device. ● Disabled: disables interrupt remapping. ● Auto: Set this parameter to Auto if Intel VT for Directed I/O is set to Auto.	Auto
X2APIC Opt Out	Enables or disables the X2APIC Opt Out feature. Options: ● Enabled: enables the X2APIC Opt Out feature. ● Disabled: disables the X2APIC Opt Out feature.	Disabled
PCIe ACSCTL	Enables or disables the overriding of the ACS control register on PCIe root ports. Options: ● Enabled: enables the overriding of the ACS control register on PCIe root ports.	Disabled

Parameter	Description	Default
	Disabled: disables the overriding of the ACS control register on PCIe root ports.	
Source Validation	Enables or disables resource validation. Options: - Enabled: enables resource validation. When this parameter is set to Enabled, the component validates the bus number in the requester ID of an upstream request. - Disabled: disables resource validation.	Disabled
Translation Blocking	Enables or disables translation blocking. Options: - Enabled: enables translation blocking. After this feature is enabled, the component blocks all upstream memory requests whose AT field is not set to the default value. - Disabled: disables translation blocking.	Disabled
P2P Request Redirect	Enables or disables P2P request redirection. Options: - Enabled: enables P2P request redirection. After this feature is enabled, the system determines when the component redirects P2P requests to the upstream. - Disabled: disables P2P request redirection.	Enabled
P2P Completion Redirect	Enables or disables P2P completion redirection. Options: - Enabled: enables P2P completion redirection. After this feature is enabled, the system determines when the component redirects P2P completion to the upstream. - Disabled: disables P2P completion redirection.	Enabled
Upstream Forwarding Enable	Enables or disables upstream forwarding. Options: - Enabled: enables upstream forwarding. After this feature is enabled, the component forwards to the upstream any requests it receives or completion TLPs, which are redirected to the upstream by lower-level components in the hierarchy. - Disabled: disables upstream forwarding.	Enabled

3.4.5.4 Intel VMD technology

Figure 3-103 shows the **Intel VMD technology** screen.

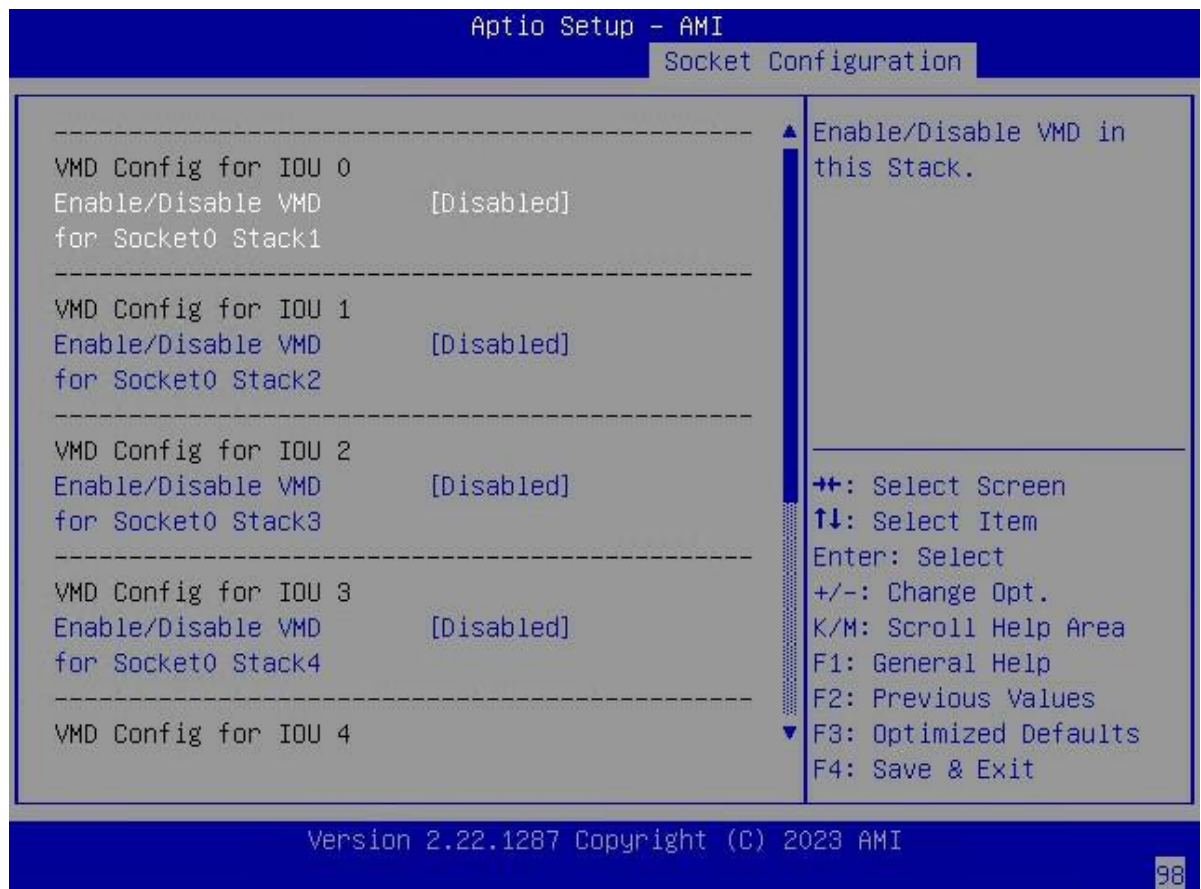
Figure 3-103 Intel VMD Technology Screen



For a description of the parameters on the **Intel VMD technology** screen, refer to [Table 3-72](#).

Table 3-72 Parameter Descriptions for the Intel VMD Technology Screen

Parameter	Description	Default
Intel VMD Support	Enables or disables the VMD technology. - Enabled: enables the VMD technology. - Disabled: disables the VMD technology.	Disabled
Intel VMD for Volume Management Device on Socket 0	VMD configurations of socket 0, see Figure 3-104 .	-
Intel VMD for Volume Management Device on Socket 1	VMD configurations of socket 1, which is similar to those of socket 0.	-

Figure 3-104 Intel VMD Configurations on Socket 0

For a description of the parameters on the **Socket 0 VMD** screen, refer to [Table 3-73](#).

Table 3-73 Parameter Descriptions for the Socket 0 VMD Screen

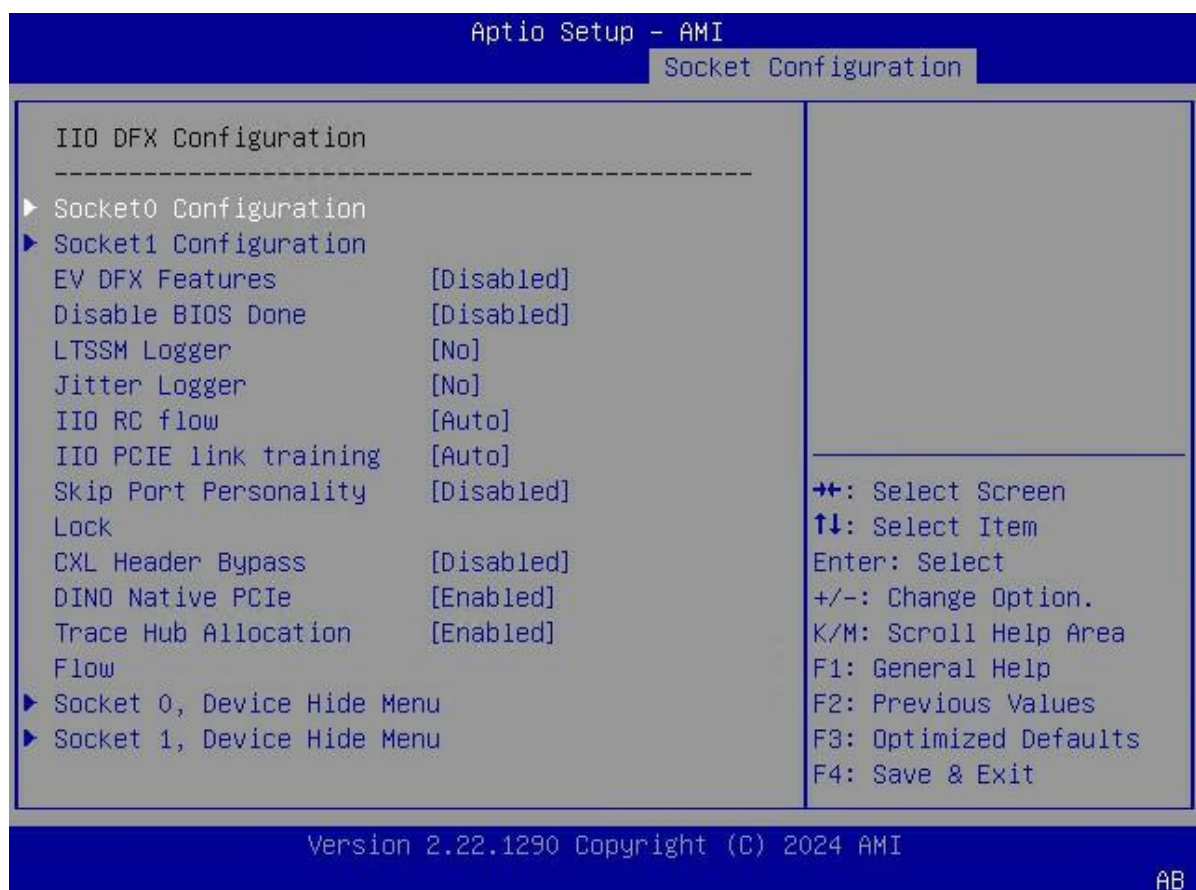
Parameter	Description	Default
Enable/Disable VMD for Socket0 Stack1	Enables or disables the VMD technology for Socket0 Stack1. - Enabled: enables the VMD technology. - For Disabled: disables the VMD technology.	Disabled
Enable/Disable VMD for Socket0 Stack2	Enables or disables the VMD technology for Socket0 Stack2. - Enabled: enables the VMD technology. - Disabled: disables the VMD technology.	Disabled
Enable/Disable VMD for Socket0 Stack3	Enables or disables the VMD technology for Socket0 Stack3. - Enabled: enables the VMD technology. - Disabled: disables the VMD technology.	Disabled
Enable/Disable VMD for Socket0 Stack4	Enables or disables the VMD technology for Socket0 Stack4. Enabled: enables the VMD technology.	Disabled

Parameter	Description	Default
	Disabled: disables the VMD technology.	
Enable/Disable VMD for Socket0 Stack5	Enables or disables the VMD technology for Socket0 Stack5. - Enabled: enables the VMD technology. - Disabled: disables the VMD technology.	Disabled
Enable/Disable VMD for Socket0 Stack6	Enables or disables the VMD technology for Socket0 Stack6. - Enabled: enables the VMD technology. - Disabled: disables the VMD technology.	Disabled

3.4.5.5 IIO DFX Configuration

Figure 3-105 shows the **IIO DFX Configuration** screen.

Figure 3-105 IIO DFX Configuration Screen



For a description of the parameters on the **IIO DFX Configuration** screen, refer to [Table 3-74](#).

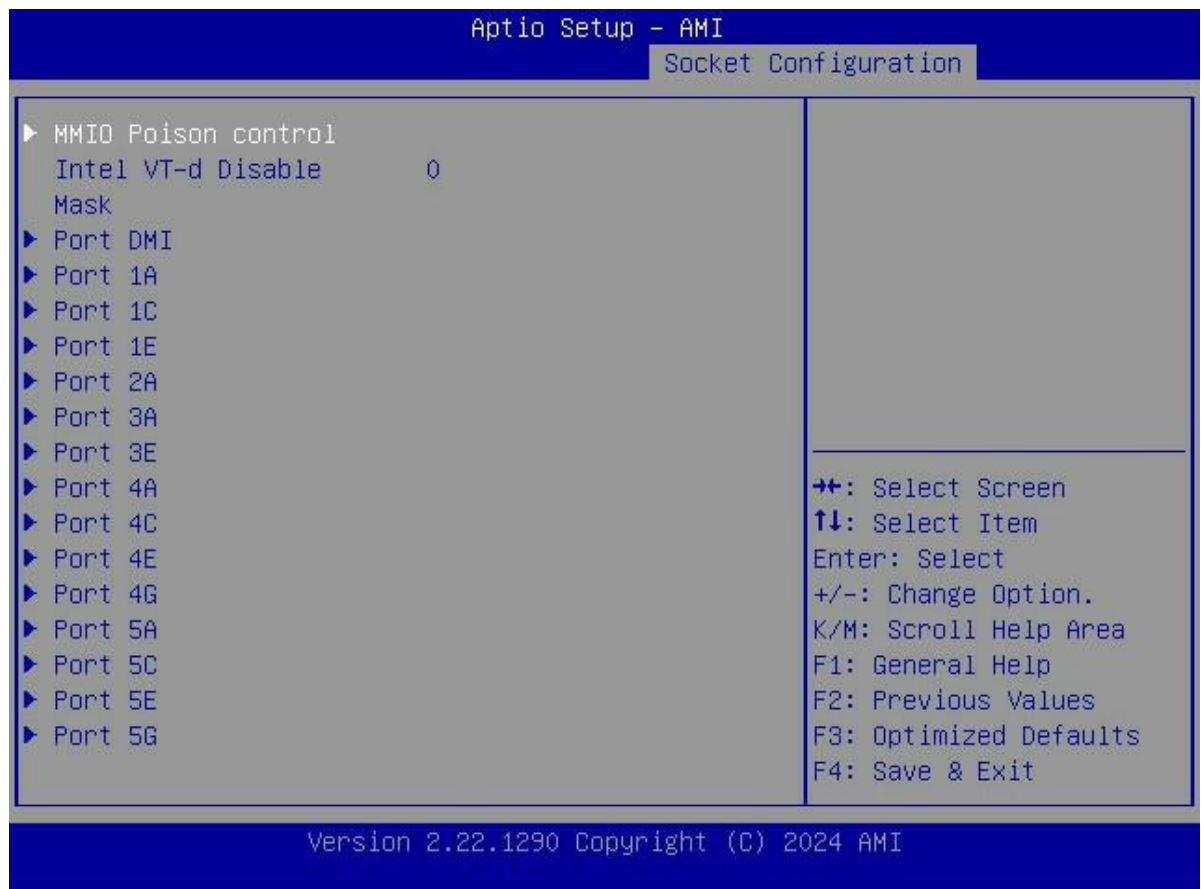
Table 3-74 Parameter Descriptions for the IIO DFX Configuration Screen

Parameter	Description	Default
Socket0 Configuration	Socket0 configuration.	-

Parameter	Description	Default
	Press the Enter key. The Socket0 Configuration screen is displayed, as shown in Figure 3-106 .	
Socket1 Configuration	Socket1 configuration, which is similar to the Socket0 configuration.	-
EV DFX Features	Enables or disables exposure of IIO DFX and other CPU devices (such as PMON). Options: ● Enabled: enables exposure of IIO DFX and other CPU devices (such as PMON). ● Disabled: disables exposure of IIO DFX and other CPU devices (such as PMON).	Disabled
Disable BIOS Done	Enables or disables the boot initialization completion notification sent to processors through MSR 151H . This parameter does not need to be set. Options: ● Enabled: enables the boot initialization completion notification sent to processors through MSR 151H. ● Disabled: disables the boot initialization completion notification sent to processors through MSR 151H.	Disabled
LTSSM Logger	Enables or disables the LTSSM logger for the PCIe feature. Options: ● Yes: enables the LTSSM logger for the PCIe feature. ● No: disables the LTSSM logger for the PCIe feature.	No
Stop	Stop value of the LTSSM logger.	99
Speed	Speed value of the LTSSM logger. Options: ● Gen 1 (2.5 GT/s) ● Gen 2 (5 GT/s) ● Gen 3 (8 GT/s)	Gen 1 (2.5GT/s)
Mask	Mask value of the LTSSM logger.	FF
Jitter Logger	Enables or disables the Jitter logger for the PCIe feature. Options: ● Yes: enables the Jitter logger for the PCIe feature. ● No: disables the Jitter logger for the PCIe feature.	No
IIO RC flow	Enables or disables the IIO RC flow. Options: ● Enabled: enables the IIO RC flow. ● Disabled: disables the IIO RC flow. ● Auto: enables the IIO RC flow.	Auto

Parameter	Description	Default
IIO PCIe link training	Enables or disables PCIe link training. Options: ● Enabled: enables PCIe link training. ● Disabled: disables PCIe link training. ● Auto.	Auto
Skip Port Personality Lock	Enables or disables the skipping of the port personality lock. Options: ● Enabled: enables the skipping of the port personality lock. When this parameter is set to Enabled, capability registers of PCI and DMI ports are not locked. ● Disabled: disables the skipping of the port personality lock.	Disabled
CXL Header Bypass	Enables or disables the CXL header bypass feature. Options: ● Enabled: enables the CXL header bypass feature. ● Disabled: disables the CXL header bypass feature.	Disabled
DINO Native PCIe	Enables or disables the native PCIe for the DINO device. Options: ● Enabled: enables the native PCIe for the DINO device. ● Disabled: disables the native PCIe for the DINO device.	Enabled
Trace Hub Allocation Flow	Enables or disables the flow for resource allocation for the Trace Hub. Options: ● Enabled: enables the flow for resource allocation for the Trace Hub. ● Disabled: disables the flow for resource allocation for the Trace Hub.	Enabled
Socket 0, Device Hide Menu	Hidden menu for devices connected to Socket0. Press the Enter key. The Socket 0, Device Hide Menu screen is displayed, as shown in Figure 3-112 .	-
Socket 1, Device Hide Menu	Hidden menu for devices connected to Socket1. This is similar to the hidden menu for devices connected to Socket0.	-

Figure 3-106 Socket0 Configuration Screen



For a description of the parameters on the **Socket0 Configuration** screen, refer to [Table 3-75](#).

Table 3-75 Socket0 Configuration Parameter Descriptions

Parameter	Description	Default
MMIO Poison control	MMIO poison control menu. Press the Enter key. The MMIO Poison control screen is displayed, as shown in Figure 3-107 .	-
Intel VT-d Disable Mask	Disables the bitmap of VT-d engines for debugging or diagnostic purposes.	0
Port DMI	Detailed port DMI configurations, as shown in Figure 3-108 through Figure 3-109 .	-
Port 1A	Detailed port 1A configurations, as shown in Figure 3-110 through Figure 3-111 .	-
Port 2A	Detailed port 2A configurations, which are similar to detailed port 1A configurations.	-
Port 2E	Detailed port 2E configurations, which are similar to detailed port 1A configurations.	-

Parameter	Description	Default
Port 3A	Detailed port 3A configurations, which are similar to detailed port 1A configurations.	-
Port 3E	Detailed port 3E configurations, which are similar to detailed port 1A configurations.	-
Port 4A	Detailed port 4A configurations, which are similar to detailed port 1A configurations.	-
Port 4C	Detailed port 4C configurations, which are similar to detailed port 1A configurations.	-
Port 4E	Detailed port 4E configurations, which are similar to detailed port 1A configurations.	-
Port 4G	Detailed port 4G configurations, which are similar to detailed port 1A configurations.	-
Port 5A	Detailed port 5A configurations, which are similar to detailed port 1A configurations.	-
Port 5C	Detailed port 5C configurations, which are similar to detailed port 1A configurations.	-
Port 5E	Detailed port 5E configurations, which are similar to detailed port 1A configurations.	-
Port 5G	Detailed port 5G configurations, which are similar to detailed port 1A configurations.	-

Figure 3-107 MMIO Poison Control Screen



For a description of the parameters on **MMIO Poison control** screen, refer to [Table 3-76](#).

Table 3-76 Parameter Descriptions for the MMIO Poison Control Screen

Parameter	Description	Default
Enable MMIO read cmpl poison for STACK_0	Enables or disables the poison feature for STACK_0 upon MMIO read completion. Options: ● Enabled: enables the poison feature for STACK_0 upon MMIO read completion. ● Disabled: disables the poison feature for STACK_0 upon MMIO read completion.	Disabled
Enable MMIO read cmpl poison for STACK_1	Enables or disables the poison feature for STACK_1 upon MMIO read completion. Options: ● Enabled: enables the poison feature for STACK_1 upon MMIO read completion. ● Enabled: disables the poison feature for STACK_1 upon MMIO read completion.	Disabled

Parameter	Description	Default
Enable MMIO read cmpl poison for STACK_2	Enables or disables the poison feature for STACK_2 upon MMIO read completion. Options: ● Enabled: enables the poison feature for STACK_2 upon MMIO read completion. ● Enabled: disables the poison feature for STACK_2 upon MMIO read completion.	Disabled
Enable MMIO read cmpl poison for STACK_3	Enables or disables the poison feature for STACK_3 upon MMIO read completion. Options: ● Enabled: enables the poison feature for STACK_3 upon MMIO read completion. ● Enabled: disables the poison feature for STACK_3 upon MMIO read completion.	Disabled
Enable MMIO read cmpl poison for STACK_4	Enables or disables the poison feature for STACK_4 upon MMIO read completion. Options: ● Enabled: enables the poison feature for STACK_4 upon MMIO read completion. ● Enabled: disables the poison feature for STACK_4 upon MMIO read completion.	Disabled
Enable MMIO read cmpl poison for STACK_5	Enables or disables the poison feature for STACK_5 upon MMIO read completion. Options: ● Enabled: enables the poison feature for STACK_5 upon MMIO read completion. ● Enabled: disables the poison feature for STACK_5 upon MMIO read completion.	Disabled

Figure 3-108 Port DMI Screen—1

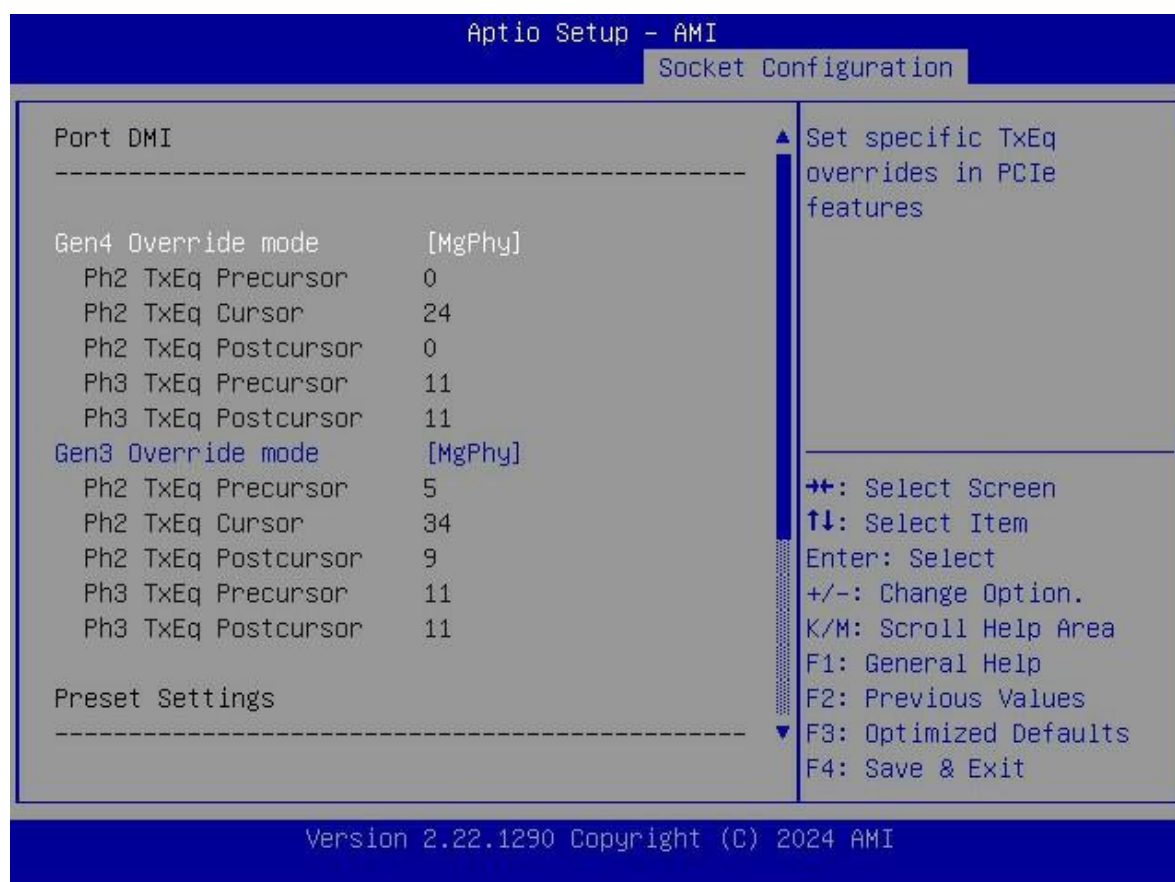
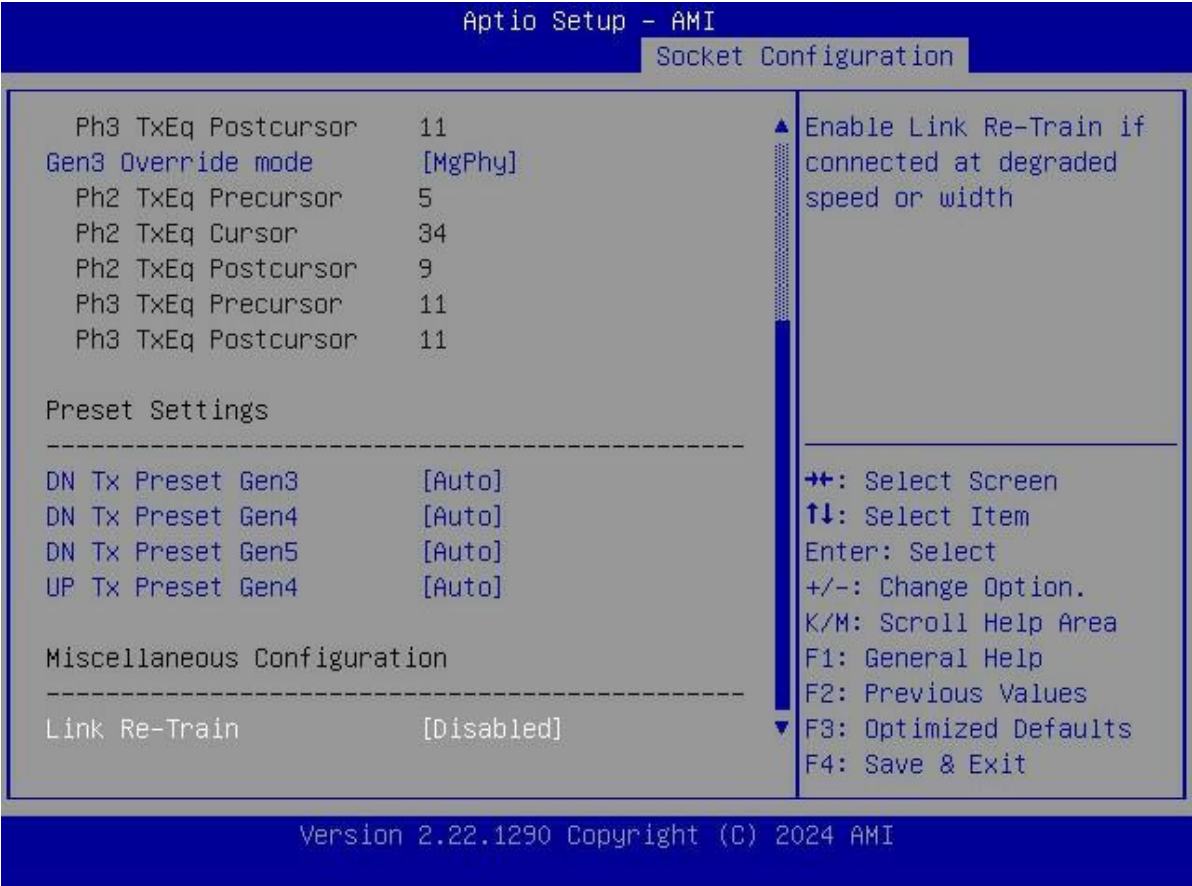


Figure 3-109 Port DMI Screen—2



For a description of the parameters on the **Port DMI** screen, refer to [Table 3-77](#).

Table 3-77 Parameter Descriptions for the Port DMI Screen

Parameter	Description	Default
Gen4 Override mode	Configures specific TxEq override mode in PCIe features. Options: ● MgPhy ● Manual ● Manual Ph2 ● Manual Ph3 ● Test Card	MgPhy
Ph2 TxEq Precursor	Overrides the Ph2 TXEQ pre-cursor.	0
Ph2 TxEq Cursor	Overwrites the Ph2 TXEQ cursor.	24
Ph2 TxEq Postcursor	Overrides the Ph2 TXEQ post-cursor.	0
Ph3 TxEq Precursor	Overrides the Ph3 TXEQ pre-cursor.	11
Ph3 TxEq Postcursor	Overrides the Ph3 TXEQ post-cursor.	11
Gen3 Override mode	Gen3 Override mode.	MgPhy

Parameter	Description	Default
Ph2 TxEq Cursor	Overwrites the Ph2 TxEq cursor.	5
Ph2 TxEq Postcursor	Overrides the Ph2 TXEQ post-cursor.	34
Ph3 TxEq Precursor	Overrides the Ph3 TXEQ pre-cursor.	9
Ph3 TxEq Postcursor	Overrides the Ph3 TXEQ post-cursor.	11
DN TX Preset Gen3	Presets PCIe downstream Tx for Gen3. Options: ● Auto ● P0(-6.0)/0.0dB ● P1(-3.5)/0.0 dB ● P2(-4.5)/0.0 dB ● P3(-2.5)/0.0 dB ● P4(0.0)/0.0dB ● P5(0.0)/2.0 dB ● P6(0.0)/2.5 dB ● P7(-6.0)/3.5 dB ● P8(-3.5)/3.5dB ● P9(0.0)/3.5 dB	11
DN TX Preset Gen4	Presets PCIe downstream Tx for Gen4. Options: ● Auto ● P0(-6.0)/0.0dB ● P1(-3.5)/0.0 dB ● P2(-4.5)/0.0 dB ● P3(-2.5)/0.0 dB ● P4(0.0)/0.0dB ● P5(0.0)/2.0 dB ● P6(0.0)/2.5 dB ● P7(-6.0)/3.5 dB ● P8(-3.5)/3.5dB ● P9(0.0)/3.5 dB	Auto
DN TX Preset Gen5	Presets PCIe downstream Tx for Gen5. Options: ● Auto ● P0(-6.0)/0.0dB ● P1(-3.5)/0.0 dB ● P2(-4.5)/0.0 dB ● P3(-2.5)/0.0 dB ● P4(0.0)/0.0dB ● P5(0.0)/2.0 dB ● P6(0.0)/2.5 dB	Auto

Parameter	Description	Default
	● P7(-6.0)/3.5 dB ● P8(-3.5)/3.5dB ● P9(0.0)/3.5 dB	
UP TX Preset Gen4	Presets PCIe upstream Tx for Gen4. Options: ● Auto ● P0(-6.0)/0.0dB ● P1(-3.5)/0.0 dB ● P2(-4.5)/0.0 dB ● P3(-2.5)/0.0 dB ● P4(0.0)/0.0dB ● P5(0.0)/2.0 dB ● P6(0.0)/2.5 dB ● P7(-6.0)/3.5 dB ● P8(-3.5)/3.5dB ● P9(0.0)/3.5 dB	Auto
Link Re-Train	Enables or disables link retraining. Link retraining need to be enabled if the speed or bandwidth for connection is reduced. Options: ● Enabled: enables link retraining. ● Disabled: disables link retraining.	Disabled

Figure 3-110 Port 1A Screen—1

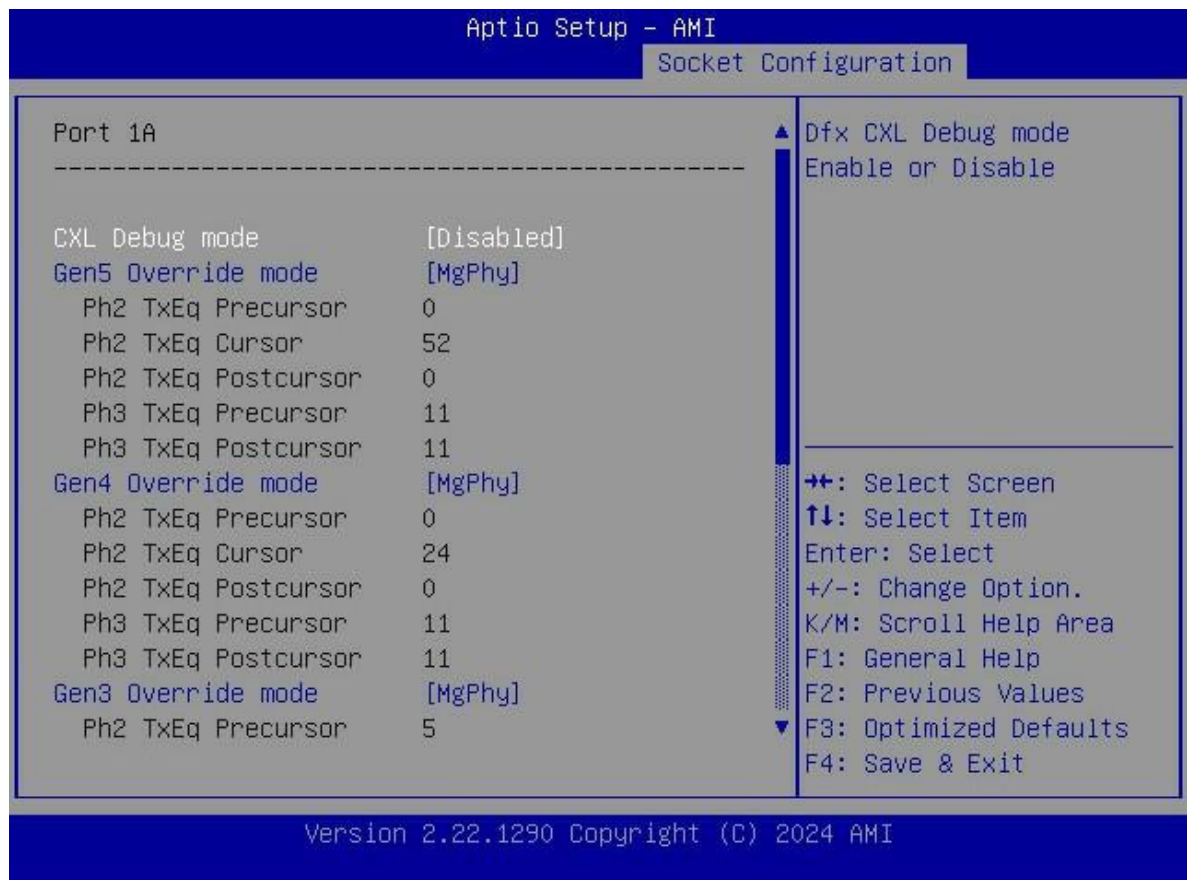
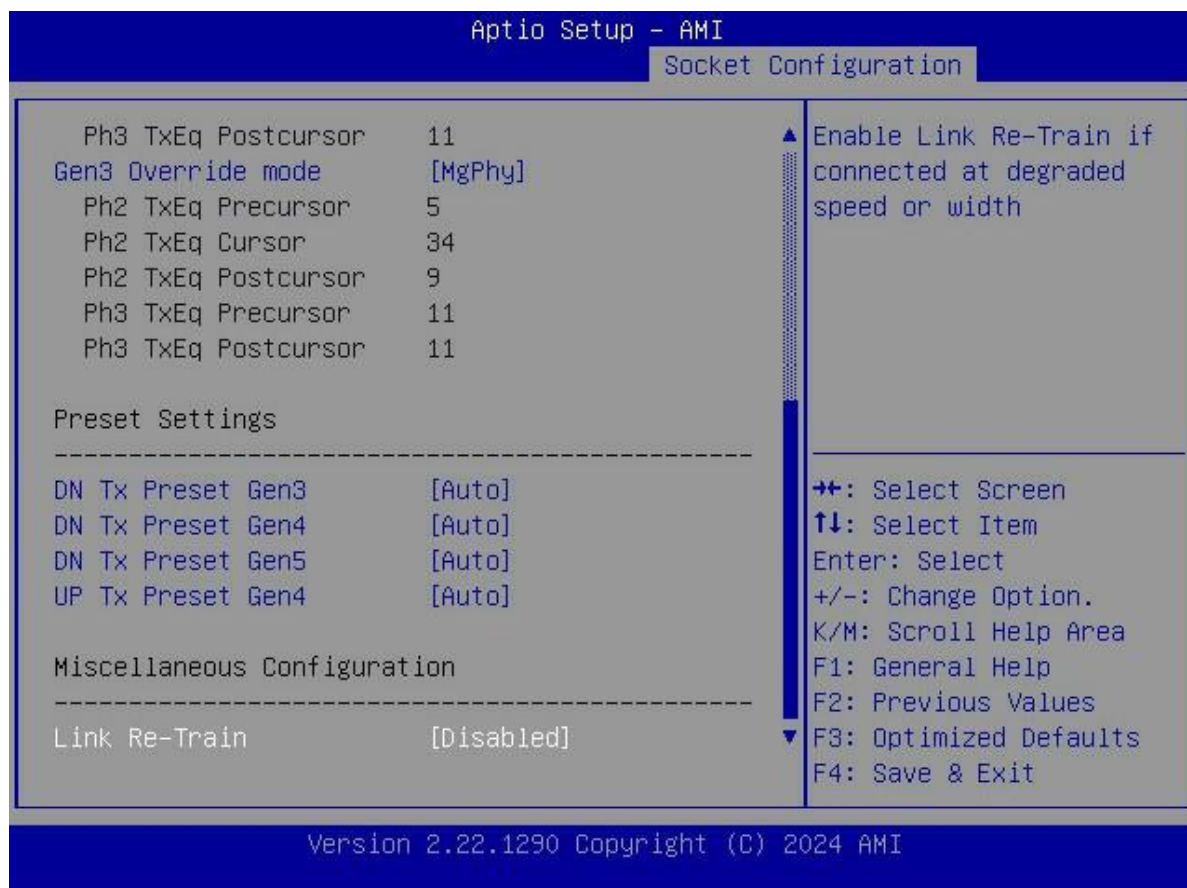


Figure 3-111 Port 1A Screen—2

For a description of the parameters on the **Port 1A** screen, refer to [Table 3-78](#).

Table 3-78 Port 1A Parameter Descriptions

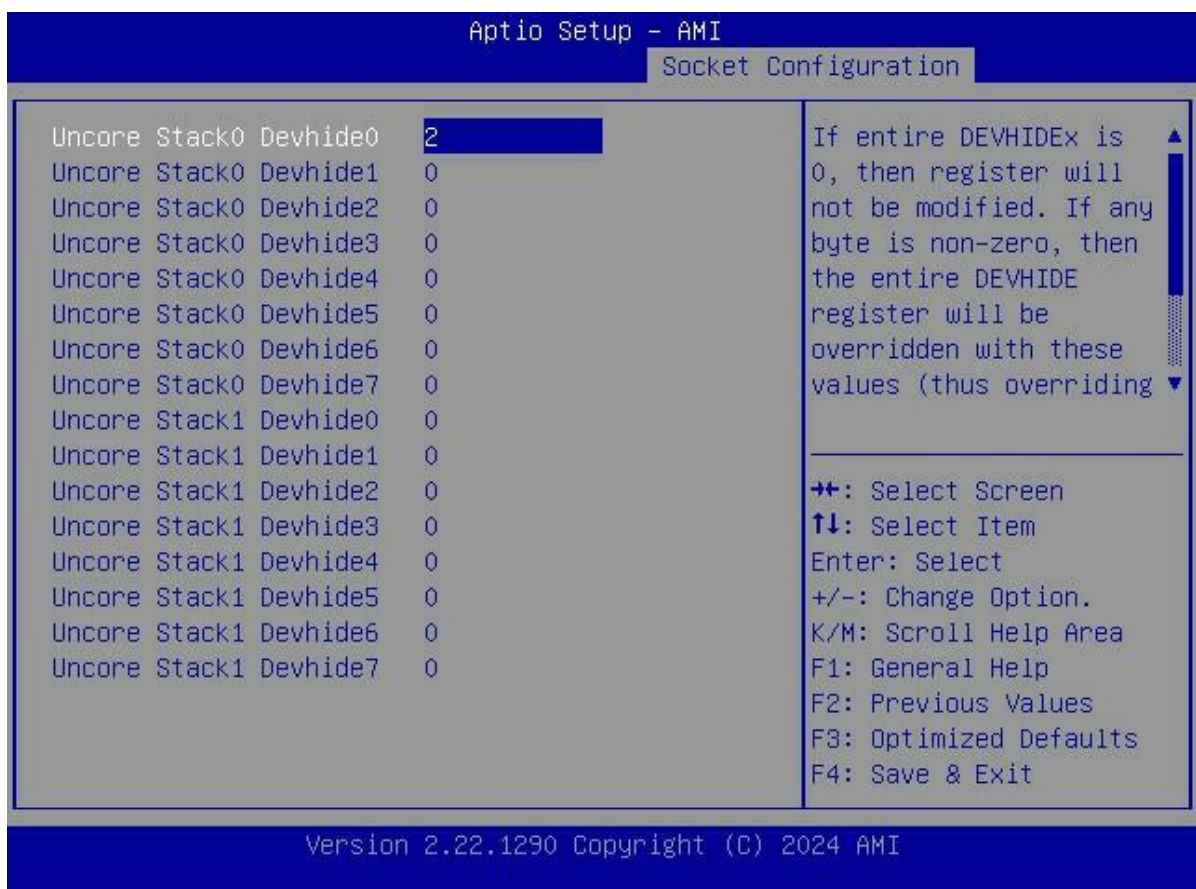
Parameter	Description	Default
CXL Debug mode	Enables or disables CXL debugging mode. Options: - Enabled: enables CXL debugging mode. - Disabled: disables CXL debugging mode.	Disabled
Gen5 Override mode	Configures specific TXEQ override mode in PCIe features. Options: - MgPhy - Manual - Manual Ph2 - Manual Ph3 - Test Card	MgPhy
Ph2 TxEq Precursor	Overrides the Ph2 TXEQ pre-cursor.	0
Ph2 TxEq Cursor	Overrides the Ph2 TXEQ cursor.	52

Parameter	Description	Default
Ph2 TxEq Postcursor	Overrides the Ph2 TXEQ post-cursor.	0
Ph3 TxEq Precursor	Overrides the Ph3 TXEQ pre-cursor.	11
Ph3 TxEq Postcursor	Overrides the Ph3 TXEQ post-cursor.	11
Gen4 Override mode	Configures specific TXEQ override mode in PCIe features. Options: ● MgPhy ● Manual ● Manual Ph2 ● Manual Ph3 ● Test Card	MgPhy
Ph2 TxEq Precursor	Overrides the Ph2 TXEQ pre-cursor.	0
Ph2 TxEq Cursor	Overrides the Ph2 TXEQ cursor.	24
Ph2 TxEq Postcursor	Overrides the Ph2 TXEQ post-cursor.	0
Ph3 TxEq Precursor	Overrides the Ph3 TXEQ pre-cursor.	11
Ph3 TxEq Postcursor	Overrides the Ph3 TXEQ post-cursor.	11
Gen3 Override mode	Configures specific TXEQ override mode in PCIe features. Options: ● MgPhy ● Manual ● Manual Ph2 ● Manual Ph3 ● Test Card	MgPhy
Ph2 TxEq Precursor	Overrides the Ph2 TXEQ pre-cursor.	5
Ph2 TxEq Cursor	Overrides the Ph2 TXEQ cursor.	34
Ph2 TxEq Postcursor	Overrides the Ph2 TXEQ post-cursor.	9
Ph3 TxEq Precursor	Overrides the Ph3 TXEQ pre-cursor.	11
Ph3 TxEq Postcursor	Overrides the Ph3 TXEQ post-cursor.	11
DN TX Preset Gen3	Presets PCIe downstream Tx for Gen3. Options: ● Auto ● P0(-6.0)/0.0dB ● P1(-3.5)/0.0 dB ● P2(-4.5)/0.0 dB ● P3(-2.5)/0.0 dB	Auto

Parameter	Description	Default
	● P4(0.0)/0.0dB ● P5(0.0)/2.0 dB ● P6(0.0)/2.5 dB ● P7(-6.0)/3.5 dB ● P8(-3.5)/3.5dB ● P9(0.0)/3.5 dB	
DN TX Preset Gen4	Presets PCIe downstream Tx for Gen4. Options: ● Auto ● P0(-6.0)/0.0dB ● P1(-3.5)/0.0 dB ● P2(-4.5)/0.0 dB ● P3(-2.5)/0.0 dB ● P4(0.0)/0.0dB ● P5(0.0)/2.0 dB ● P6(0.0)/2.5 dB ● P7(-6.0)/3.5 dB ● P8(-3.5)/3.5dB ● P9(0.0)/3.5 dB	Auto
DN TX Preset Gen5	Presets PCIe downstream Tx for Gen5. Options: ● Auto ● P0(-6.0)/0.0dB ● P1(-3.5)/0.0 dB ● P2(-4.5)/0.0 dB ● P3(-2.5)/0.0 dB ● P4(0.0)/0.0dB ● P5(0.0)/2.0 dB ● P6(0.0)/2.5 dB ● P7(-6.0)/3.5 dB ● P8(-3.5)/3.5dB ● P9(0.0)/3.5 dB	Auto
UP TX Preset Gen4	Presets PCIe upstream Tx for Gen4. Options: ● Auto ● P0(-6.0)/0.0dB ● P1(-3.5)/0.0 dB ● P2(-4.5)/0.0 dB ● P3(-2.5)/0.0 dB ● P4(0.0)/0.0dB ● P5(0.0)/2.0 dB ● P6(0.0)/2.5 dB	Auto

Parameter	Description	Default
	● P7(-6.0)/3.5 dB) ● P8(-3.5)/3.5dB) ● P9(0.0)/3.5 dB)	
Link Re-Train	Enables or disables link retraining. Link retraining need to be enabled if the speed or bandwidth for connection is reduced. Options: ● Enabled: enables link retraining. ● Disabled: disables link retraining.	Disabled

Figure 3-112 Socket 0, Device Hide Menu Screen



For a description of the parameters on the **Socket 0, Device Hide Menu** screen, refer to [Table 3-79](#).

Table 3-79 Parameter Descriptions for the Socket 0, Device Hide Menu Screen

Parameter	Description	Default
Uncore Stack0 Devhide0	If the entire DEVHIDEx is 0, it is not modified. If any byte is non-zero, the entire DEVHIDE register is overridden with these values (thus	0

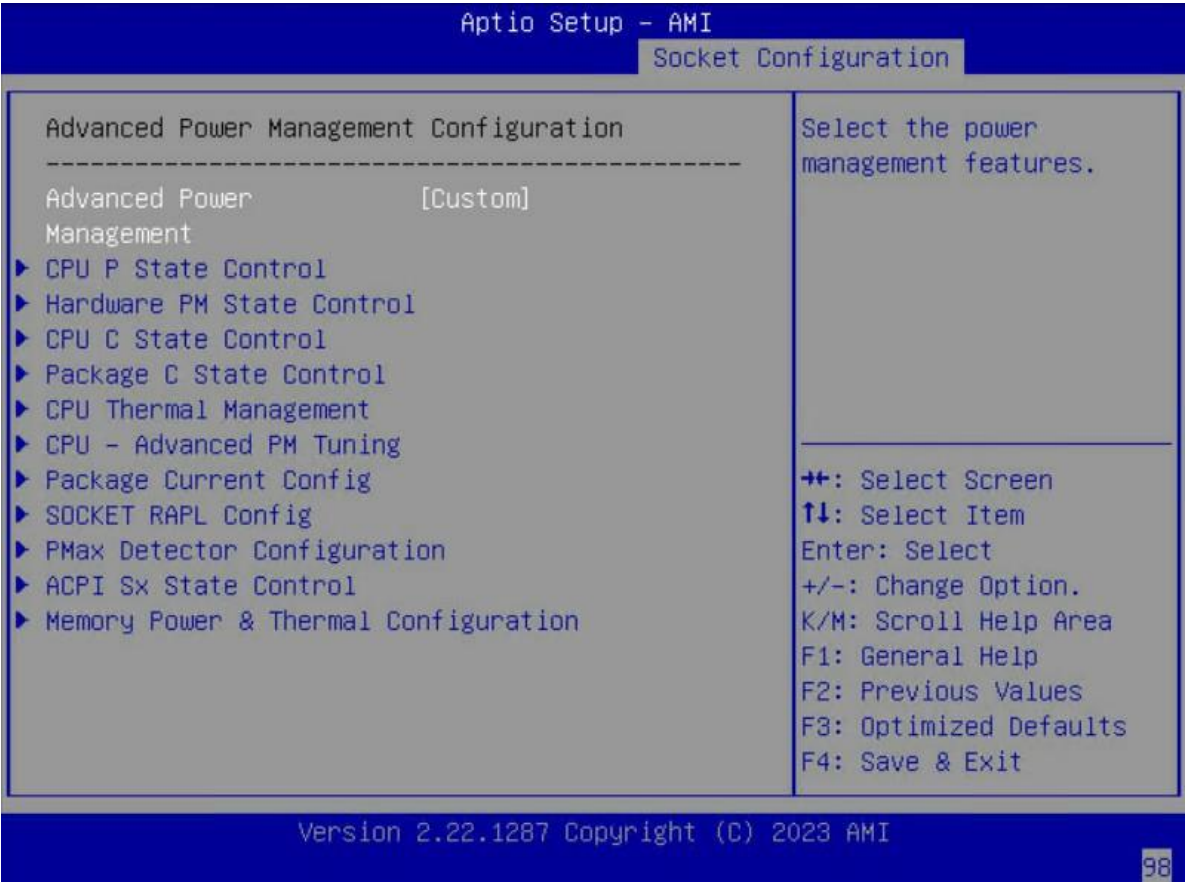
Parameter	Description	Default
	overriding any other HIDE option in setup such as PCIe port hide questions).	
Uncore Stack0 Devhide1	If the entire DEVHIDEx is 0, it is not modified. If any byte is non-zero, the entire DEVHIDE register is overridden with these values (thus overriding any other HIDE option in setup such as PCIe port hide questions).	0
Uncore Stack0 Devhide2	If the entire DEVHIDEx is 0, it is not modified. If any byte is non-zero, the entire DEVHIDE register is overridden with these values (thus overriding any other HIDE option in setup such as PCIe port hide questions).	0
Uncore Stack0 Devhide3	If the entire DEVHIDEx is 0, it is not modified. If any byte is non-zero, the entire DEVHIDE register is overridden with these values (thus overriding any other HIDE option in setup such as PCIe port hide questions).	0
Uncore Stack0 Devhide4	If the entire DEVHIDEx is 0, it is not modified. If any byte is non-zero, the entire DEVHIDE register is overridden with these values (thus overriding any other HIDE option in setup such as PCIe port hide questions).	0
Uncore Stack0 Devhide5	If the entire DEVHIDEx is 0, it is not modified. If any byte is non-zero, the entire DEVHIDE register is overridden with these values (thus overriding any other HIDE option in setup such as PCIe port hide questions).	0
Uncore Stack0 Devhide6	If the entire DEVHIDEx is 0, it is not modified. If any byte is non-zero, the entire DEVHIDE register is overridden with these values (thus overriding any other HIDE option in setup such as PCIe port hide questions).	0
Uncore Stack0 Devhide7	If the entire DEVHIDEx is 0, it is not modified. If any byte is non-zero, the entire DEVHIDE register is overridden with these values (thus overriding any other HIDE option in setup such as PCIe port hide questions).	0
Uncore Stack1 Devhide0	If the entire DEVHIDEx is 0, it is not modified. If any byte is non-zero, the entire DEVHIDE	0

Parameter	Description	Default
	register is overridden with these values (thus overriding any other HIDE option in setup such as PCIe port hide questions).	
Uncore Stack1 Devhide1	If the entire DEVHIDEx is 0, it is not modified. If any byte is non-zero, the entire DEVHIDE register is overridden with these values (thus overriding any other HIDE option in setup such as PCIe port hide questions).	0
Uncore Stack1 Devhide2	If the entire DEVHIDEx is 0, it is not modified. If any byte is non-zero, the entire DEVHIDE register is overridden with these values (thus overriding any other HIDE option in setup such as PCIe port hide questions).	0
Uncore Stack1 Devhide3	If the entire DEVHIDEx is 0, it is not modified. If any byte is non-zero, the entire DEVHIDE register is overridden with these values (thus overriding any other HIDE option in setup such as PCIe port hide questions).	0
Uncore Stack1 Devhide4	If the entire DEVHIDEx is 0, it is not modified. If any byte is non-zero, the entire DEVHIDE register is overridden with these values (thus overriding any other HIDE option in setup such as PCIe port hide questions).	0
Uncore Stack1 Devhide5	If the entire DEVHIDEx is 0, it is not modified. If any byte is non-zero, the entire DEVHIDE register is overridden with these values (thus overriding any other HIDE option in setup such as PCIe port hide questions).	0
Uncore Stack1 Devhide6	If the entire DEVHIDEx is 0, it is not modified. If any byte is non-zero, the entire DEVHIDE register is overridden with these values (thus overriding any other HIDE option in setup such as PCIe port hide questions).	0
Uncore Stack1 Devhide7	If the entire DEVHIDEx is 0, it is not modified. If any byte is non-zero, the entire DEVHIDE register is overridden with these values (thus overriding any other HIDE option in setup such as PCIe port hide questions).	0

3.4.6 Advanced Power Management Configuration

Figure 3-113 shows the **Advanced Power Management Configuration** screen.

Figure 3-113 Advanced Power Management Configuration Screen



For a description of the parameters on the **Advanced Power Management Configuration** screen, refer to [Table 3-80](#).

Table 3-80 Parameter Descriptions for the Advanced Power Management Configuration Screen

Parameter	Description	Default
Advanced Power Management	Sets the power policy. Options: ● Performance: performance mode. ● Efficient: energy-saving mode. ● Custom: user-defined mode. ● Latency-Performance: low latency mode. ● Maximum-Performance: maximum performance mode. ● Low Latency: low latency mode. ● Virtualization-Performance: virtualization performance mode. ● Transactional Application Processing: transactional application processing mode.	Custom

Parameter	Description	Default
	- General Throughput Compute: general throughput computation mode. - Advanced Reliability Mode: advanced reliability mode. - Graphic Processing: graphic processing mode. - AI Optimized: AI optimization mode.	
CPU P State Control	Sets CPU P-state control parameters. Enables or disables Turbo mode and EIST . For details, refer to 3.4.6.1 CPU P State Control .	-
Hardware PM State Control	Sets hardware PM state control parameters. For details, refer to 3.4.6.2 Hardware PM State Control .	-
CPU C State Control	Sets CPU C-state control parameters. The purpose is to control the CPU power consumption in idle state. For details, refer to 3.4.6.3 CPU C State Control .	-
Package C State Control	Sets the Package C-state control parameters. For details, refer to 3.4.6.4 Package C State Control .	-
CPU Thermal Management	Sets the CPU thermal management parameters. For details, refer to 3.4.6.5 CPU Thermal Management .	-
CPU-Advanced PM Tuning	Sets CPU advanced PM adjustment parameters. For details, refer to 3.4.6.6 CPU-Advanced PM Tuning .	-
Package Current Config	Sets the current Package parameters. For details, refer to 3.4.6.7 Package Current Config .	-
SOCKET RAPL Config	Sets SOCKET RAPL parameters. For details, refer to 3.4.6.8 SOCKET RAPL Config .	-
PMax Detector Configuration	Sets PMax probe parameters. For details, refer to 3.4.6.9 PMAX Detector Configuration .	-
ACPI Sx State Control	Sets ACPI Sx state control parameters. For details, refer to 3.4.6.10 ACPI Sx State Control .	-
Memory Power & Thermal Configuration	Sets memory power and thermal parameters. For details, refer to 3.4.6.11 Memory Power & Thermal Configuration .	-

3.4.6.1 CPU P State Control

[Figure 3-114](#) through [Figure 3-115](#) show the **CPU P State Control** screen.

Figure 3-114 CPU P State Control Screen—1

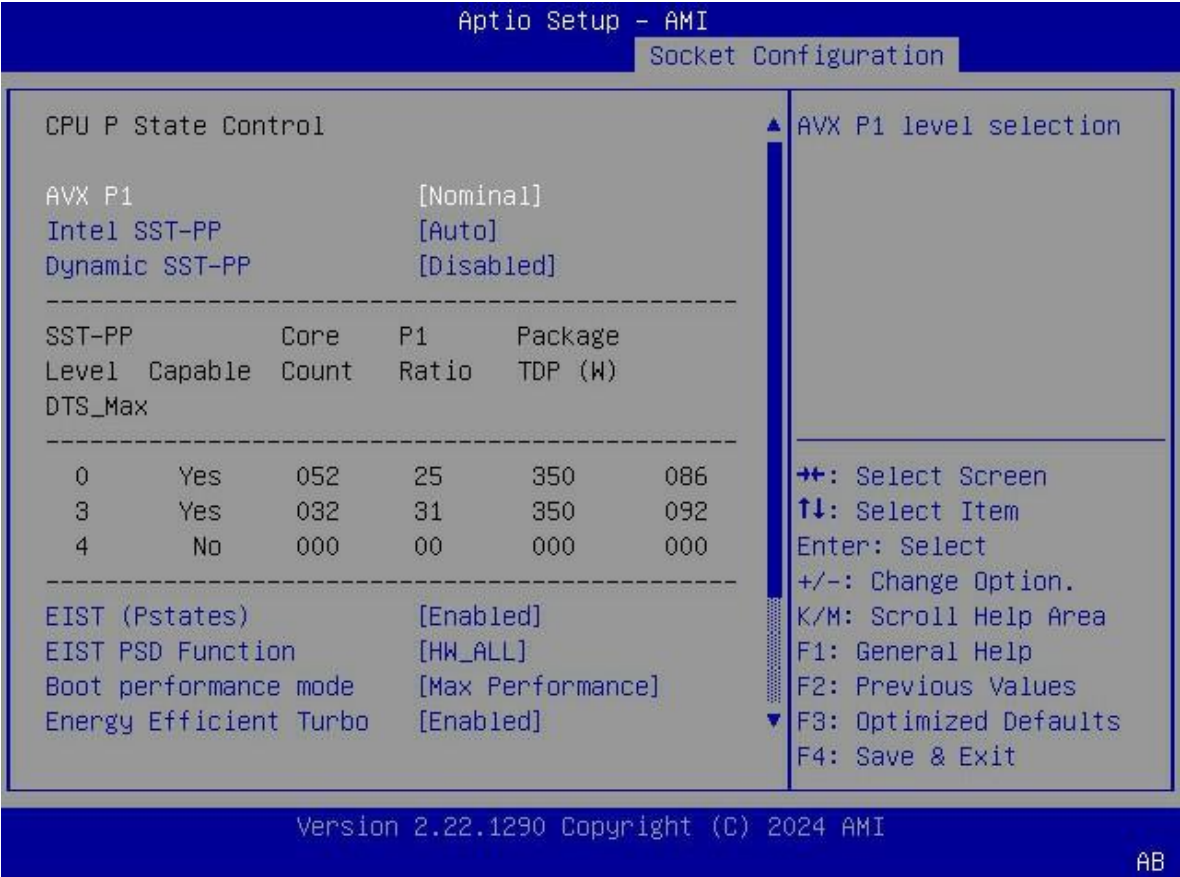
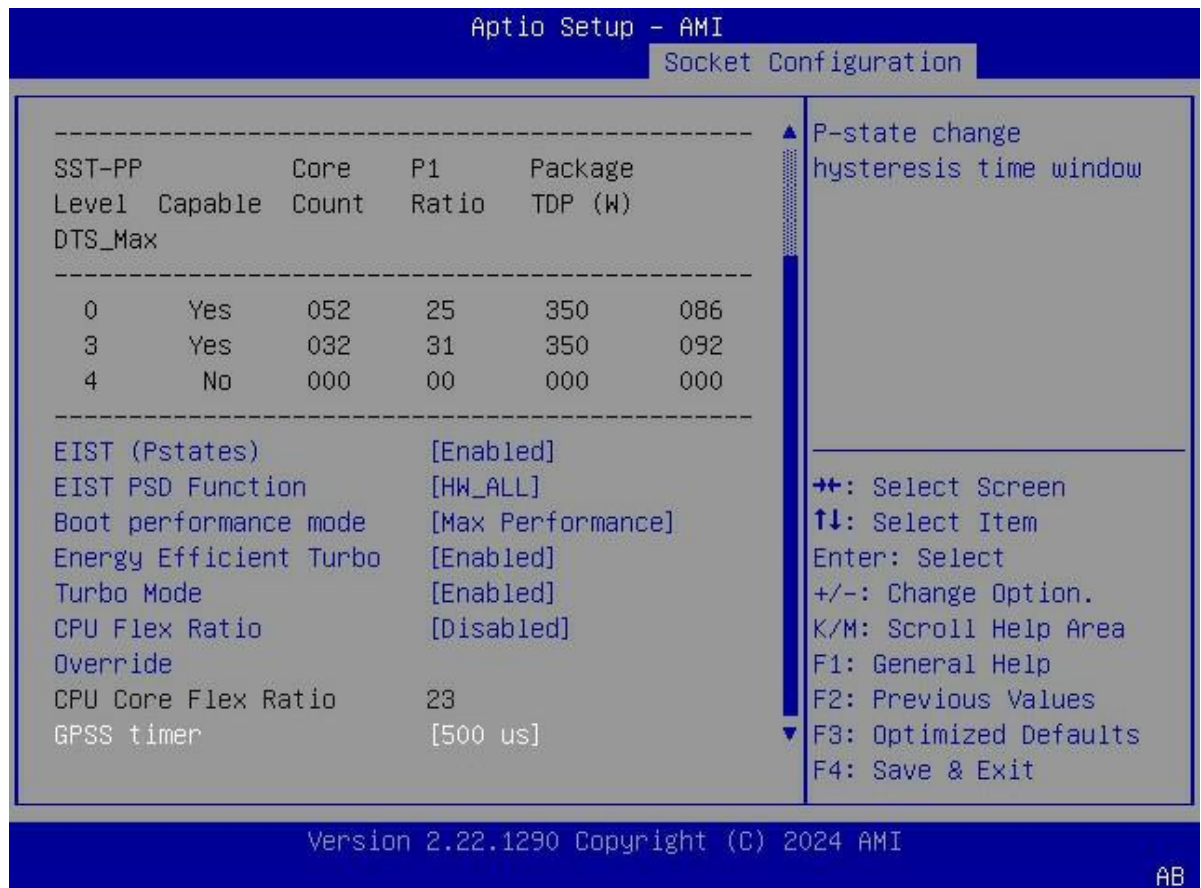


Figure 3-115 CPU P State Control Screen—2



For a description of the parameters on the **CPU P State Control** screen, refer to [Table 3-81](#).

Table 3-81 Parameter Descriptions for the CPU P State Control Screen

Parameter	Description	Default
AVX P1	This parameter is displayed when EIST (Pstates) is set to Enabled. Sets the AVX P1 level. Options: ● Nominal ● Level 1 ● Level 2	Nominal
Intel SST-PP	This parameter is displayed when EIST (Pstates) is set to Enabled. Select the level that Intel SST-PP allows the user to select. Options: ● Auto ● Level 0 ● Level 3 ● Level 4	Auto

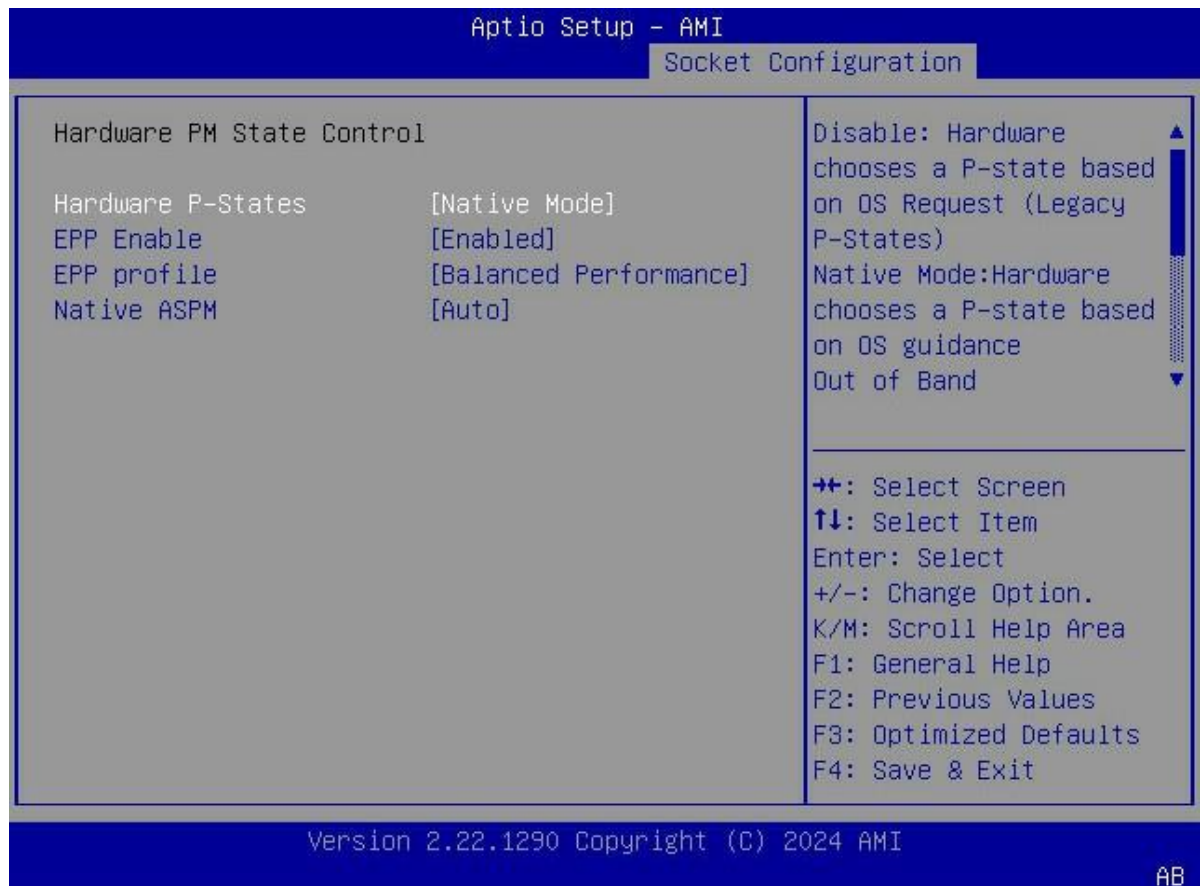
Parameter	Description	Default
EIST (Pstates)	Enables or disables the EIST feature. Options: ● Enabled: enables the EIST feature. ● Disabled: disables the EIST feature.	Enabled
EIST PSD Function	This parameter can be configured when EIST (Pstates) is set to Enabled . Sets the EIST PSD feature. Options: ● HW_ALL ● SW_ALL	HW_ALL
Boot Performance Mode	This parameter can be configured when EIST (Pstates) is set to Enabled . Select the boot performance mode. Options: ● Max Performance: maximum performance mode. ● Max Efficient: maximum efficient mode. ● Set by Intel Node Manager: The boot performance mode is controlled by the ME.	Max Performance
Energy Efficient Turbo	Enables or disables the energy efficient Turbo mode. Options: ● Enabled: enables energy efficient Turbo mode. ● Disabled: disables energy efficient Turbo mode.	Enabled
Turbo Mode	This parameter is displayed when EIST (Pstates) is set to Enabled . Enables or disables Turbo mode. Options: ● Enabled: enables Turbo mode. ● Disabled: disables Turbo mode.	Enabled
CPU Flex Ratio Override	Enables or disables the setting of the processor flex ratio. Options: ● Enabled: enables the setting of the processor flex ratio. ● Disabled: disables the setting of the processor flex ratio.	Disabled
CPU Core Flex Ratio	Enter the processor flex ratio.	23
GPSS timer	Select the time window for P-state handover delay. Options: ● 0 us	500 us

Parameter	Description	Default
	• 50 us • 500 us	

3.4.6.2 Hardware PM State Control

Figure 3-116 shows the **Hardware PM State Control** screen.

Figure 3-116 Hardware PM State Control Screen



For a description of the parameters on the **Hardware PM State Control** screen, refer to [Table 3-82](#).

Table 3-82 Parameter Descriptions for the Hardware PM State Control Screen

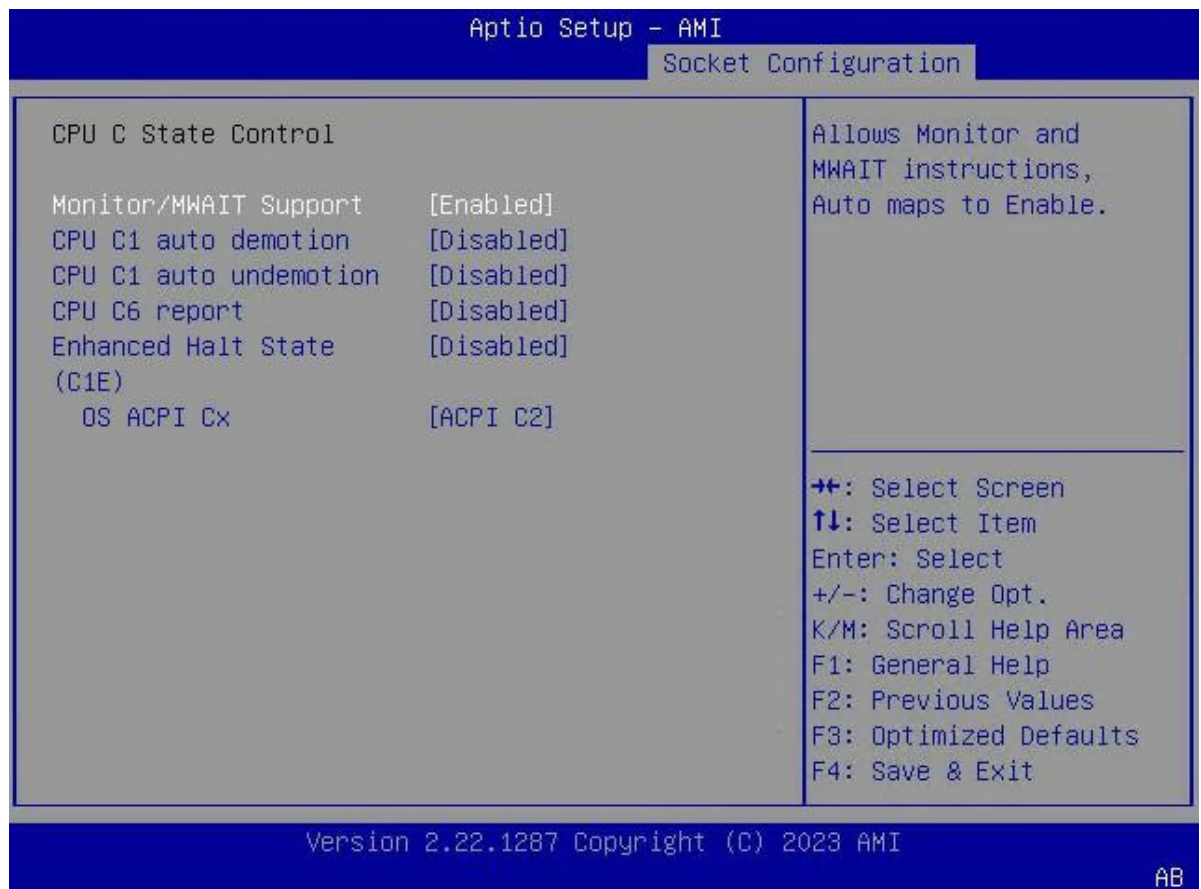
Parameter	Description	Default
Hardware P-States	Sets hardware P-states. Options: • Native Mode: Hardware autonomously chooses a P-state based on OS guidance. • Out of Band Mode: Hardware autonomously chooses a P-state (no OS guidance).	Disabled

Parameter	Description	Default
	- Native Mode with No Legacy Support: Hardware autonomously chooses a P-state based on OS guidance (without Legacy support). - Disabled: disables the hardware P-state feature. Hardware chooses a Legacy P-state based on an OS request.	
EPP Enable	This parameter cannot be set when Hardware P-States is set to Disabled. Enables or disables the EPP feature. Options: - Enabled: enables the EPP feature. - Disabled: disables the EPP feature.	Enabled
EPP profile	This parameter is displayed when Hardware P-States is set to Out of Band Mode. This parameter cannot be set when EPP Enable is set to Disabled. Sets the EPP mode. Options: - Performance: performance mode. - Balanced Performance: balanced performance mode. - Balanced Power: balanced energy-saving mode. - Power: power saving mode.	Balanced Performance
Native ASPM	Enables or disables the ASPM feature. Options: - Enabled: enables the ASPM feature, which is controlled by the OS. - Disabled: disables the ASPM feature. - Auto: enables the ASPM feature, which is controlled by the BIOS.	Auto

3.4.6.3 CPU C State Control

Figure 3-117 shows the **CPU C State Control** screen.

Figure 3-117 CPU C State Control Screen



For a description of the parameters on the **CPU C State Control** screen, refer to [Table 3-83](#).

Table 3-83 Parameter Descriptions for the CPU C State Control Screen

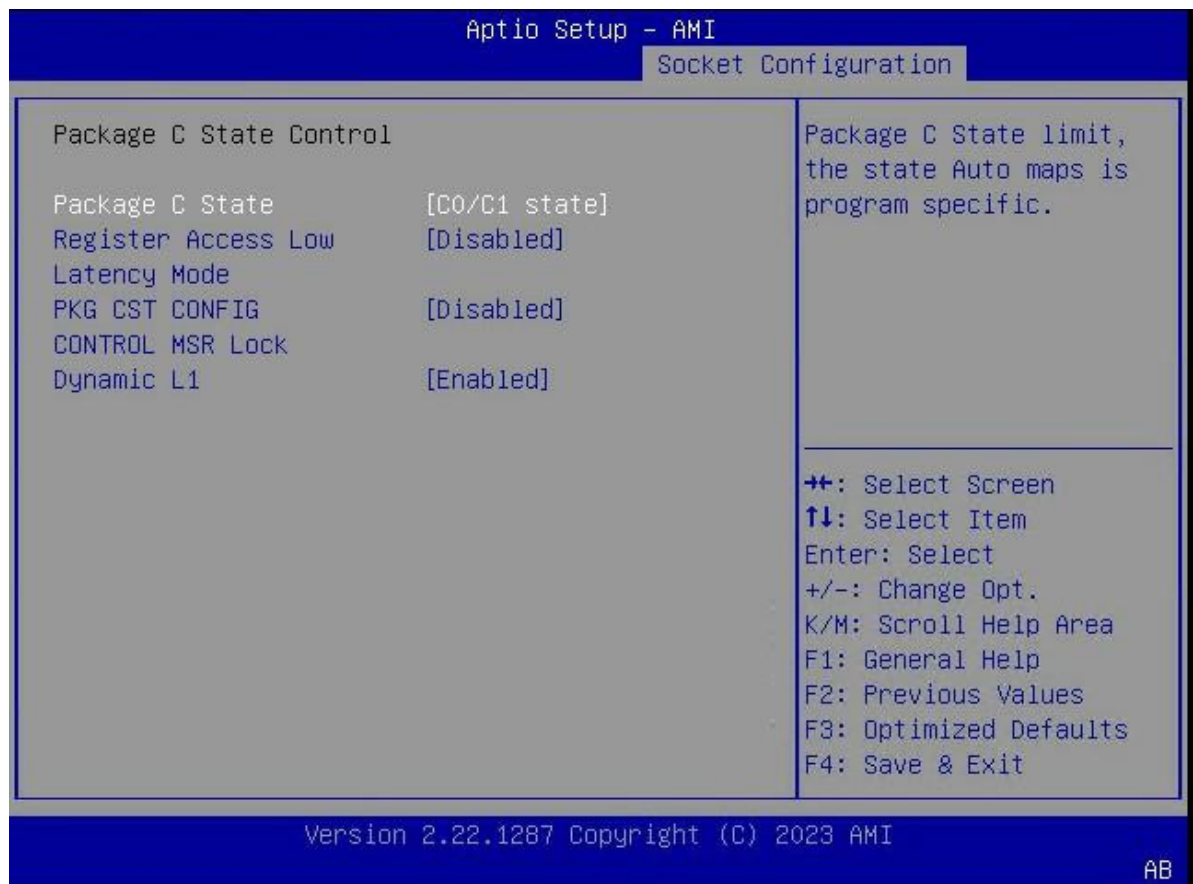
Parameter	Description	Default
Monitor/MWAIT Support	Enables or disables Monitor/Mwait instructions. Options: ● Enabled: enables Monitor/Mwait instructions. ● Disabled: disables Monitor/Mwait instructions. ● Auto. For some OSs , you must disable both Monitor/Mwait and C State to completely disable C State.	Enabled
CPU C1 auto demotion	Sets whether to allow the CPUs to automatically demote themselves to C1. The modification takes effect after the system is restarted. Options: ● Enabled: enables automatic CPU demotion to C1. ● Disabled: disables automatic CPU demotion to C1.	Disabled

Parameter	Description	Default
CPU C1 auto undemotion	Sets whether to allow the CPUs to automatically undemote from C1. The modification takes effect after the system is restarted. Options: ● Enabled: enables the CPUs to automatically undemote from C1. ● Disabled: disables the automatic CPU undemotion from C1.	Disabled
CPU C6 report	Sets whether to report the C6 state to the OS. Options: ● Enabled: enables C6 state reporting to the OS. ● Disabled: disables C6 state reporting to the OS ● Auto: enables C6 state reporting to the OS.	Disabled
Enhanced Halt State(C1E)	Enables or disables the Enhanced Halt State feature. Options: ● Enabled: enables the Enhanced Halt State feature. When this parameter is set to Enabled, the OS can adjust the C state. ● Disabled: disables the Enhanced Halt State feature.	Disabled
OS ACPI Cx	Sets the mapping relationship between CPU C-states and ACPI C-states. Options: ● ACPI C2: ACPI C2 mode. ● ACPI C3: ACPI C3 mode.	ACPI C2

3.4.6.4 Package C State Control

Figure 3-118 shows the **Package C State Control** screen.

Figure 3-118 Package C State Control Screen



For a description of the parameters on the **Package C State Control** screen, refer to [Table 3-84](#).

Table 3-84 Parameter Descriptions for the Package C State Control Screen

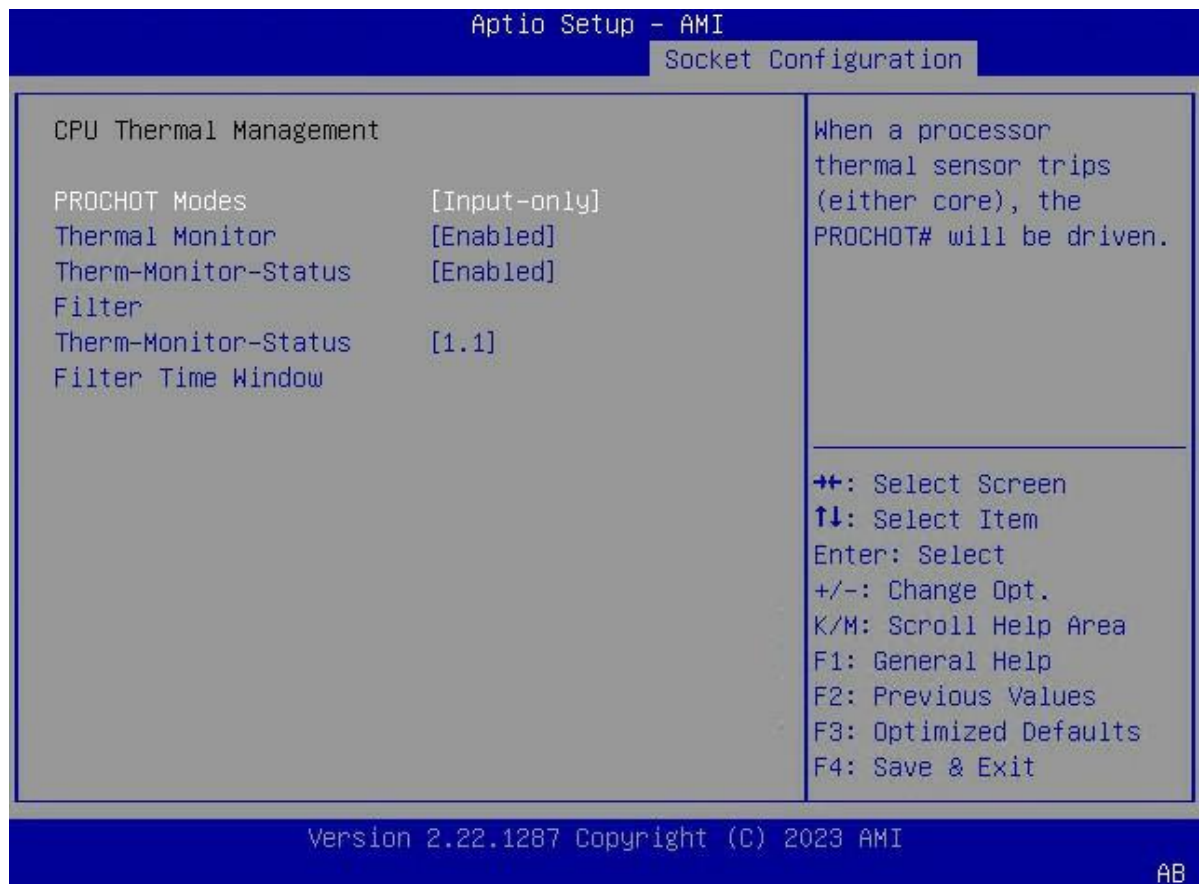
Parameter	Description	Default
Package C State	Sets the Package C State limit. Options: ● C2 state ● C6 (non Retention) state ● C6(Retention) state ● No Limit ● Auto: automatically sets this parameter based on the CPU configuration: ➔ If SPR D0 CPUs are configured and no more than four CPUs are present, this parameter is set to C6(Retention) state. ➔ If EMR CPUs are configured and no more than two CPUs are present, this parameter is set to C6(Retention) state.	C0/C1 state

Parameter	Description	Default
	➔ In other cases, this parameter is set to C0/C1 state.	
Register Access Low Latency Mode	Enables or disables low latency mode for register access. Options: ● Enabled: enables low latency mode for register access. ● Disabled: disables low latency mode for register access.	Disabled
PKG CST CONFIG CONTROL MSR Lock	Enables or disables the MSR E2h lock. Options: ● Enabled: enables the MSR E2h lock. ● Disabled: disables the MSR E2h lock.	Disabled
Dynamic L1	Enables or disables the dynamic L1 feature. Options: ● Enabled: enables the dynamic L1 feature. ● Disabled: disables the dynamic L1 feature.	Enabled

3.4.6.5 CPU Thermal Management

Figure 3-119 shows the **CPU Thermal Management** screen.

Figure 3-119 CPU Thermal Management Screen



For a description of the parameters on the **CPU Thermal Management** screen, refer to [Table 3-85](#).

Table 3-85 Parameter Descriptions for the CPU Thermal Management Screen

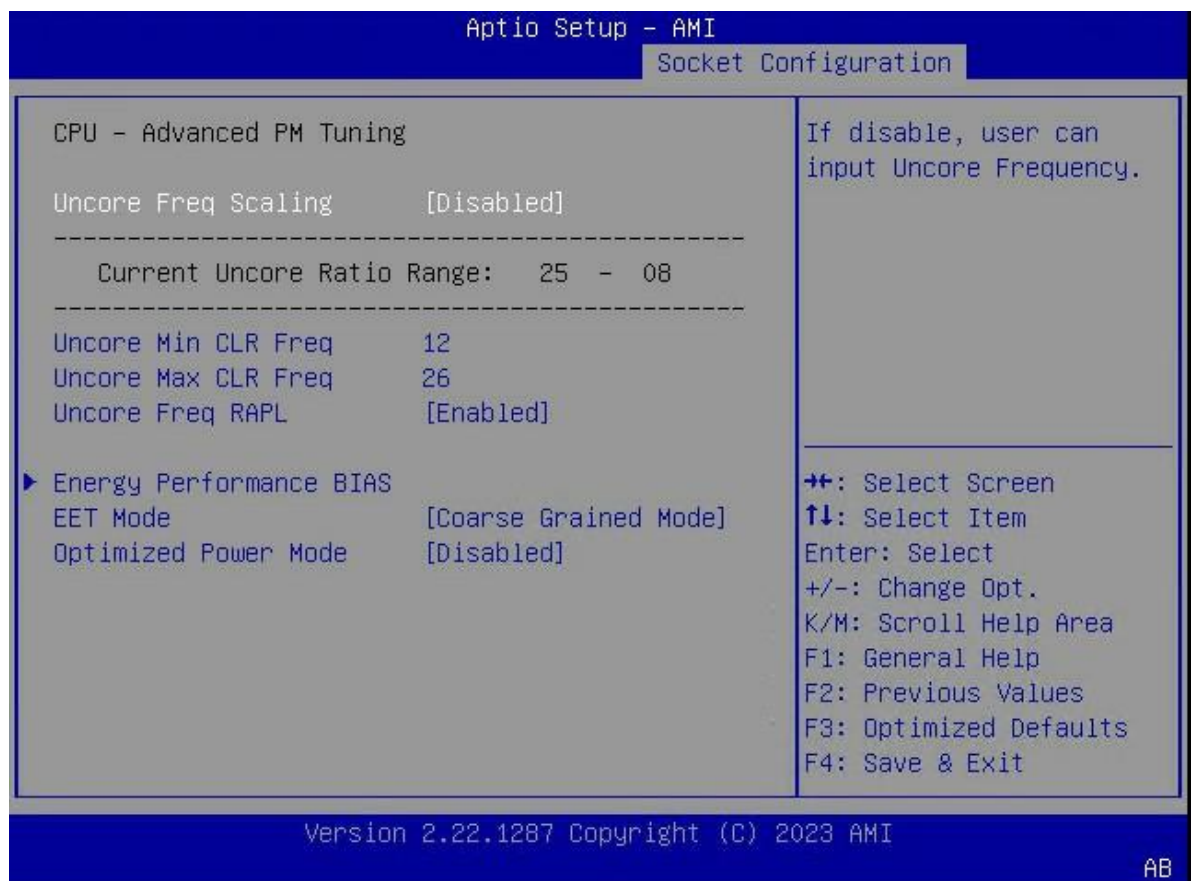
Parameter	Description	Default
PROCHOT Modes	Enables or disables PROCHOT. Options: - Input-only: enables PROCHOT when the processor thermal sensor trips (any core). - Disabled: disables PROCHOT.	Input-only
Thermal Monitor	Enables or disables thermal sensor. Options: - Enabled: enables thermal sensor. - Disabled: disables thermal sensor. When this parameter is set to Disabled , the parameters below are hidden.	Enabled
Therm-Monitor-Status Filter	Enables or disables the filter based on thermal sensor. Options:	Disabled

Parameter	Description	Default
	- Enabled: enables the filter. - Disabled: disables the filter. When this parameter is set to Disabled, the parameters below are hidden.	
Therm-Monitor-Status Filter Time Window	This parameter is displayed when Therm-Monitor-Status Filter is set to Enabled. Select the time window for the filter.	1.1

3.4.6.6 CPU-Advanced PM Tuning

Figure 3-120 shows the **CPU-Advanced PM Tuning** screen.

Figure 3-120 CPU-Advanced PM Tuning Screen



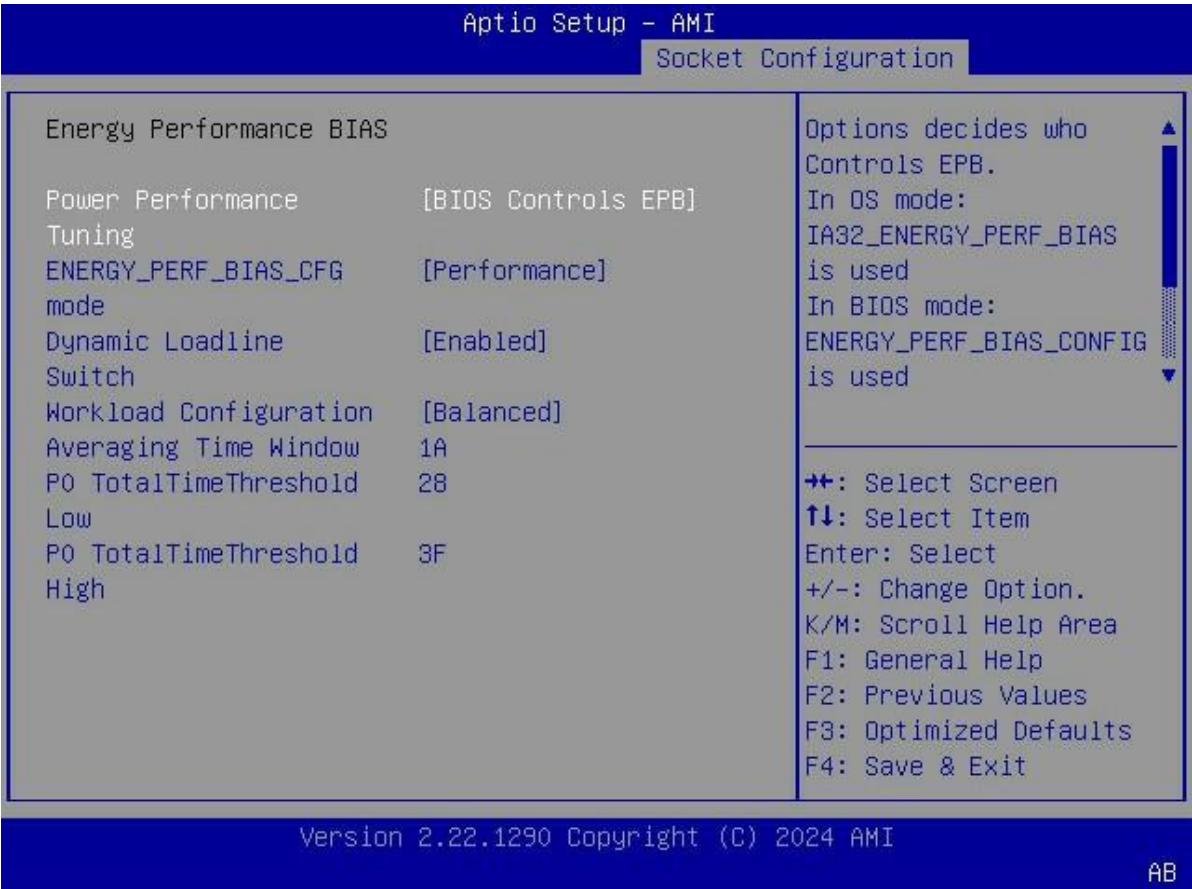
For a description of the parameters on the **CPU-Advanced PM Tuning** screen, refer to [Table 3-86](#).

Table 3-86 Parameter Descriptions for the CPU-Advanced PM Tuning Screen

Parameter	Description	Default
Uncore Freq Scaling	Enables or disables the frequency scaling of the non-core parts of the CPU.	Enabled

Parameter	Description	Default
	Options: ● Enabled: enables the frequency scaling of the non-core parts of the CPU. ● Disabled: disables the frequency scaling of the non-core parts of the CPU.	
Uncore Min CLR Freq	This parameter is displayed when Uncore Freq Scaling is set to Disabled . Enter the minimum CLR frequency of the non-core parts of the CPU.	12
Uncore Max CLR Freq	This parameter is displayed when Uncore Freq Scaling is set to Disabled . Enter the maximum CLR frequency of the non-core parts of the CPU.	26
Uncore Freq RAPL	Enables or disables the non-core frequency RAPL . Options: ● Enabled: enables the non-core frequency RAPL. ● Disabled: disables the non-core frequency RAPL.	Enabled
Energy Performance BIAS	Sets the energy performance BIAS parameters, see Figure 3-121 .	-
EET Mode	Select EET mode. Options: ● Coarse Grained Mode ● Fine Grained Mode	Coarse Grained Mode
Optimized Power Mode	Enables or disables optimized power mode. Options: ● Enabled: enables optimized power mode. ● Disabled: disables optimized power mode.	Disabled

Figure 3-121 Energy Performance BIAS Screen



For a description of the parameters on the **Energy Performance BIAS** screen, refer to [Table 3-87](#).

Table 3-87 Parameter Descriptions for the Energy Performance BIAS Screen

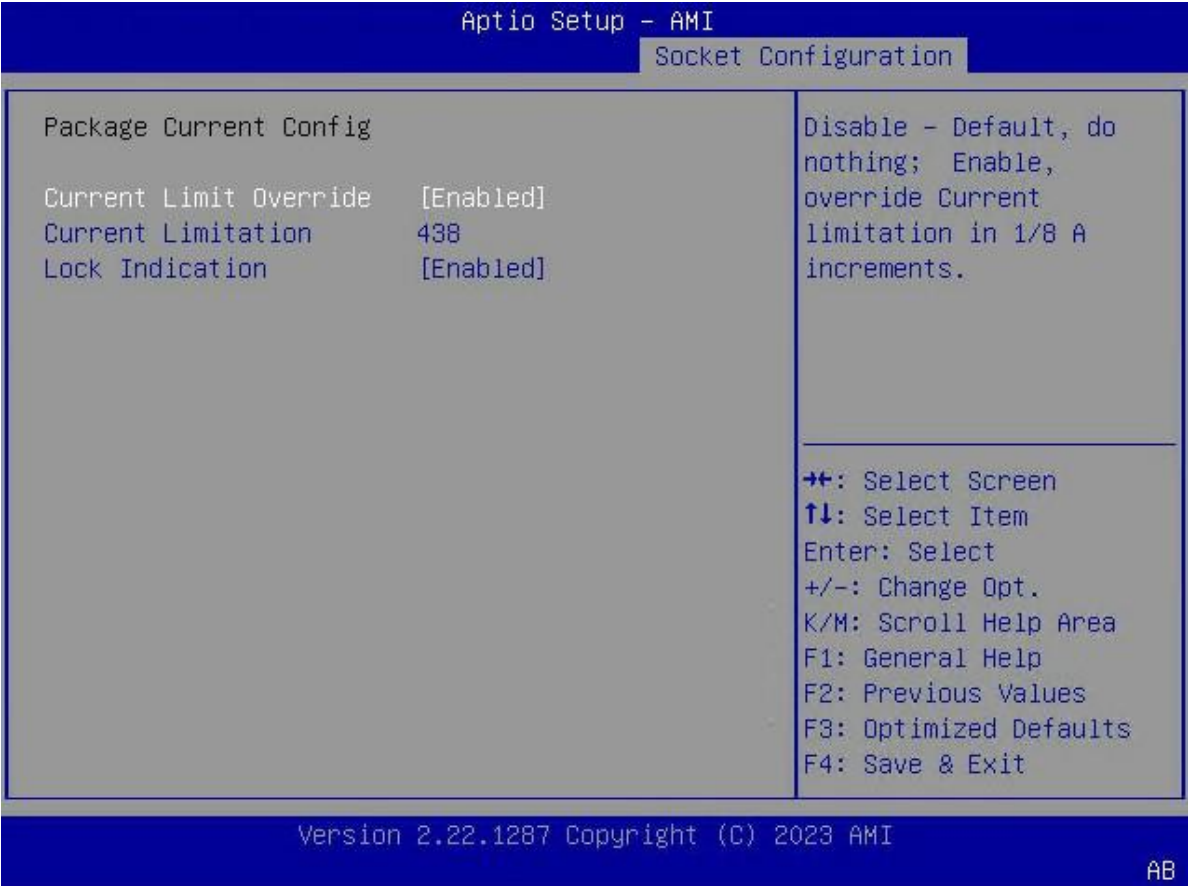
Parameter	Description	Default
Power Performance Tuning	Select a power performance tuning policy. Options: ● OS Controls EPB ● BIOS Controls EPB ● PECI Controls EPB	BIOS Controls EPB
ENERGY_PERF_BIAS_CFG mode	This parameter can be configured only when Power Performance Tuning is set to BIOS Controls EPB . Select an energy-saving performance management mode. Options: ● Balanced Performance: balanced performance mode. ● Balanced Power: balanced energy-saving mode. ● Performance: performance mode. ● Power: power saving mode.	Performance

Parameter	Description	Default
	Selecting any option will override the CPU energy-saving performance tuning configuration of the OS.	
Dynamic Loadine Switch	Enables or disables dynamic loading. Options: ● Enabled: enables dynamic loading. ● Disabled: disables dynamic loading.	Enabled
Workload Configuration	Select a workload mode. Options: ● Balanced: balanced mode. ● I/O sensitive: I/O-sensitive mode.	Balanced
Averaging Time Window	Controls the average time of C0 and P0.	1A
P0 TotalTimeThreshold Low	Enter the low threshold for the total P0 time. When the total P0 time drops below this threshold, the HW switching mechanism disables the performance setting.	28
P0 TotalTimeThreshold High	Enter the high threshold for the total P0 time. When the total P0 time exceeds this threshold, the HW switching mechanism enables the performance setting.	3F

3.4.6.7 Package Current Config

[Figure 3-122](#) shows the **Package Current Config** screen.

Figure 3-122 Package Current Config Screen



For a description of the parameters on the **Package Current Config** screen, refer to [Table 3-88](#).

Table 3-88 Parameter Descriptions for the Package Current ConfigScreen

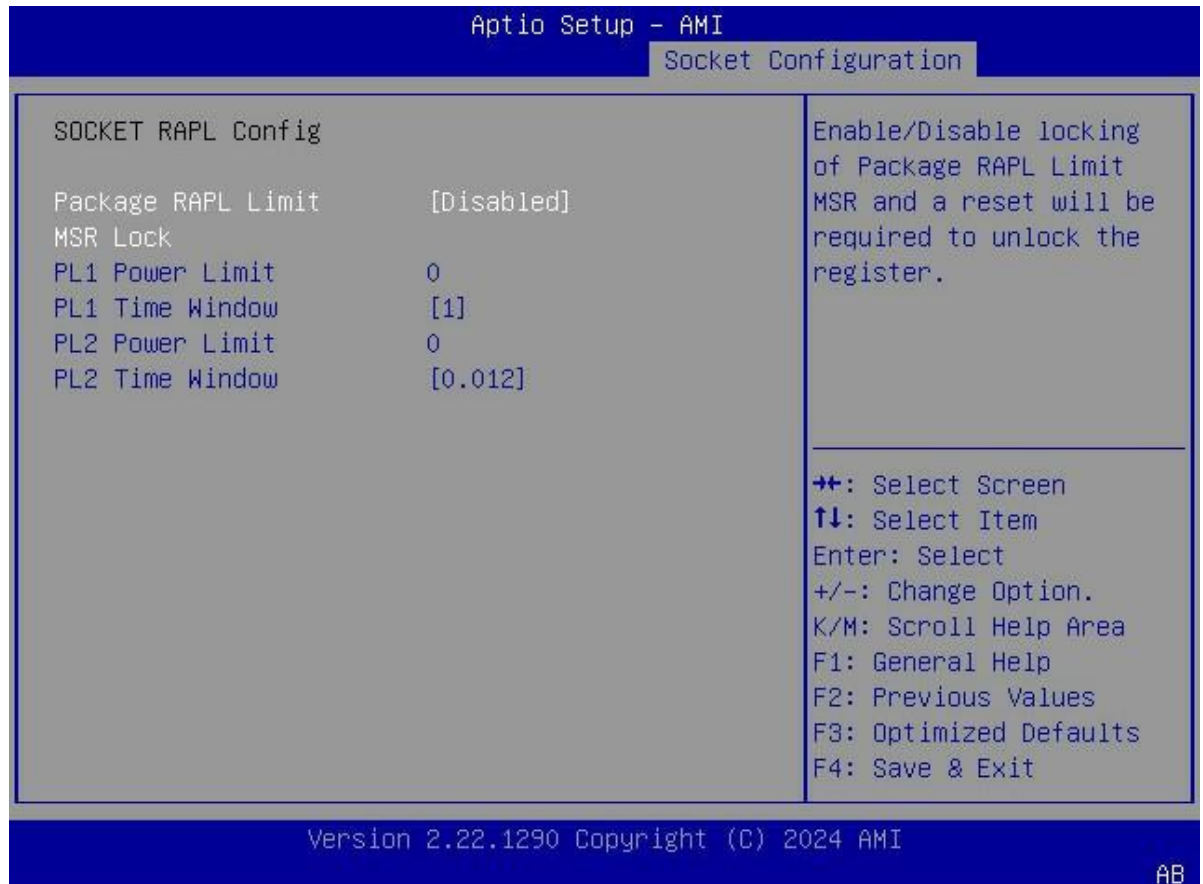
Parameter	Description	Default
Current Limit Override	Enables or disables the current limit overriding feature. Options: ● Enabled: enables the current limit overriding feature. ● Disabled: disables the current limit overriding feature.	Disabled
Current Limitation	This parameter is displayed when Current Limit Override is set to Enabled . Enter the current limit value. Unit: 1/8A.	438
Lock Indication	Sets whether to lock the current limit value. Options: ● Enabled: locks the current limit value.	Enabled

Parameter	Description	Default
	Disabled: indicates that the current limit value is not locked.	

3.4.6.8 SOCKET RAPL Config

Figure 3-123 shows the **SOCKET RAPL Config** screen.

Figure 3-123 SOCKET RAPL Config Screen



For a description of the parameters on the **SOCKET RAPL Config** screen, refer to [Table 3-89](#).

Table 3-89 Parameter Description for the Socket RAPL Config Screen

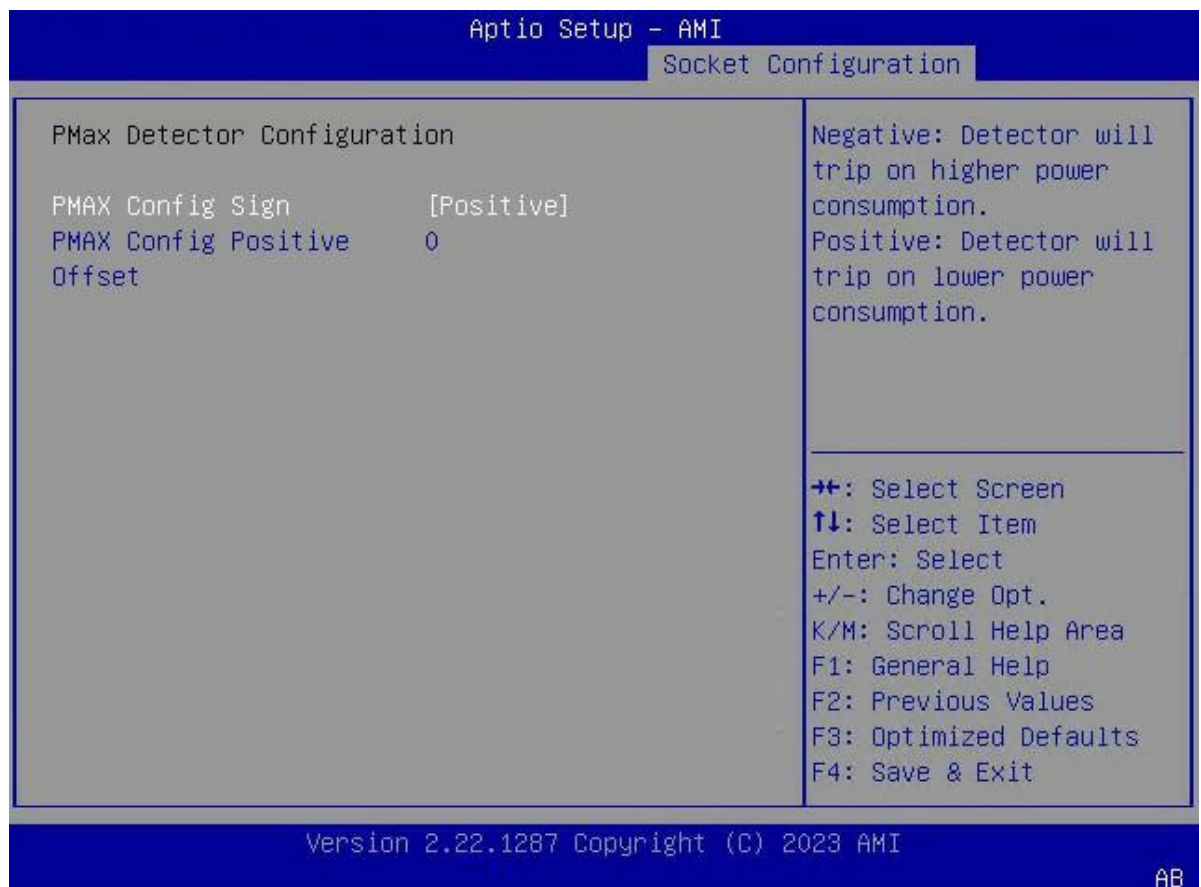
Parameter	Description	Default
Package RAPL Limit MSR Lock	Enables or disables the Package RAPL Limit MSR Lock feature. Options: - Enabled: enables or disables the Package RAPL Limit MSR Lock feature. - Disabled: disables the Package RAPL Limit MSR Lock feature.	Disabled

Parameter	Description	Default
PL1 Power Limit	Enter the PL1 power limit in watts, ranging from zero to the fused value. Value 0 indicates that the fused value is used.	0
PL1 Time Window	Select the PL1 time window.	1
PL2 Power Limit	Enter the PL2 power limit in watts, ranging from zero to the fused value. If the PL2 power limit is set to 0, it indicates that the fused value is used.	0
PL2 Time Window	Select the PL2 time window.	0.012

3.4.6.9 PMAX Detector Configuration

Figure 3-124 shows the **PMAX Detector Configuration** screen.

Figure 3-124 PMAX Detector Configuration Screen



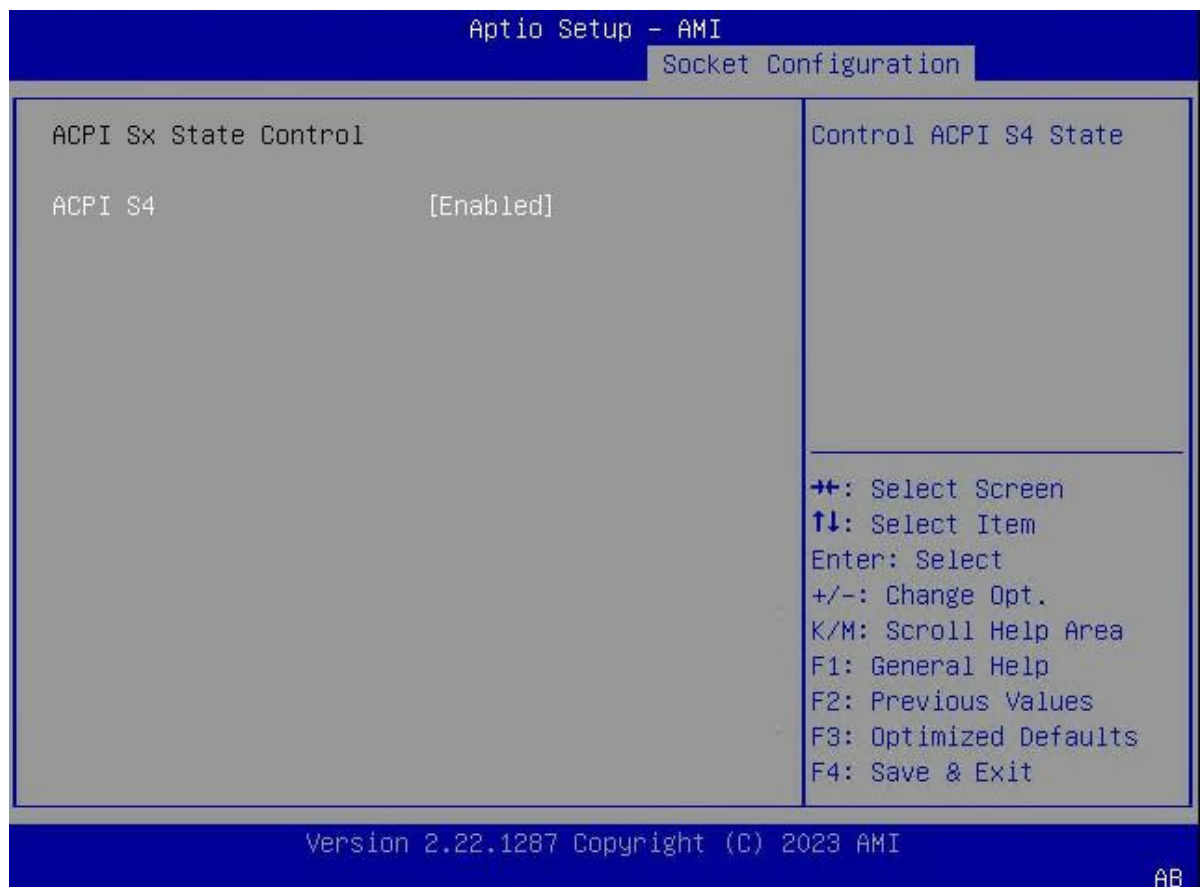
For a description of the parameters on the **PMAX Detector Configuration** screen, refer to [Table 3-90](#).

Table 3-90 Parameter Descriptions for the PMAX Detector Configuration Screen

Parameter	Description	Default
PMAX Config Sign	Sets how the PMax detector is triggered. Options: - Negative: The detector is triggered at higher power. - Positive: The detector is triggered at lower power.	Positive
PMAX Config Positive Offset	This parameter is displayed when PMAX Config Sign is set to Positive . Enter a decimal offset factor, range: 0–31.	0
PMAX Config Negative Offset	This parameter is displayed when PMAX Config Sign is set to Negative . Enter a decimal offset factor, range: 0–6.	0

3.4.6.10 ACPI Sx State Control

Figure 3-125 shows the **ACPI Sx State Control** screen.

Figure 3-125 ACPI Sx State Control Screen

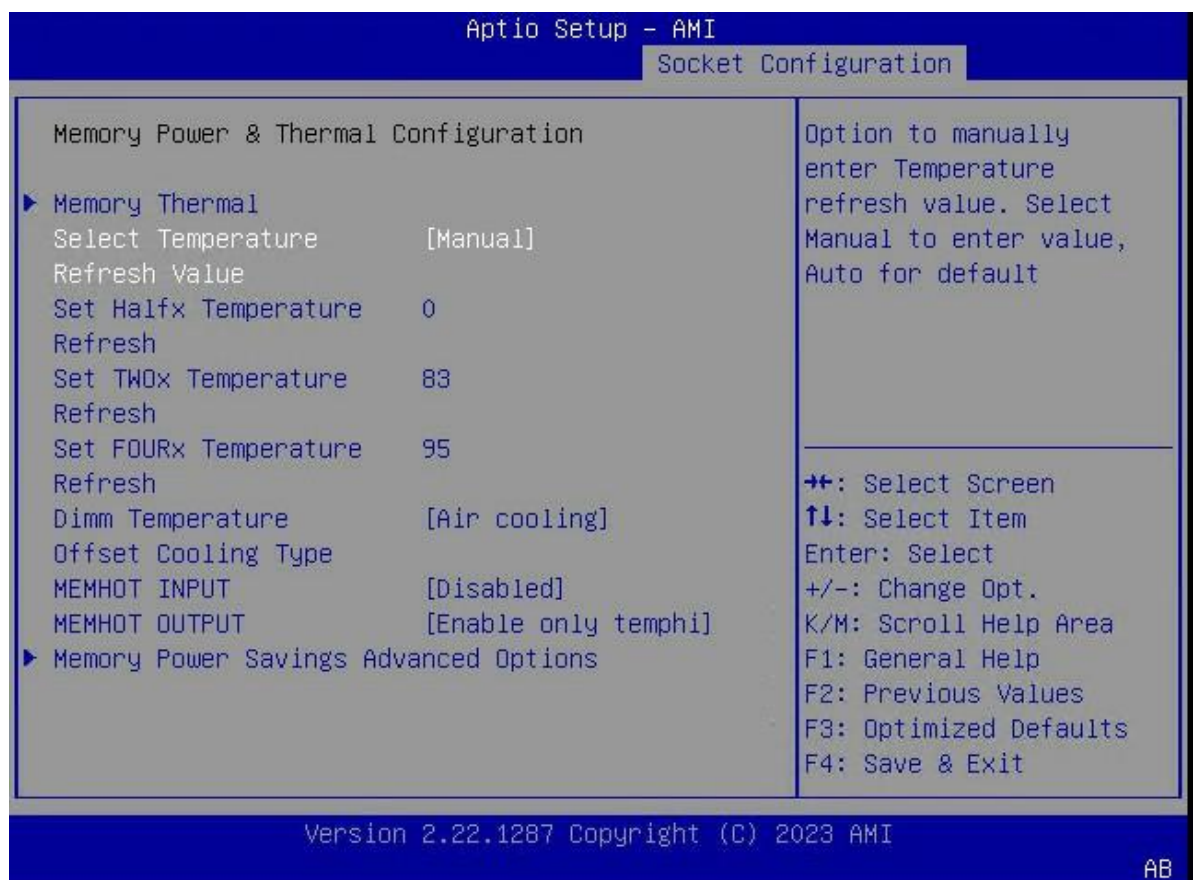
For a description of the parameters on the **ACPI Sx State Control** screen, refer to [Table 3-91](#).

Table 3-91 Parameter Descriptions for the ACPI Sx State Control Screen

Parameter	Description	Default
ACPI S4	Enables or disables the ACPI S4 status. Options: - Enabled: enables the ACPI S4 status. - Disabled: disables the ACPI S4 status.	Enabled

3.4.6.11 Memory Power & Thermal Configuration

[Figure 3-126](#) shows the **Memory Power & Thermal Configuration** screen.

Figure 3-126 Memory Power & Thermal Configuration Screen

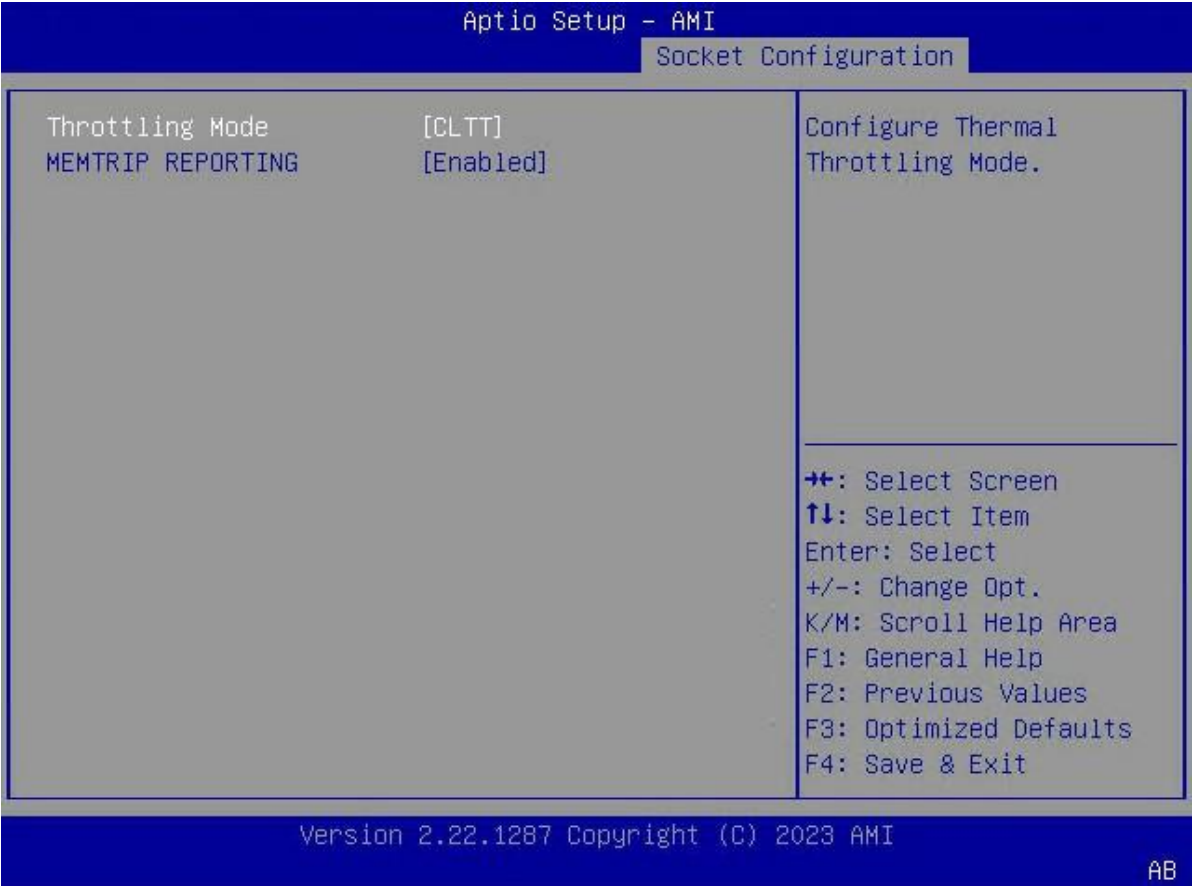
For a description of the parameters on the **Memory Power & Thermal Configuration** screen, refer to [Table 3-92](#).

Table 3-92 Parameter Descriptions for the Memory Power & Thermal Configuration Screen

Parameter	Description	Default
Memory Thermal	Sets memory thermal parameters, see Figure 3-127 .	-
Select Temperature Refresh Value	Sets the temperature refresh mode. Options: Auto: automatic mode.	Auto

Parameter	Description	Default
	Manual: manual mode.	
Set Halfx Temperature Refresh	This parameter is displayed when Select Temperature Refresh Value is set to Enabled . Enter the Halfx temperature refresh value.	0
Set TWOx Temperature Refresh	This parameter is displayed when Select Temperature Refresh Value is set to Enabled . Enter the TWOx temperature refresh value.	83
Set FOURx Temperature Refresh	This parameter is displayed when Select Temperature Refresh Value is set to Enabled . Enter the FOURx temperature refresh value.	95
Dimm Temperature Offset Cooling Type	Select the type of DIMM temperature offset cooling system. Options: - Air cooling - Liquid cooling (tube) - Immersion cooling	Air cooling
MEMHOT INPUT	Enables or disables the MEMHOT input feature. Options: - Enabled: enables the MEMHOT input feature. - Disabled: disables the MEMHOT input feature.	Disabled
MEMHOT OUTPUT	Enables or disables the MEMHOT output feature. Menu options: Disabled Enable only temphi Enable only temphi & mid Enable only temphi, mid and low Options: - Disabled: disables the MEMHOT output feature. - Enable only temphi: enables the MEMHOT output feature and outputs only temphi. - Enable only temphi&mid: enables the MEMHOT output feature and outputs only temphi and mid. - Enable only temphi, mid and low: enables the MEMHOT output feature and outputs only temphi, mid, and low.	Enable only temphi
Memory Power Savings Advanced Options	Sets the advanced memory power efficiency parameters, see Figure 3-128 .	-

Figure 3-127 Memory Thermal Screen

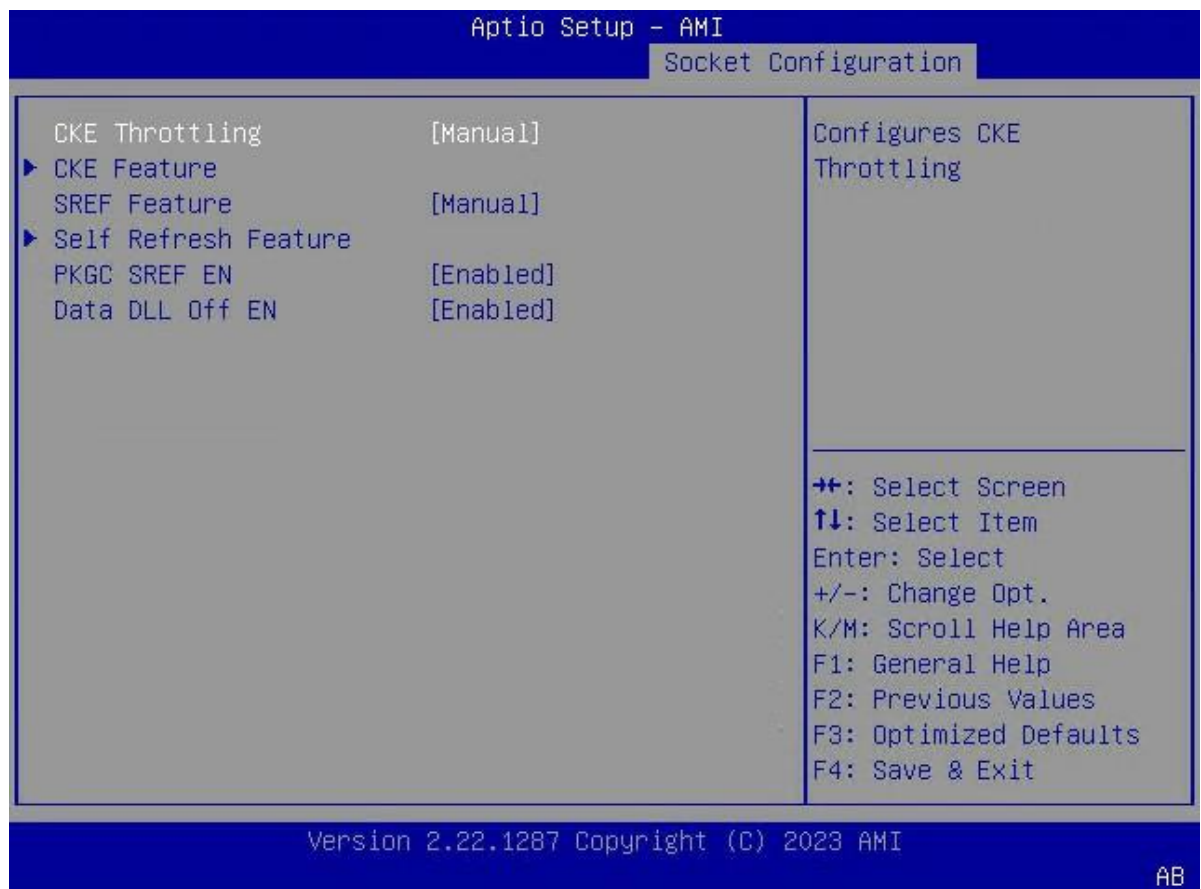


For a description of the parameters on the **Memory Thermal** screen, refer to [Table 3-93](#).

Table 3-93 Parameter Descriptions for the Memory Thermal Screen

Parameter	Description	Default
Throttling Mode	Select thermal throttling mode. Options: ● CLTT: CLTT mode. ● CLTT with PECI: CLTT mode with PECI. ● Disabled: disables thermal throttling mode.	CLTT
MEMTRIP REPORTING	This parameter is hidden when Throttling Mode is set to Disabled . Enables or disables the MEMTRIP reporting feature. Options: ● Enabled: The processor contains all MEMTRIPs. ● Disabled: The processor ignores all MEMTRIPs.	Enabled

Figure 3-128 Memory Power Savings Advanced Options Screen



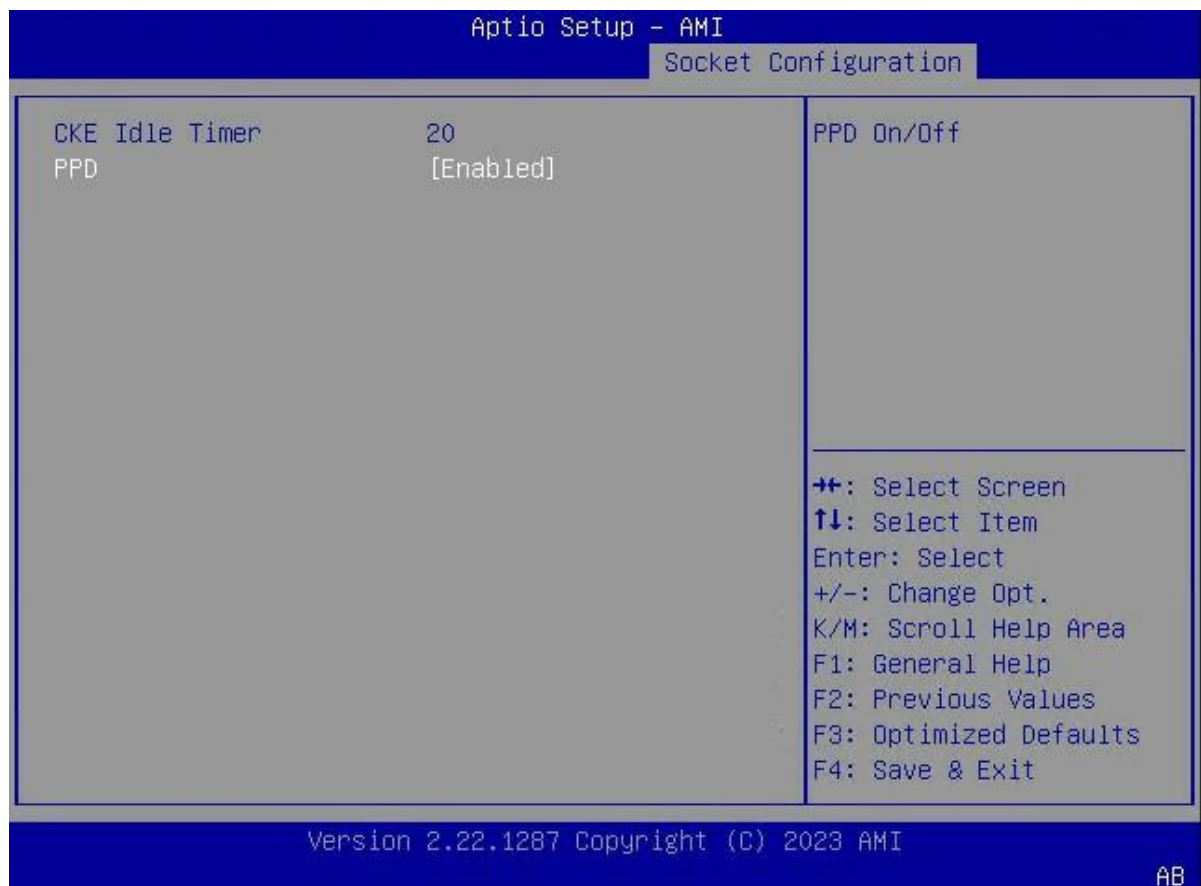
For a description of the parameters on the **Memory Power Savings Advanced Options** screen, refer to [Table 3-94](#).

Table 3-94 Parameter Descriptions for the Memory Power Savings Advanced Options Screen

Parameter	Description	Default
CKE Throttling	Select the CKE Throttling mode. Options: ● Auto: automatic mode. ● Manual: manual mode.	Auto
CKE Feature	This parameter is displayed when CKE Throttling is set to Manual . Sets CKE parameters, see Figure 3-129 .	-
SREF Feature	Select the self-refresh mode. Options: ● Auto: automatic mode. ● Manual: manual mode.	Auto
Self Refresh Feature	This parameter is displayed when SREF Feature is set to Manual . Sets self-refresh parameters, see Figure 3-130 .	-

Parameter	Description	Default
PKGC SREF EN	Enables or disables the PKGC self-refresh feature. Options: - Enabled: enables the PKGC self-refresh feature. - Disabled: disables the PKGC self-refresh feature.	Enabled
Data DLL Off EN	Enables or disables the data DLL feature in low power mode. Options: - Enabled: enables the data DLL feature. - Disabled: disables the data DLL feature.	Enabled

Figure 3-129 CKE Feature Screen



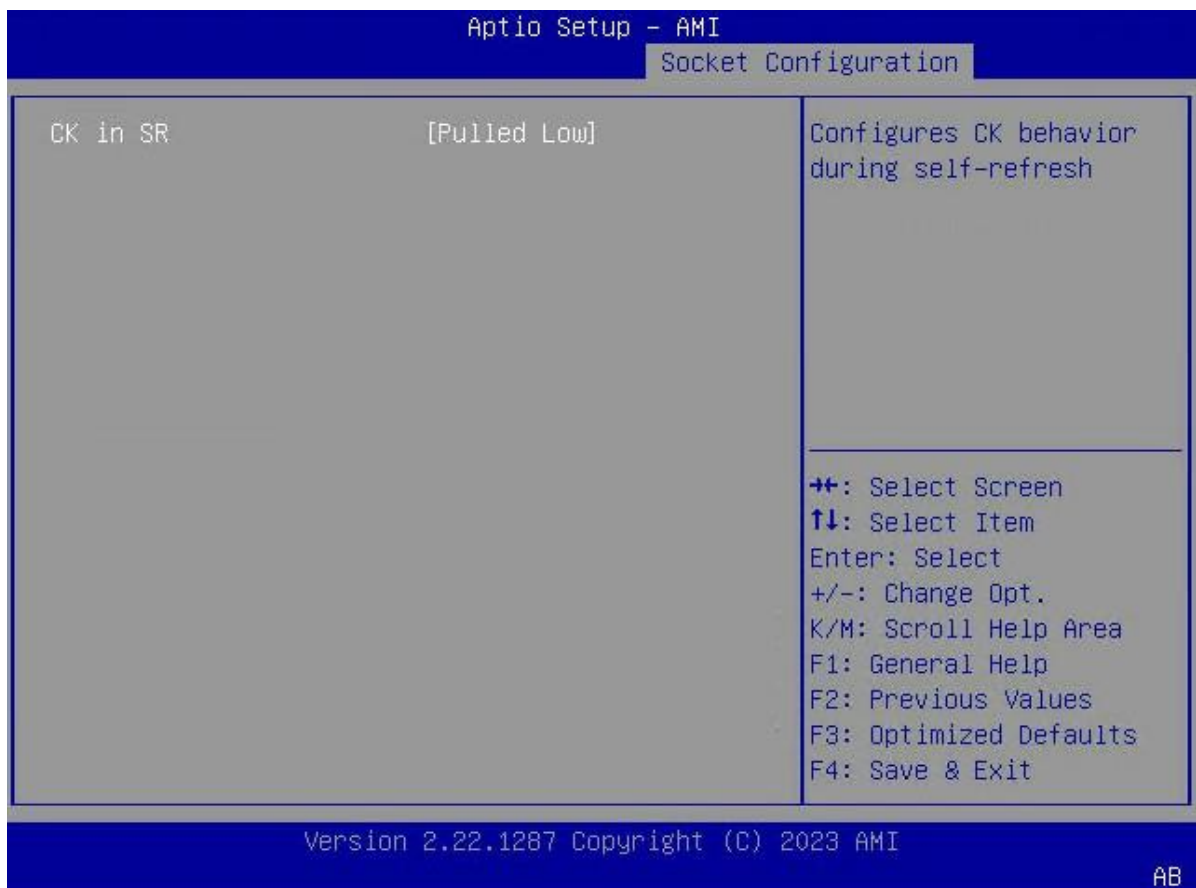
For a description of the parameters on the **CKE Feature** screen, refer to [Table 3-95](#).

Table 3-95 Parameter Descriptions for the CKE Feature Screen

Parameter	Description	Default
CKE Idle Timer	Enter the time, in nanoseconds, for the CKE idle timer.	20
PPD	Enables or disables PPD mode.	Enabled

Parameter	Description	Default
	This mode is entered if all Banks in the DDR are pre-charged when the CKE is not set. The power saving effect of this mode is medium. Options: • Enabled: enables PPD mode. • Disabled: Disable PPD mode.	

Figure 3-130 Self Refresh Feature Screen



For a description of the parameters on the **Self Refresh Feature** screen, refer to [Table 3-96](#).

Table 3-96 Parameter Descriptions for the Self Refresh Feature Screen

Parameter	Description	Default
CK in SR	Select a CK behavior during self-refresh. Options: • Driven • Pulled Low	Pulled Low

3.5 Server Mgmt

[Figure 3-131](#) through [Figure 3-132](#) show the **Server Mgmt** screen.

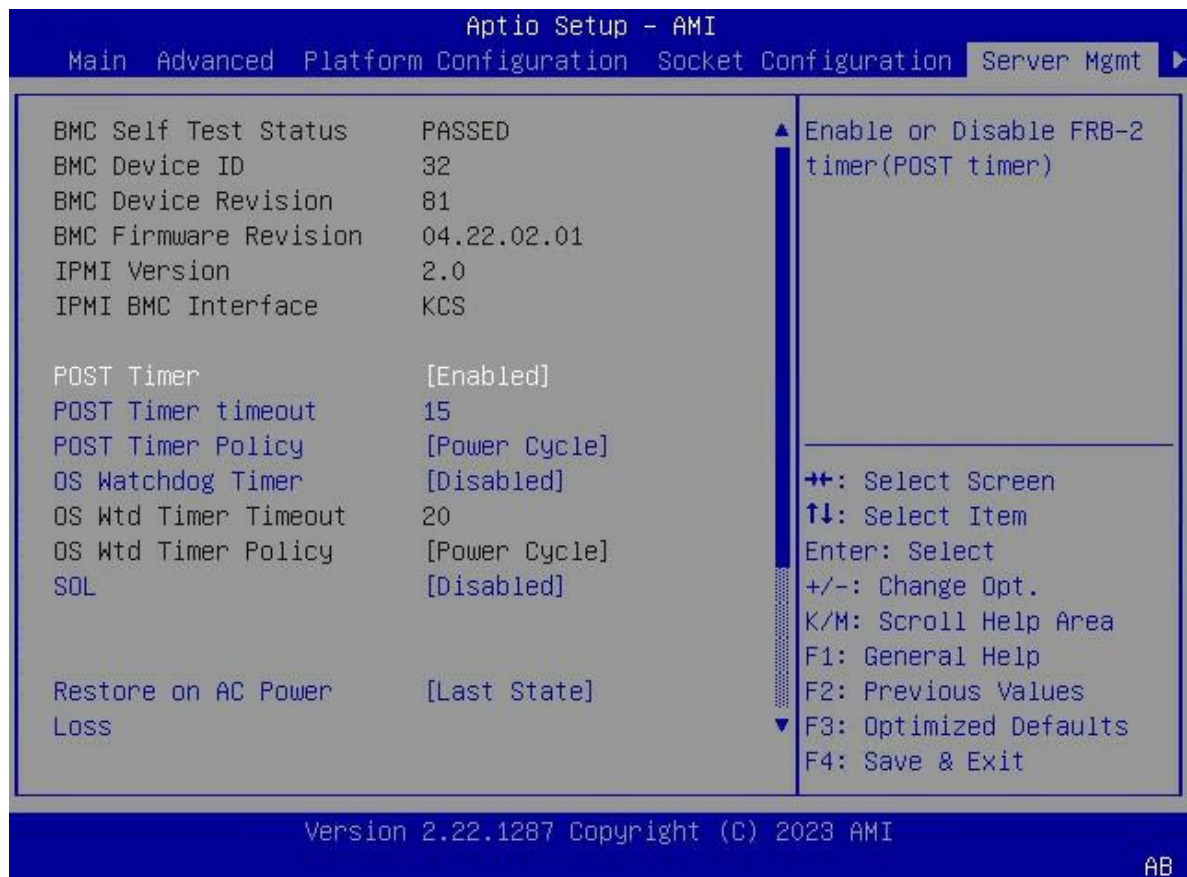
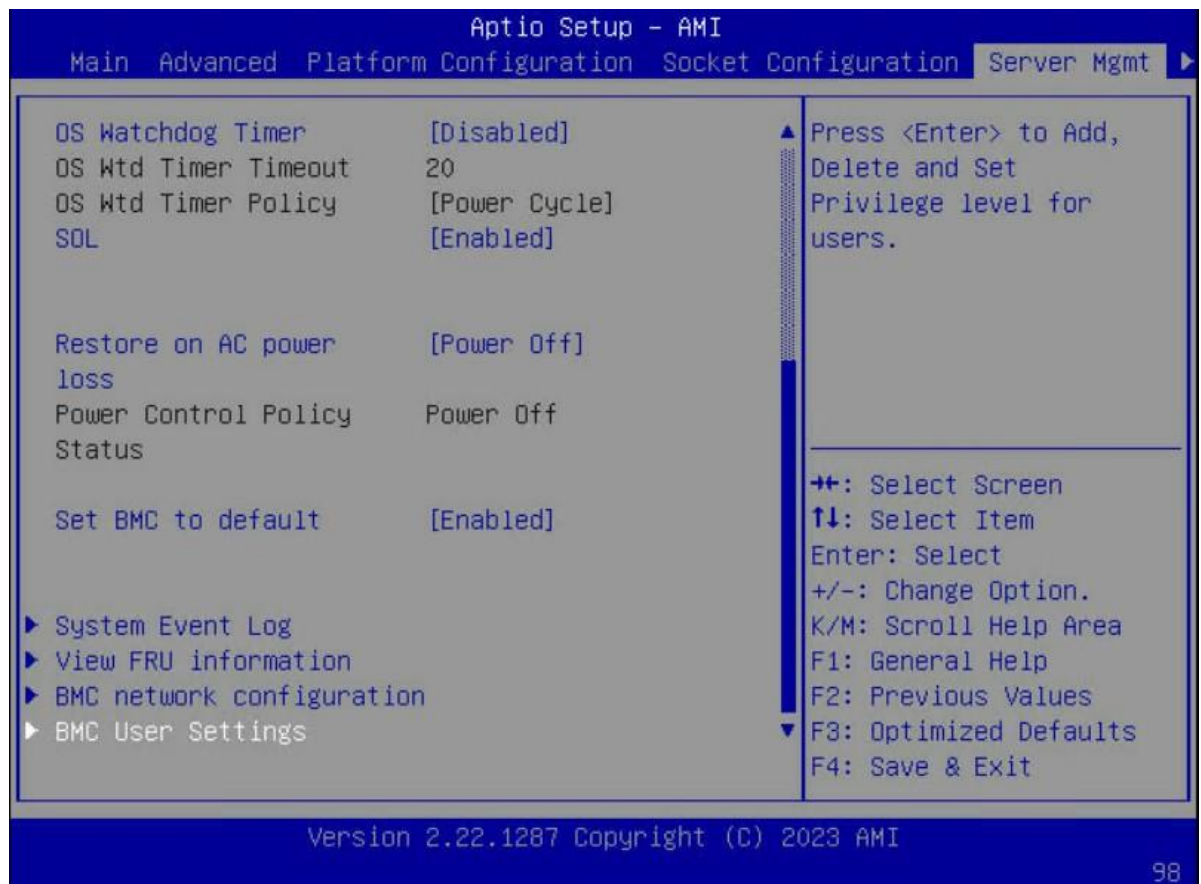
Figure 3-131 Server Mgmt Screen—1

Figure 3-132 Server Mgmt Screen—2



For a description of the parameters on the **Server Mgmt** screen, refer to [Table 3-97](#).

Table 3-97 Parameter Descriptions for the Server Mgmt Screen

Parameter	Description	Default
BMC Self Test Status	BMC self-test status.	PASSED
BMC Device ID	ID of the BMC device.	32
BMC Device Revision	Version number of the BMC device.	81
BMC Firmware Revision	Version number of the BMC firmware.	04.22.01.02
IPMI Version	Version number of the IPMI.	2.0
IPMI BMC Interface	IPMI BMC interface.	KCS
POST Timer	Enables or disables the FRB-2 timer, that is, the POST timer. Options: - Enabled: enables the POST timer. - Disabled: disables the POST timer.	Enabled
POST Timer timeout	Enter the timeout time of the POST timer. Range: 3–30, unit: minutes.	15

Parameter	Description	Default
POST Timer Policy	Sets how the system responds when the POST timer expires. Options: ● Do Nothing: No operation is performed. ● Reset: resets the timer. ● Power Down: powers off the server. ● Power Cycle: powers off the server and then powers it on again.	Reset
OS Watchdog Timer	Enables or disables the OS watchdog timer. Options: ● Enabled: enables the OS watchdog timer. After the parameter is set to Enabled, a BIOS timer is started. This timer can only be disabled by the management software after the OS is loaded. ● Disabled: disables the OS watchdog timer.	Disabled
OS Wtd Timer Timeout	Enter the timeout time of the OS watchdog timer. Range: 3–30, unit: minutes.	20
OS Wtd Timer Policy	Sets how the system responds when the OS watchdog timer expires. Options: ● Do Nothing: No operation is performed. ● Reset: resets the timer. ● Power Down: powers off the server. ● Power Cycle: powers off the server and then powers it on again.	Power Cycle
SOL	Enables or disables the BMC SOL control feature. Options: ● Enabled: enables the BMC SOL control feature. ● Disabled: disables the BMC SOL control feature.	Enabled
Restore on AC power loss	Sets the system action to take upon AC power loss recovery. Options: ● Power Off: powers off the server. ● Last State: keeps the last state. ● Power On: powers on the server.	Power On
Set BMC to default	Enables or disables BMC default settings. Options: ● Enabled: enables BMC default settings. ● Disabled: disables BMC default settings.	Disabled

Parameter	Description	Default
System Event Log	Sets system event log parameters. For details, refer to 3.5.1 System Event Log .	-
View FRU information	Views FRU information. For details, refer to 3.5.2 View FRU information .	-
BMC network configuration	Sets BMC network parameters. For details, refer to 3.5.3 BMC network configuration .	-
BMC User Settings	Sets BMC user parameters. For details, refer to 3.5.4 BMC User Settings .	-

3.5.1 System Event Log

[Figure 3-133](#) shows **System Event Log** Screen.

Figure 3-133 System Event Log Screen



For a description of the parameters on the **System Event Log** screen, refer to [Table 3-98](#).

Table 3-98 Parameter Descriptions for the System Event Log Screen

Parameter	Description	Default
SEL Components	Enables or disables event logging for error/progress codes during boot. Options: ● Enabled: enables event logging for error/progress codes. ● Disabled: disables event logging for error/progress codes.	Enabled
Erase SEL	Select the option to erase the SEL. Options: ● No ● Yes, On next reset ● Yes, On every reset	No
When SEL is Full	Select the option to react when the SEL is full. Options: ● Do Nothing ● Erase Immediately ● Delete Oldest Record	Do Nothing
Log EFI Status Codes	Select the option to record EFI status codes. Options: ● Disabled ● Both ● Error code ● Progress code	Error code

3.5.2 View FRU information

Figure 3-134 shows the **View FRU information** screen.

Figure 3-134 View FRU Information Screen



3.5.3 BMC network configuration

Figure 3-135 through Figure 3-140 show the **BMC network configuration** screen.

Figure 3-135 BMC Network Configuration Screen—1

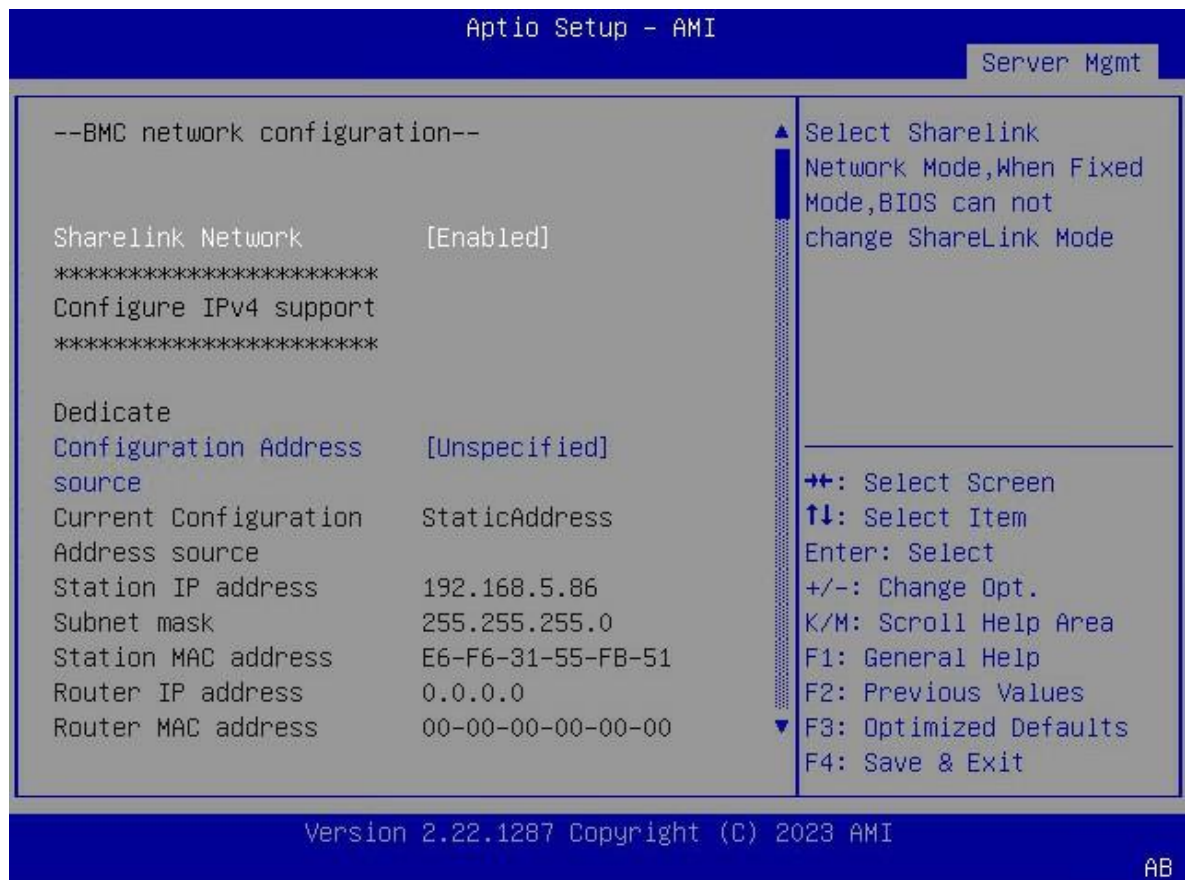


Figure 3-136 BMC Network Configuration Screen—2

Aptio Setup - AMI

Server Mgmt

ShareLink		▲ Enable or Disable
Configuration Address	[Unspecified]	Dedicate IPv6 Support
source		
Current Configuration	Unspecified	
Address source		
Station IP address	0.0.0.0	
Subnet mask	0.0.0.0	
Station MAC address	00-00-00-00-00-00	
Router IP address	0.0.0.0	
Router MAC address	00-00-00-00-00-00	

Configure IPv6 support		

Dedicate		
IPv6 Support	[Enabled]	▼

++: Select Screen
 ↑↓: Select Item
 Enter: Select
 +/-: Change Opt.
 K/M: Scroll Help Area
 F1: General Help
 F2: Previous Values
 F3: Optimized Defaults
 F4: Save & Exit

Version 2.22.1287 Copyright (C) 2023 AMI

AB

Figure 3-137 BMC Network Configuration Screen—3

Aptio Setup - AMI		Server Mgmt
Configuration Address source	[Unspecified]	▲ Select to configure LAN channel parameters statically or dynamically (by BIOS or BMC). Unspecified option will not modify any BMC network parameters during BIOS
Current Configuration Address source	DynamicAddressBmcDhcp	
Station IPv6 address	::	
Prefix Length	0	
IPv6 address status	Disabled	⇄: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. K/M: Scroll Help Area F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit
IPv6 DHCP Algorithm	DHCPv6	
Configuration Router	[Unspecified]	
Lan1 Address source	DynamicAddressBmcDhcp	
Current Router	DynamicAddressBmcDhcp	
Configuration Address source		

Version 2.22.1287 Copyright (C) 2023 AMI

AB

Figure 3-138 BMC Network Configuration Screen—4

Aptio Setup - AMI		Server Mgmt
IPv6 Router IP Address ::	▲ Enable or Disable ShareLink IPv6 Support	
IPv6 Router Prefix Length 255		
IPv6 Router Prefix Value ::		
ShareLink		
IPv6 Support [Enabled]	↔: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. K/M: Scroll Help Area F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit	
Configuration Address source [Unspecified]		
Current Configuration Address source -		

Version 2.22.1287 Copyright (C) 2023 AMI

AB

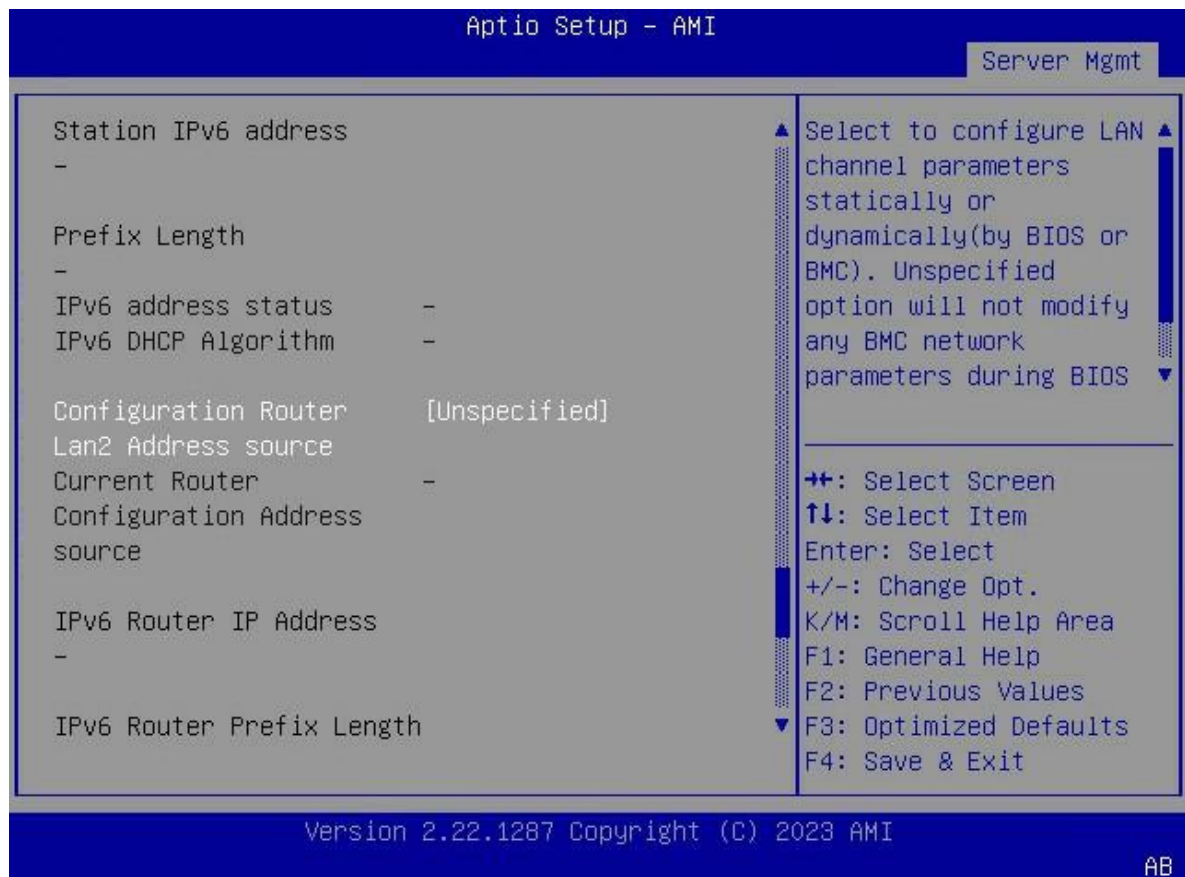
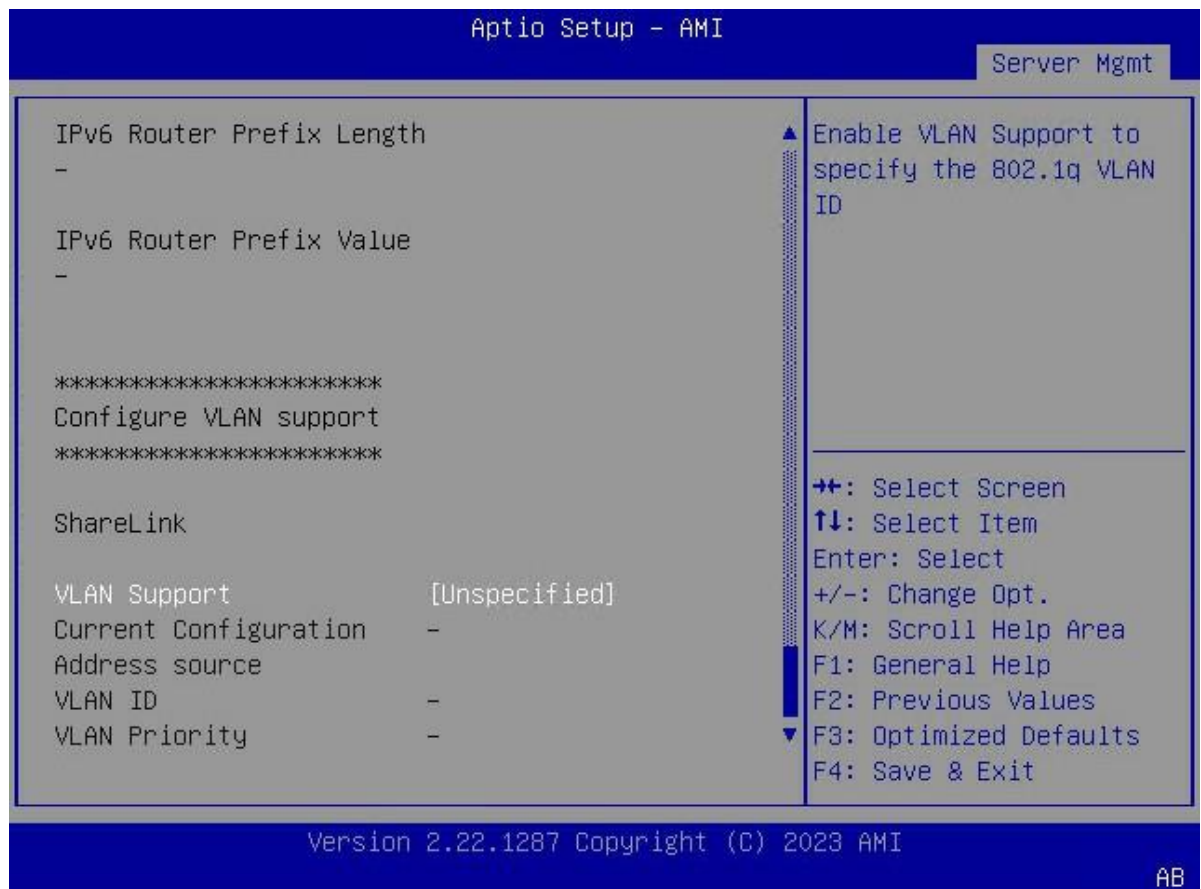
Figure 3-139 BMC Network Configuration Screen—5

Figure 3-140 BMC Network Configuration Screen—6



For a description of the parameters on the **BMC network configuration** screen, refer to [Table 3-99](#).

Table 3-99 Parameter Descriptions for the BMC Network Configuration Screen

Parameter	Description	Default
Sharelink Network	Enables or disables the shared network port. In fixed mode, the BIOS cannot enable or disable the shared network port. Options: ● Auto: automatic mode. ● Enabled: enables the shared network port. ● Disabled: disables the shared network port.	Enabled
Configure IPv4 support		
Delicate		

Parameter	Description	Default
Configuration Address source	Sets the configuration mode of the IPv4 address of the dedicated network interface: Options: ● Unspecified: undefined. In the BIOS phase, the setting is not changed based on the network parameter setting in the BMC. ● Static: static mode. You need to manually set the IP address. ● DynamicBmcDhcp: obtained dynamically through BMC DHCP. ● DynamicBmcNonDhcp: obtained dynamically through the BMC.	Unspecified
Current Configuration Address source	Displays the currently configured address source.	StaticAddress
Station IP address	Enter the IP address of the dedicated network interface.	0.0.0.0
Subnet mask	Enter the subnet mask.	0.0.0.0
Station MAC address	Enter the MAC address of the dedicated network interface.	DE-AD-CC-F5-12-59
Router IP address	Enter the IP address of the gateway.	0.0.0.0
Router MAC address	Enter the MAC address of the gateway.	00-00-00-00-00-00
ShareLink		
Configuration Address source	Sets the configuration mode of the IPv4 address of the shared network interface: Options: ● Unspecified: undefined. In the BIOS phase, the setting is not changed based on the network parameter setting in the BMC. ● Static: static mode. You need to manually set the IP address. ● DynamicBmcDhcp: Obtained dynamically through BMC DHCP. ● DynamicBmcNonDhcp: obtained dynamically through the BMC.	Unspecified

Parameter	Description	Default
Current Configuration Address source	Displays the currently configured address source.	Unspecified
Station IP address	Enter the IP address of the shared network interface.	0.0.0.0
Subnet mask	Enter the subnet mask.	0.0.0.0
Station MAC address	Enter the MAC address of the shared network interface.	00-00-00-00-00-00
Router IP address	Enter the IP address of the gateway.	0.0.0.0
Router MAC address	Enter the MAC address of the gateway.	00-00-00-00-00-00
Configure IPv6 support		
Delicate		
IPv6 Support	Enables or disables the IPv6 support for the dedicated network interface. Options: ● Enabled: enables the IPv6 support for the dedicated network interface. ● Disabled: disables the IPv6 support for the dedicated network interface.	Enabled
Configuration Address source	Sets the configuration mode of the IPv6 address of the dedicated network interface. Options: ● Unspecified: undefined. In the BIOS phase, the setting is not changed based on the network parameter setting in the BMC. ● Static: static mode. You need to manually set the IP address. ● DynamicBmcDhcp: obtained dynamically through BMC DHCP.	Unspecified
Current Configuration Address source	Displays the currently configured address source.	DynamicAddressBmcDhcp
Station IPv6 Address	Enter the IPv6 address of the dedicated network interface.	::
Prefix Length	Enter the prefix length of the IPv6 address.	0
IPv6 address status	Displays the Pv6 address status.	Disabled

Parameter	Description	Default
IPv6 DHCP Algorithm	Displays the IPv6 DHCP algorithm.	DHCPv6
Configuration Router Lan1 Address source	Sets the configuration mode of the IPv6 address of the gateway LAN1. Options: ● Unspecified: undefined. In the BIOS phase, the setting is not changed based on the network parameter setting in the BMC. ● Static: static mode. You need to manually set the IP address. ● DynamicBmcDhcp: obtained dynamically through BMC DHCP.	Unspecified
Current Router Configuration Address source	Displays the address source configured for the current gateway.	DynamicAddressBmcDhcp
IPv6 Router IP Address	Enter the IPv6 address of the gateway.	::
IPv6 Router Prefix Length	Enter the prefix length of the IPv6 address.	255
IPv6 Router Prefix Value	Enter the prefix value for the gateway IPv6 address.	::
ShareLink		
IPv6 Support	Enables or disables the IPv6 support for the shared network interface. Options: ● Enabled: enables the IPv6 support for the shared network interface. ● Disabled: disables the IPv6 support for the shared network interface.	Enabled
Configuration Address source	Sets the configuration mode of the IPv6 address of the shared network interface: Options: ● Unspecified: undefined. In the BIOS phase, the setting is not changed based on the network parameter setting in the BMC. ● Static: static mode. You need to manually set the IP address. ● DynamicBmcDhcp: obtained dynamically through BMC DHCP.	Unspecified

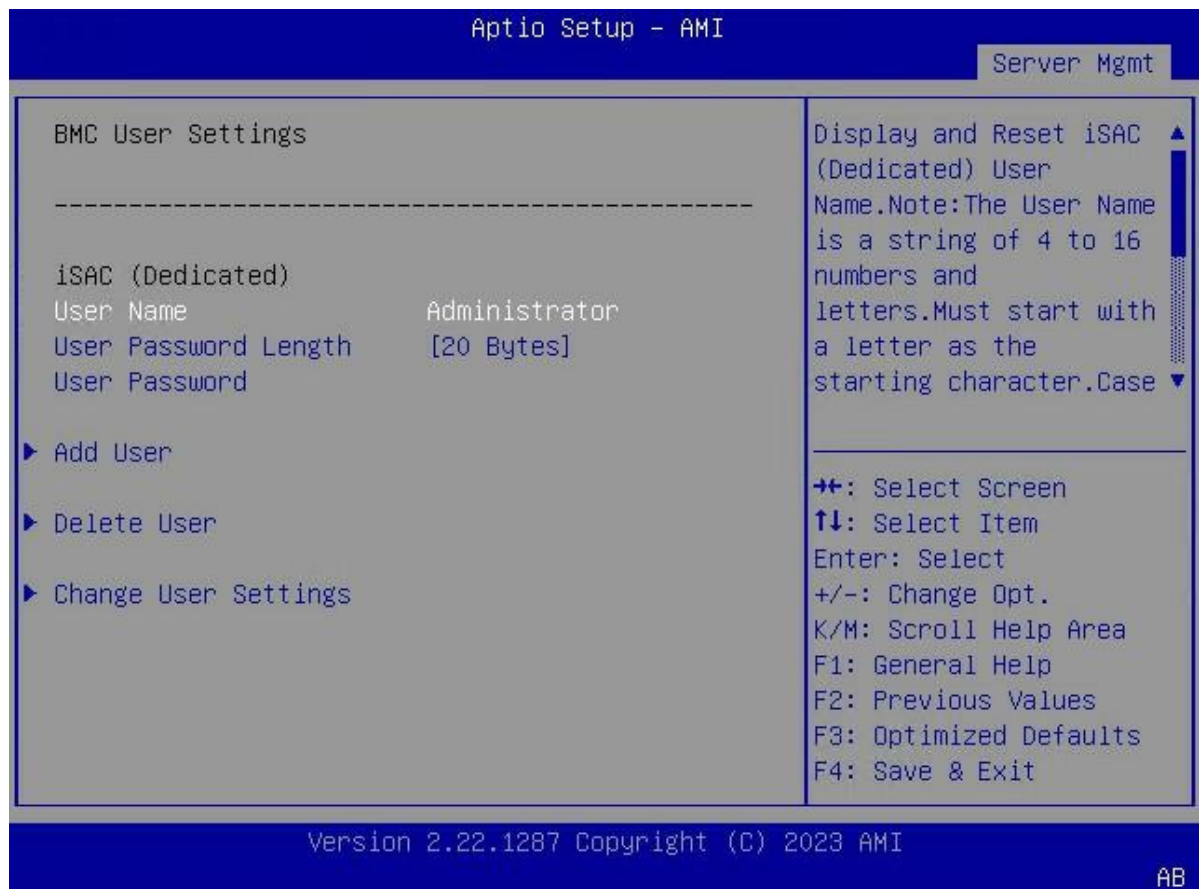
Parameter	Description	Default
Current Configuration Address source	Displays the currently configured address source.	-
Station IPv6 Address	Enter the IPv6 address of the shared network interface.	-
Prefix Length	Enter the prefix length of the IPv6 address.	-
IPv6 address status	Displays the IPv6 address status.	-
IPv6 DHCP Algorithm	Displays the IPv6 DHCP algorithm.	-
Configuration Router Lan1 Address source	Sets the configuration mode of the IPv6 address of the gateway LAN2. Options: ● Unspecified: undefined. In the BIOS phase, the setting is not changed based on the network parameter setting in the BMC. ● Static: static mode. You need to manually set the IP address. ● DynamicBmcDhcp: obtained dynamically through BMC DHCP.	Unspecified
Current Router Configuration Address source	Displays the address source configured for the current gateway.	-
IPv6 Router IP Address	Enter the IPv6 address of the gateway.	-
IPv6 Router Prefix Length	Enter the prefix length for the gateway IPv6 address.	-
IPv6 Router Prefix Value	Enter the prefix value for the gateway IPv6 address.	-
Configure VLAN support		
VLAN Support	Sets whether to enable the VLAN support for the network interface. Options: ● Unspecified: unspecified. ● Enabled: The network interface supports VLAN configuration. ● Disabled: The network interface does not support VLAN configuration.	Unspecified
Current Configuration Address source	Displays the currently configured address source.	-

Parameter	Description	Default
VLAN ID	Enter the VLAN ID, range: 0–4094. Value 0 indicates that VLAN is disabled.	-
VLAN Priority	Enter the VLAN priority.	-

3.5.4 BMC User Settings

Figure 3-141 shows the **BMC User Settings** screen.

Figure 3-141 BMC User Settings Screen



For a description of the parameters on the **BMC User Settings** screen, refer to [Table 3-100](#).

Table 3-100 Parameter Descriptions for the BMC User Settings Screen

Parameter	Description	Default
User Name	Displays and resets the username of the iSAC management interface. The username is a case-sensitive character string of 4 to 16 characters including digits and letters. It must start with a letter. Allowed special characters are hyphens (-), underscores (_), and at symbols (@).	Administrator

Parameter	Description	Default
	The following usernames are not allowed: • anonymous • root • admin • users • nobody • username • sysadmin	
User Password Length	Select the maximum length of the user password for the iSAC management interface. The modification of this parameter takes effect only after the User Password is modified. • For IPMI v1.5-compliant BMC, the maximum password length is sixteen bytes. • For an IPMI v2.0-compliant BMC, the maximum password length is 20 bytes.	20 Bytes
User Password	Resets the user password of the iSAC management interface. The minimum password length is 8 bytes. Strong passwords must contain four character types: • Uppercase letters • Lowercase letters • Numbers • Special characters	-
Add User	Adds a user. For details, refer to 3.5.4.1 Add User.	-
Delete User	Deletes a user. For details, refer to 3.5.4.2 Delete User.	-
Change User Settings	Modifies user settings. For details, refer to 3.5.4.3 Change User Settings.	-

3.5.4.1 Add User

[Figure 3-142](#) shows the **Add User** screen.

Figure 3-142 Add User Dialog Box



For a description of the parameters on the **Add User** screen, refer to [Table 3-101](#).

Table 3-101 Parameter Descriptions for the Add User Screen

Parameter	Description	Default
User name	Enter the BMC username.	-
User Password	Enter the password of the BMC user. The following parameters can be set only after you enter the username and password.	-
User Access	Enables or disables user access. Options: ● Enabled: enables user access. ● Disabled: disables user access.	Disabled
Channel No	Enter the Channel number.	0
User Privilege Limit	Sets the user privilege restrictions.	No Access

3.5.4.2 Delete User

[Figure 3-143](#) shows the **Delete User** screen.

Figure 3-143 Delete User Screen

Aptio Setup - AMI

Server Mgmt

BMC Delete User Details

User Name

User Password

Enter BMC User Name

++: Select Screen
 ↑↓: Select Item
 Enter: Select
 +/-: Change Opt.
 K/M: Scroll Help Area
 F1: General Help
 F2: Previous Values
 F3: Optimized Defaults
 F4: Save & Exit

Version 2.22.1287 Copyright (C) 2023 AMI

98

For a description of the parameters on the **Delete User** screen, refer to [Table 3-102](#).

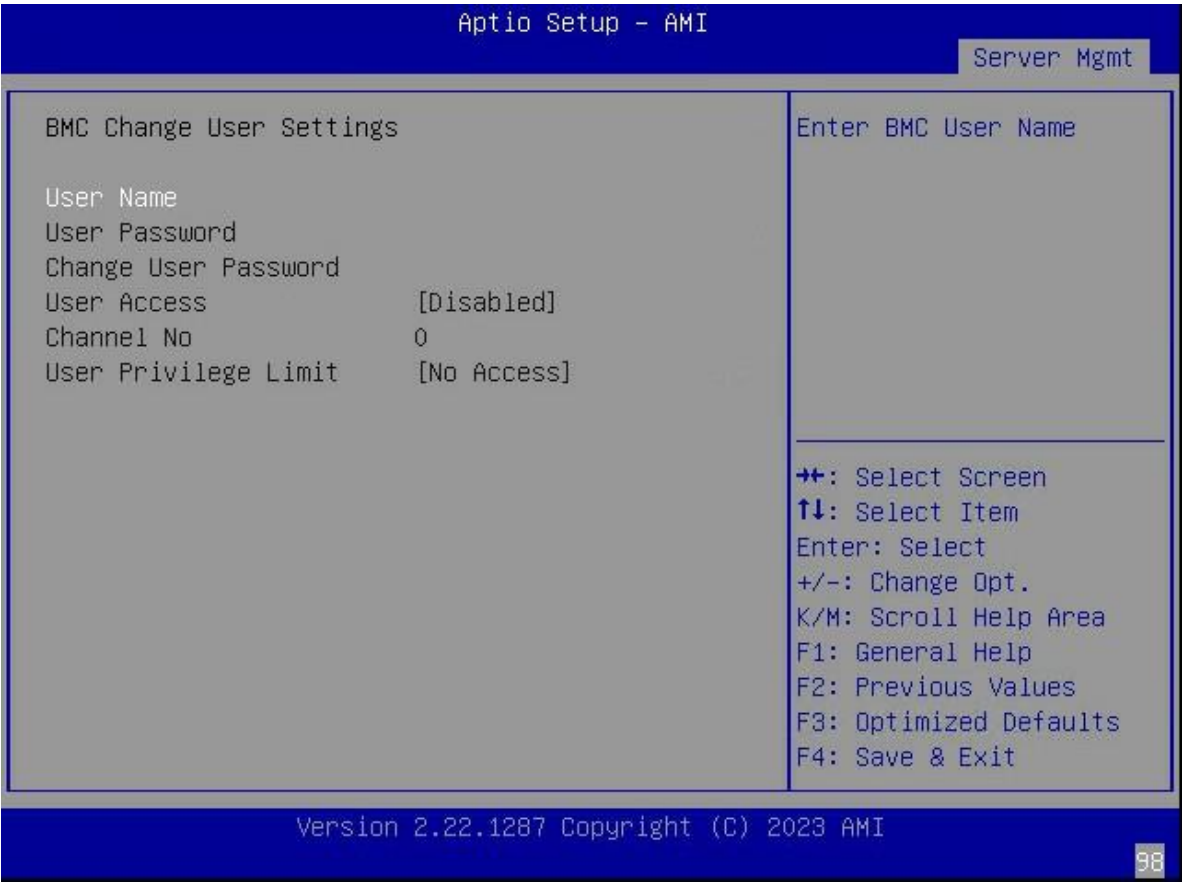
Table 3-102 Parameter Descriptions for the Delete User Screen

Parameter	Description
User Name	Enter the username of the BMC user to be deleted.
User Password	Enter the password of the BMC user to be deleted.

3.5.4.3 Change User Settings

[Figure 3-144](#) shows the **Change User Settings** screen.

Figure 3-144 Change User Settings Screen



For a description of the parameters on the **Change User Settings** screen, refer to [Table 3-103](#).

Table 3-103 Parameter Descriptions for the Change User Settings Screen

Parameter	Description	Default
User Name	Enter the BMC username to be modified.	-
User Password	Enter the current BMC user password to be modified.	-
Change User Password	Enter the new password of the BMC user.	-
User Access	Enables or disables user access. Options: ● Enabled: enables user access. ● Disabled: disables user access.	Disabled
Channel No	Enter the channel number.	0
User Privilege Limit	Sets the user privilege restrictions.	No Access

3.6 Security

The **Security** screen contains the administrator and user password settings, see [Figure 3-145](#) and [Figure 3-146](#).

Figure 3-145 Security Screen—1

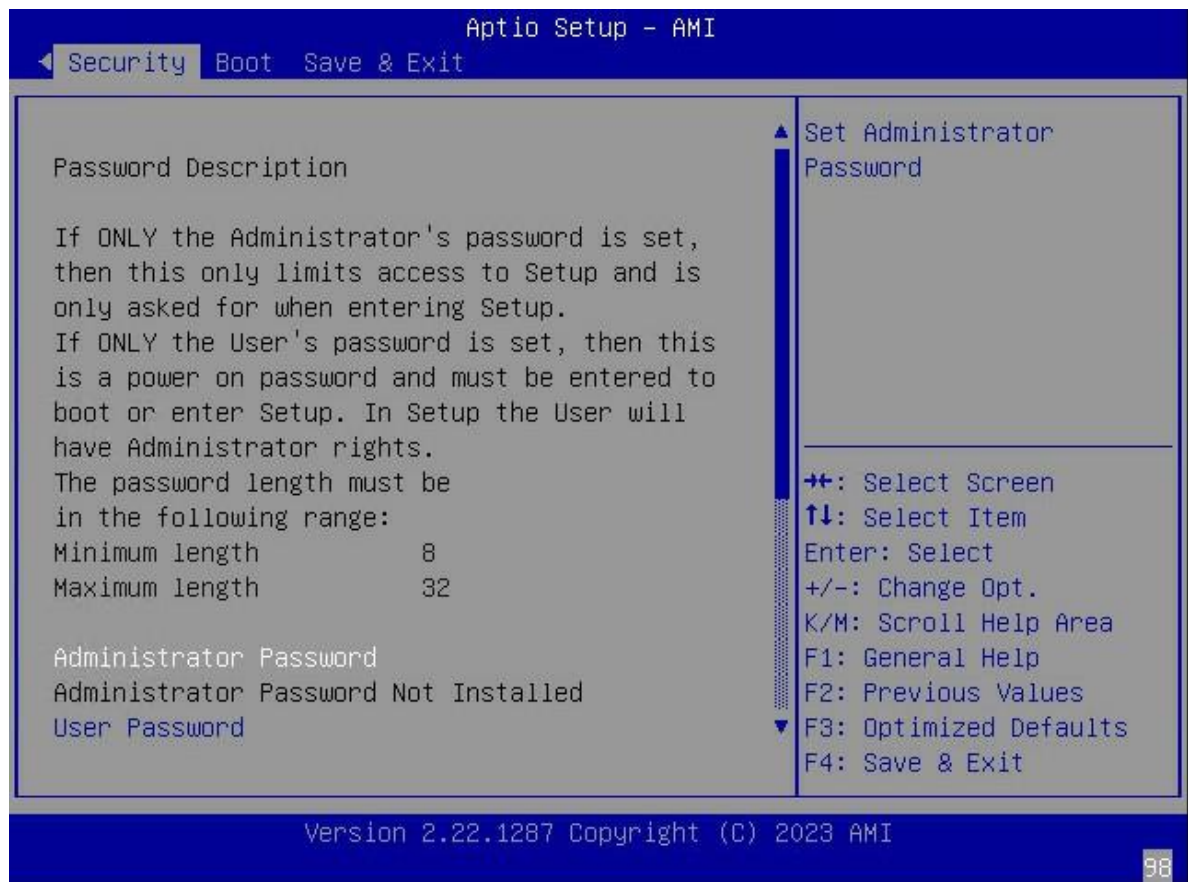
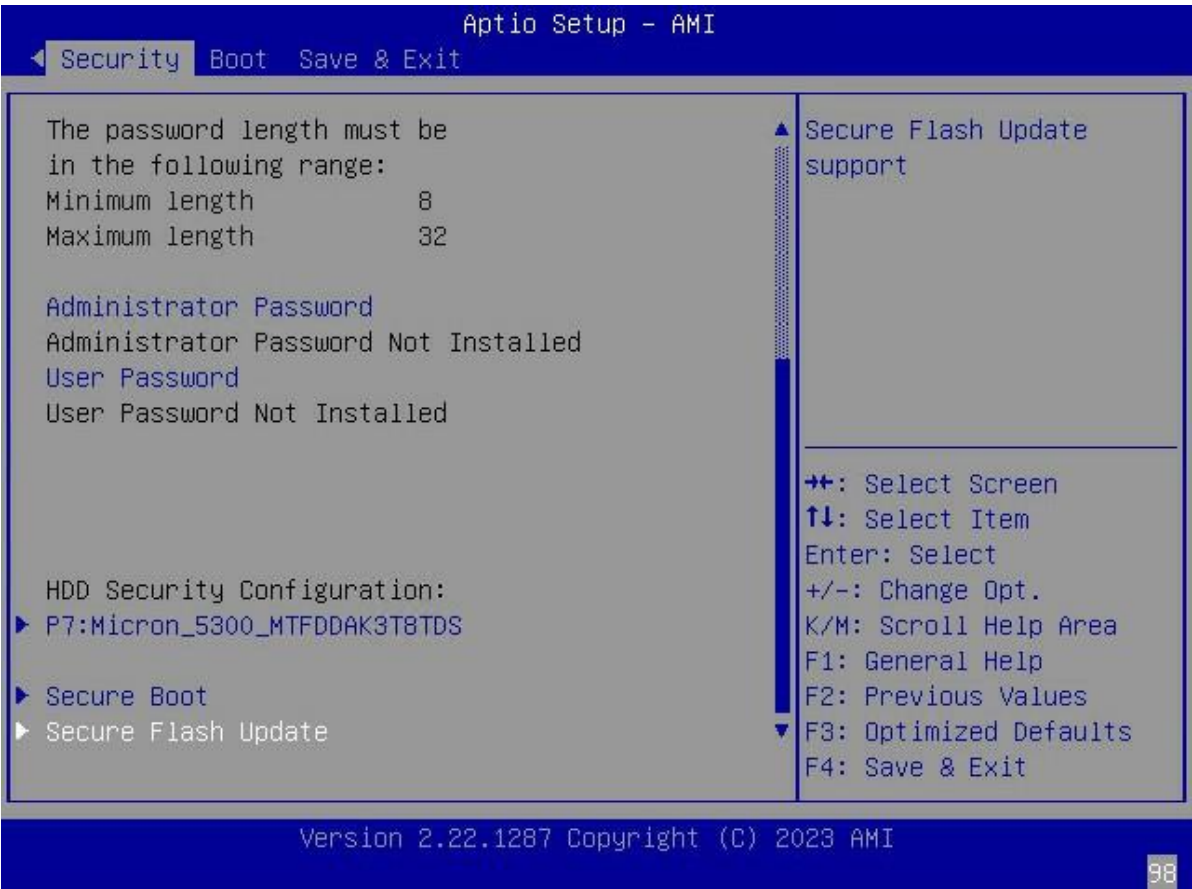


Figure 3-146 Security Screen—2



For a description of the parameters on the **Security** screen, refer to [Table 3-104](#).

Table 3-104 Parameter Descriptions for the Security Screen

Parameter	Description	Default
Administrator Password	Enter the administrator password.	-
User Password	Enter the password.	-
HDD Security Configuration	Sets the HDD security parameters. For details, refer to 3.6.1 HDD Security Configuration .	-
Secure Boot	Sets secure boot parameters. For details, refer to 3.6.2 Secure Boot .	-
Secure Flash Update	Sets secure flash update parameters. For details, refer to 3.6.3 Secure Flash Update .	-
Security Freeze Lock	Enables or disables the security freeze lock. Options: ● Enabled: enables the security freeze lock. ● Disabled: disables the security freeze lock.	Disabled

3.6.1 HDD Security Configuration

Figure 3-147 shows the **HDD Security Configuration** screen.

Figure 3-147 HDD Security Configuration Screen



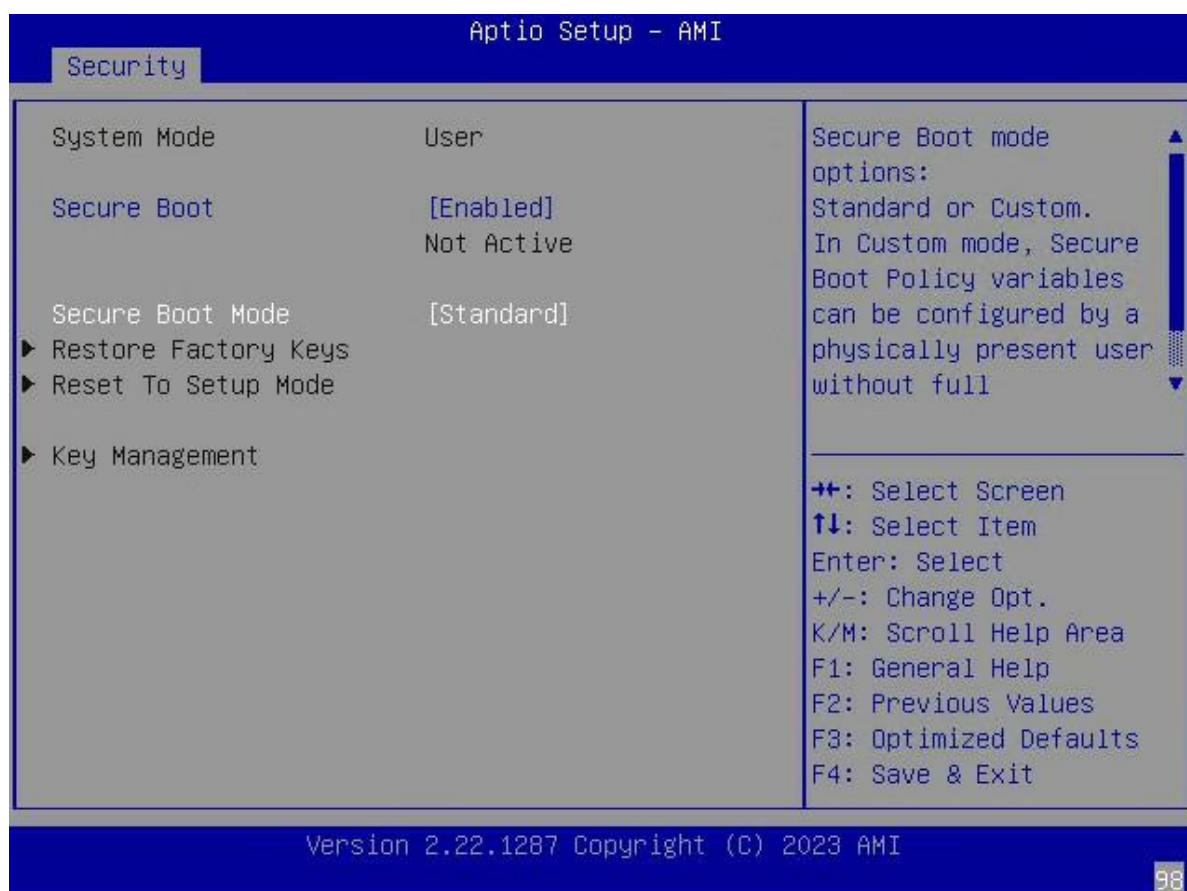
For a description of the parameters on the **HDD Security Configuration** screen, refer to [Table 3-105](#).

Table 3-105 Parameter Descriptions for the HDD Security Configuration Screen

Parameter	Description
Set User Password	Sets the password of the HDD user. The HDD user password is the basis for the HDD security. It is recommended that you restart the system after entering the password.

3.6.2 Secure Boot

Figure 3-148 shows the **Secure Boot** screen.

Figure 3-148 Secure Boot Screen

For a description of the parameters on the **Secure Boot** screen, refer to [Table 3-106](#).

Table 3-106 Parameter Descriptions for the Secure Boot Screen

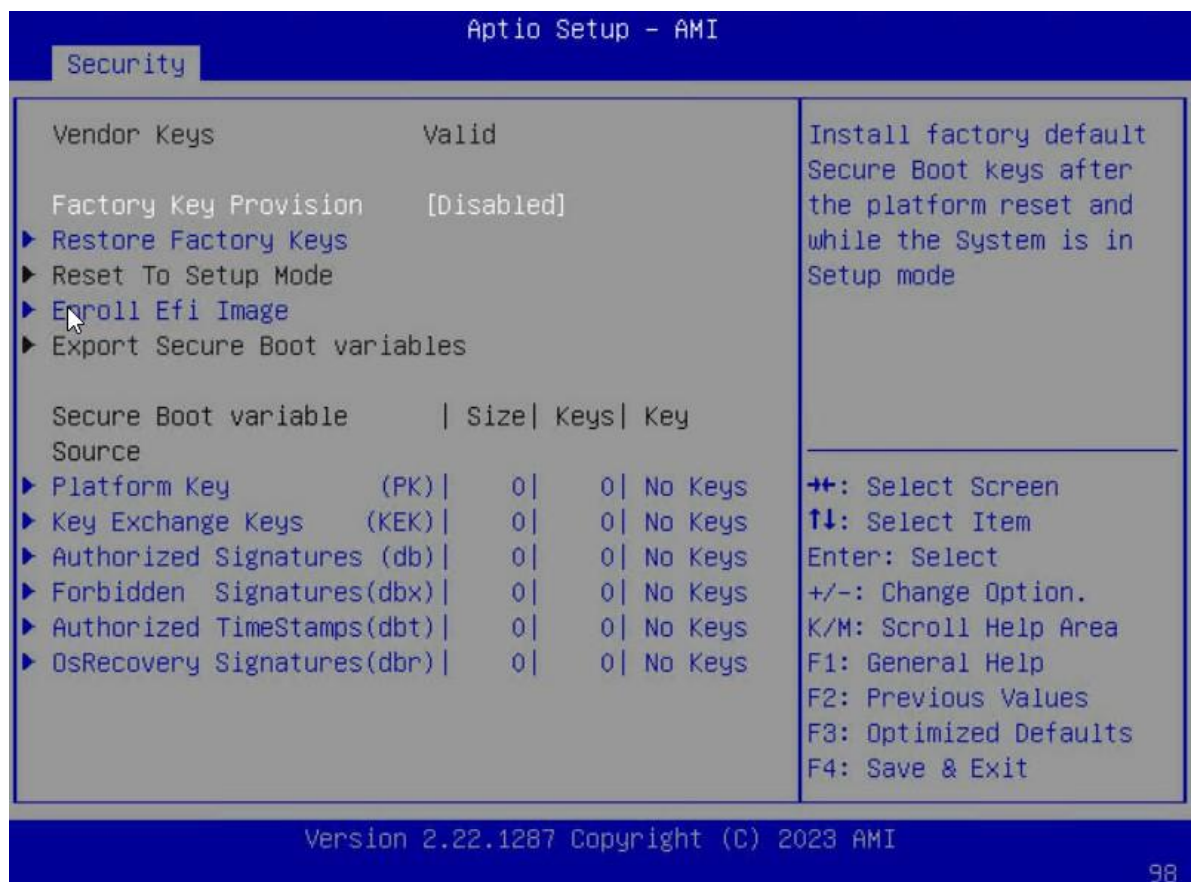
Parameter	Description	Default
System Mode	Current system mode.	User
Secure Boot	Enables or disables the secure boot feature. Options: ● Enabled: enables the secure boot feature. After the feature is enabled, the PK is registered, and the system enters user mode. You need to restart the system to apply the changes to this mode. ● Disabled: disables the secure boot feature.	Enabled
Secure Boot Mode	Sets the secure boot mode. Options: ● Standard: standard mode. ● Custom: user-defined mode.	Standard

Parameter	Description	Default
	In self-defined mode, the variables of the secure boot policy can be set by the current user without the need of complete authentication.	
Restore Factory Keys	Sets whether to forcibly change the system mode to user mode and install the default secure boot key database.	-
Reset To Setup Mode	Sets whether to delete all secure boot key databases from the NVRAM .	-
Key Management	Enables professional users to modify the variables of the secure boot policy without variable authentication. For details, refer to 3.6.2.1 Key Management .	-

3.6.2.1 Key Management

[Figure 3-149](#) shows the **Key Management** screen.

Figure 3-149 Key Management Screen



For a description of the parameters on the **Key Management** screen, refer to [Table 3-107](#).

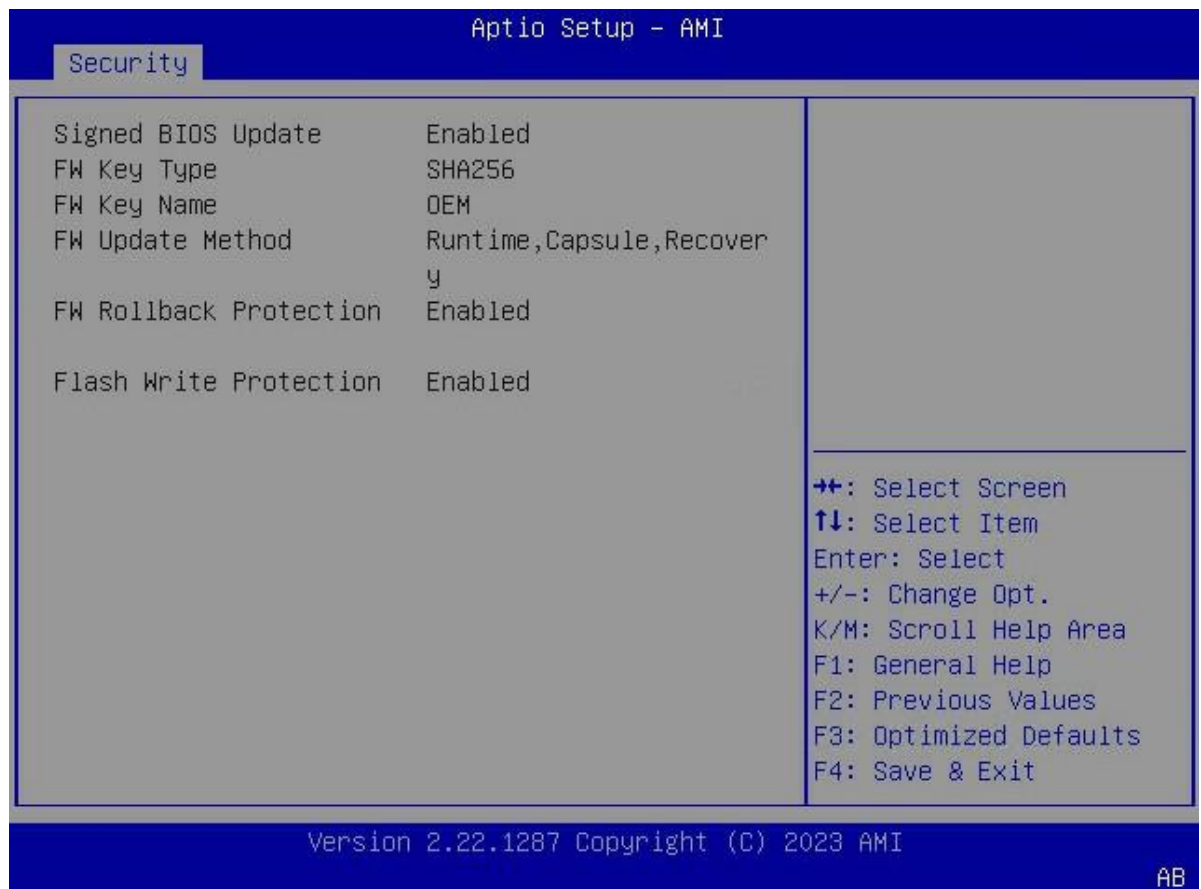
Table 3-107 Parameter Descriptions for the Key Management Screen

Parameter	Description	Default
Vendor Keys	Displays the vendor key.	-
Factory Key Provision	Sets whether to install the factory default secure boot key after the system is restarted or in setup mode. Options: ● Enabled: yes. ● Disabled: no.	Disabled
Restore Factory Keys	Sets whether to forcibly change system mode to user mode and install the default secure boot key database.	-
Reset To Setup Mode	Sets whether to delete all secure boot key databases from the NVRAM .	-
Enroll Efi Image	Allows the EFI image to run in secure boot to enroll a SHA256 hash of the PE image in the Authorized Signature Database.	-
Export Secure Boot variables	Saves the secure boot variable contents in the NVRAM to a file.	-
Platform Key	Displays the platform keys.	-
Key Exchange Keys	Displays the exchange keys.	-
Authorized Signatures	Displays the authorized signatures.	-
Forbidden Signatures	Displays banned signatures.	-
Authorized TimeStamps	Displays the authorized timestamps.	-
OsRecovery Signatures	Displays the signatures restored in the OS.	-

3.6.3 Secure Flash Update

[Figure 3-150](#) shows the **Secure Flash Update** screen.

Figure 3-150 Secure Flash Update Screen



For a description of the parameters on the **Secure Flash Update** screen, refer to [Table 3-108](#).

Table 3-108 Parameter Descriptions for the Secure Flash Update Screen

Parameter	Description	Default
Signed BIOS Update	Enables or disables the signed BMC update feature. Options: - Enabled: enables the signed BMC update feature. - Disabled: disables the signed BMC update feature.	Enabled
FW Key Type	Sets the key type of the firmware.	SHA256
FW Key Name	Sets the key name of the firmware.	OEM
FW Update Method	Sets the firmware update mode.	Runtime, Capsule, Recovery
FW Rollback Protection	Enables or disables the firmware rollback protection feature. Options: Enabled: enables the firmware rollback protection feature.	Enabled

Parameter	Description	Default
	Disabled: disables the FW rollback protection feature.	
Flash Write Protection	Enables or disables flash drive write protection. Options: - Enabled: enables flash drive write protection. - Disabled: disables flash drive write protection.	Enabled

3.7 Boot

Figure 3-151 through Figure 3-152 show the **Boot** screen.

Figure 3-151 Boot Screen—1

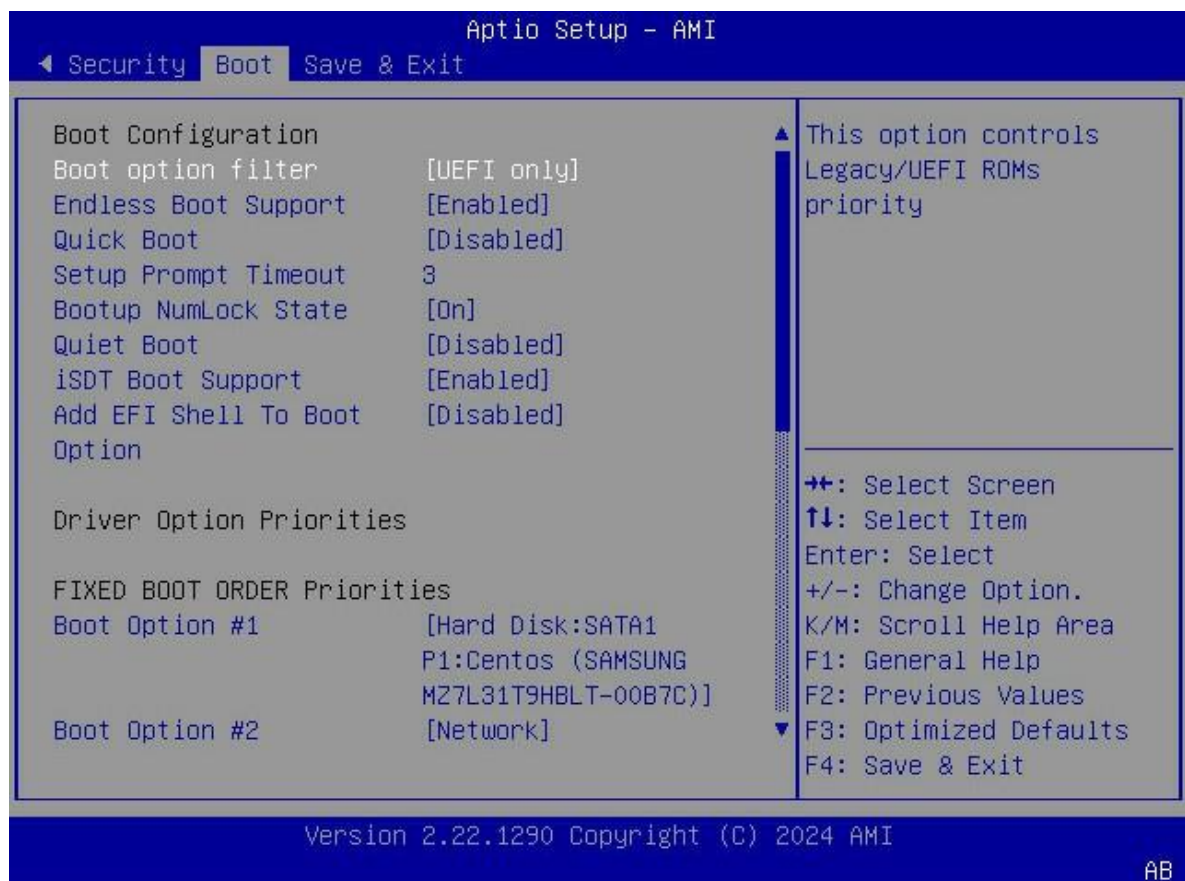
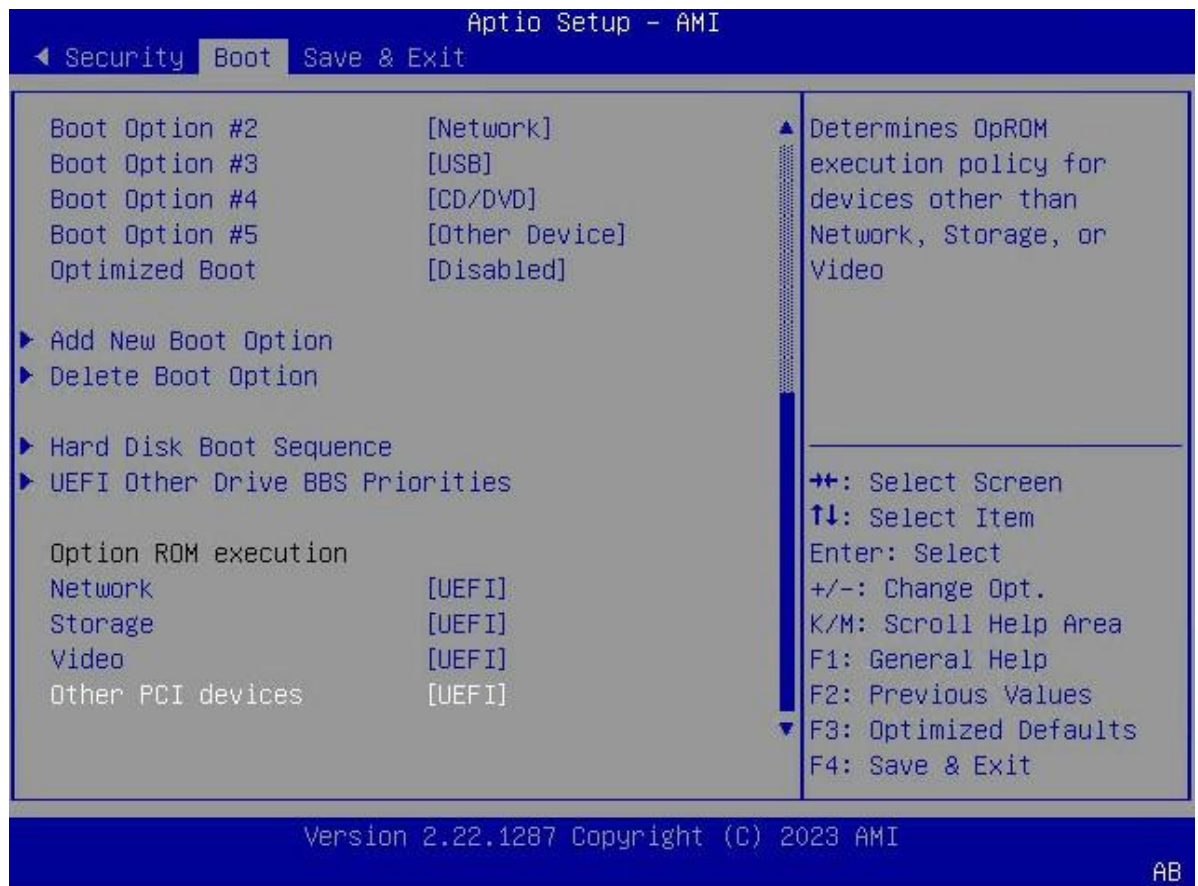


Figure 3-152 Boot Screen—2



For a description of the parameters on the **Boot** screen, refer to [Table 3-109](#).

Table 3-109 Parameter Descriptions for the Boot Screen

Parameter	Description	Default
Boot option filter	Select a boot option filter to control the priority levels of Legacy and UEFI ROM . Options: • UEFI only • Legacy only	UEFI Only
Endless Boot Support	Sets whether the system automatically reboots all bootable devices. Options: • Enabled: enables boot retry. • Disabled: disables boot retry.	Enabled
Quick Boot	Enables or disables the quick boot feature. Options: • Enabled: enables the quick boot feature.	Disabled

Parameter	Description	Default
	After the feature is enabled, the boot time is shortened by skipping the memory test during board boot. Disabled: disables the quick boot feature. After the feature is disabled, a complete memory test is performed, and the boot time is long.	
Boot Logo	Enables or disables the display of the logo during the boot process. - Enabled: The logo is displayed during the boot process. - Disabled: The logo is not displayed during the boot process.	Enabled
Wait Time For BF2 Card	Sets wait time of the BlueField-2 card, range: 0–5, unit: Minutes.	3
Setup Prompt Timeout	Enter the number of seconds to wait for the setup activation key. Value 65535 indicates indefinite waiting. - To increase the value by one, press +. - To decrease the value by one, press -. - To specify a value, press the corresponding number key.	3
Bootup NumLock State	Select the state of the NumLock key after startup. Options: - On - Off	On
Quiet Boot	Enables or disables the quiet boot feature. Options: - Enabled: enables the quiet boot feature. After the feature is enabled, the hot key information is not displayed on the logo screen during startup. - Disabled: disables the quiet boot feature. After the feature is disabled, the hot key information is displayed on the logo screen during startup.	Enabled
Skip Mix Load Default	Enables or disables the feature of skipping Mix and restoring to defaults. Options: Enabled: enables the feature of skipping Mix and restoring to defaults.	Enabled

Parameter	Description	Default
	● Disabled: disables the feature of skipping Mix and restoring to defaults.	
Add EFI Shell To Boot Option	Enables or disables the built-in shell. Options: ● Enabled: enables the built-in shell. ● Disabled: disables the built-in shell.	Disabled
Boot Option #1	Press the up/down key to select another device that will serve as the first boot device in the boot sequence. Options: ● Hard Disk ● Network ● USB ● CD/DVD ● Other Device ● Disabled The displayed boot items vary with boards.	Hard Disk: SATA0 P0:Redhat Boot Manager(GG7ZT240S3CN6)
Boot Option #2	Press the up/down key to select another device that will serve as the second boot device in the boot sequence. Options: ● Hard Disk ● Network ● USB ● CD/DVD ● Other Device ● Disabled The displayed boot items vary with boards.	Network
Boot Option #3	Press the up/down key to select another device that will serve as the third boot device in the boot sequence. Options: ● Hard Disk ● Network ● USB ● CD/DVD ● Other Device ● Disabled The displayed boot items vary with boards.	USB

Parameter	Description	Default
Boot Option #4	Press the up/down key to select another device that will serve as the fourth boot device in the boot sequence. Options: ● Hard Disk ● Network ● USB ● CD/DVD ● Other Device ● Disabled The displayed boot items vary with boards.	CD/DVD
Boot Option #5	Press the up/down key to select another device that will serve as the fifth boot device in the boot sequence. Options: ● Hard Disk ● Network ● USB ● CD/DVD ● Other Device ● Disabled The displayed boot items vary with boards.	Other Device
Optimized Boot	Enables or disables the optimized boot feature. Options: ● Enabled: enables the optimized boot feature. After this feature is enabled, CSM support is disabled and connections to network devices are disabled to reduce the boot time. ● Disabled: disables the optimized boot feature.	Disabled
Add New Boot Option	Adds a new EFI boot option to the boot order list. For details, refer to 3.7.1 Add New Boot Option.	-
Delete Boot Option	Removes an EFI boot option from the boot order list. For details, refer to 3.7.2 Delete Boot Option.	-
Hard Disk Boot Sequence	Specifies the boot priorities of available UEFI hard disk drivers. For details, refer to 3.7.3 Hard Disk Boot Sequence.	-
UEFI Other Drive BBS Priorities	Specifies the boot priorities of other available UEFI drivers. For details, refer to 3.7.5 UEFI Other Drive BBS Priorities.	-

Parameter	Description	Default
Network	Controls the execution of the network device Option ROMs in UEFI mode and Legacy mode. Options: ● Do not launch: disables the network devices. ● UEFI: launches the network devices in UEFI mode only. ● UEFI: launches the network devices in Legacy mode only.	UEFI
Storage	Controls the execution of the storage device Option ROMs in UEFI mode and Legacy mode. Options: ● Do not launch: disables the storage devices. ● UEFI: launches the storage devices in UEFI mode only. ● Legacy: launches the storage devices in Legacy mode only.	UEFI
Video	Controls the execution of the video device Option ROMs in UEFI mode and Legacy mode. Options: ● Do not launch: disables the video card devices. ● UEFI: launches the video card devices in UEFI mode only. ● Legacy: launches the video card devices in Legacy mode only.	UEFI
Other PCI devices	Controls the execution of Option ROMs of other PCI device in UEFI mode and Legacy mode. Options: ● Do not launch: disables other PCI devices. ● UEFI: launches other PCI devices in UEFI mode only. ● Legacy: launches other PCI devices in Legacy mode only.	UEFI

3.7.1 Add New Boot Option

[Figure 3-153](#) shows the **Add New Boot Option** screen.

Figure 3-153 Add New Boot Option Screen



For a description of the parameters on the **Add New Boot Option** screen, refer to [Table 3-110](#).

Table 3-110 Parameter Descriptions for the Add New Boot Option Screen

Parameter	Description
Add boot option	Enter a name for the new boot option.
Path for boot option	Enter or select the boot path for the new boot option. ● Format: <i>fsx:\path\ilename.ei</i>. ● You can use the arrow keys and the Enter key to select the path of the boot option. The selected path is then displayed in Boot option File Path.
Boot option File Path	Displays the path of the boot option file.
Create	Creates a boot option.

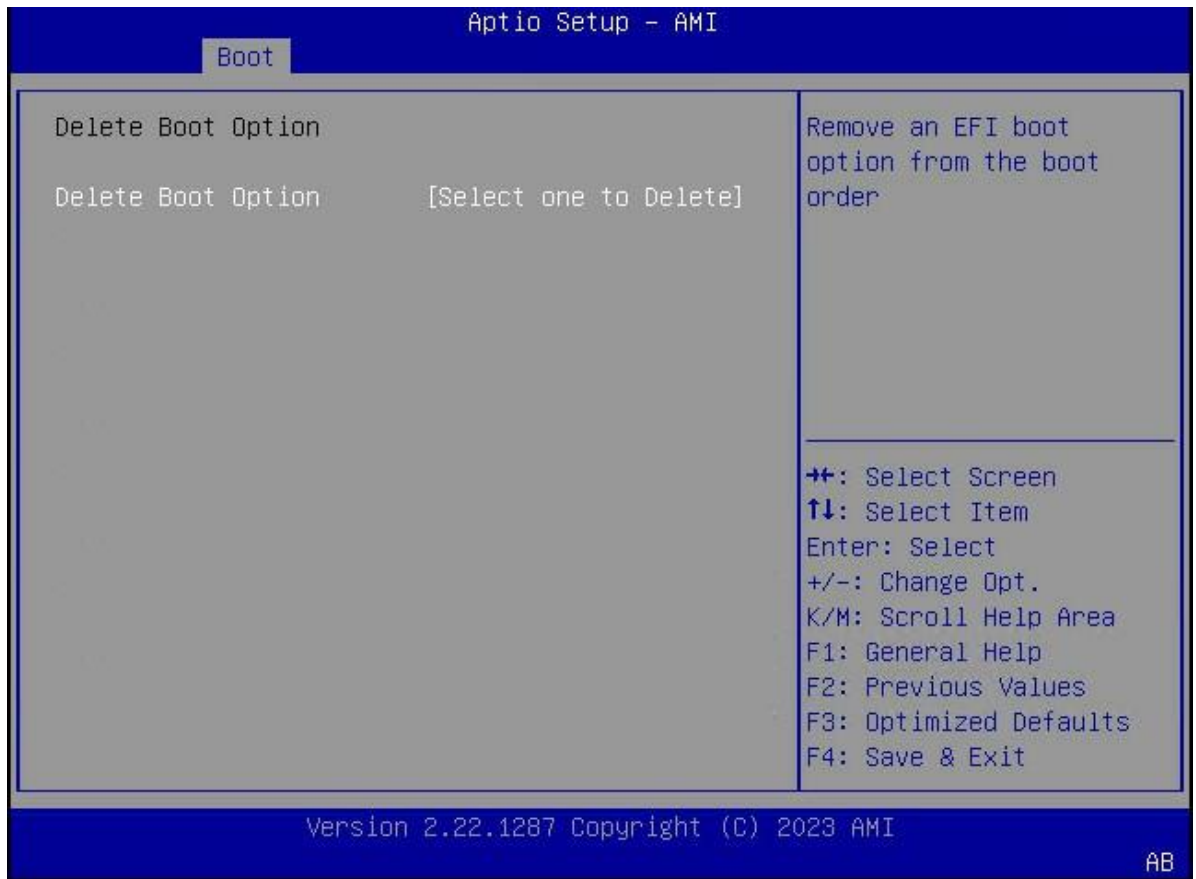
 Note

The added boot option is displayed on the **Hard Disk Boot Sequence** screen and can be deleted on the **Delete Boot Option** screen.

3.7.2 Delete Boot Option

Figure 3-154 shows the **Delete Boot Option** screen.

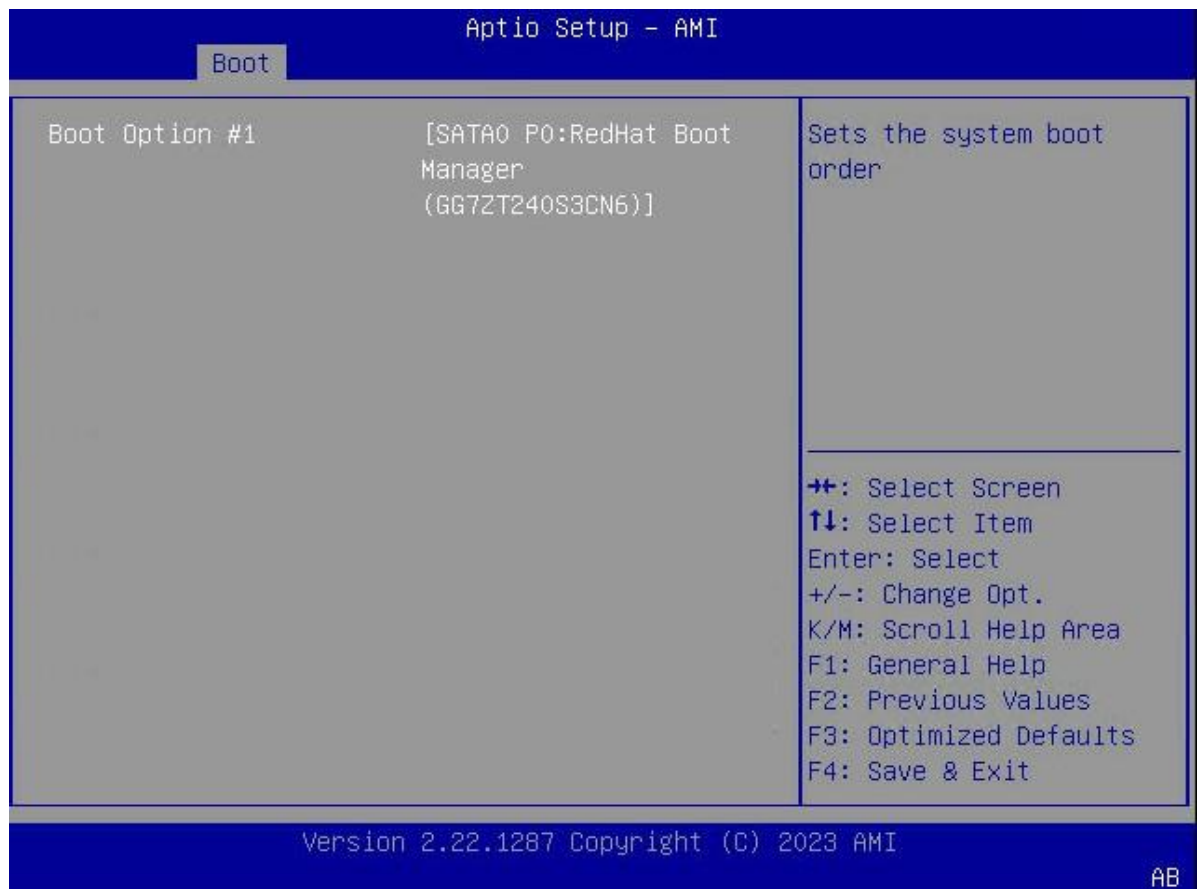
Figure 3-154 Delete Boot Option Screen



On the **Delete Boot Option** screen, you can delete an **EFI** option in the boot priority.

3.7.3 Hard Disk Boot Sequence

Figure 3-155 shows the **Hard Disk Boot Sequence** screen.

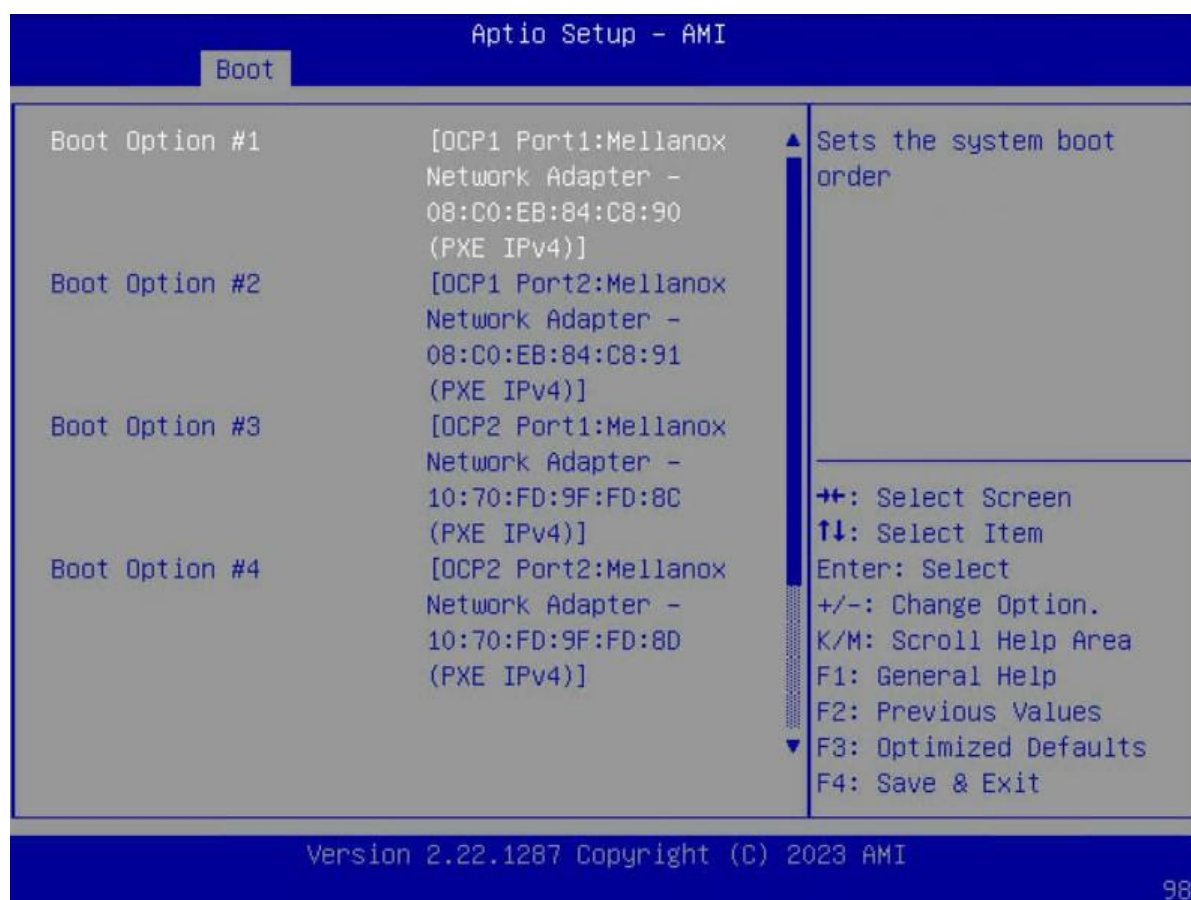
Figure 3-155 Hard Disk Boot Sequence Screen

On the **Hard Disk Boot Sequence** screen, you can set the hard disk boot sequence.

3.7.4 UEFI NETWORK Drive BBS Priorities

Figure 3-156 shows the **UEFI NETWORK Drive BBS Priorities** screen.

Figure 3-156 UEFI NETWORK Drive BBS Priorities Screen



On the **UEFI NETWORK Drive BBS Priorities** screen, you can set the boot sequence of NETWORK bootable Drives.

3.7.5 UEFI Other Drive BBS Priorities

Figure 3-157 shows the **UEFI Other Drive BBS Priorities** screen.

Figure 3-157 UEFI Other Drive BBS Priorities Screen



On the **UEFI Other Drive BBS Priorities** screen, you can set the boot sequence of other bootable Drives.

3.8 Save & Exit

Figure 3-158 through Figure 3-159 show the **Save & Exit** screen.

Figure 3-158 Save&Exit Screen—1

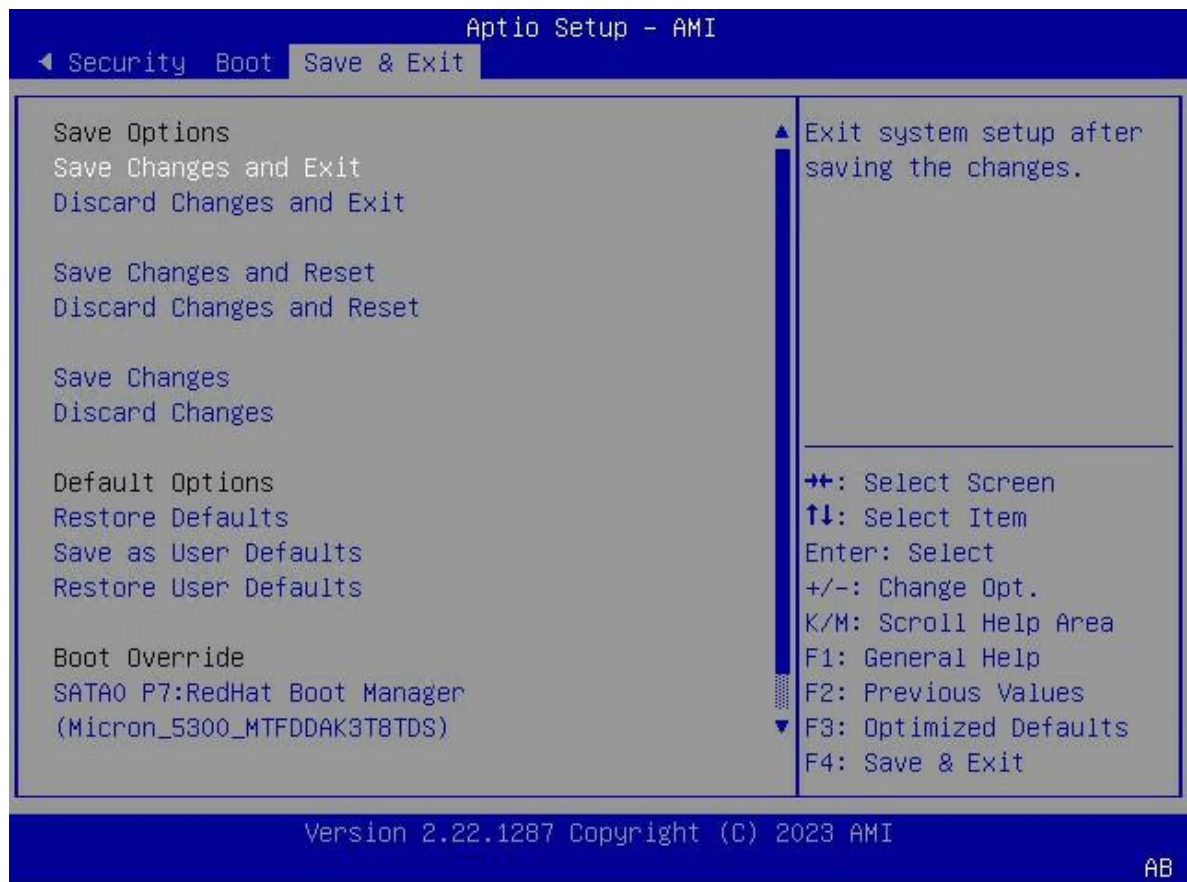
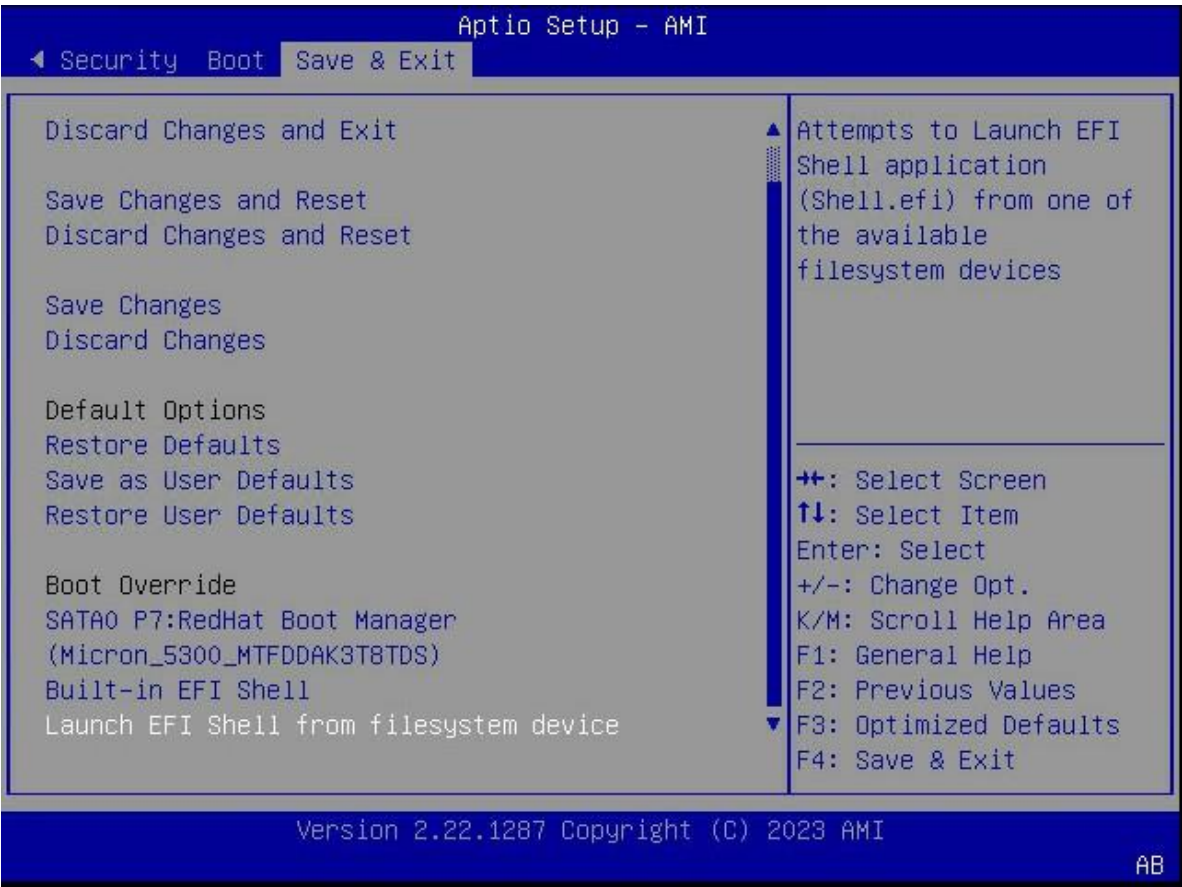


Figure 3-159 Save&Exit Screen—2



For a description of the parameters on the **Save & Exit** screen, refer to [Table 3-111](#).

Table 3-111 Parameter Descriptions for the Save & Exit Screen

Parameter	Description
Saving Changes and Exit	Saves the changes and exits the BIOS.
Discard Changes and Exit	Exits the BIOS without saving any changes.
Saving Changes and Reset	Saves the changes and restarts the system.
Discard Changes and Reset	Restarts the system without saving any changes.
Save Changes	Saves all parameter changes.
Discard Changes	Discards any parameter changes.
Restore Defaults	Restores the default settings of all parameters.
Save as User Defaults	Saves any parameter changes as the user default settings.
Restore User Defaults	Restores all parameters to user default settings.
Launch EFI Shell from filesystem device	Tries launching the EFI Shell application (Shell.efi) from one of the available file system devices.

Chapter 4

Reference: Control Keys for BIOS Setup

For a description of the available control keys in the BIOS of the **Eagle Stream** platform, refer to [Table 4-1](#).

Table 4-1 Descriptions of Control Keys

Control Key	Description
←/→	Moves the cursor left or right.
↑/↓	Moves the cursor up or down.
Enter	Selects an item or enters a submenu.
+/-	Changes the value of an item.
Esc	Exits the screen.
F1	Opens the help screen, where the descriptions of the available keys are displayed.
F2	Loads the last settings.
F3	Loads the default settings.
F4	Saves the settings and exits the BIOS.

Figures

Figure 1-1 BIOS in a System.....1

Figure 2-1 Logo on the Screen.....4

Figure 2-2 Boot Manager Screen5

Figure 2-3 Aptio Setup Screen6

Figure 2-4 System Language Dialog Box7

Figure 2-5 Server Configuration Information.....8

Figure 2-6 CPU Information.....9

Figure 2-7 Memory Information..... 10

Figure 2-8 Advanced Screen..... 11

Figure 2-9 Mainboard Information Screen 12

Figure 2-10 LAN MAC Information Screen..... 13

Figure 2-11 Slot Information Screen..... 14

Figure 2-12 Detailed NIC Information 15

Figure 2-13 Advanced Screen 16

Figure 2-14 Mainboard Information Screen 17

Figure 2-15 OnBoard Device Information Screen..... 18

Figure 2-16 Advanced Screen 19

Figure 2-17 Mainboard Information Screen 20

Figure 2-18 Slot Information Screen..... 21

Figure 2-19 Detailed Standard RAID Card Information..... 22

Figure 2-20 Hard Disk Information 23

Figure 2-21 Setting the Date.....	25
Figure 2-22 Setting the Time	26
Figure 2-23 Boot Option Filter Dialog Box.....	27
Figure 2-24 Boot Option #1 Dialog Box	29
Figure 2-25 Create New Password Dialog Box.....	31
Figure 2-26 Enter Current Password Dialog Box.....	32
Figure 2-27 Enter Current Password Dialog Box.....	33
Figure 2-28 WARNING Dialog Box.....	34
Figure 2-29 Socket1 Configuration Screen.....	35
Figure 2-30 Port 1A Screen	36
Figure 2-31 PCI-E Port Dialog Box.....	37
Figure 2-32 Console Redirection Dialog Box.....	38
Figure 2-33 BMC Network Configuration Screen.....	39
Figure 2-34 BMC Network Configuration Screen.....	40
Figure 2-35 Advanced Screen	42
Figure 2-36 PXE Configuration Screen	43
Figure 2-37 Socket Configuration Screen	45
Figure 2-38 Intel VT for Directed I/O (VT-d) Screen	46
Figure 2-39 Processor Configuration Screen.....	47
Figure 2-40 Advanced Screen	48
Figure 2-41 PCI Subsystem Settings Screen.....	49
Figure 2-42 Socket Configuration Screen	50
Figure 2-43 Common RefCode Configuration Screen.....	51
Figure 2-44 Socket Configuration Screen	54

Figure 2-45 Advanced Power Management Configuration Screen.....	55
Figure 2-46 CPU P State Control Screen	56
Figure 2-47 CPU C State Control Screen.....	57
Figure 2-48 Package C State Control Screen.....	58
Figure 2-49 Advanced Screen	59
Figure 2-50 Trusted Computing Screen.....	60
Figure 2-51 Advanced Screen	62
Figure 2-52 Managing a RAID Controller.....	63
Figure 2-53 Setting Advanced Configuration Options for the RAID Controller.....	64
Figure 2-54 Configuring the RAID Controller.....	65
Figure 2-55 Port CN0 Mode Dialog Box.....	66
Figure 2-56 Configuring the Mode of a Port.....	67
Figure 2-57 Configuring the Mode of Another Port.....	68
Figure 2-58 Port Mode Set Successfully.....	69
Figure 2-59 SATA And RST Configuration Screen.....	70
Figure 2-60 Controller 1 SATA And RST Configuration Screen	71
Figure 2-61 Create RAID Volume Screen.....	72
Figure 2-62 RAID Volume Successfully Created	73
Figure 2-63 Load Optimal Defaults Dialog Box.....	74
Figure 3-1 Main Screen—1.....	76
Figure 3-2 Main Screen—2.....	77
Figure 3-3 Advanced Screen—1.....	79
Figure 3-4 Advanced Screen—2.....	80
Figure 3-5 Mainboard Information Screen	82

Figure 3-6 OnBoard Device Information Screen	83
Figure 3-7 LAN MAC Information Screen	84
Figure 3-8 Graphics Card Information Screen	85
Figure 3-9 Slot Information Screen	86
Figure 3-10 Trusted Computing Screen—1	87
Figure 3-11 Trusted Computing Screen—2	88
Figure 3-12 ACPI Settings Screen	90
Figure 3-13 Redfish Host Interface Settings Screen	91
Figure 3-14 Serial Port Console Redirection Screen	92
Figure 3-15 Console Redirection Settings Screen	94
Figure 3-16 Legacy Console Redirection Settings Screen	97
Figure 3-17 Console Redirection Settings Screen	98
Figure 3-18 SIO Common Setting Screen	100
Figure 3-19 SIO Configuration Screen	101
Figure 3-20 Serial Port 1 Screen	102
Figure 3-21 PCI Subsystem Settings Screen	103
Figure 3-22 USB Configuration Screen	105
Figure 3-23 Network Stack Configuration Screen	106
Figure 3-24 IPv4 PXE Boot Timeout Screen	108
Figure 3-25 CSM Configuration Screen	110
Figure 3-26 NVMe Configuration Screen	111
Figure 3-27 Emulation Configuration Screen	112
Figure 3-28 PXE Configuration Screen	113
Figure 3-29 Tls Auth Configuration Screen	114

Figure 3-30 Server CA Configuration Screen	115
Figure 3-31 Enroll Cert Screen	116
Figure 3-32 Delete Cert Screen.....	117
Figure 3-33 RAM Disk Configuration Screen.....	118
Figure 3-34 Create Raw Screen	119
Figure 3-35 Driver Health Screen.....	120
Figure 3-36 Platform Configuration Screen.....	121
Figure 3-37 PCH-IO Configuration Screen—1	122
Figure 3-38 PCH-IO Configuration Screen—2	123
Figure 3-39 PCI Express Configuration Screen	126
Figure 3-40 SATA And RST Configuration Screen.....	127
Figure 3-41 Controller 1 SATA And RST Configuration Screen	128
Figure 3-42 Software Feature Mask Configuration	130
Figure 3-43 USB Configuration Screen	133
Figure 3-44 Global Reset Mask Configuration Screen.....	135
Figure 3-45 Miscellaneous Configuration Screen.....	136
Figure 3-46 Server ME Configuration Screen—1.....	138
Figure 3-47 Server ME Configuration Screen—2.....	139
Figure 3-48 Server ME Configuration Screen—3.....	140
Figure 3-49 Runtime Error Logging Screen—1	141
Figure 3-50 Runtime Error Logging Screen—2.....	142
Figure 3-51 EMCA Settings Screen.....	144
Figure 3-52 Whea Settings Screen.....	147
Figure 3-53 Error Injection Settings Screen.....	148

Figure 3-54 Memory Error Enabling Screen—1.....	150
Figure 3-55 Memory Error Enabling Screen—2.....	151
Figure 3-56 Ilo Error Enabling Screen—1.....	153
Figure 3-57 Ilo Error Enabling Screen—2.....	154
Figure 3-58 Ilo Error Enabling Screen—3.....	155
Figure 3-59 PCIe Error Enabling Screen—1	161
Figure 3-60 PCIe Error Enabling Screen—2	162
Figure 3-61 PCIe Error Enabling Screen—3	163
Figure 3-62 Error Control Setting Screen.....	167
Figure 3-63 Socket Configuration Screen	169
Figure 3-64 Processor Configuration Screen—1.....	170
Figure 3-65 Processor Configuration Screen—2.....	171
Figure 3-66 Processor Configuration Screen—3.....	172
Figure 3-67 Processor Configuration Screen—4.....	173
Figure 3-68 Processor Configuration Screen—5.....	174
Figure 3-69 PSMI Configuration Screen.....	182
Figure 3-70 Socket 0 Configuration Screen.....	183
Figure 3-71 Common RefCode Configuration Screen.....	185
Figure 3-72 Uncore Configuration Screen.....	186
Figure 3-73 Uncore General Configuration Screen—1.....	187
Figure 3-74 Uncore General Configuration Screen—2.....	188
Figure 3-75 Uncore Status Screen.....	193
Figure 3-76 Uncore Dfx Configuration Screen	194
Figure 3-77 Memory Configuration Screen—1.....	195

Figure 3-78 Memory Configuration Screen—2.....	196
Figure 3-79 Memory Configuration Screen—3.....	197
Figure 3-80 Memory Configuration Screen—4.....	198
Figure 3-81 Memory Configuration Screen—5.....	199
Figure 3-82 Adv MemTest Rank Selection Screen.....	209
Figure 3-83 FADR Configuration Screen.....	210
Figure 3-84 Memory Topology Screen.....	212
Figure 3-85 Page Policy Screen.....	213
Figure 3-86 Memory Training Screen.....	214
Figure 3-87 Memory I/O Health Check Screen—1.....	216
Figure 3-88 Memory I/O Health Check Screen—2.....	217
Figure 3-89 Memory Map Screen.....	219
Figure 3-90 Memory RAS Configuration Screen—1.....	220
Figure 3-91 Memory RAS Configuration Screen—2.....	221
Figure 3-92 Memory Dfx Configuration Screen.....	225
Figure 3-93 RMT Configuration Menu Screen.....	228
Figure 3-94 IIO Configuration Screen—1.....	231
Figure 3-95 IIO Configuration Screen—2.....	232
Figure 3-96 Socket0 Configuration Screen.....	236
Figure 3-97 Port DMI Screen.....	240
Figure 3-98 Port 1A Screen—1.....	242
Figure 3-99 Port 1A Screen—2.....	243
Figure 3-100 IOAT Configuration Screen.....	245
Figure 3-101 Intel VT for Directed I/O (VT-d) Screen—1.....	246

Figure 3-102 Intel VT for Directed I/O (VT-d) Screen—2	247
Figure 3-103 Intel VMD Technology Screen.....	250
Figure 3-104 Intel VMD Configurations on Socket 0	251
Figure 3-105 IIO DFX Configuration Screen.....	252
Figure 3-106 Socket0 Configuration Screen.....	255
Figure 3-107 MMIO Poison Control Screen.....	257
Figure 3-108 Port DMI Screen—1.....	259
Figure 3-109 Port DMI Screen—2.....	260
Figure 3-110 Port 1A Screen—1	263
Figure 3-111 Port 1A Screen—2	264
Figure 3-112 Socket 0, Device Hide Menu Screen	267
Figure 3-113 Advanced Power Management Configuration Screen.....	270
Figure 3-114 CPU P State Control Screen—1.....	272
Figure 3-115 CPU P State Control Screen—2.....	273
Figure 3-116 Hardware PM State Control Screen	275
Figure 3-117 CPU C State Control Screen.....	277
Figure 3-118 Package C State Control Screen.....	279
Figure 3-119 CPU Thermal Management Screen.....	281
Figure 3-120 CPU-Advanced PM Tuning Screen	282
Figure 3-121 Energy Performance BIAS Screen	284
Figure 3-122 Package Current Config Screen.....	286
Figure 3-123 SOCKET RAPL Config Screen	287
Figure 3-124 PMAX Detector Configuration Screen.....	288
Figure 3-125 ACPI Sx State Control Screen.....	289

Figure 3-126 Memory Power & Thermal Configuration Screen	290
Figure 3-127 Memory Thermal Screen.....	292
Figure 3-128 Memory Power Savings Advanced Options Screen.....	293
Figure 3-129 CKE Feature Screen.....	294
Figure 3-130 Self Refresh Feature Screen.....	295
Figure 3-131 Server Mgmt Screen—1.....	296
Figure 3-132 Server Mgmt Screen—2.....	297
Figure 3-133 System Event Log Screen	299
Figure 3-134 View FRU Information Screen.....	301
Figure 3-135 BMC Network Configuration Screen—1.....	302
Figure 3-136 BMC Network Configuration Screen—2.....	303
Figure 3-137 BMC Network Configuration Screen—3.....	304
Figure 3-138 BMC Network Configuration Screen—4.....	305
Figure 3-139 BMC Network Configuration Screen—5.....	306
Figure 3-140 BMC Network Configuration Screen—6.....	307
Figure 3-141 BMC User Settings Screen.....	312
Figure 3-142 Add User Dialog Box	314
Figure 3-143 Delete User Screen.....	315
Figure 3-144 Change User Settings Screen.....	316
Figure 3-145 Security Screen—1	317
Figure 3-146 Security Screen—2	318
Figure 3-147 HDD Security Configuration Screen	319
Figure 3-148 Secure Boot Screen.....	320
Figure 3-149 Key Management Screen.....	321

Figure 3-150 Secure Flash Update Screen.....	323
Figure 3-151 Boot Screen—1.....	324
Figure 3-152 Boot Screen—2.....	325
Figure 3-153 Add New Boot Option Screen	330
Figure 3-154 Delete Boot Option Screen.....	331
Figure 3-155 Hard Disk Boot Sequence Screen.....	332
Figure 3-156 UEFI NETWORK Drive BBS Priorities Screen	333
Figure 3-157 UEFI Other Drive BBS Priorities Screen.....	334
Figure 3-158 Save&Exit Screen—1	335
Figure 3-159 Save&Exit Screen—2	336

Tables

Table 2-1 Descriptions of Hot Keys for BIOS Startup.....	5
Table 2-2 Hard Disk Information Parameter Descriptions	23
Table 2-3 Boot Device Descriptions.....	29
Table 2-4 Descriptions of the Items Not Available for the User	30
Table 2-5 BMC Network Parameter Descriptions	40
Table 2-6 Common Virtualization Parameter Descriptions	44
Table 2-7 Common Power Parameter Descriptions	51
Table 2-8 Functions of the Menus on the Controller Management Screen	63
Table 2-9 RAID Volume Parameter Descriptions.....	72
Table 3-1 Main Screen Parameter Descriptions	77
Table 3-2 Advanced Parameter Descriptions	80
Table 3-3 Parameter Descriptions for the Mainboard Information screen.....	82
Table 3-4 Parameter Descriptions for the OnBoard Device Information Screen	84
Table 3-5 Parameter Descriptions for the Graphics Card Information Screen.....	85
Table 3-6 Parameter Descriptions for the Slot Information Screen.....	86
Table 3-7 Parameter Descriptions for the Trusted Computing Screen	88
Table 3-8 Parameter Descriptions for the ACPI Settings Screen.....	90
Table 3-9 Parameter Descriptions for the Redfish Host Interface Settings Screen	91
Table 3-10 Parameter Descriptions for the Serial Port Console Redirection Screen.....	92
Table 3-11 Parameter Descriptions for the Console Redirection Settings Screen.	94

Table 3-12 Parameter Descriptions for the Legacy Console Redirection Settings Screen.....	97
Table 3-13 Parameter Descriptions for the Console Redirection Settings Screen.	98
Table 3-14 Parameter Descriptions for the SIO Common Setting Screen	100
Table 3-15 Parameter Descriptions for the SIO Configuration Screen	101
Table 3-16 Parameter Descriptions for the Serial Port 1 Screen.....	102
Table 3-17 Parameter Descriptions for the PCI Subsystem Settings Screen	104
Table 3-18 Parameter Descriptions for the USB Configuration Screen.....	105
Table 3-19 Parameter Descriptions for the Network Stack Configuration Screen	107
Table 3-20 Parameter Descriptions for the IPv4 PXE Boot Timeout Screen	108
Table 3-21 Parameter Descriptions for the CSM Configuration Screen	110
Table 3-22 Parameter Descriptions for the Emulation Configuration Screen.....	112
Table 3-23 Parameter Descriptions for the PXE Configuration Screen	113
Table 3-24 Parameter Descriptions for the Tls Auth Configuration Screen.....	114
Table 3-25 Parameter Descriptions for the Server CA Configuration Screen	115
Table 3-26 Parameter Descriptions for the Enroll Cert Screen.....	116
Table 3-27 Parameter Descriptions for the Delete Cert Screen	117
Table 3-28 Parameter Descriptions for the RAM Disk Configuration Screen.....	118
Table 3-29 Parameter Descriptions for the Create Raw Screen.....	119
Table 3-30 Parameter Descriptions for the Platform Configuration Screen.....	121
Table 3-31 Parameter Descriptions for the PCH-IO Configuration Screen	123
Table 3-32 Parameter Descriptions for the PCI Express Configuration Screen	126
Table 3-33 Controller 1 SATA And RST Configuration Parameter Descriptions	128
Table 3-34 Parameter Descriptions for the Software Feature Mask Configuration Screen.....	130

Table 3-35 Parameter Descriptions for the USB Configuration Screen.....	133
Table 3-36 Parameter Descriptions for the Global Reset Mask Configuration Screen.....	135
Table 3-37 Parameter Descriptions for the Miscellaneous Configuration Screen	136
Table 3-38 Parameter Descriptions for the Server ME Configuration Screen.....	140
Table 3-39 Parameter Descriptions for the Runtime Error Logging Screen	142
Table 3-40 Parameter Descriptions for the eMCA Settings Screen	145
Table 3-41 Parameter Descriptions for the Whea Settings Screen.....	147
Table 3-42 Parameter Descriptions for the Error Injection Settings Screen.....	149
Table 3-43 Parameter Descriptions for the Memory Error Enabling Screen	151
Table 3-44 Parameter Descriptions for the Ilo Error Enabling Screen.....	155
Table 3-45 Parameter Descriptions for the PCIe Error Enabling Screen.....	163
Table 3-46 Parameter Descriptions for the Error Control Setting Screen.....	167
Table 3-47 Parameter Descriptions for the Socket Configuration Screen	169
Table 3-48 Parameter Descriptions for the Processor Configuration Screen.....	174
Table 3-49 Parameter Descriptions for the PSMI Configuration Screen.....	182
Table 3-50 Parameter Descriptions for the Socket 0 Configuration Screen.....	183
Table 3-51 Parameter Descriptions for the Common RefCode Configuration Screen.....	185
Table 3-52 Parameter Descriptions for the Uncore Configuration Screen.....	186
Table 3-53 Parameter Descriptions for the Uncore General Configuration Screen.....	188
Table 3-54 Parameter Descriptions for the Uncore Dfx Configuration Screen.....	194
Table 3-55 Parameter Descriptions for the Memory Configuration Screen.....	199

Table 3-56 Parameter Descriptions for the Adv MemTest Rank Selection Screen.....	210
Table 3-57 Parameter Descriptions for the fADR Configuration Screen.....	210
Table 3-58 Parameter Descriptions for the Memory Topology Screen.....	212
Table 3-59 Parameter Descriptions for the Page Policy Screen.....	213
Table 3-60 Parameter Descriptions for the Memory Training Screen.....	214
Table 3-61 Parameter Descriptions for the Memory I/O Health Check Screen	217
Table 3-62 Parameter Descriptions for the Memory Map Screen	219
Table 3-63 Parameter Descriptions for the Memory RAS Configuration Screen ...	221
Table 3-64 Parameter Descriptions for the Memory Dfx Configuration Screen	225
Table 3-65 Parameter Descriptions for the RMT Configuration Menu Screen.....	228
Table 3-66 Parameter Descriptions for the IIO Configuration Screen.....	232
Table 3-67 Parameter Descriptions for the Socket0 Configuration Screen.....	236
Table 3-68 Parameter Descriptions for the Port DMI Screen.....	240
Table 3-69 Parameter Descriptions for the Port 1A Screen.....	243
Table 3-70 Parameter Descriptions for the IOAT Configuration Screen.....	246
Table 3-71 Parameter Descriptions for the Intel VT for Directed I/O (VT-d) Screen.....	247
Table 3-72 Parameter Descriptions for the Intel VMD Technology Screen.....	250
Table 3-73 Parameter Descriptions for the Socket 0 VMD Screen.....	251
Table 3-74 Parameter Descriptions for the IIO DFX Configuration Screen.....	252
Table 3-75 Socket0 Configuration Parameter Descriptions.....	255
Table 3-76 Parameter Descriptions for the MMIO Poison Control Screen.....	257
Table 3-77 Parameter Descriptions for the Port DMI Screen.....	260
Table 3-78 Port 1A Parameter Descriptions	264

Table 3-79 Parameter Descriptions for the Socket 0, Device Hide Menu Screen	267
Table 3-80 Parameter Descriptions for the Advanced Power Management Configuration Screen.....	270
Table 3-81 Parameter Descriptions for the CPU P State Control Screen	273
Table 3-82 Parameter Descriptions for the Hardware PM State Control Screen ...	275
Table 3-83 Parameter Descriptions for the CPU C State Control Screen	277
Table 3-84 Parameter Descriptions for the Package C State Control Screen.....	279
Table 3-85 Parameter Descriptions for the CPU Thermal Management Screen ...	281
Table 3-86 Parameter Descriptions for the CPU-Advanced PM Tuning Screen	282
Table 3-87 Parameter Descriptions for the Energy Performance BIAS Screen.....	284
Table 3-88 Parameter Descriptions for the Package Current ConfigScreen	286
Table 3-89 Parameter Description for the Socket RAPL Config Screen.....	287
Table 3-90 Parameter Descriptions for the PMAX Detector Configuration Screen.....	289
Table 3-91 Parameter Descriptions for the ACPI Sx State Control Screen.....	290
Table 3-92 Parameter Descriptions for the Memory Power & Thermal Configuration Screen.....	290
Table 3-93 Parameter Descriptions for the Memory Thermal Screen.....	292
Table 3-94 Parameter Descriptions for the Memory Power Savings Advanced Options Screen	293
Table 3-95 Parameter Descriptions for the CKE Feature Screen	294
Table 3-96 Parameter Descriptions for the Self Refresh Feature Screen	295
Table 3-97 Parameter Descriptions for the Server Mgmt Screen.....	297
Table 3-98 Parameter Descriptions for the System Event Log Screen	300
Table 3-99 Parameter Descriptions for the BMC Network Configuration Screen.	307

Table 3-100 Parameter Descriptions for the BMC User Settings Screen.....	312
Table 3-101 Parameter Descriptions for the Add User Screen.....	314
Table 3-102 Parameter Descriptions for the Delete User Screen	315
Table 3-103 Parameter Descriptions for the Change User Settings Screen.....	316
Table 3-104 Parameter Descriptions for the Security Screen.....	318
Table 3-105 Parameter Descriptions for the HDD Security Configuration Screen.....	319
Table 3-106 Parameter Descriptions for the Secure Boot Screen	320
Table 3-107 Parameter Descriptions for the Key Management Screen.....	322
Table 3-108 Parameter Descriptions for the Secure Flash Update Screen.....	323
Table 3-109 Parameter Descriptions for the Boot Screen.....	325
Table 3-110 Parameter Descriptions for the Add New Boot Option Screen.....	330
Table 3-111 Parameter Descriptions for the Save & Exit Screen.....	336
Table 4-1 Descriptions of Control Keys.....	337

Glossary

AC

- Alternating Current

ACPI

- Advanced Configuration and Power Interface

ADDDC

- Adaptive Double Device Data Correction

ADR

- Automatic DIMM Refresh

AER

- Advanced Error Reporting

AHCI

- Advanced Host Controller Interface

ANSI

- American National Standards Institute

APIC

- Advanced Programmable Interrupt Controller

ASCII

- American Standard Code for Information Interchange

ASPM

- Active State Power Management

AVX

- Advanced Vector Extensions

BIOS

- Basic Input/Output System

BIST

- Built-In Self-Test

BMC

- Baseboard Management Controller

BSP

- Board Support Package

CD

- Compact Disk

CLR

- Cell Loss Ratio

CLTT

- Close Loop Thermal Throttling

CMCI

- Corrected Machine Check Interrupt

COM

- Component Object Model

CPU

- Central Processing Unit

CXL

- Compute Express Link

DAC

- Digital Analog Converter

DCU

- Data Collection Unit

DDR

- Double Data Rate

DFX

- Design for X

DHCP

- Dynamic Host Configuration Protocol

DIMM

- Dual Inline Memory Module

DMA

- Direct Memory Access

DMI

- Direct Media Interface

DRAM

- Dynamic Random Access Memory

DVD

- Digital Versatile Disc

ECC

- Error Check and Correction

eDPC

- Enhanced Downstream Port Containment

EET

- Energy Efficient Turbo

EFI

- Extensible Firmware Interface

EIST

- Enhanced Intel Speed Step Technology

eMCA

- Enhanced Machine Check Architecture

EPP

- Energy Performance Preference

FRU

- Field Replaceable Unit

HBA

- Host Bus Adapter

HDD

- Hard Disk Drive

HTTP

- Hypertext Transfer Protocol

I/O

- Input/Output

ID

- Identification

IIO

- Integrated I/O Module

IP

- Internet Protocol

IPMI

- Intelligent Platform Management Interface

IPv4

- Internet Protocol Version 4

IPv6

- Internet Protocol Version 6

iSAC

- Integrated Server Administrator Controller

KCS

- Keyboard Controller Style

LAN

- Local Area Network

LED

- Light Emitting Diode

LLC

- Logic Link Control

LMCE

- Local Machine Check Exception

LRDIMM

- Load Reduced Dual Inline Memory Module

MAC

- Media Access Control

MCA

- Machine Check Architecture

MCTP

- Management Component Transport Protocol

ME

- Management Engine

MSR

- Model-Specific Register

NIC

- Network Interface Card

NMI

- Non-Maskable Interrupt

NTB

- Non-Transparent Bridge

NUMA

- Non-Uniform Memory Access Architecture

NVDIMM

- Non-Volatile Dual In-Line Memory Module

NVMe

- Non-Volatile Memory Express

NVRAM

- Non-Volatile Random Access Memory

OCP

- Open Computer Project

OOB

- Out of Band

OS

- Operating System

PC

- Personal Computer

PCC

- Protection Communication Channel

PCH

- Platform Controller Hub

PCI

- Peripheral Component Interconnect

PCIe

- Peripheral Component Interconnect Express

PCLS

- Partial Cache Line Sparing

PECI

- Platform Environment Control Interface

PFD

- Packet Flow Description

PM

- Power Module

PM

- Power Management

PMC

- Power Management Controller

POST

- Power-On Self-Test

PPIN

- Protected Processor Identification Number

PXE

- Preboot eXecution Environment

RAID

- Redundant Array of Independent Disks

RAM

- Random Access Memory

RAPL

- Running Average Power Limit

RAS

- Reliability, Availability and Serviceability

RFO

- Read-For-Ownership

ROM

- Read-Only Memory

RTP

- Real-time Transport Protocol

SATA

- Serial ATA

SEL

- System Event Log

SGPIO

- Serial GPIO

SMI

- System Management Interruption

SOL

- Serial Over LAN

SPD

- Serial Presence Detect

SR-IOV

- Single-Root I/O Virtualization

TDP

- Thermal Design Power

TDR

- Transaction Detail Record

TLP

- Transaction Layer Packet

TPM

- Trusted Platform Module

TXEQ

- Transmit Equalizer

TXT

- Trusted Execution Technology

UCE

- UMA Creation Environment

UEFI

- Unified Extensible Firmware Interface

UMA

- Uniform Memory Access

UPI

- Ultra Path Interconnect

USB

- Universal Serial Bus

VC

- Virtual Channel

VGA

- Video Graphic Adapter

VLAN

- Virtual Local Area Network

VM

- Virtual Machine

VMD

- Volume Management Device

VMM

- Virtual Machine Monitor

VMX

- Virtual Machine Extension

WHEA

- Windows Hardware Error Architecture

XPT

- Xtended Prediciton Table