



NETAŞ Server

BIOS User Guide (Genoa)

Version: R1.0

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 2024 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 <http://support.NETAŞ.com.cn> 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
R1.0	2024-02-04	First edition.

Serial Number: SJ-20230907115354-010

Publishing Date: 2024-02-04 (R1.0)

Contents

1 BIOS Overview.....	1
1.1 Basic Concepts.....	1
1.2 Precautions.....	1
1.3 Applicable Server Models.....	2
Common Operations.....	3
2.1 Entering the BIOS.....	3
2.2 Setting the BIOS Language.....	5
2.3 Querying Server Configurations.....	6
2.4 Querying CPU Information.....	7
2.5 Querying Memory Information.....	9
2.6 Querying NIC Information.....	11
2.7 Querying Hard Disk Information.....	15
2.8 Setting the BIOS Time.....	17
2.9 Setting the Boot Mode.....	19
2.10 Setting the Boot Order.....	20
2.11 Setting the BIOS Password.....	22
2.12 Deleting a BIOS Password.....	24
2.13 Setting the Console Redirection Feature.....	26
2.14 Querying BMC Network Parameter Settings.....	28
2.15 Setting BMC Network Parameters.....	30
2.16 Setting the PXE Feature for a NIC.....	34
2.17 Setting Virtualization Parameters.....	35
2.18 Setting Memory Parameters.....	40
2.19 Setting Power Parameters.....	42
2.20 Restoring the Default BIOS Settings.....	48
Setup Parameter Descriptions.....	50
3.1 Main.....	50
3.2 Advanced.....	53
3.2.1 Mainboard Information.....	58
3.2.2 Trusted Computing.....	63
3.2.3 PSP Firmware Versions.....	65
3.2.4 ACPI Settings.....	67

3.2.5 Redfish Host Interface Settings.....	68
3.2.6 CRB Board.....	70
3.2.7 AMD CBS.....	71
3.2.8 UEFI Variables Protection.....	198
3.2.9 Serial Port Console Redirection.....	199
3.2.10 Debug Port Table Configuration.....	209
3.2.11 PCI Subsystem Settings.....	210
3.2.12 USB Configuration.....	216
3.2.13 Network Stack Configuration.....	220
3.2.14 CSM Configuration.....	222
3.2.15 NVMe Configuration.....	223
3.2.16 Offboard SATA Controller Configuration.....	224
3.2.17 SATA Configuration.....	225
3.2.18 CPU Configuration.....	226
3.2.19 PXE Configuration.....	228
3.2.20 AMD Mem Configuration Status.....	230
3.2.21 Tls Auth Configuration.....	235
3.2.22 RAM Disk Configuration.....	239
3.2.23 AMD PBS.....	242
3.2.24 Driver Health.....	249
3.2.25 Advanced Power Management Configuration.....	250
3.3 Chipset.....	251
3.3.1 South Bridge.....	252
3.3.2 North Bridge.....	260
3.4 Security.....	263
3.4.1 HDD Security Configuration.....	265
3.4.2 Secure Boot.....	267
3.4.3 Secure Flash Update.....	268
3.5 Boot.....	269
3.5.1 Add New Boot Option.....	274
3.5.2 Delete Boot Option.....	275
3.5.3 UEFI App Boot.....	275
3.6 Save & Exit.....	276
3.7 Firmware Update.....	278
3.8 Event Logs.....	278

3.8.1 Change Smbios Event Log Settings.....	279
3.8.2 View Smbios Event Log.....	282
3.9 Server Mgmt.....	283
3.9.1 System Event Log.....	288
3.9.2 FRU Information.....	289
3.9.3 BMB Self Test Log.....	292
3.9.4 BMC network configuration.....	293
3.9.5 BMC User Settings.....	298
4 Reference: Control Keys for BIOS Setup.....	303
Glossary.....	304

About This Manual

Purpose

This manual describes the common operations and parameters of the [BIOS](#) of the Genoa 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 and appendixes.

Chapter 1, BIOS Overview	Describes the basic BIOS concepts, 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.

	Danger: indicates an imminently hazardous situation. Failure to comply will result in death or serious personal injury.
	Warning: indicates a potentially hazardous situation. Failure to comply can result in death or serious personal injury.
	Caution: indicates a potentially hazardous situation. Failure to comply can result in moderate or minor personal injury.

	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.
	Note: provides additional information about a topic.

Chapter 1

BIOS Overview

Table of Contents

Basic Concepts.....1

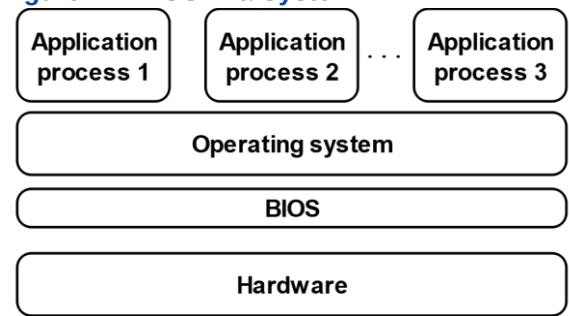
Precautions.....1

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 manual applies to NETAŞ NCS6722A N4 rack servers developed based on the **Genoa** platform.

Chapter 2

Common Operations

Table of Contents

Entering the BIOS.....	3
Setting the BIOS Language.....	5
Querying Server Configurations.....	6
Querying CPU Information.....	7
Querying Memory Information.....	9
Querying NIC Information.....	11
Querying Hard Disk Information.....	15
Setting the BIOS Time.....	17
Setting the Boot Mode.....	19
Setting the Boot Order.....	20
Setting the BIOS Password.....	22
Deleting a BIOS Password.....	24
Setting the Console Redirection Feature.....	26
Querying BMC Network Parameter Settings.....	28
Setting BMC Network Parameters.....	30
Setting the PXE Feature for a NIC.....	34
Setting Virtualization Parameters.....	35
Setting Memory Parameters.....	40
Setting Power Parameters.....	42
Restoring the Default BIOS Settings.....	48

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](#) (for BMC V4).

2. Power on the server. The server starts and the [POST](#) is performed. The NETAŞ logo is displayed on the screen, as shown in [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](#).

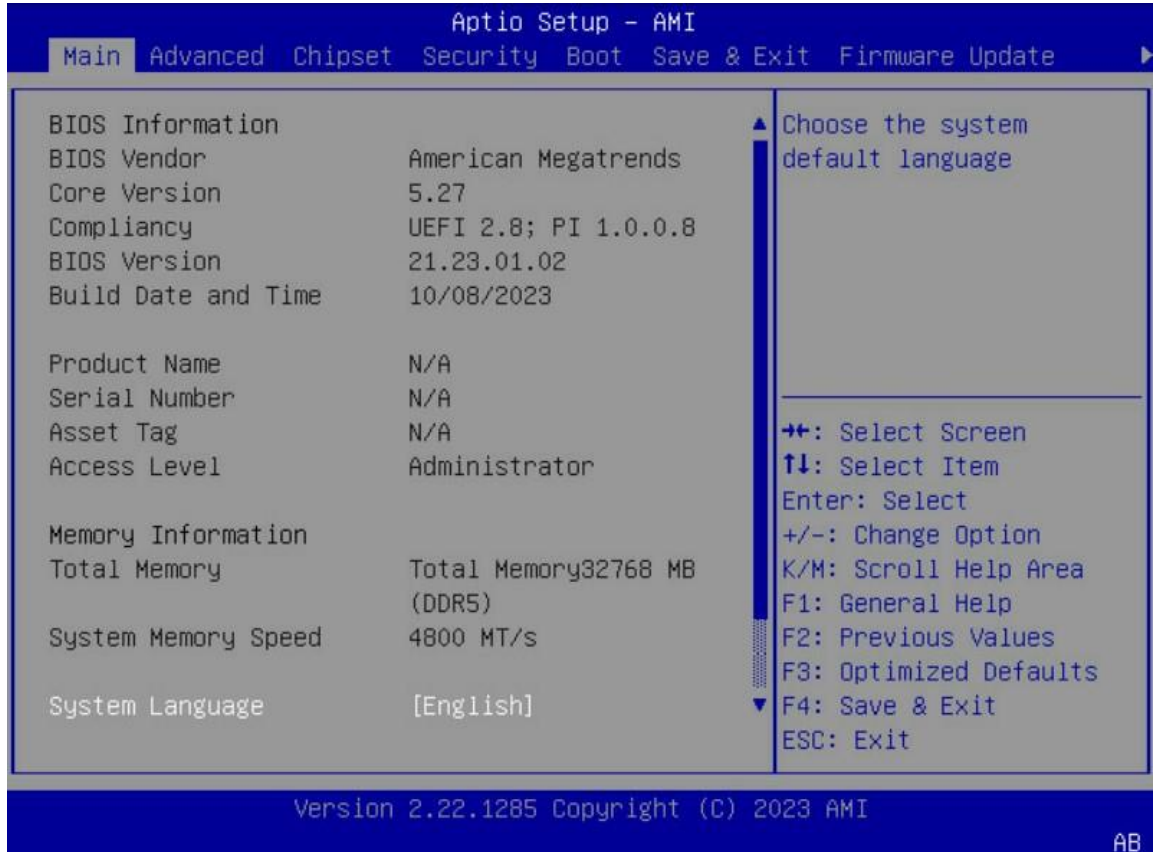
Table 2-1 Descriptions of Hot Keys for BIOS Startup

Hot Key	Description
F2/DEL	Press the key to enter the Aptio Setup screen.
F11	Press the key to enter the boot manager.
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.
Enter the Aptio Setup screen	Press F1 or DEL . The Aptio Setup screen is displayed, as shown in Figure 2-2 .

Figure 2-2 Setup Screen



Note

- For a description of the parameters on 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](#).

1.2 Setting the BIOS Language

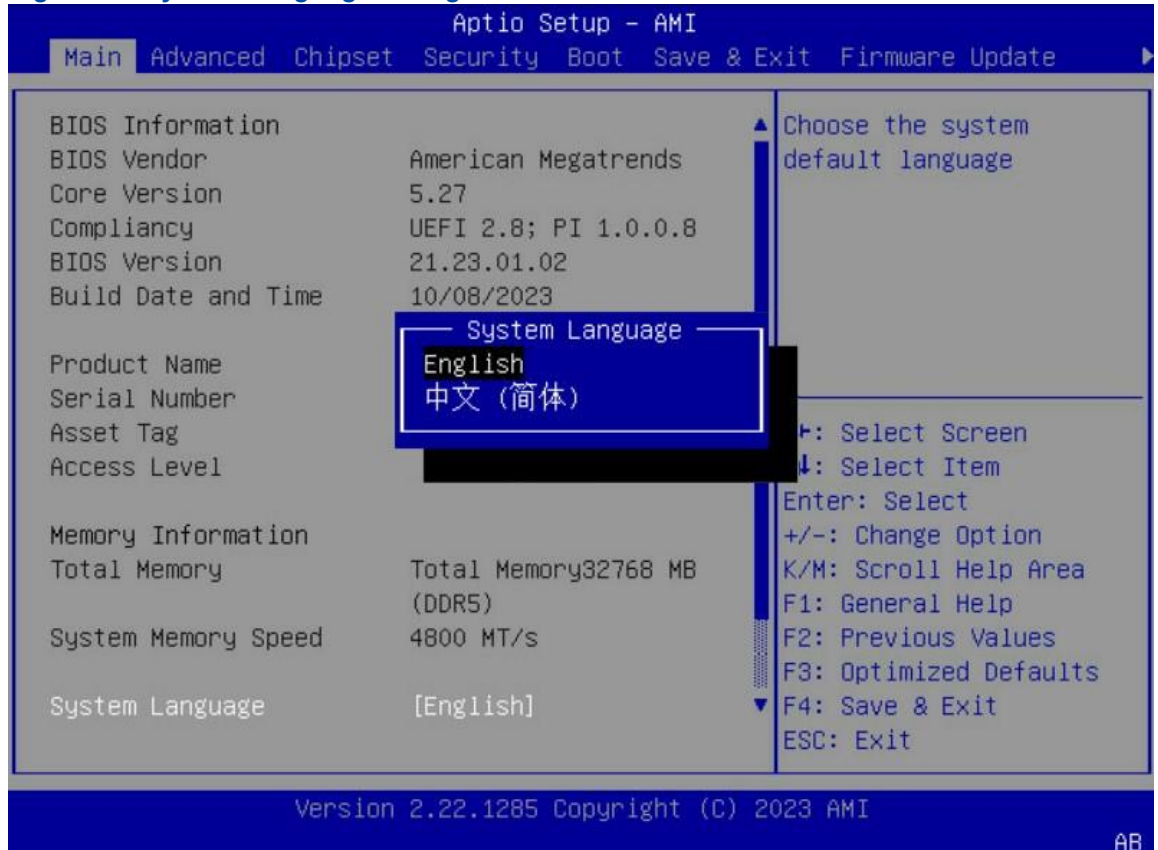
Abstract

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** and then press **Enter**. The **System Language** dialog box is displayed, as shown in [Figure 2-3](#).

Figure 2-3 System Language Dialog Box



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

2.3 Querying Server Configurations

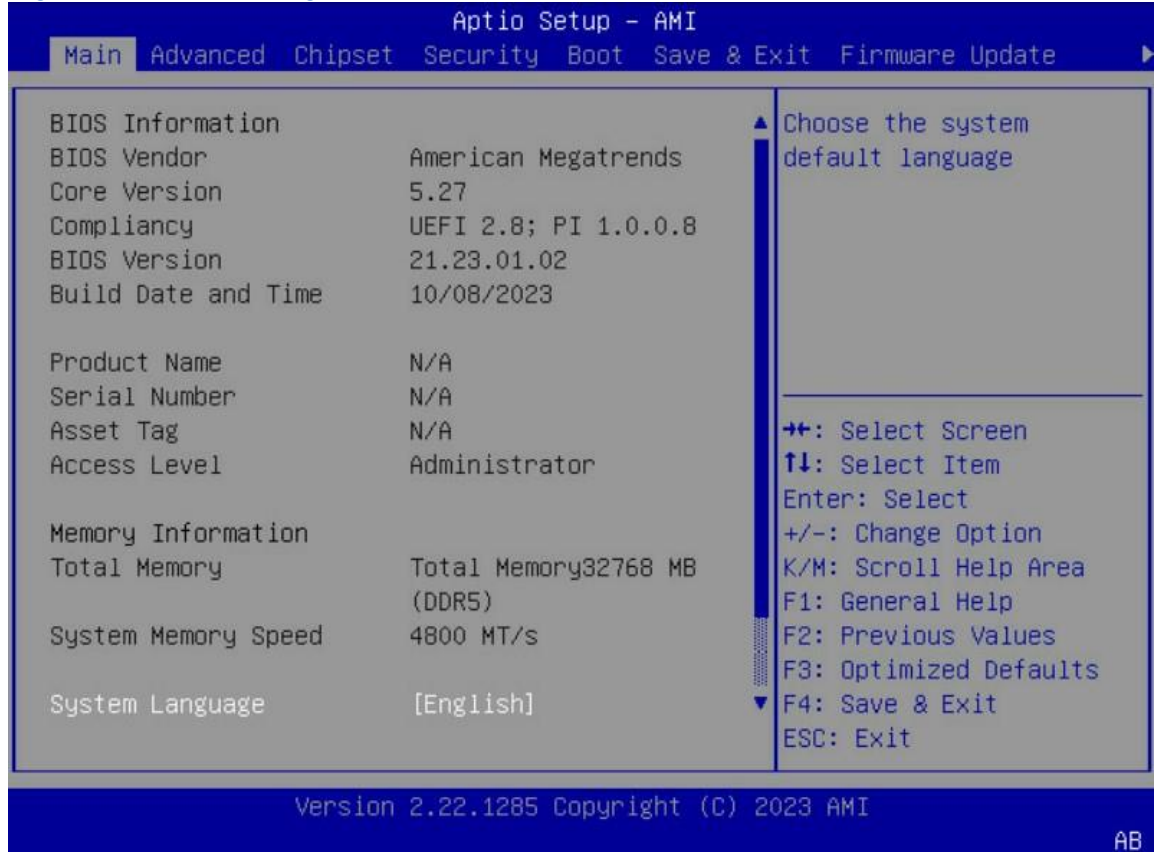
Abstract

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, as shown in [Figure 2-4](#).

Figure 2-4 Server Configuration Information



2.4 Querying CPU Information

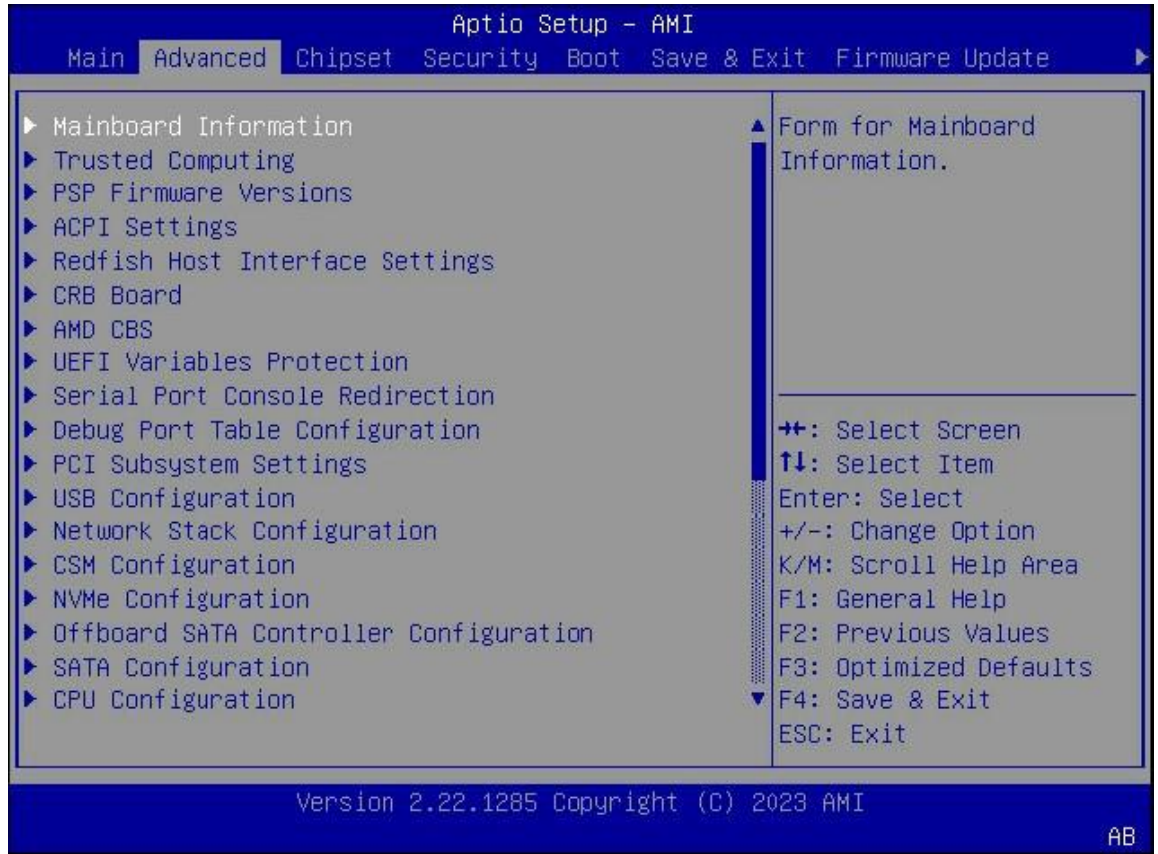
Abstract

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

Steps

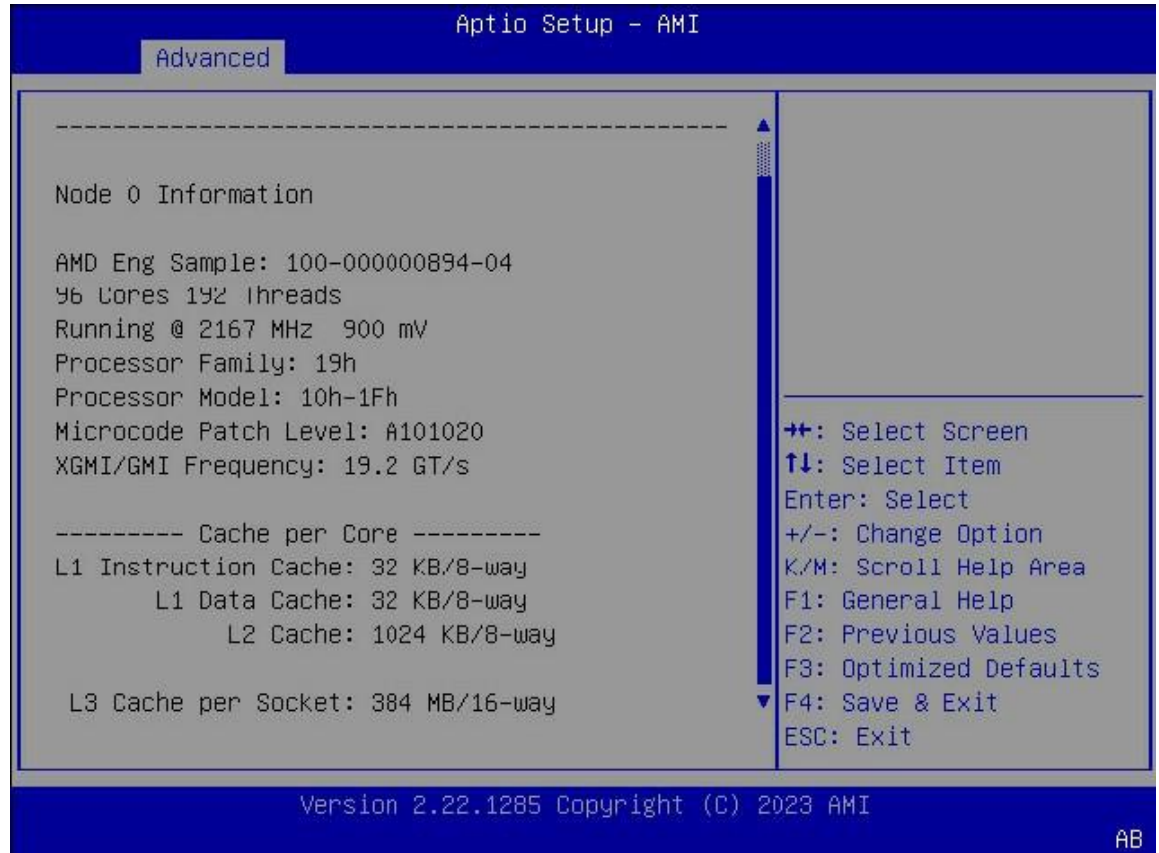
1. On the **Aptio Setup** screen, select **Advanced**. The **Advanced** screen is displayed, as shown in [Figure 2-5](#).

Figure 2-5 Advanced Screen



2. Select **CPU Configuration > Node 0 Information** and press **Enter**. The CPU information is displayed, as shown in [Figure 2-6](#).

Figure 2-6 CPU Information

**Note**

The parameters on the **Node 1 Information** screen are the same as those on the **Node 0 Information** screen. This procedure uses the **Node 0 Information** screen as an example.

2.5 Querying Memory Information

Abstract

This procedure describes how to query memory parameter settings.

Steps

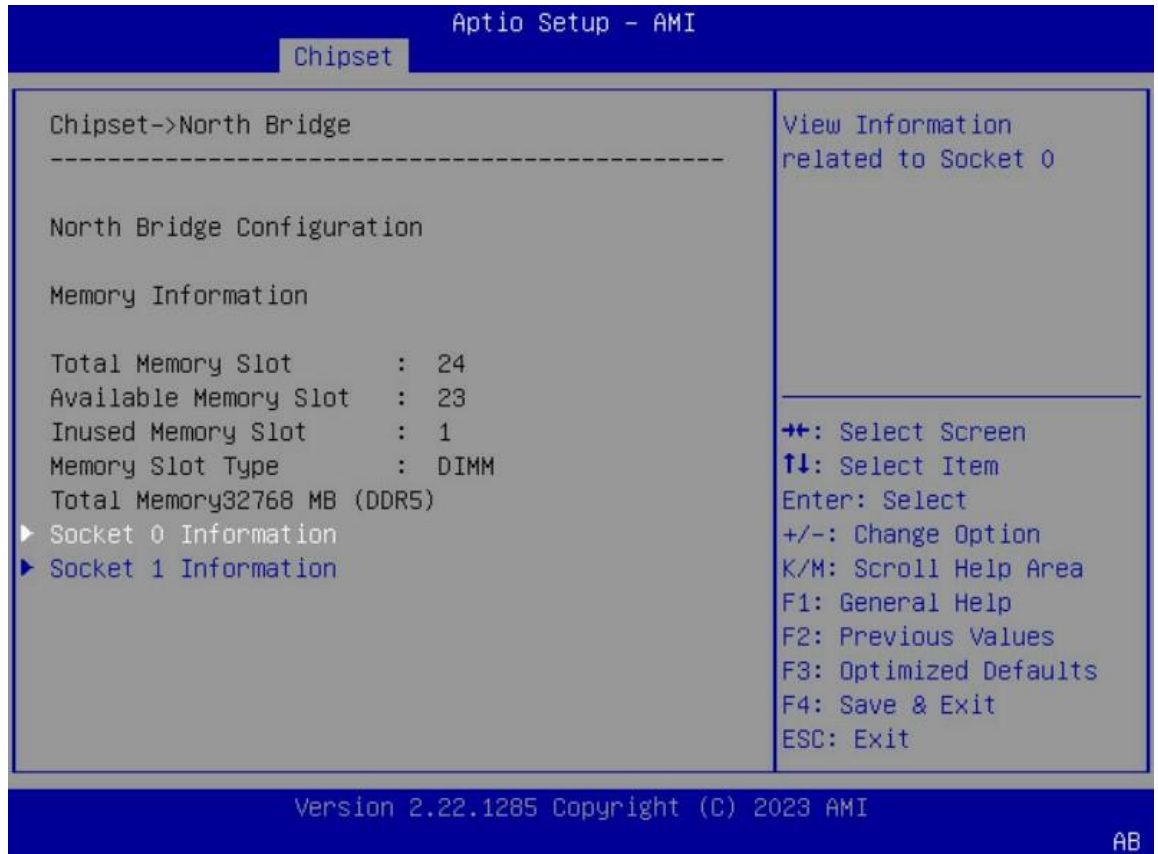
1. On the **Aptio Setup** screen, select the **Chipset** menu. The **Chipset** screen is displayed, as shown in [Figure 2-7](#).

Figure 2-7 Chipset Screen



2. Select **North Bridge**, and press the **Enter** key. The memory information is displayed, as shown in [Figure 2-8](#).

Figure 2-8 Memory Information



2.6 Querying NIC Information

Abstract

This procedure describes how to query [NIC](#) configuration information, such as the [MAC](#) address and NIC details.

Prerequisite

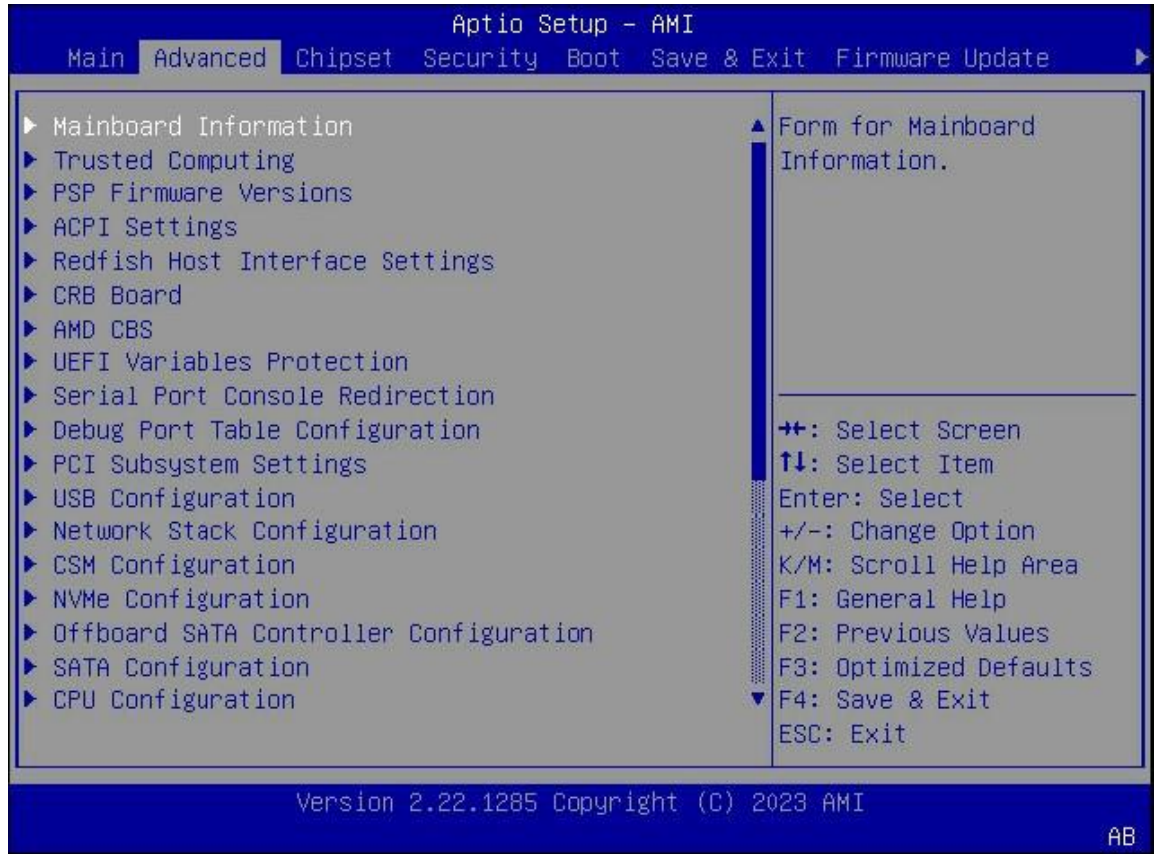
The boot mode is already set to [UEFI](#) in the BIOS. For details, refer to "[2.9 Setting the Boot Mode](#)".

Steps

Querying Port Numbers and MAC Addresses

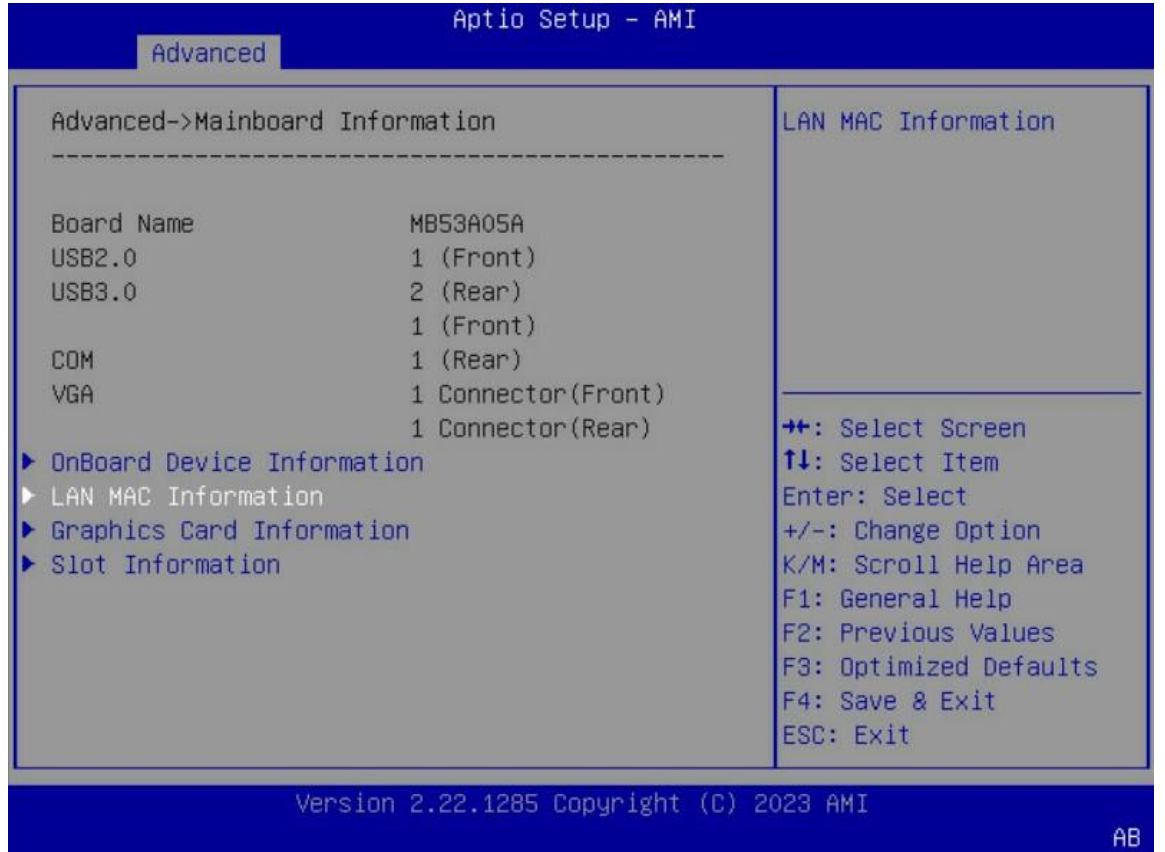
1. On the **Aptio Setup** screen, select **Advanced**. The **Advanced** screen is displayed, as shown in [Figure 2-9](#).

Figure 2-9 Advanced Screen



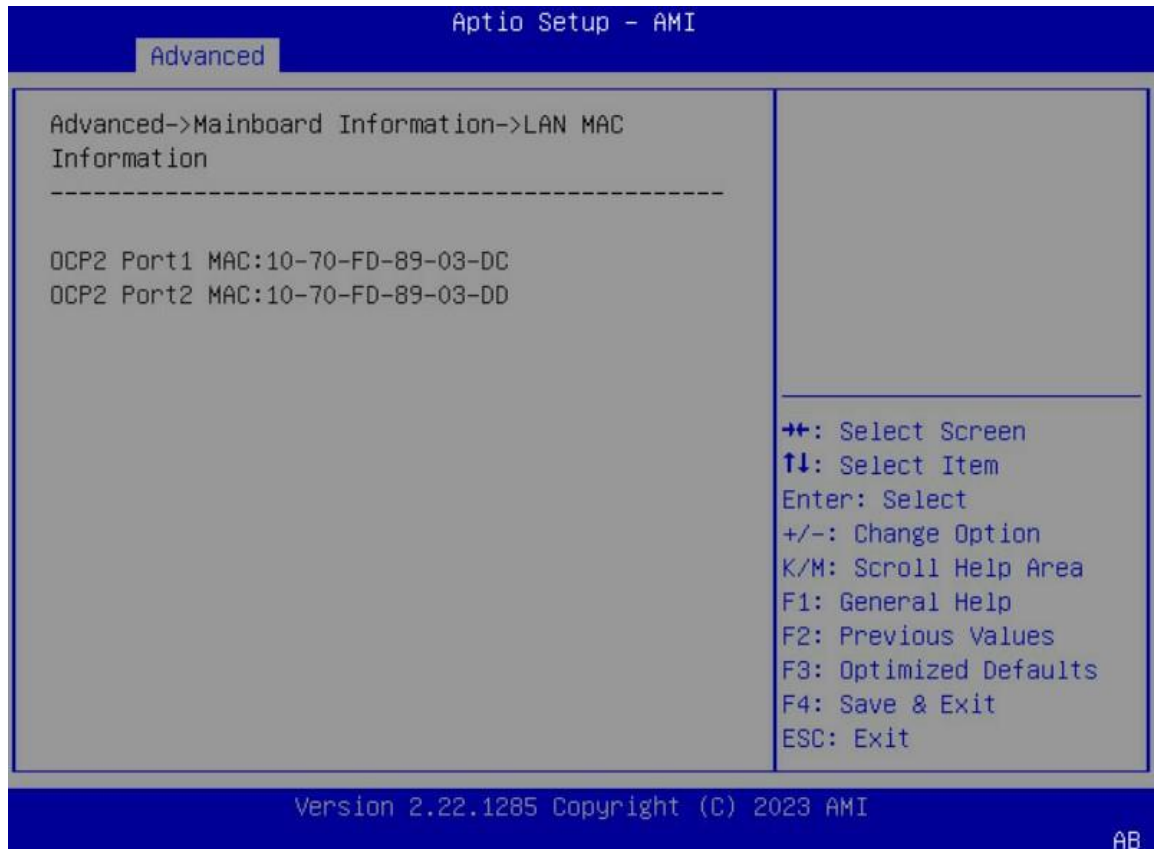
2. Select **Mainboard Information**, and then press **Enter**. The **Mainboard Information** screen is displayed, as shown in [Figure 2-10](#).

Figure 2-10 Mainboard Information Screen



3. Select **LAN MAC Information**, and then press **Enter**. The **LAN MAC Information** screen is displayed, as shown in [Figure 2-11](#).

Figure 2-11 LAN MAC Information Screen



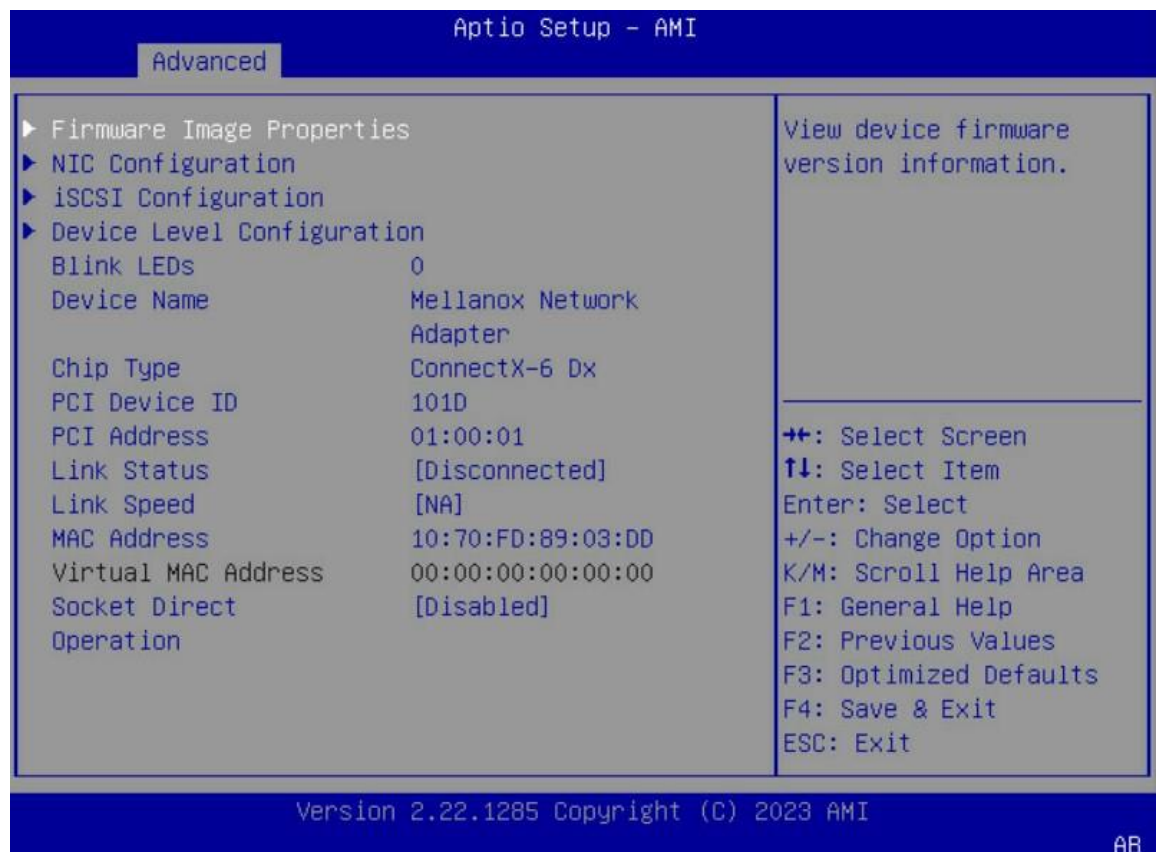
4. Press **Esc** twice to return to the **Advanced** screen.

Querying the Details of a NIC

5. Select a NIC, for example, **Mellanox Network Adapter - 10:. 70: FD: 89: 03: DD**. Press **Enter**.

The detailed information about the NIC is displayed, as shown in [Figure 2-12](#).

Figure 2-12 Detailed NIC Information



2.7 Querying Hard Disk Information

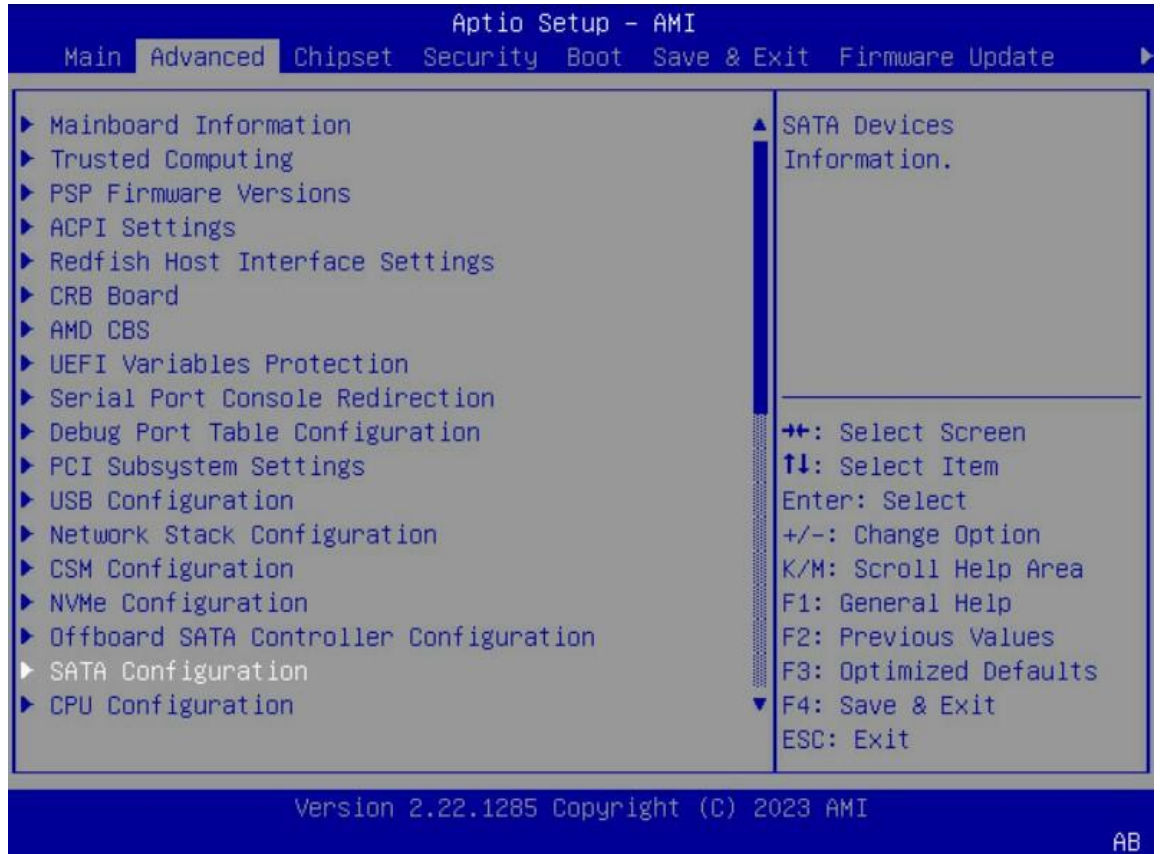
Abstract

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

Steps

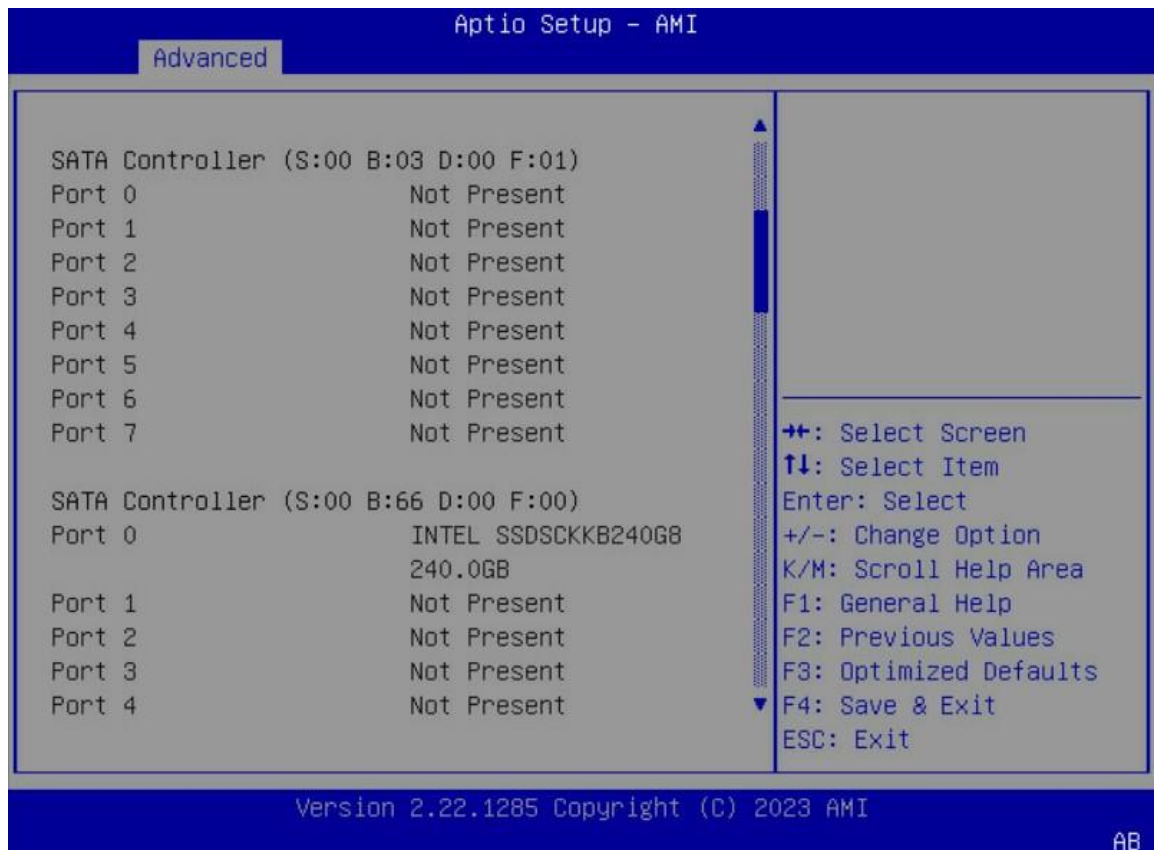
1. On the **Aptio Setup** screen, select **Advanced**. The **Advanced** screen is displayed, as shown in [Figure 2-13](#).

Figure 2-13 Advanced Screen



2. Select **SATA Configuration** and press **Enter**. The hard disk information is displayed, as shown in [Figure 2-14](#).

Figure 2-14 Hard Disk Information Screen



2.8 Setting the BIOS Time

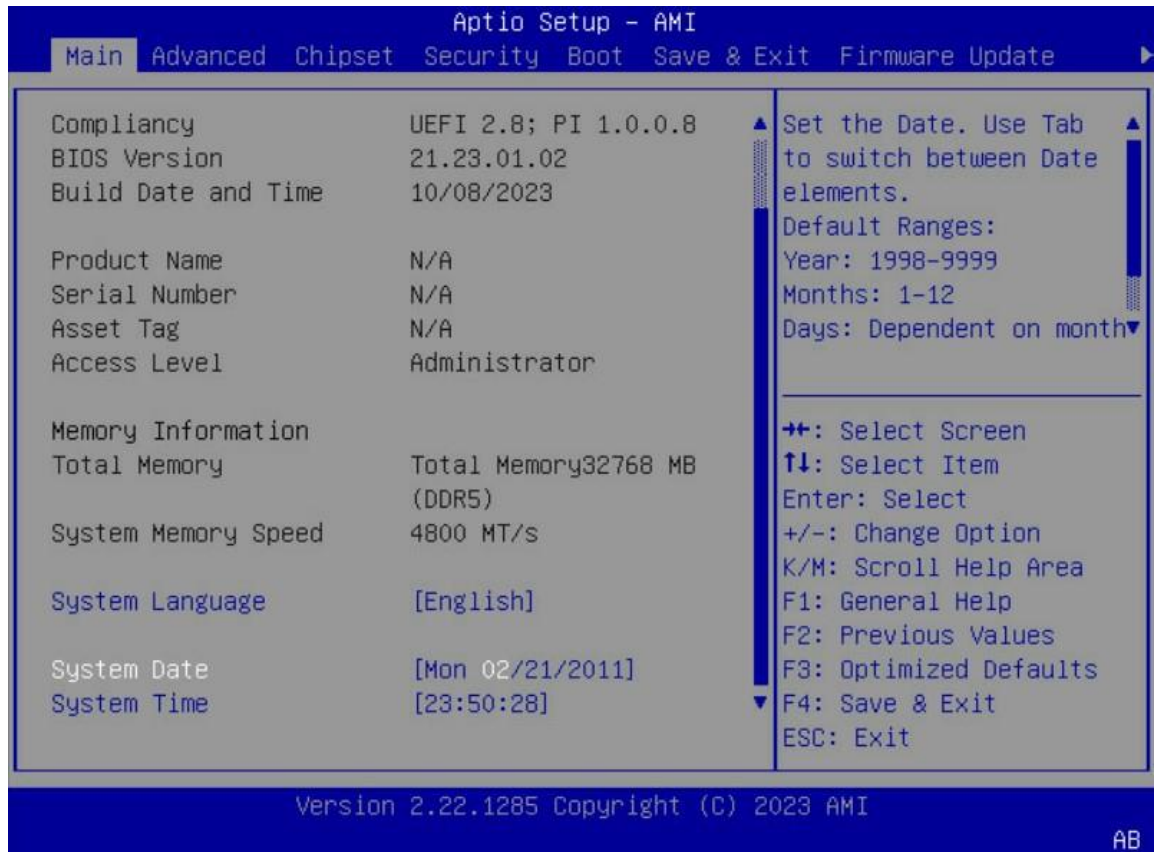
Abstract

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 then press **Enter** to move the cursor to the date, as shown in [Figure 2-15](#).

Figure 2-15 Setting the Date



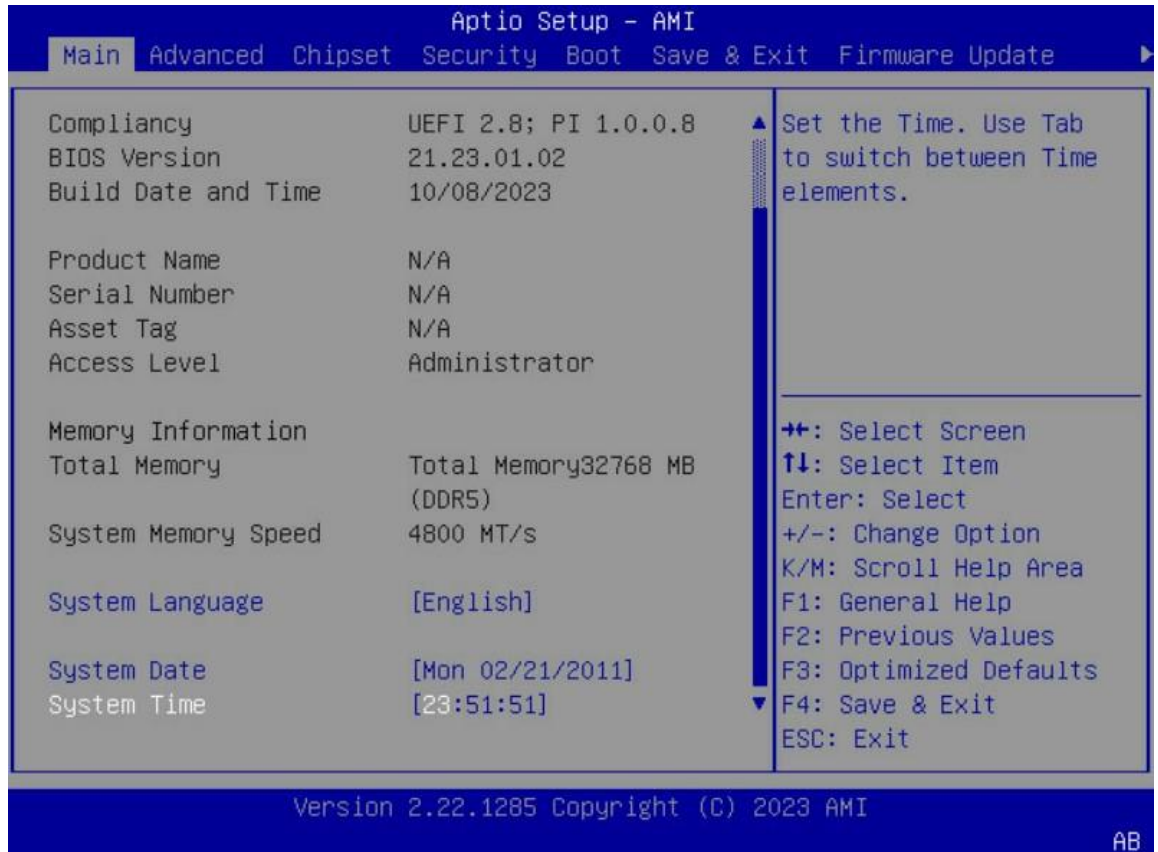
3. Set the date.

The date is displayed in MM/DD/YYYY format. Press **Enter** or **Tab** to switch between the month, day, and year 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 then press **Enter** to move the cursor to the time, as shown in [Figure 2-16](#).

Figure 2-16 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 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**.

2.9 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, as shown in [Figure 2-17](#).

Figure 2-17 Boot Option Filter Dialog Box



3. Select **Legacy only** or **UEFI only** and then press **Enter**.



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**.

2.10 Setting the Boot Order

Abstract

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

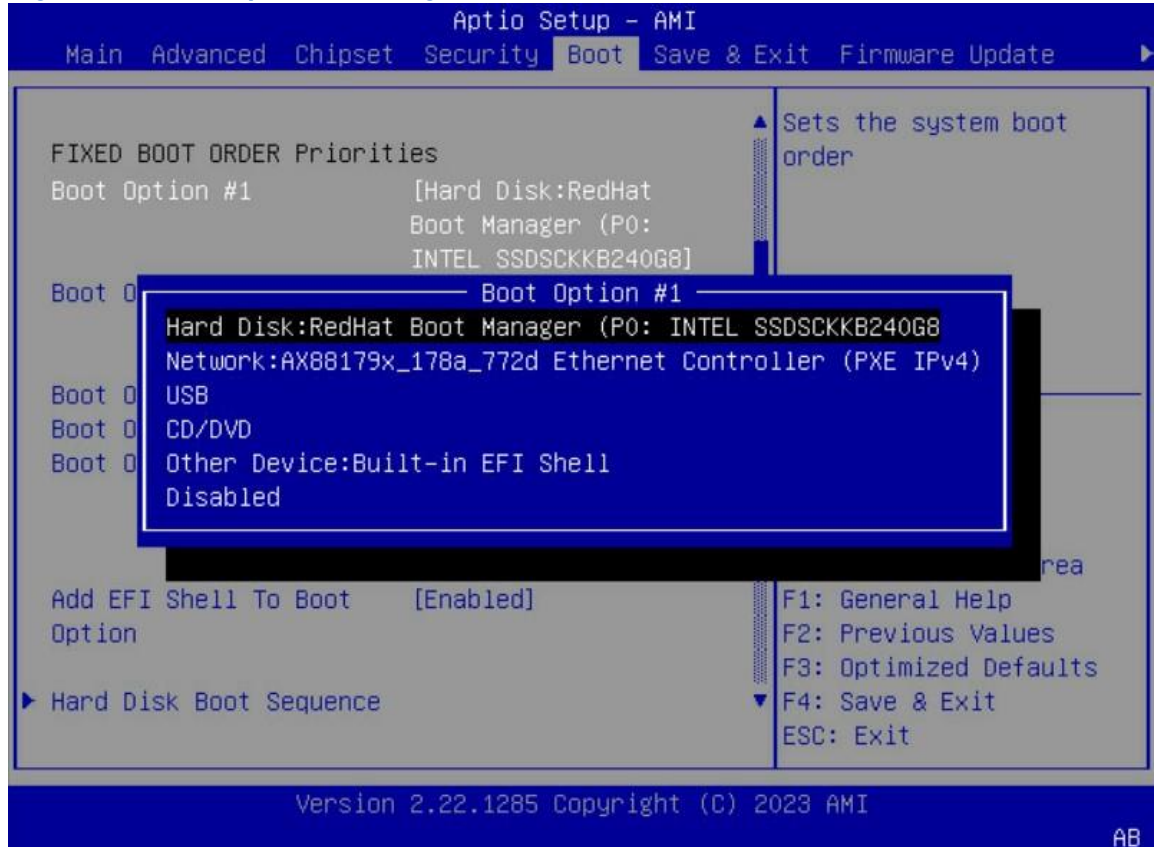
1. Hard disk
2. Network
3. [USB](#)
4. CD/DVD drive
5. Other devices

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 then press **Enter**. The **Boot Option #1** dialog box is displayed, as shown in [Figure 2-18](#).

Figure 2-18 Boot Option #1 Dialog Box



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

Table 2-2 Boot Device Descriptions

Boot Device	Description
Hard Disk	Boots the OS from a hard disk.
Network	Boots the OS from a network device.
USB	Boots the OS from a USB device.
CD/DVD	Boots the OS from a CD/DVD-ROM drive.
Other Device	Boots the OS from other devices.
Disabled	Disables this option.

3. Select a device that will serve as the first boot device and then press **Enter**.
4. (Optional) Adjust the priority of other boot devices by referring to [Step 2](#) and [Step 3](#).
5. Press **F4**. In the displayed dialog box, select **Yes**.

2.11 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. The set BIOS passwords cannot be cleared forcibly.



Note

This procedure describes how to set the administrator password. You can set 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 then press **Enter**. The **Create New Password** dialog box is displayed, as shown in [Figure 2-19](#).

Figure 2-19 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 operations:

1. On the **Security** screen, select **Administrator Password** and then press **Enter**. The **Enter Current Password** dialog box is displayed, as shown in [Figure 2-20](#).

Figure 2-20 Enter Current Password Dialog Box



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

**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**.

2.12 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. Without the correct password, deletion is not permitted. 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, as shown in [Figure 2-21](#).

Figure 2-21 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, as shown in [Figure 2-22](#).

Figure 2-22 WARNING Dialog Box



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

2.13 Setting the Console Redirection Feature

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 **Advanced**. The **Advanced** screen is displayed, as shown in [Figure 2-23](#).

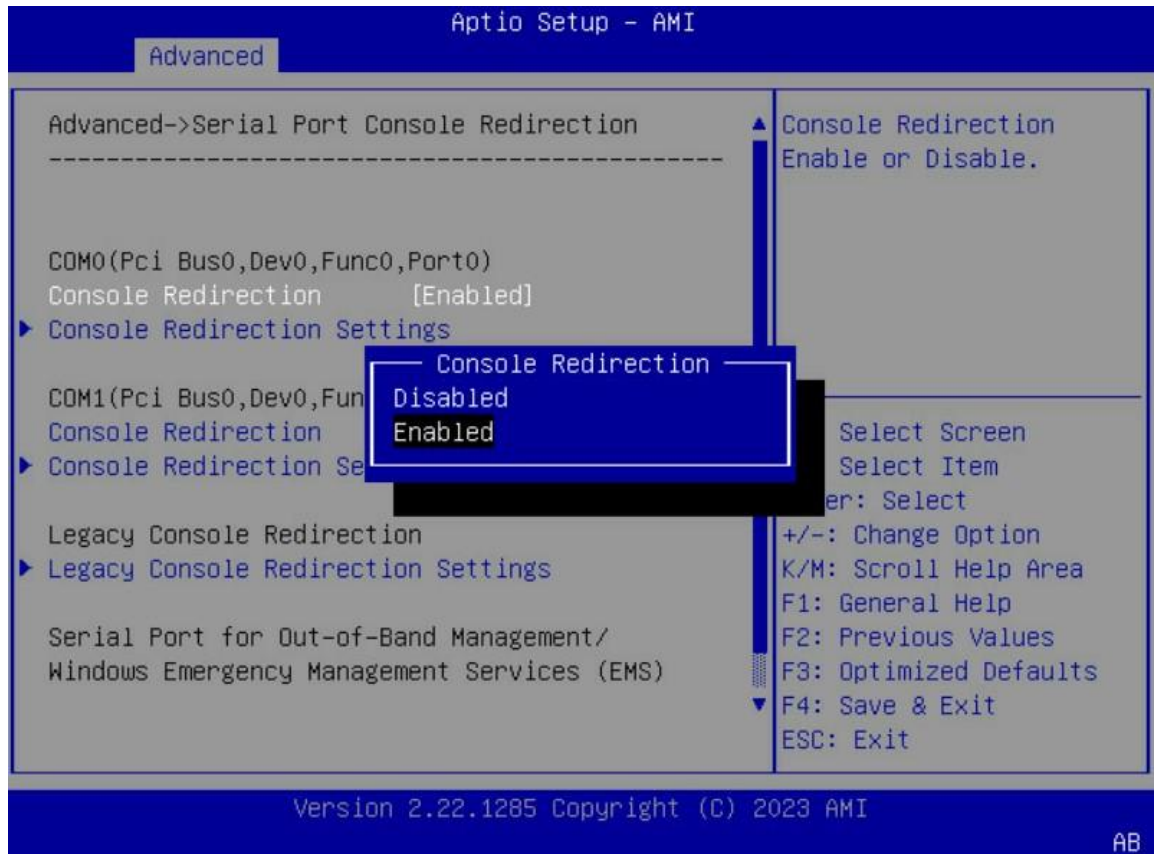
Figure 2-23 Advanced Screen



2. Select **Serial Port Console Redirection > Console Redirection** and then press **Enter**.

The **Console Redirection** dialog box is displayed, as shown in [Figure 2-24](#).

Figure 2-24 Console Redirection Dialog Box



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

2.14 Querying BMC Network Parameter Settings

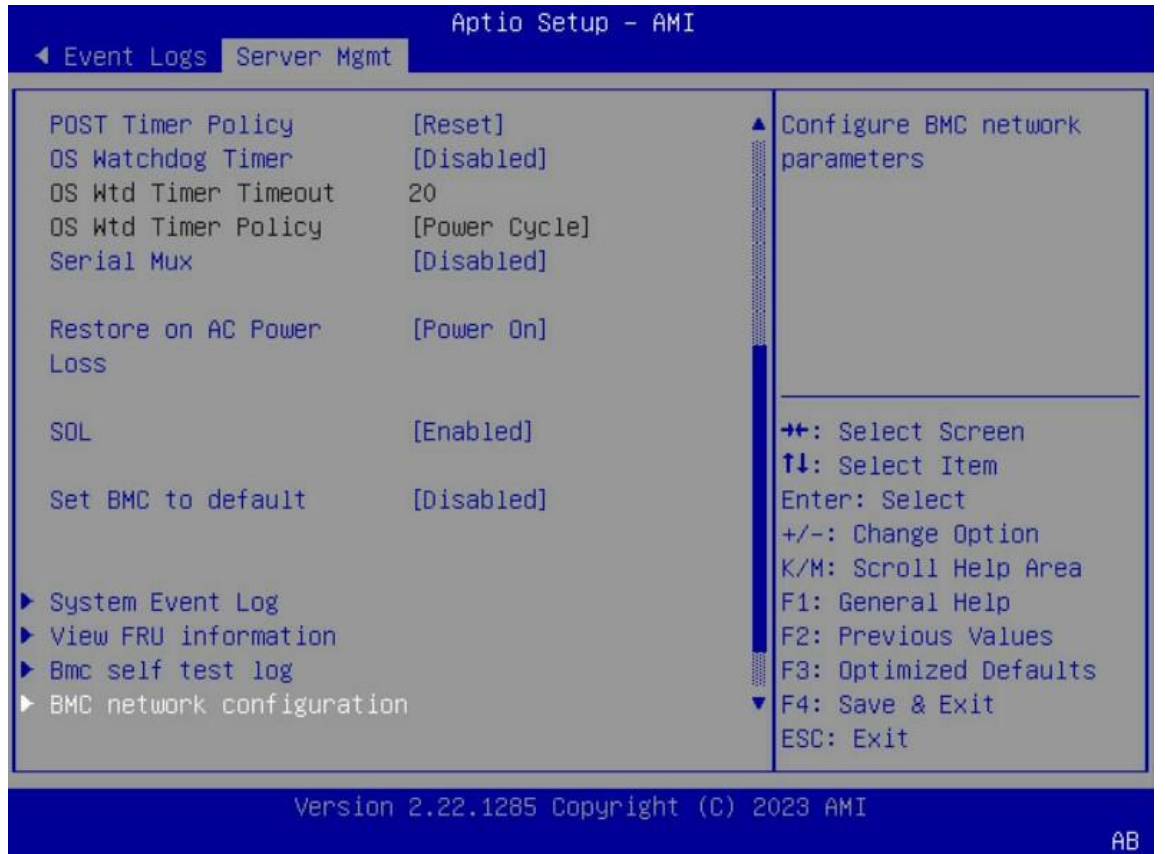
Abstract

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

Steps

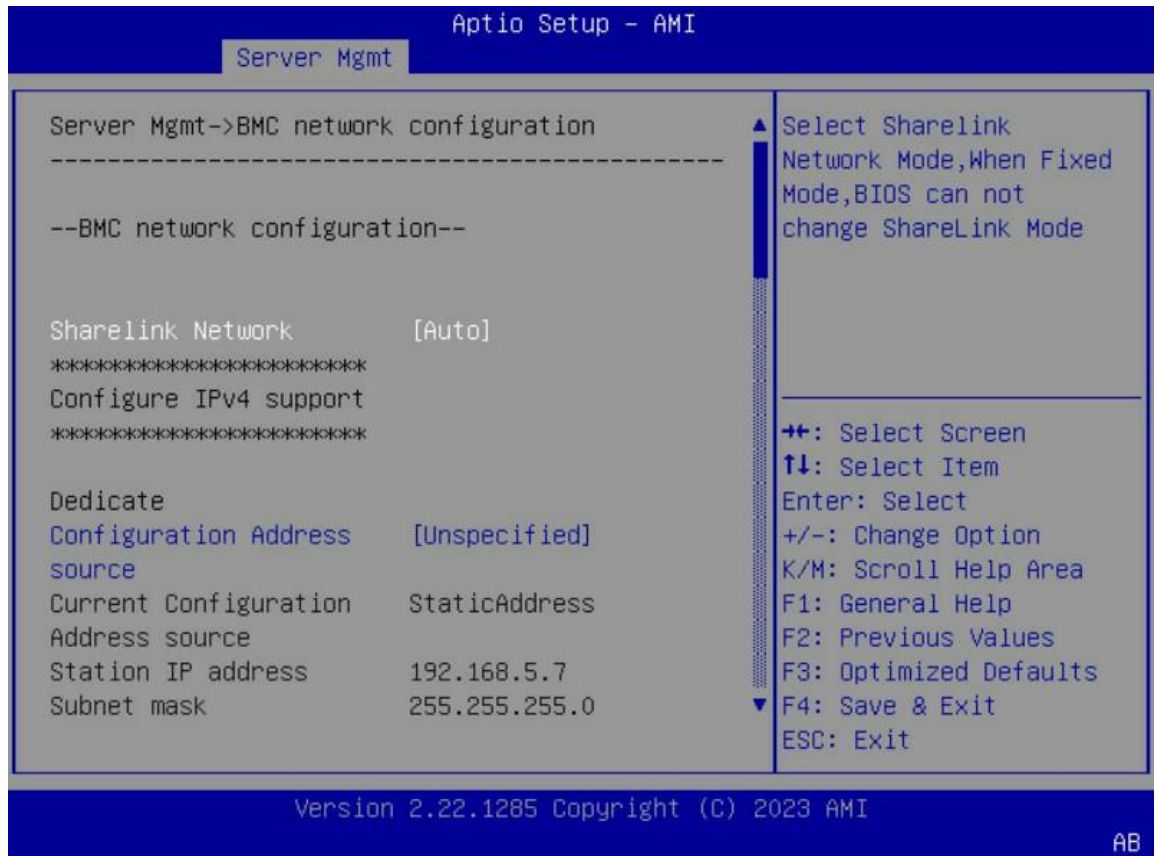
1. On the **Aptio Setup** screen, select the **Server Mgmt** menu. The **Server Mgmt** screen is displayed, as shown in [Figure 2-25](#).

Figure 2-25 Server Mgmt Screen



2. Select **BMC network configuration** and then press **Enter**. The **BMC network configuration** screen is displayed, as shown in [Figure 2-26](#).

Figure 2-26 BMC Network Configuration Screen



2.15 Setting BMC Network Parameters

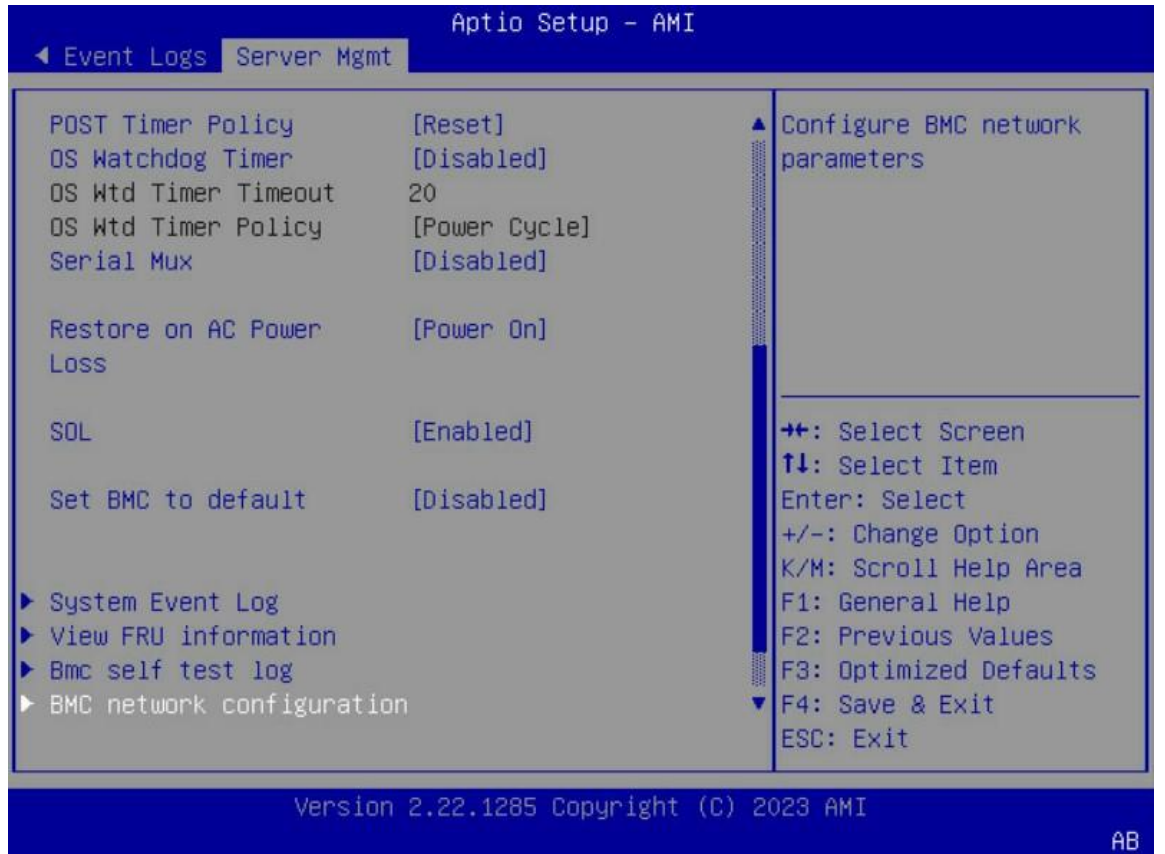
Abstract

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

Steps

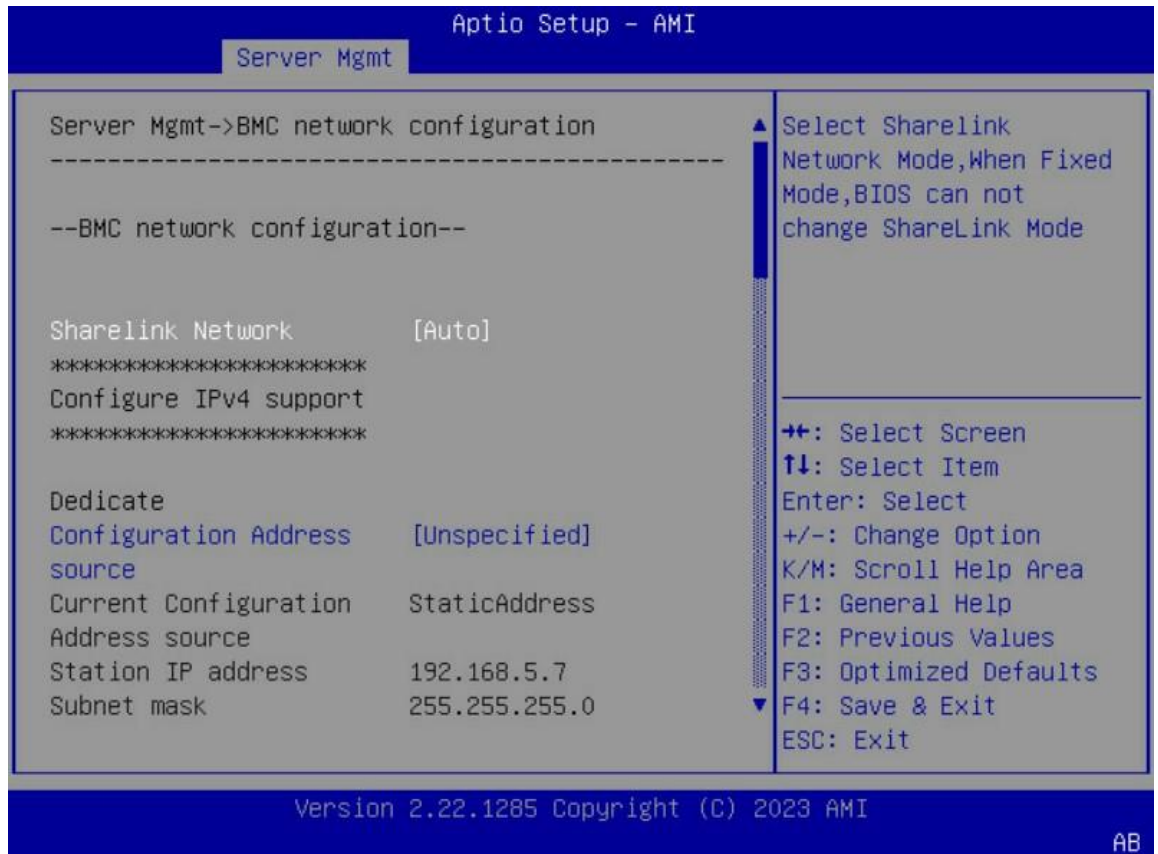
1. On the **Aptio Setup** screen, select the **Server Mgmt** menu. The **Server Mgmt** screen is displayed, as shown in [Figure 2-27](#).

Figure 2-27 Server Mgmt Screen



2. Select **BMC network configuration** and then press **Enter**. The **BMC network configuration** screen is displayed, as shown in [Figure 2-28](#).

Figure 2-28 BMC Network Configuration Screen



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

Table 2-3 Parameter Descriptions for the BMC Network Configuration Screen

Parameter	Description
Sharelink Network	Enables or disables the shared network port feature. Options: ● Auto. ● Enable: enables the shared network port feature. ● Disabled: disables the shared network port feature.
Configure IPv4 support	
Configuration Address source	Sets the configuration mode of the IPv4 address of the dedicated network port. Options: ● Unspecified: undefined. ● Static: static mode, in which the IP address is manually set. ● DynamicBmcDhcp: The IP address is dynamically obtained through BMC DHCP.

Parameter	Description
	● DynamicBmcNonDhcp: The IP address is dynamically obtained through the BMC.
Configure IPv6 support	
IPv6 Support	Sets whether the dedicated network port supports IPv6. Options: ● Enable: IPv6 is supported. When Enable is selected, the IPv6 parameters below Configure IPv6 support can be configured. ● Disabled: IPv6 is not supported. When Disabled is selected, the IPv6 parameters below Configure IPv6 support cannot be configured.
Configuration Address source	Sets the configuration mode of the IPv6 address of the dedicated network port. Options: ● Unspecified: undefined. ● Static: static mode, in which the IP address is manually set. ● DynamicBmcDhcp: The IP address is dynamically obtained through BMC DHCP.
Configuration Router Lan1 Address source	Sets the gateway LAN1 address type. Options: ● Unspecified ● Static ● DynamicBmcDhcp
Configure VLAN support	
VLAN Support	Sets whether the shared network port supports VLAN. ● Enabled: VLAN is supported. When Enabled is selected, the VLAN parameters below can be configured. ● Disabled: VLAN is not supported. When Disabled is selected, the VLAN parameters below are hidden. ● Unspecified: undefined. When Unspecified is selected, the VLAN parameters below cannot be configured.

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

2.16 Setting the PXE Feature for a NIC

Abstract

To control a server over the network, you need to enable the **PXE** feature for a **NIC** in the server.



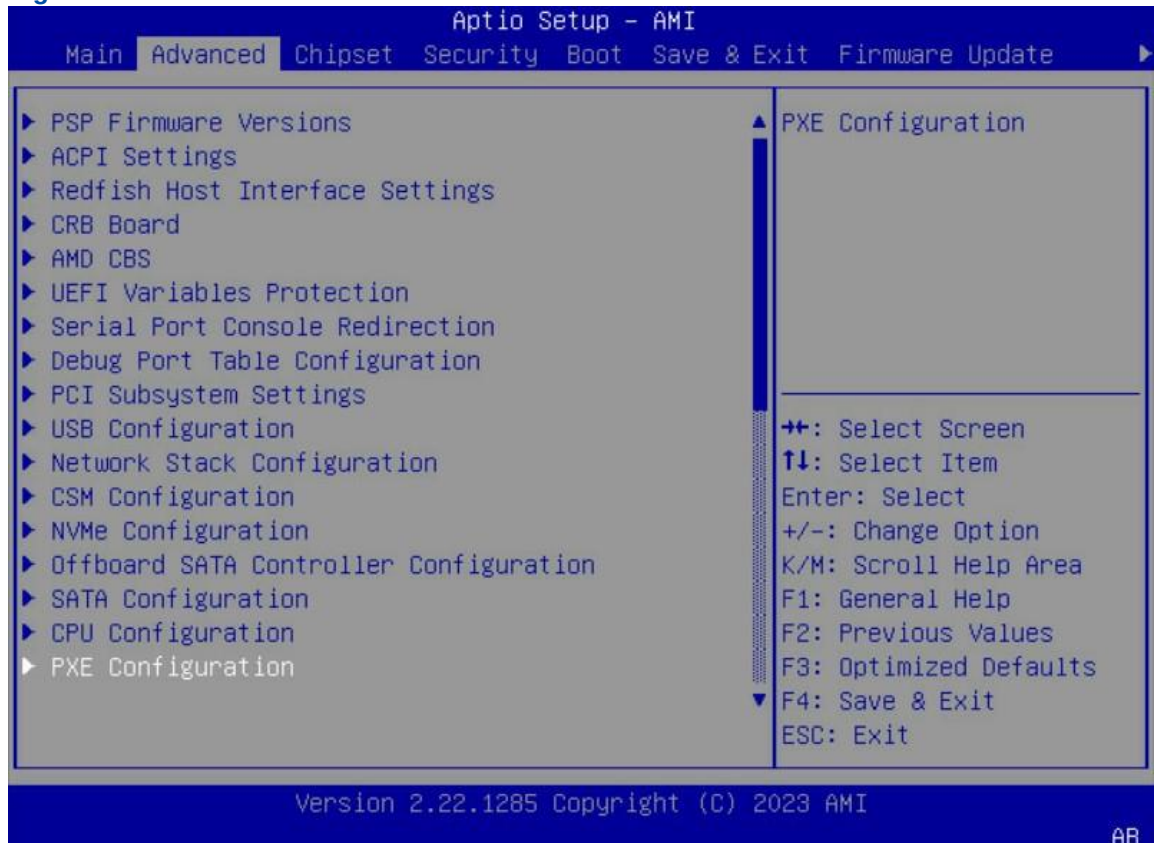
Note

PXE is a protocol designed by Intel. It enables computers to boot through the network. Operating in Client/Server mode, PXE allows the client to download the boot image from the remote server through the network and load the installation file or the entire operating system.

Steps

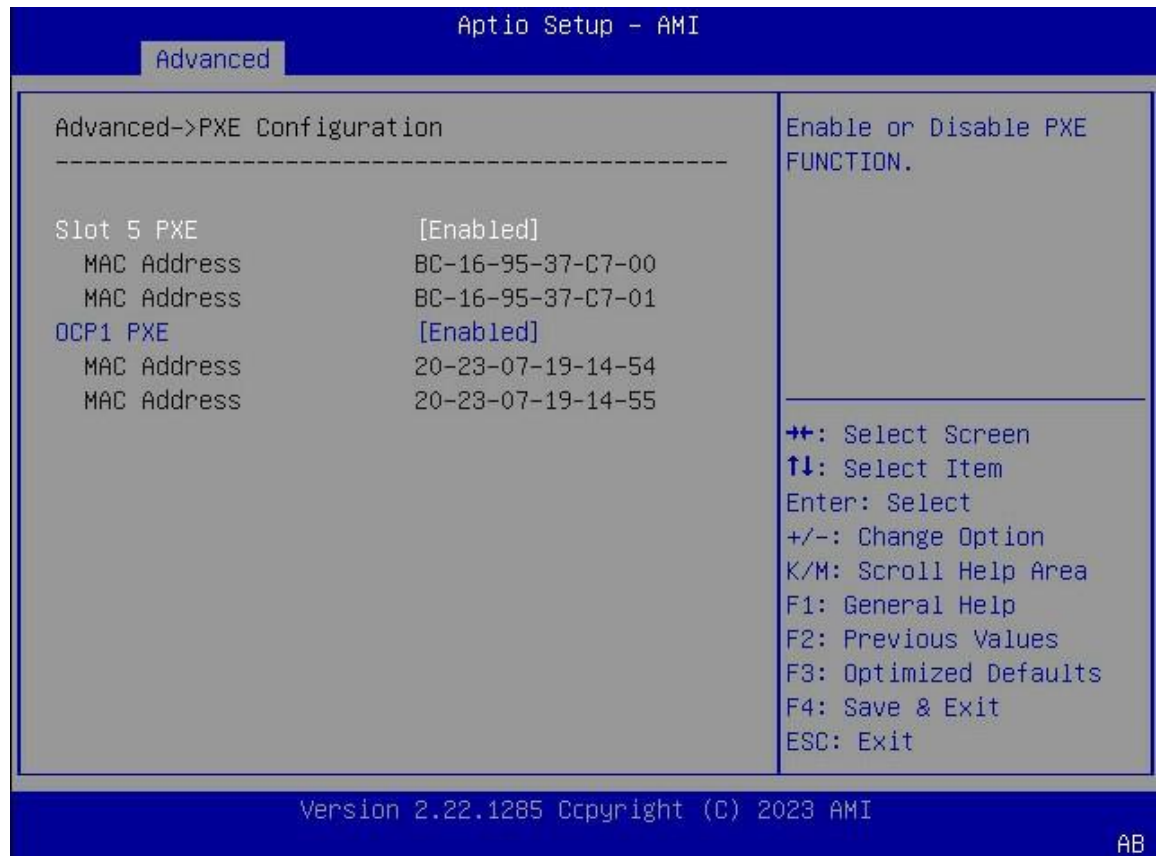
1. On the Aptio Setup screen, select **Advanced**. The **Advanced** screen is displayed, as shown in [Figure 2-29](#).

Figure 2-29 Advanced Screen



2. Select **PXE Configuration**, and then press **Enter**. The **PXE Configuration** screen is displayed, as shown in [Figure 2-30](#).

Figure 2-30 PXE Configuration Screen

**Note**

The **PXE Configuration** screen only displays the current 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 feature on the NIC.
4. Press **F4**. In the displayed dialog box, select **Yes**.

2.17 Setting Virtualization Parameters

Abstract

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

Context

For a description of common virtualization parameters, refer to [Table 2-4](#).

Table 2-4 Common Virtualization Parameter Descriptions

Parameter	Description	Recommended Configuration
IOMMU	Enables or disables the IOMMU feature. When the IOMMU feature is enabled, addressing in the virtual memory is allowed for a system device, that is, the virtual memory is mapped to a physical memory address.	Enabled
SVM Mode	Enables or disables CPU virtualization. After CPU virtualization 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	Enables or disables the SR-IOV feature. After the SR-IOV feature is enabled, a physical I/O device (typically a network adapter) can be virtualized into multiple I/O devices for separate use by multiple VMs. This reduces the CPU load of the host and network latency, improving network performance.	Enabled

Steps**Configuring IOMMU**

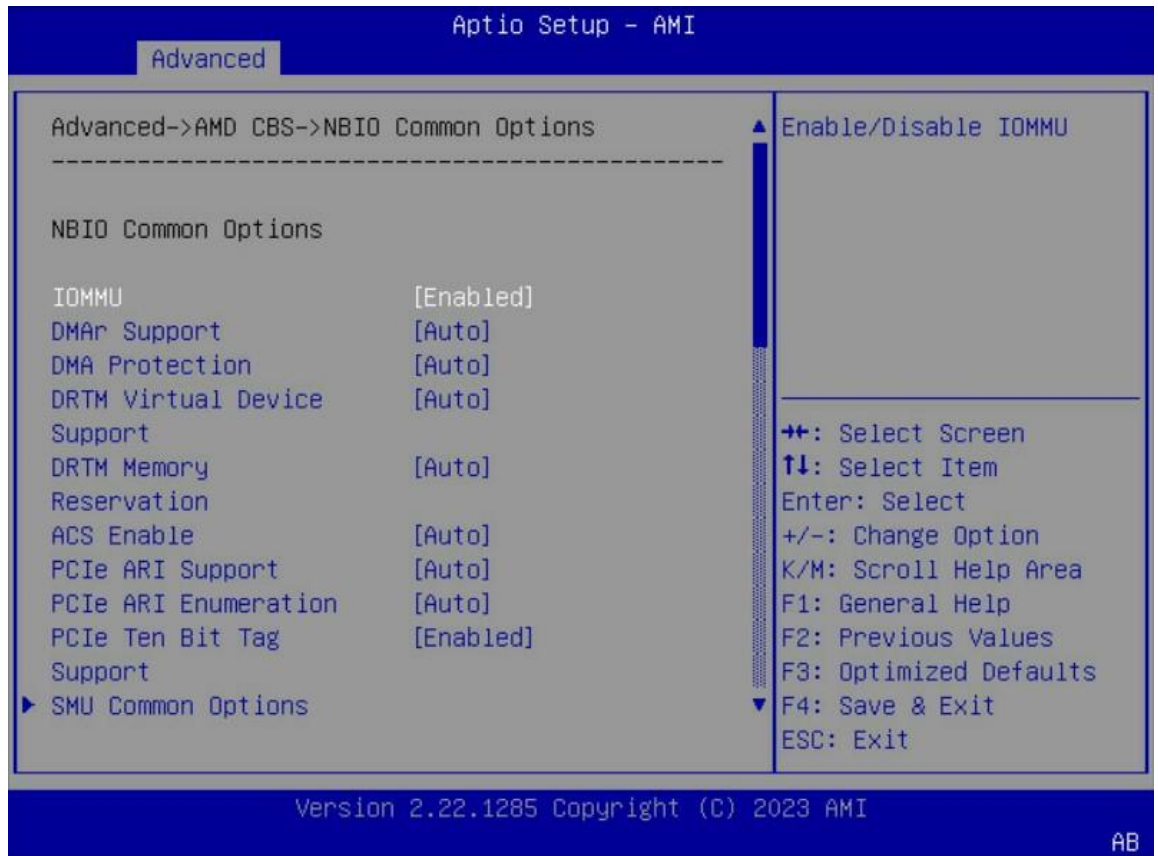
1. On the Aptio Setup screen, select **Advanced**. The **Advanced** screen is displayed, as shown in [Figure 2-31](#).

Figure 2-31 Advanced Screen



2. Select **AMD CBS > NBIO Common Options** and then press **Enter**. The **NBIO Common Options** information is displayed, as shown in [Figure 2-32](#).

Figure 2-32 Advanced Screen—NBIO Common Options

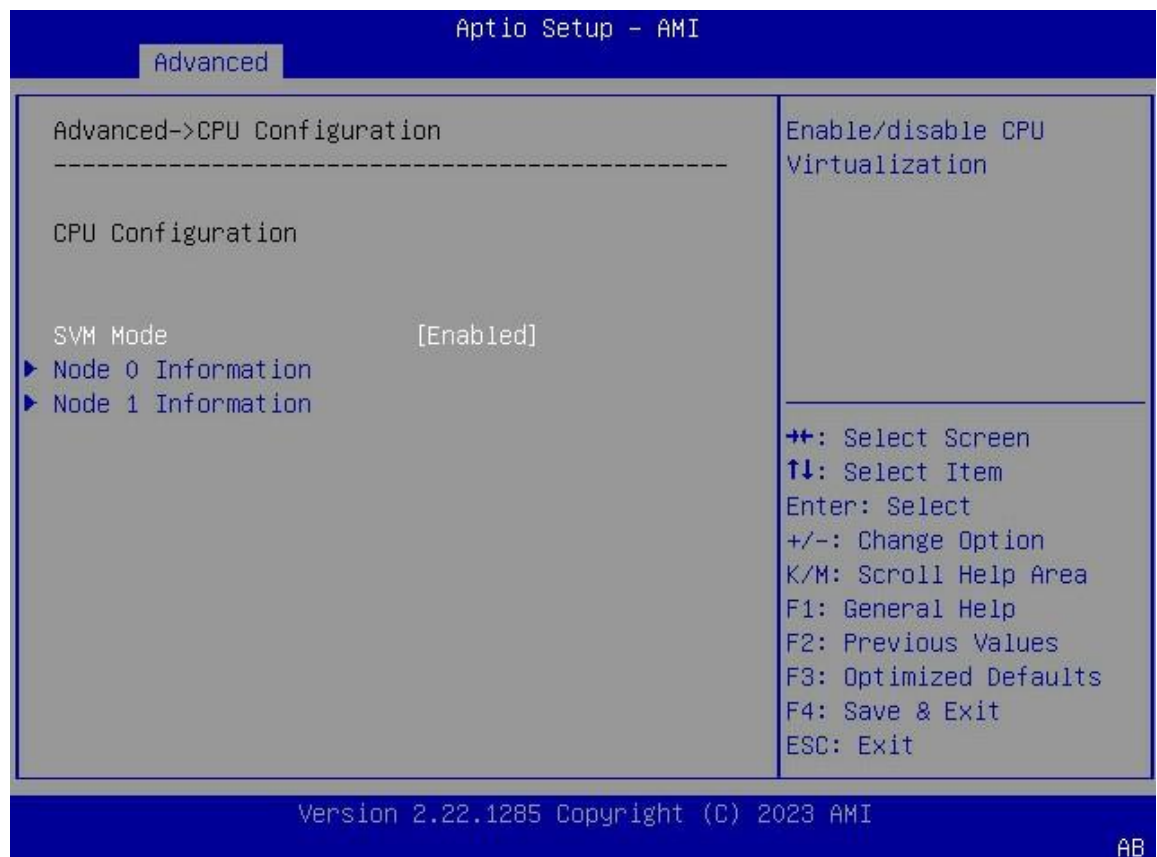


3. Select **IOMMU** and then press **Enter**. In the displayed dialog box, select **Enabled** to enable the IOMMU feature.

Configuring SVM Mode

4. On the **Advanced** screen, select **CPU Configuration** and then press **Enter**. The **CPU Configuration** screen is displayed, as shown in [Figure 2-33](#).

Figure 2-33 CPU Configuration Screen

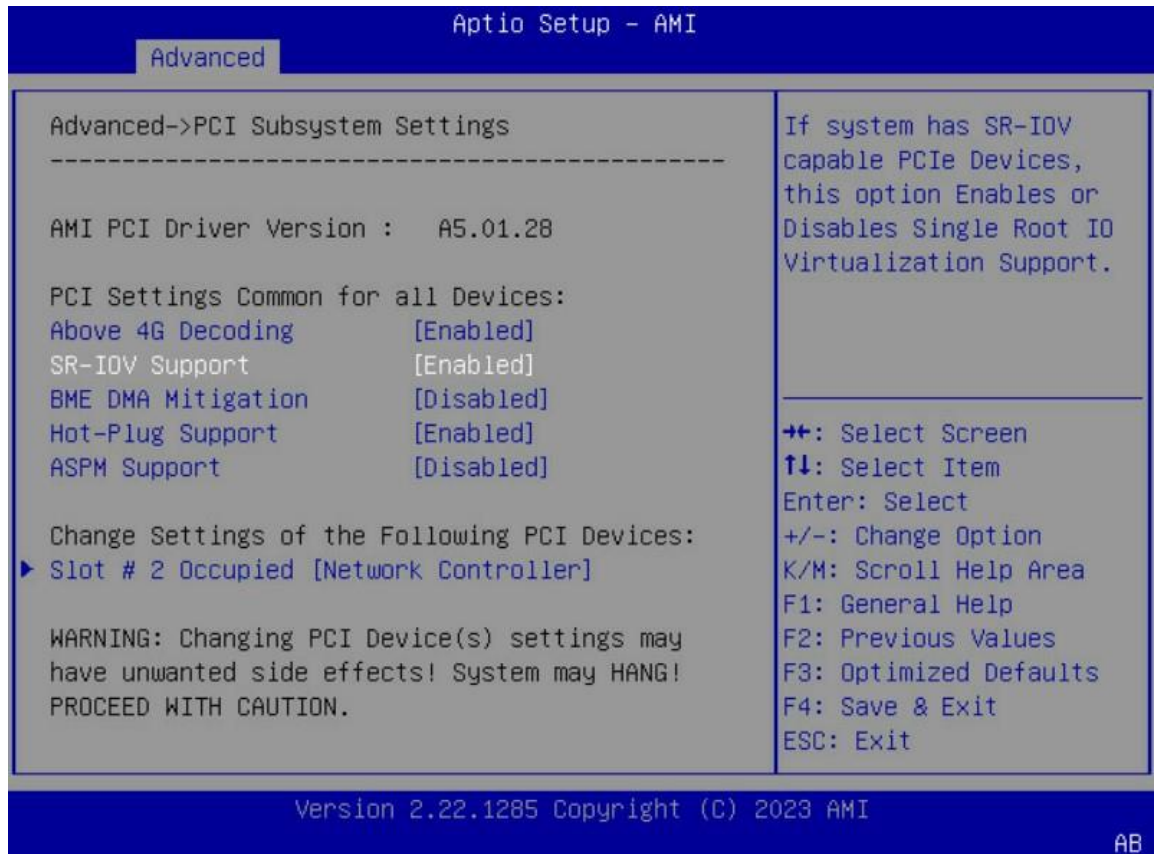


5. Select **SVM Mode** and then press **Enter**. In the displayed dialog box, select **Enabled** to enable the CPU virtualization feature.

Configuring SR-IOV Support

6. On the **Advanced** screen, select **PCI Subsystem Settings** and then press **Enter**. The **PCI Subsystem Settings** screen is displayed, as shown in [Figure 2-34](#).

Figure 2-34 PCI Subsystem Settings Screen



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

2.18 Setting Memory Parameters

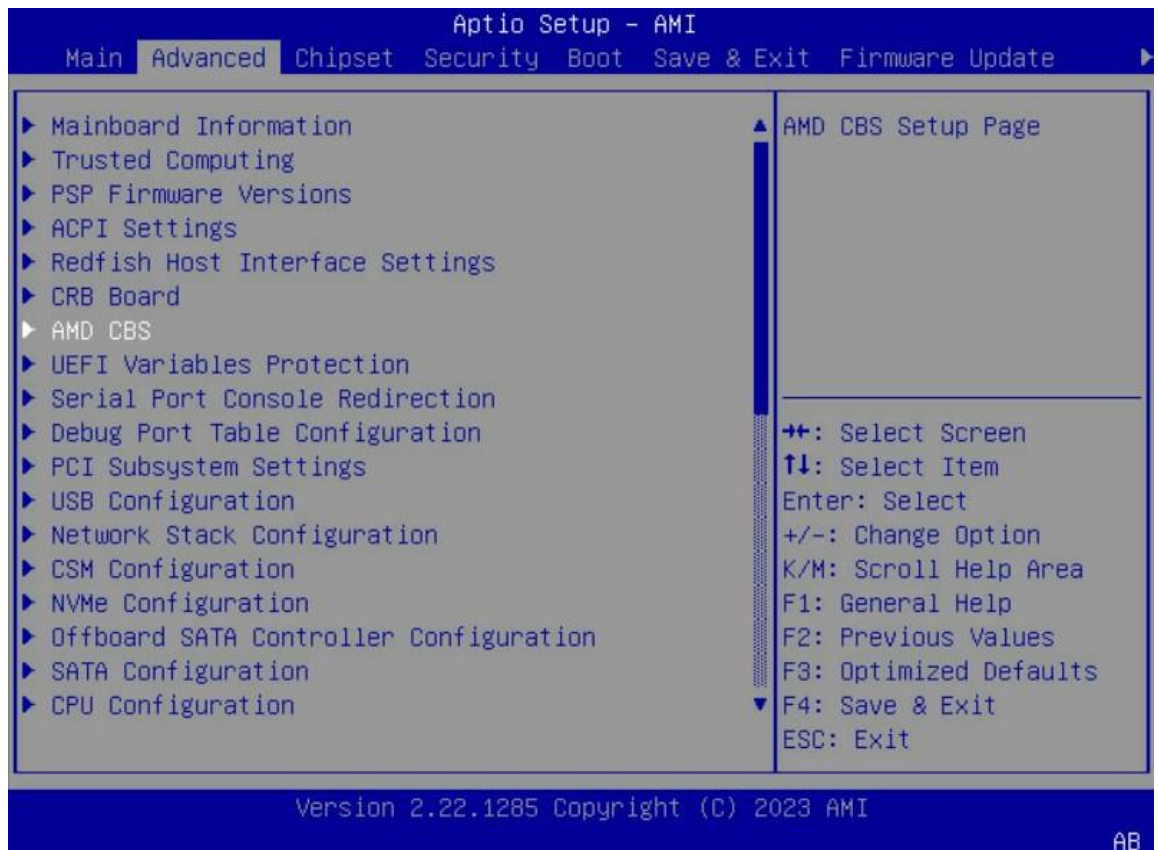
Abstract

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

Steps

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

Figure 2-35 Advanced Screen



2. Select **AMD CBS > DF Common Options > Memory Addressing** and then press **Enter**.

The **Memory Addressing** screen is displayed, as shown in [Figure 2-36](#).

Figure 2-36 Memory Addressing Screen



3. Select **NUMA nodes per socket** and then press **Enter**. In the displayed dialog box, select the number of **NUMA** nodes for each socket.
 - Auto
 - NPS0
 - NPS1
 - NPS2
 - NPS4
4. Select **SMT Control** and then press **Enter**. In the displayed dialog box, select **Enabled** to enable the memory interleaving feature.
5. Press **F4**. In the displayed dialog box, select **Yes**.

2.19 Setting Power Parameters

Abstract

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

Context

For a description of common power parameters, refer to [Table 2-5](#).

Table 2-5 Common Power Parameter Descriptions

Parameter	Description	Recommended Configuration
Power Policy Select	Power mode. Options: ● Performance: performance mode. 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. Therefore, the overall power consumption is increased. ● Efficient: energy-saving mode. This mode is applicable to most common scenarios. This mode enables energy saving provided that there is minimal impact on performance and puts some CPU cores to sleep when there is low load, to save energy 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: Latency-performance mode. This mode is applicable to the scenarios with strict requirements for latency and jitter, for example, the Real-Time Operating System (RTOS). This mode disables energy saving and other management features that may cause latency and keeps idle CPUs at their highest frequency for faster response.	Performance

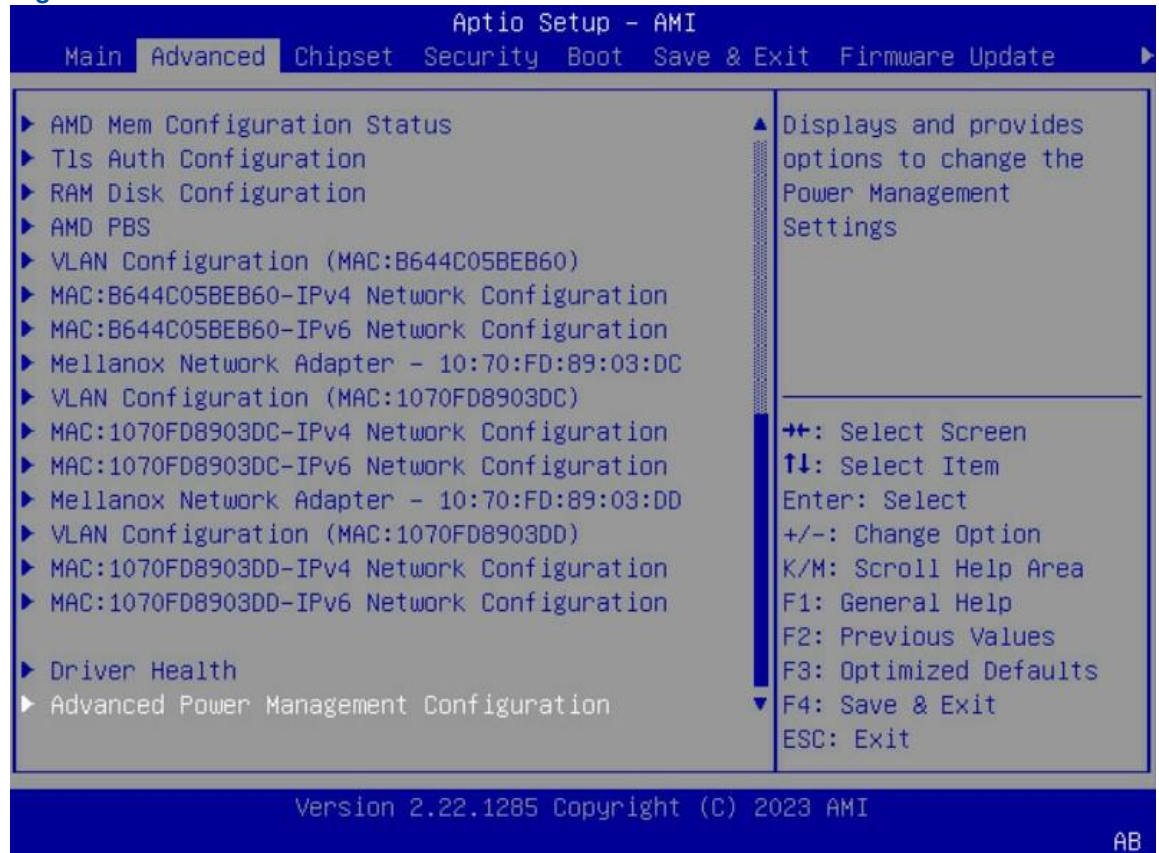
MONITOR and MWAIT disable	Specifies whether to enable the MONITOR and MWAIT instructions. Enabling the MONITOR and MWAIT instructions helps to optimize the instruction operation of CPUs. ● Enabled: disables Monitor and MWAIT instructions. If the C-state of a CPU needs to be disabled, the MONITOR and MWAIT instructions need to be disabled in specified operating systems. ● Disabled: enables the MONITOR and MWAIT instructions.	Enabled
Parameter	Description	Recommended Configuration
	If an EVC error is reported when a VM is added to a cluster or removed from a cluster, set this parameter to Disabled to enable the MONITOR and MWAIT instructions.	
Global C-state Control	Enables or disables CPU C-state energy-saving mode. Options: ● Enabled: enables the CPU C-state energy-saving mode. ● Disabled: disables the CPU C-state energy-saving mode. ● Auto.	Enabled

Steps

Configuring the Power Policy Select Parameter

1. On the **Aptio Setup** screen, select **Advanced**. The **Advanced** screen is displayed, as shown in [Figure 2-37](#).

Figure 2-37 Advanced Screen



2. Select **Advanced Power Management Configuration**, and then press **Enter**. The **Advanced Power Management Configuration** screen is displayed, as shown in [Figure 2-38](#).

Figure 2-38 Advanced Power Management Configuration Screen

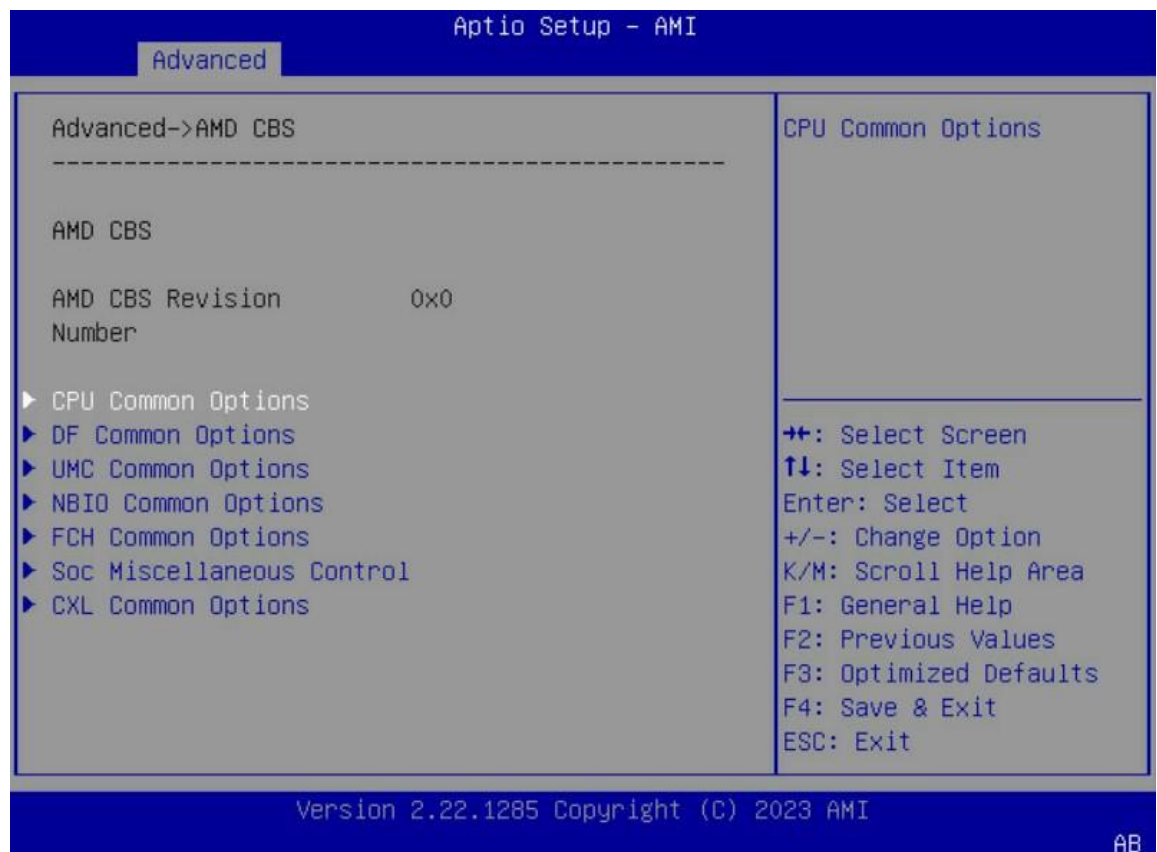


3. Select **Power Policy Select** and then press **Enter**. In the displayed dialog box, select **Custom**.

Configuring Global C-state Control

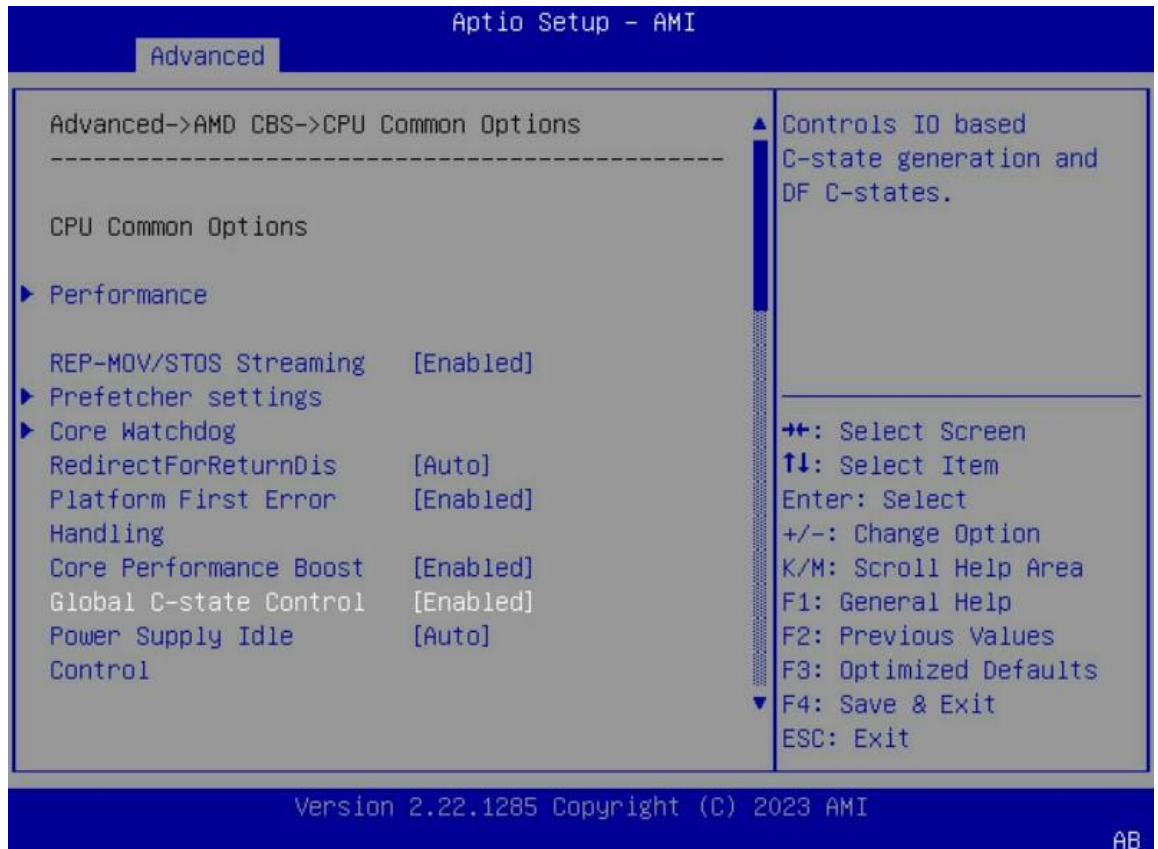
4. On the **Advanced** screen, select **AMD CBS** and then press **Enter**. The **AMD CBS** screen is displayed, as shown in [Figure 2-39](#).

Figure 2-39 AMD CBS Screen



5. Select **CPU Common Options** and then press **Enter**. The **CPU Common Options** screen is displayed, as shown in [Figure 2-40](#).

Figure 2-40 CPU Common Options Screen



6. Select **Global C-state Control** and then press **Enter**. In the displayed dialog box, select **Disabled** to enable CPU C-state energy saving.
7. Select **MONITOR and MWAIT disable** and then press **Enter**. In the displayed dialog box, select **Enabled** to disable the MONITOR and MWAIT instructions.
8. Press **F4**. In the displayed dialog box, select **Yes**.

2.20 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, as shown in [Figure 2-41](#).
 - Press **F3**.
 - Select **Save & Exit**. The **Save & Exit** screen is displayed. Select **Restore Defaults**.

Figure 2-41 Load Optimal Defaults Dialog Box



2. Select **USB** and then press the **Enter** key.
3. Press **F4**. In the displayed dialog box, select **Yes**.

Chapter 3

Setup Parameter Descriptions

Table of Contents

Main.....	50
Advanced.....	53
Chipset.....	251
Security.....	263
Boot.....	269
Save & Exit.....	276
Firmware Update.....	278
Event Logs.....	278
Server Mgmt.....	283

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

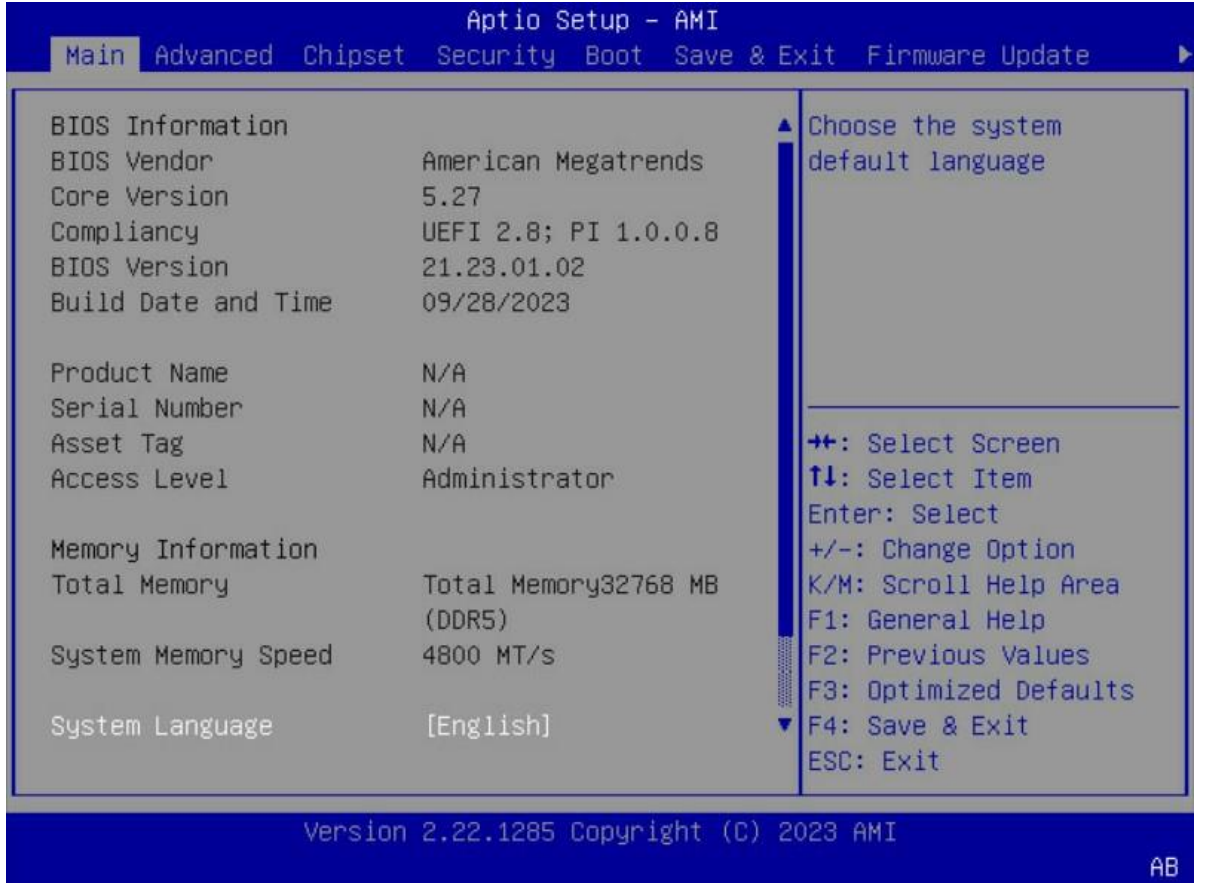
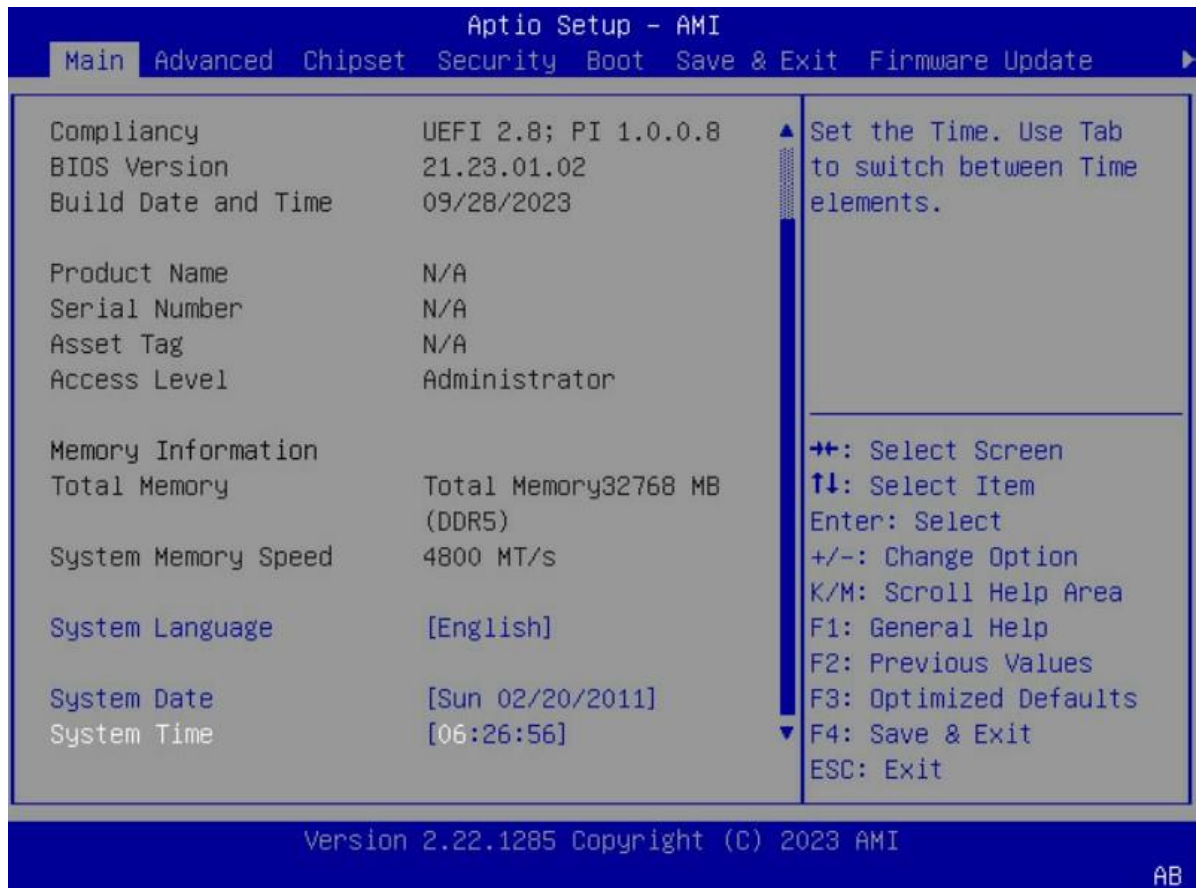


Figure 3-2 Main Screen—2



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

Table 3-1 Parameter Descriptions for the Main Screen

Parameter	Description
BIOS Vendor	Displays the BIOS vendor.
Core Version	Displays the BIOS core version.
Compliance	Displays the standards that the BIOS complies with.
BIOS Version	Displays the BIOS version.
Build Date and Time	Displays the BIOS creation date.
Product Name	Displays the product name.
Serial Number	Displays the serial number of the product.
Asset Tag	Displays the asset tag.
Access Level	Displays the access permission.

Total Memory	Displays the total amount of memory.
System Memory Speed	Displays the system memory speed.
Parameter	Description
System Language	Sets the system language. Options: ● English ● Simplified Chinese
System Date	Displays and sets the current system date. The system date is displayed in "day of week month/date/year" format. You can press Enter to switch between the month, date, and year items and change the settings as follows: To increase an item by one, press +. To decrease an item by one, press -. To specify a value, press the corresponding number key.
System Time	Displays and sets the current system time. 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 an item by one, press +. To decrease an item 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 3-5 show the **Advanced** screen.

Figure 3-3 Advanced Screen—1

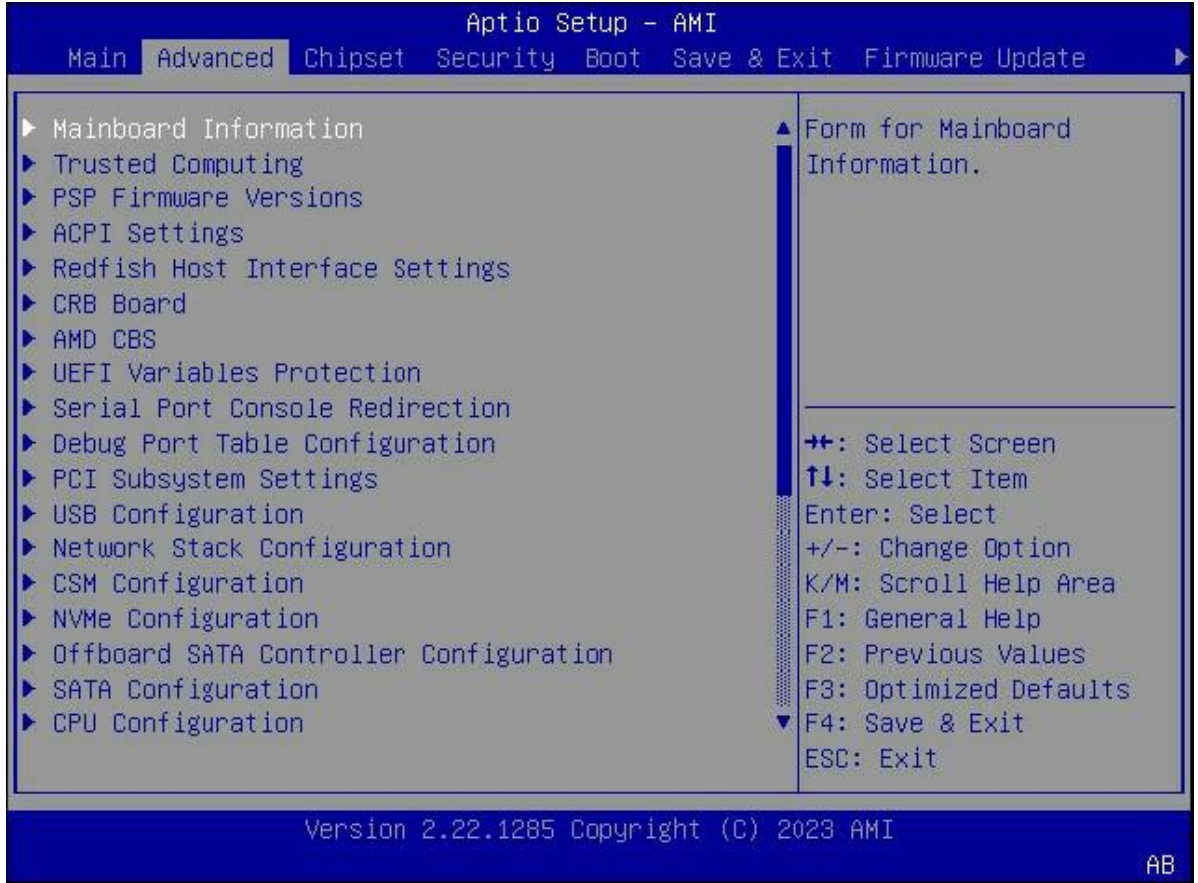


Figure 3-4 Advanced Screen—2

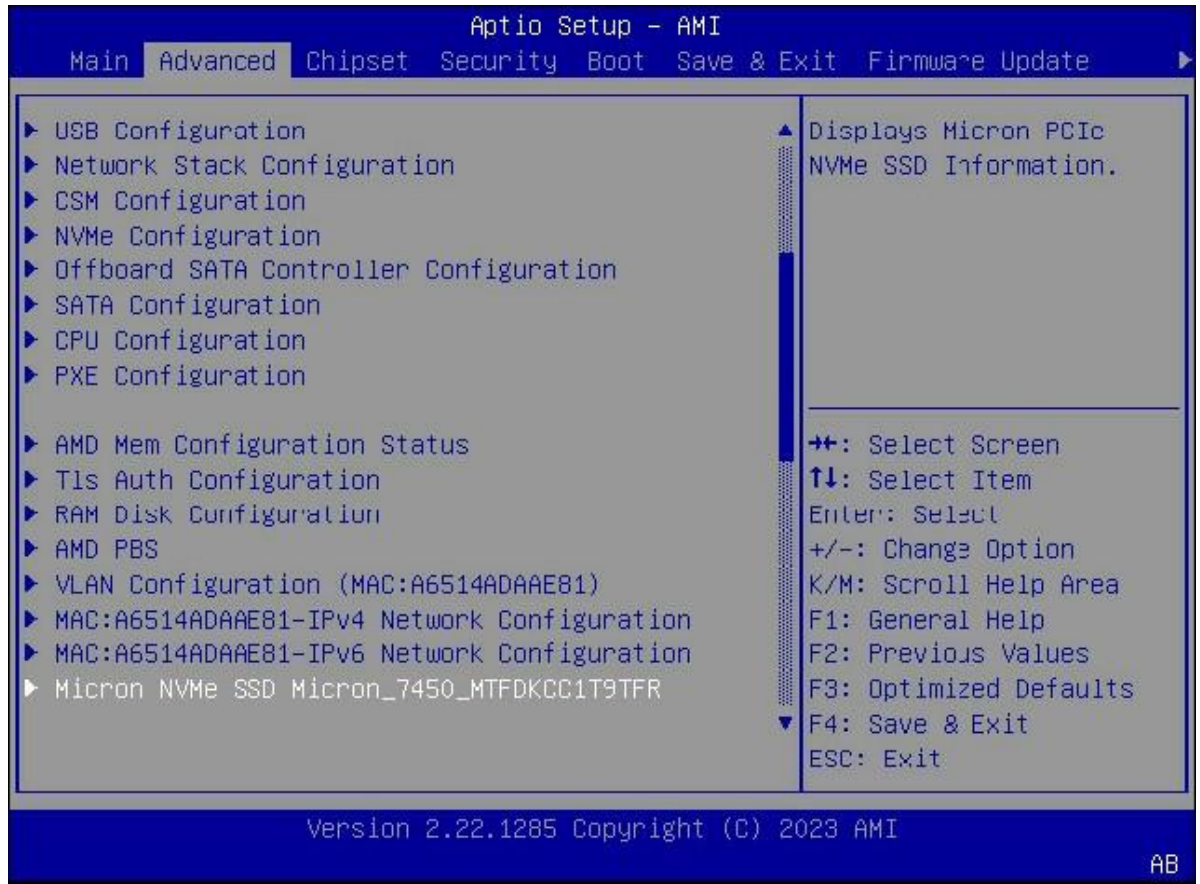
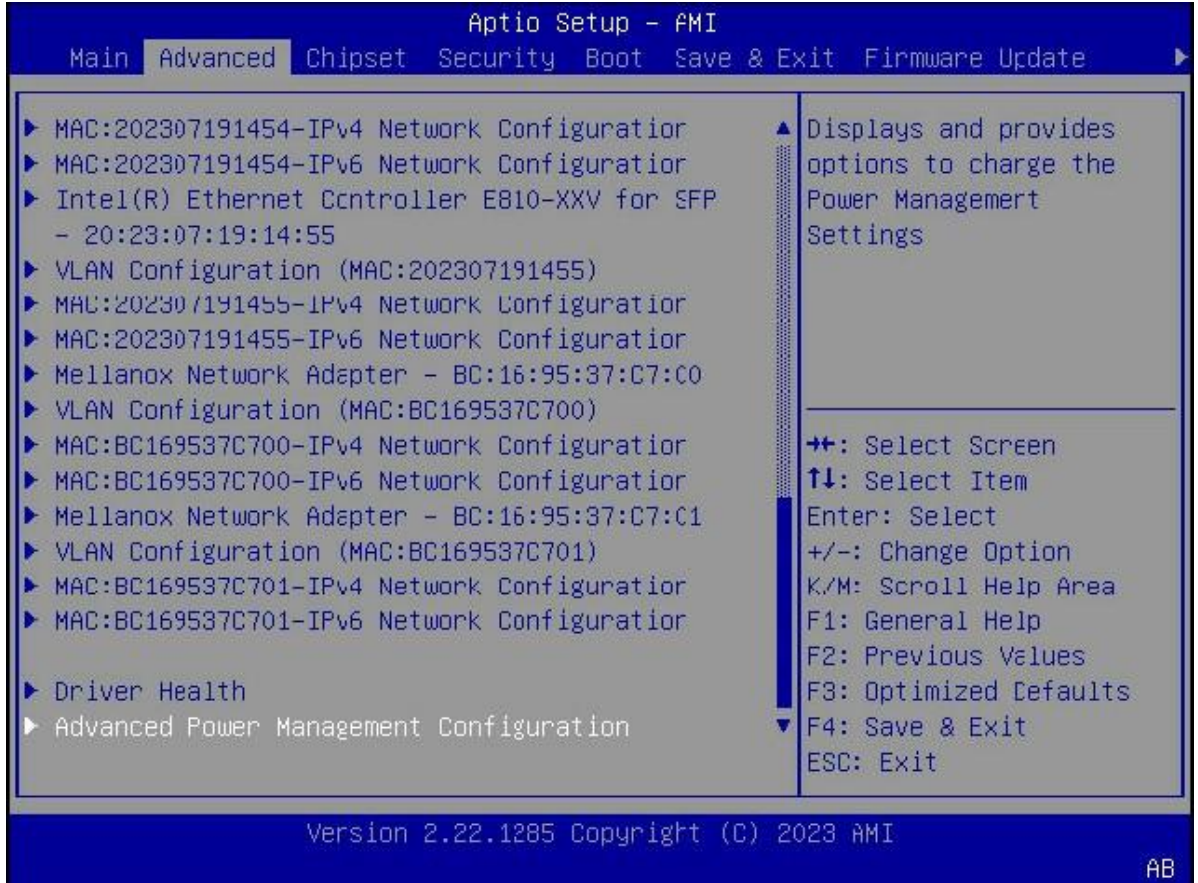


Figure 3-5 Advanced Screen—3



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

Table 3-2 Parameter Descriptions for the Advanced Screen

Parameter	Description
Mainboard Information	Displays mainboard information. For details, refer to 3.2.1 Mainboard Information .
Trusted Computing	Sets the trusted computing parameters. For details, refer to 3.2.2 Trusted Computing .
PSP Firmware Versions	Displays PSP firmware version information. For details, refer to 3.2.3 PSP Firmware Versions .
ACPI Settings	Sets ACPI parameters. For details, refer to 3.2.4 ACPI Settings .
Redfish Host Interface Settings	Sets Redfish and host interface parameters. For details, refer to 3.2.5 Redfish Host Interface Settings .
CRB Board	Sets CRB board parameters. For details, refer to 3.2.6 CRB Board .

AMD CBS	Sets AMD CBS parameters.
Parameter	Description
	For details, refer to 3.2.7 AMD CBS .
UEFI Variables Protection	Sets UEFI variable protection parameters. For details, refer to 3.2.8 UEFI Variables Protection .
Serial Port Console Redirection	Sets console redirection parameters. For details, refer to 3.2.9 Serial Port Console Redirection .
Debug Port Table Configuration	Sets debugging port parameters. For details, refer to 3.2.10 Debug Port Table Configuration .
PCI Subsystem Settings	Sets PCI subsystem parameters. For details, refer to 3.2.11 PCI Subsystem Settings .
USB Configuration	Sets USB parameters. For details, refer to 3.2.12 USB Configuration .
Network Stack Configuration	Sets network stack parameters. For details, refer to 3.2.13 Network Stack Configuration .
CSM Configuration	Sets CSM parameters. For details, refer to 3.2.14 CSM Configuration .
NVME Configuration	Sets NVME parameters. For details, refer to 3.2.15 NVMe Configuration .
Offboard SATA Controller Configuration	Sets off-board SATA controller parameters. For details, refer to 3.2.16 Offboard SATA Controller Configuration .
SATA Configuration	Sets SATA parameters. For details, refer to 3.2.17 SATA Configuration .
CPU Configuration	Sets CPU parameters. For details, refer to 3.2.18 CPU Configuration .
PXE Configuration	Sets PXE parameters. For details, refer to 3.2.19 PXE Configuration .
AMD Mem Configuration Status	Sets AMD memory configuration status. For details, refer to 3.2.20 AMD Mem Configuration Status .
Tls Auth Configuration	Sets Tls authentication parameters. For details, refer to 3.2.21 Tls Auth Configuration .

RAM Disk Configuration	Sets RAM disk parameters. For details, refer to 3.2.22 RAM Disk Configuration .
AMD PBS	Sets AMD PBS parameters. For details, refer to 3.2.23 AMD PBS .
Driver Health	Displays drive health information. For details, refer to 3.2.24 Driver Health .
Parameter	Description
Advanced Power Management Configuration	Sets advanced power management parameters. For details, refer to 3.2.25 Advanced Power Management Configuration .

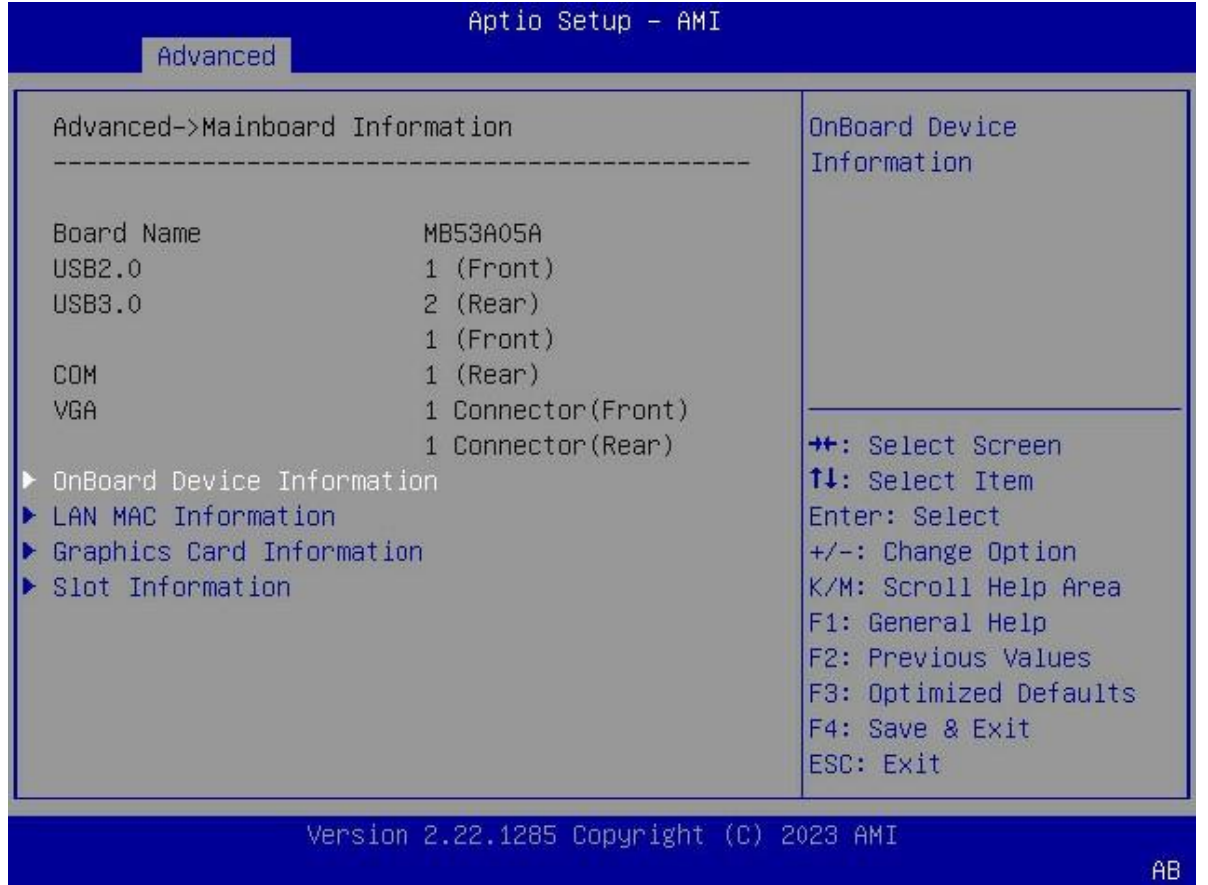
**Note**

All parameters on the **Advanced** screen except those in [Table 3-2](#) are generated by related devices. For example, for **MAC: 202307191454-IPv4 Network Configuration** in [Figure 3-5](#), 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 displays the information about mainboard interfaces and onboard devices. [Figure 3-6](#) shows the **Mainboard Information** screen.

Figure 3-6 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	Displays the mainboard name.	MB53A05A
Parameter	Description	Default
USB2.0	Displays the number and physical locations of USB 2.0 interfaces.	1(Front)
USB3.0	Displays the number and physical locations of USB 3.0 interfaces.	● 2(Rear) ● 1(Front)
COM	Displays the number and physical locations of COM interfaces.	1(Rear)
VGA	Displays the number and physical locations of VGA interfaces.	● 1(Front) ● 1(Rear)

OnBoard Device Information	Displays the onboard device information. For details, refer to 3.2.1.1 Onboard Device Information .	-
LAN MAC Information	Displays the MAC address of the Ethernet interface. For details, refer to 3.2.1.2 LAN MAC Information .	-
Graphics Card Information	Displays the information about onboard graphics cards. For details, refer to 3.2.1.3 Graphics Card Information .	-
Slot Information	Displays the information about PCIe standard card slots. For details, refer to 3.2.1.4 Slot Information .	-

3.2.1.1 Onboard Device Information

Figure 3-7 shows the **OnBcard Device Information** screen.

Figure 3-7 OnBoard Device Information Screen



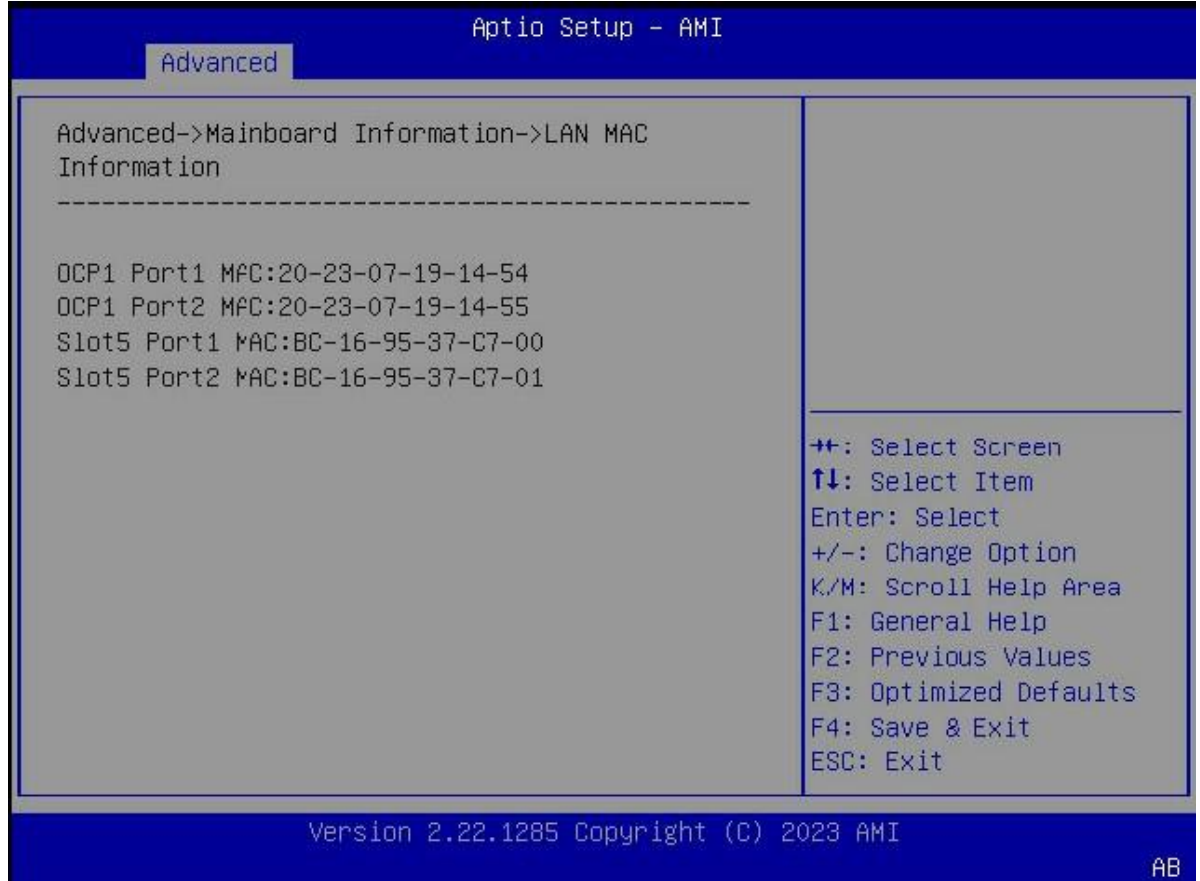
For a description of the parameters on the **OnBoard Device Information** screen, refer to [Table 3-4](#).

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

Parameter	Description
VGA	Displays the connection information about the VGA card on the mainboard. If no device is present, Not Present is displayed.

3.2.1.2 LAN MAC Information

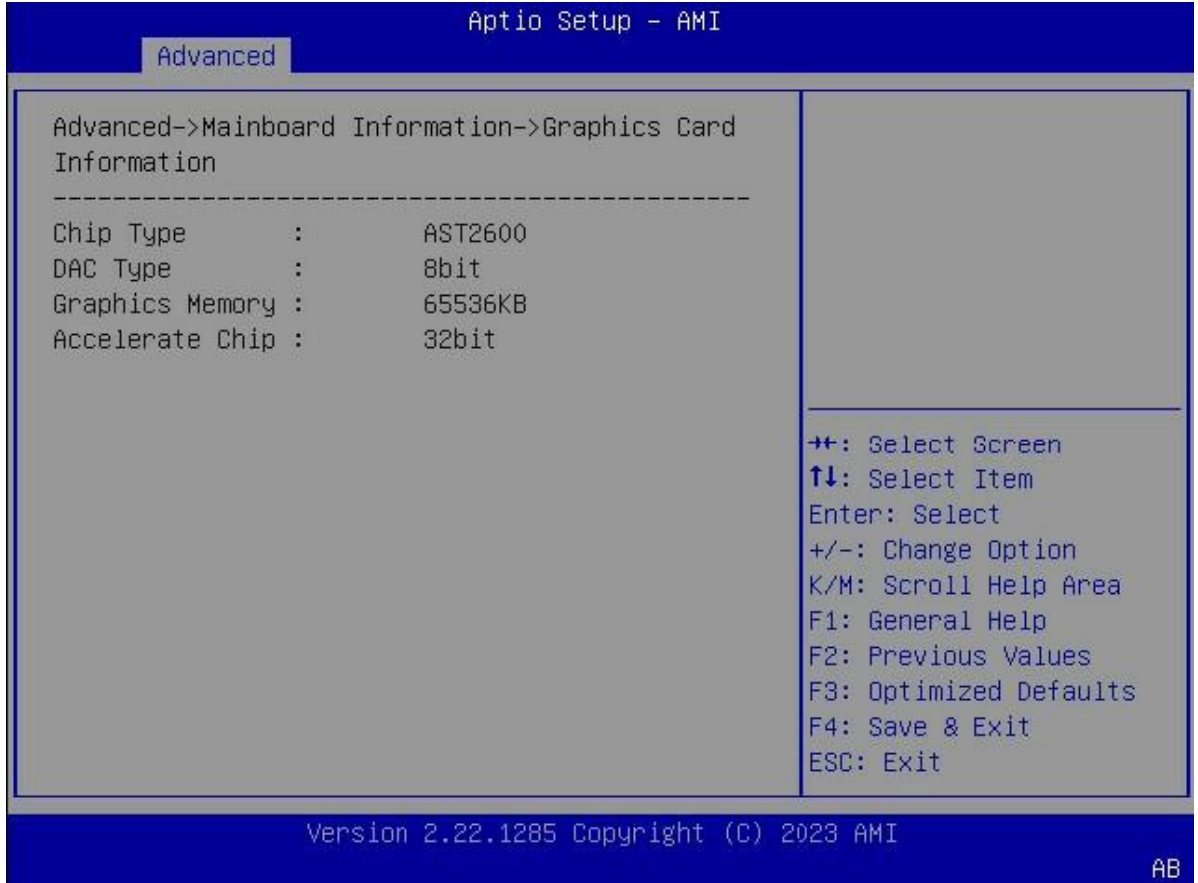
The **LAN MAC Information** screen displays MAC addresses of NICs, as shown in [Figure 3-8](#).

Figure 3-8 LAN MAC Information Screen

3.2.1.3 Graphics Card Information

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

Figure 3-9 Graphics Card Information Screen



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

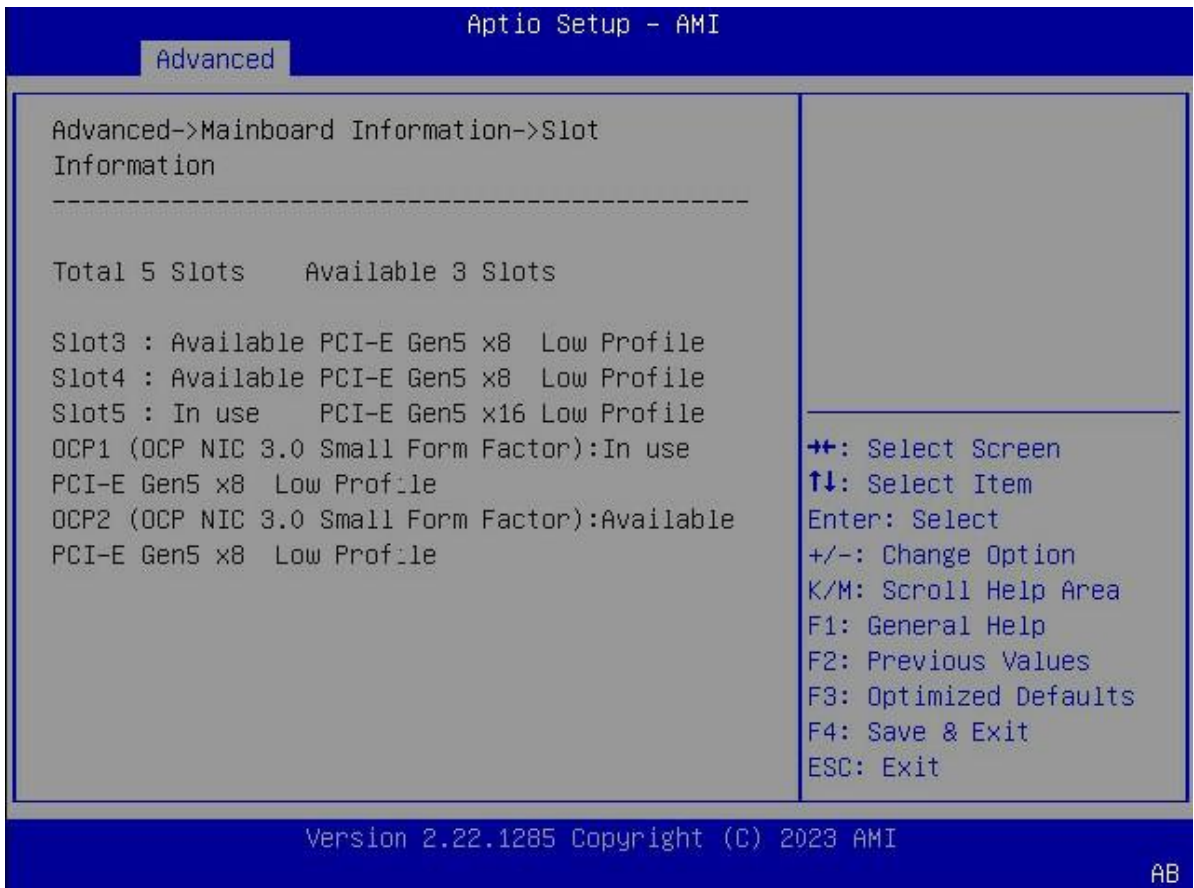
Table 3-5 Parameter Descriptions for the Graphics Card Information Screen

Parameter	Description
Chip Type	Displays the chip type of the graphics card.
DAC Type	Displays the type of DAC .
Graphics Memory	Displays the graphics card capacity.
Accelerate Chip	Displays the type of graphics accelerator.

3.2.1.4 Slot Information

[Figure 3-10](#) shows the **Slot Information** screen.

Figure 3-10 Slot Information Screen



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

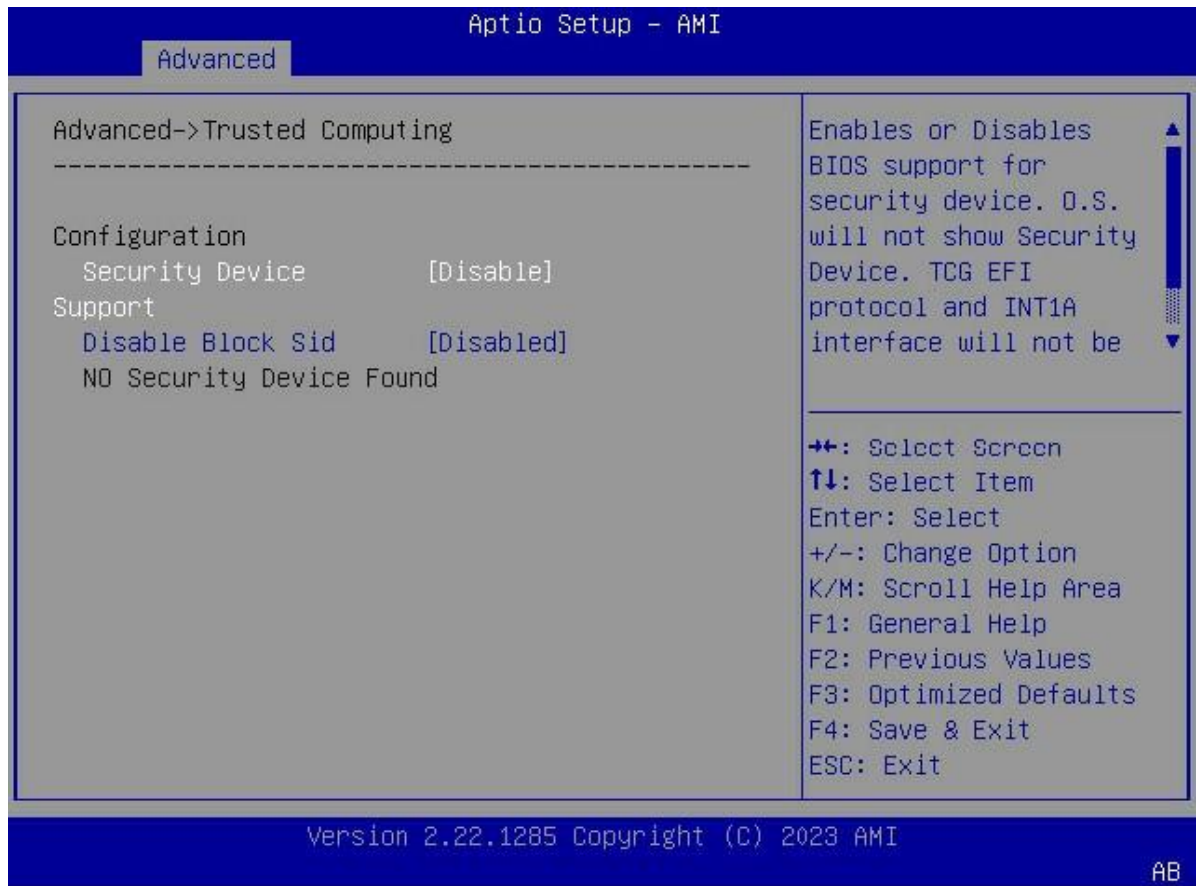
Table 3-6 Parameter Descriptions for the Slot Information Screen

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

3.2.2 Trusted Computing

[Figure 3-11](#) shows the **Trusted Computing** screen.

Figure 3-11 Trusted Computing Screen



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
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 operating system captures the information about the security device and displays the security device. ● 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.	Disabled
Disable Block Sid	Enables or disables security identifier blocking. Options:	Disabled

Parameter	Description	Default
	- Enabled: enables security identifier blocking. When this parameter is set to Enabled, the Block Sid is reloaded to allow SID authentication on TCG storage devices. - Disabled: disables security identifier blocking.	

3.2.3 PSP Firmware Versions

Figure 3-12 through Figure 3-13 show **PSP Firmware Versions**.

Figure 3-12 PSP Firmware Versions Screen—1

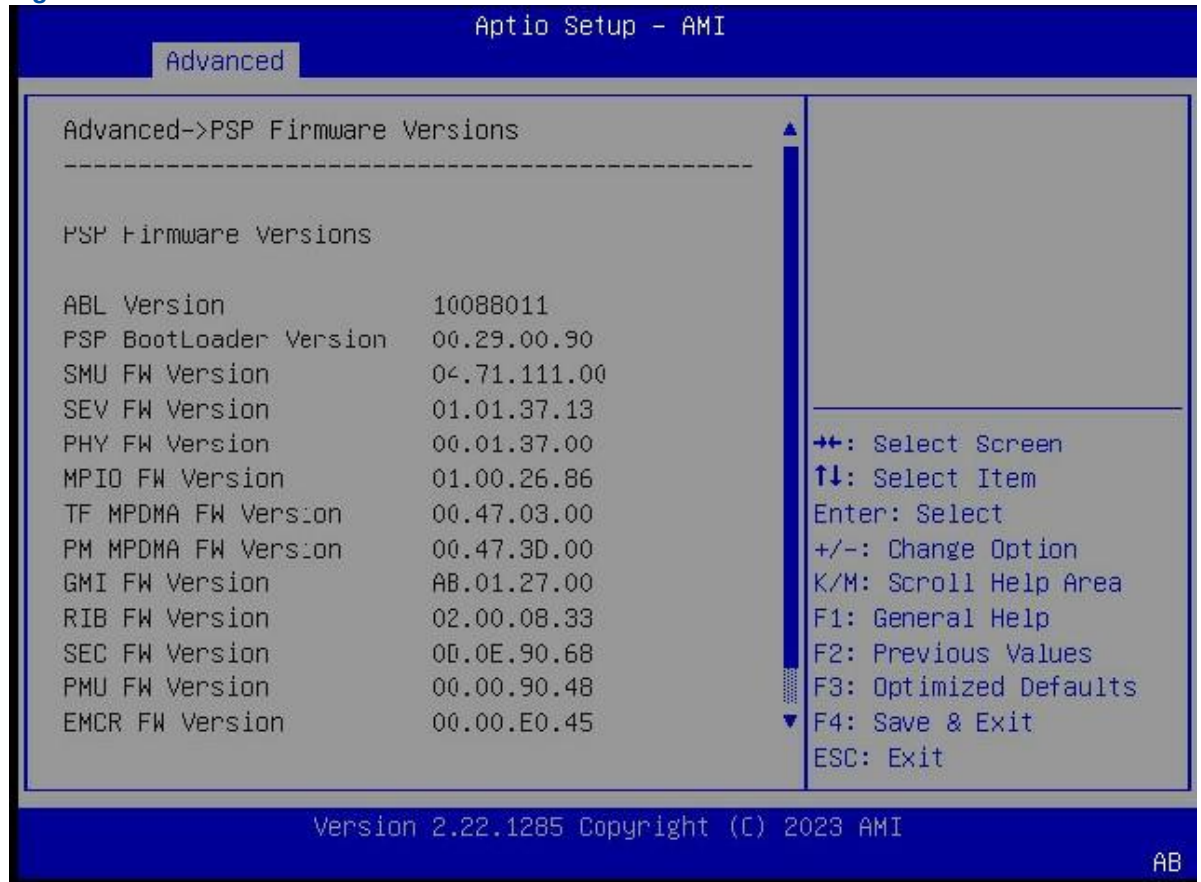
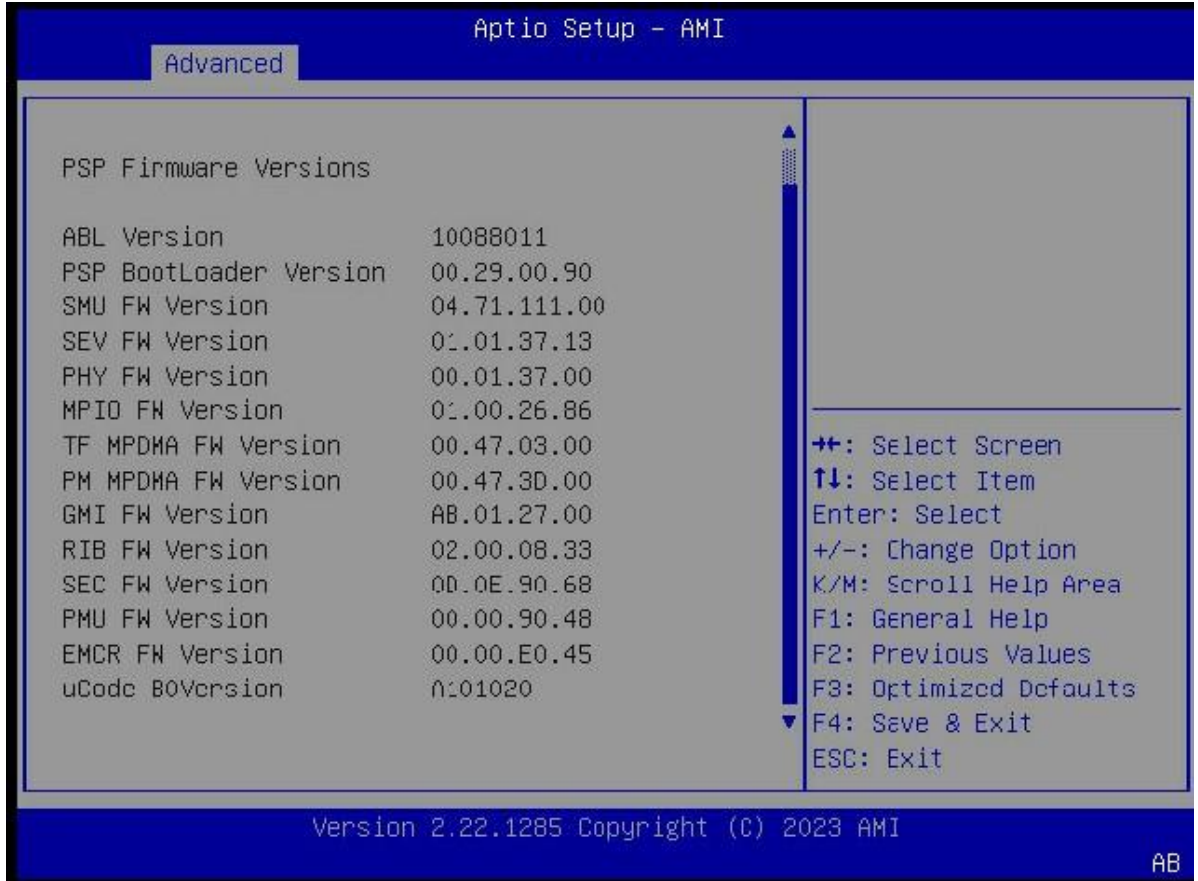


Figure 3-13 PSP Firmware Versions Screen—2



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

Table 3-8 Parameter Descriptions for the PSP Firmware Versions Screen

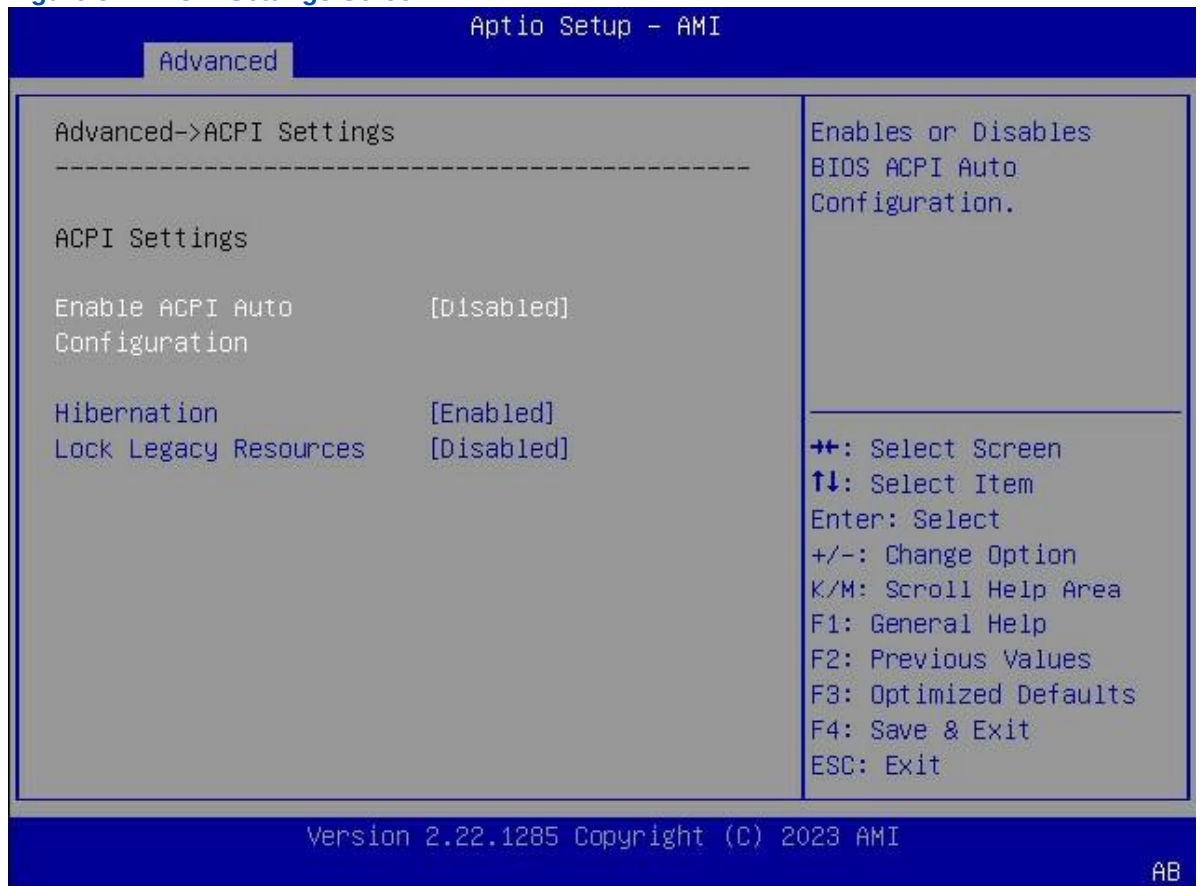
Parameter	Description
ABL Version	Displays the ABL version number.
PSP BootLoader Version	Displays the PSP loader version number.
SMU FW Version	Displays the SMU FW version number.
SEV FW Version	Displays the SEV FW version number.
PHY FW Version	Displays the PHY FW version number.
MPIO FW Version	Displays the MPIO FW version number.
TF MPDMA FW Version	Displays the TF MPDMA FW version number.
PM MPDMA FW Version	Displays the PM MPDMA FW version number.
GMI FW Version	Displays the GMI FW version number.

RIB FW Version	Displays the RIB FW version number.
SEC FW Version	Displays the SEC FW version number.
Parameter	Description
PMU FW Version	Displays the PMU FW version number.
EMCR FW Version	Displays the EMCR FW version number.
uCode B0 Version	Displays the uCode B0 version number.

3.2.4 ACPI Settings

[Figure 3-14](#) shows the **ACPI Settings** screen.

Figure 3-14 ACPI Settings Screen



For a description of the parameters on the **ACPI Settings** screen, refer to [Table 3-9](#).

Table 3-9 Parameter Descriptions for the ACPI Settings Screen

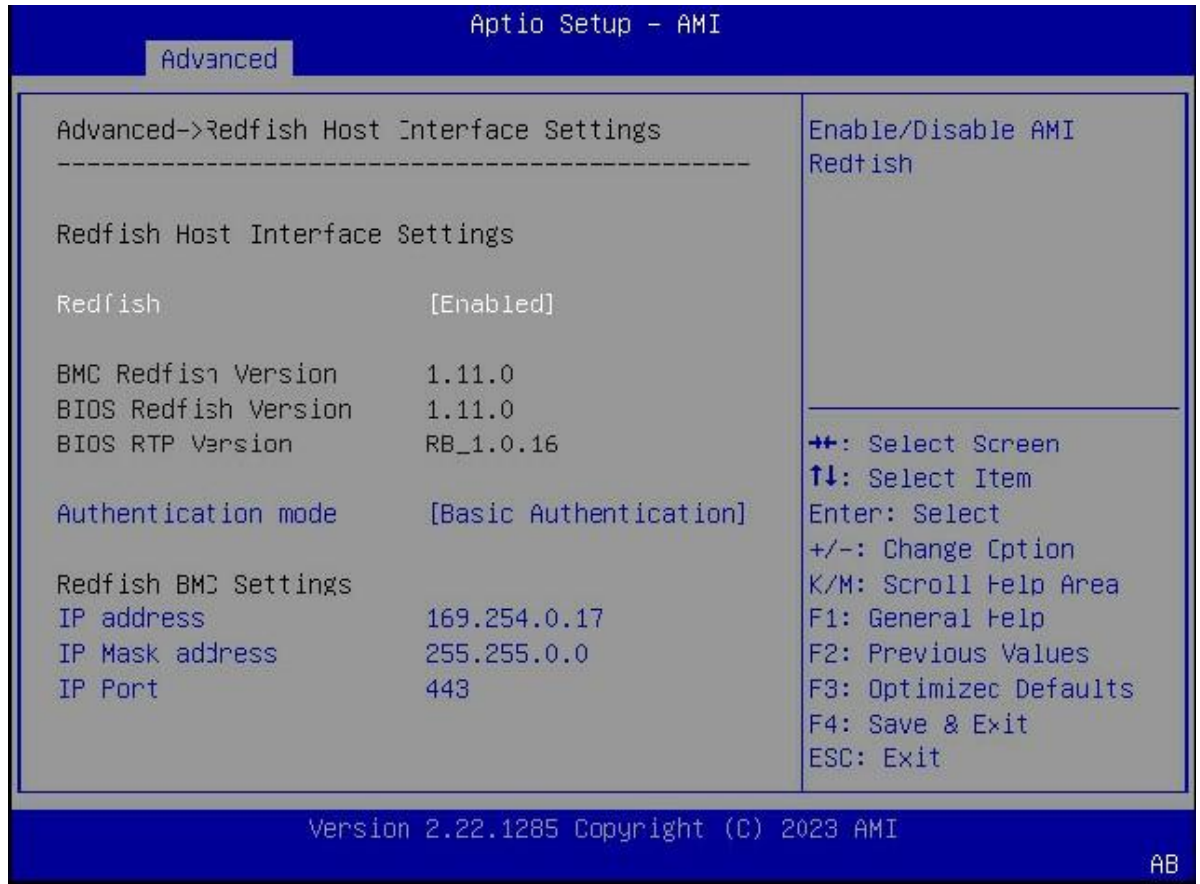
Parameter	Description	Default
-----------	-------------	---------

Enabled ACPI Auto Configuration	Enables or disables the ACPI auto-configuration feature. Options: Enabled: enables the ACPI auto-configuration feature.	Disabled
Parameter	Description	Default
	When this parameter is set to Enabled , the Hibernation and Lock Legacy Resources parameters 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
Lock Legacy Resources	Enables or disables the legacy resource locking feature. Options: - Enabled: enables the legacy resource locking feature. - Disabled: disables the legacy resource locking feature.	Disabled

3.2.5 Redfish Host Interface Settings

[Figure 3-15](#) shows the **Redfish Host Interface Settings** screen.

Figure 3-15 Redfish Host Interface Settings Screen



For a description of the parameters on the **Redfish Host Interface Settings** screen, refer to [Table 3-10](#).

Table 3-10 Parameter Descriptions for the Redfish Host Interface Settings Screen

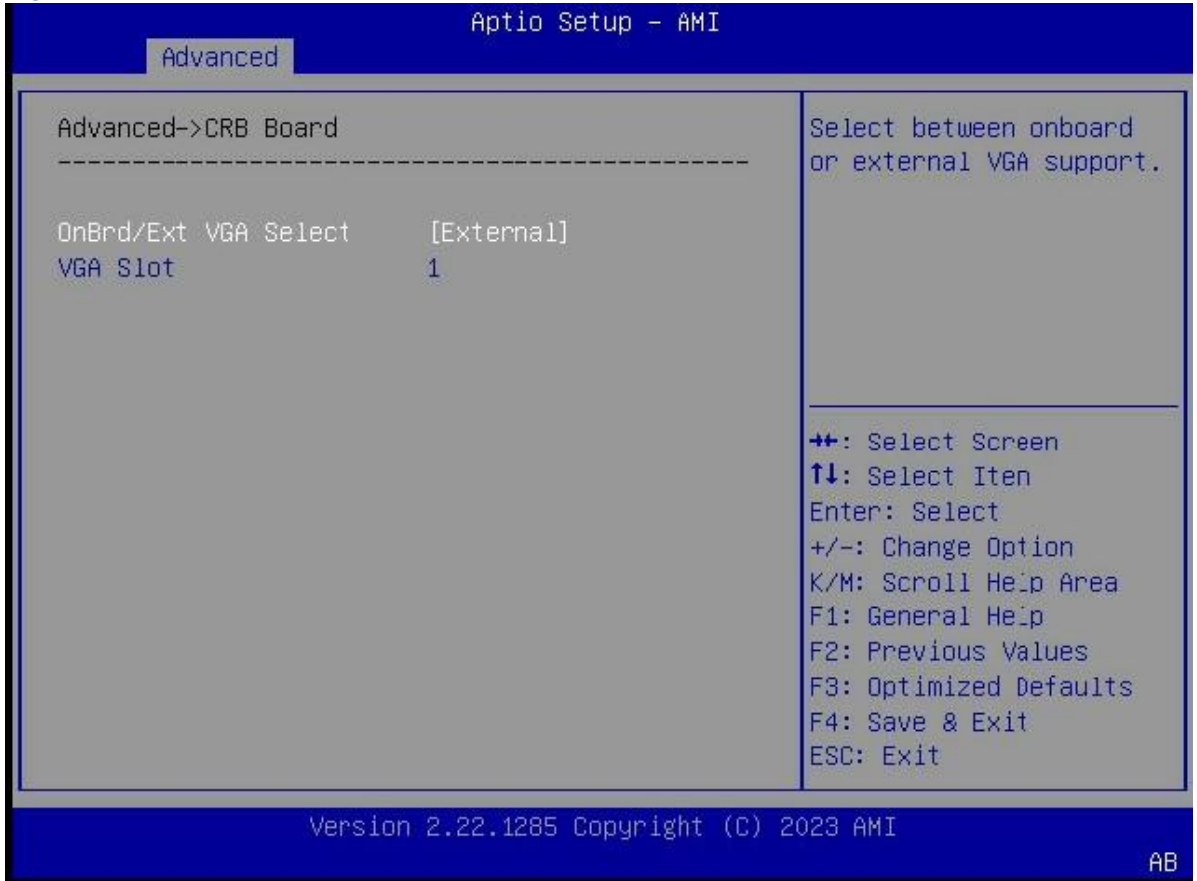
Parameter	Description	Default
Redfish	Enables or disables the AMI Redfish feature. Options: - Enabled: enables the AMI Redfish feature. - Disabled: disables the AMI Redfish feature. When this parameter is set to Disabled , all parameters below are hidden.	Enabled
BMC Redfish Version	Displays the BMC Redfish version number.	-
BIOS Redfish Version	Displays the BIOS Redfish version number.	-
BIOS RTP Version	Displays the BIOS RTP version number.	-

Authentication mode	Select an authentication mode. Options:	Basic Authentication
Parameter	Description	Default
	- Basic Authentication - Session Authentication	
IP address	Sets an IP address.	-
IP Mask address	Sets the IP address of the gateway.	-
IP Port	Sets the IP port.	-

3.2.6 CRB Board

Figure 3-16 shows the **CRB Board** screen.

Figure 3-16 CRB Board Screen



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

Table 3-11 Parameter Descriptions for the CRB Board Screen

Parameter	Description	Default
-----------	-------------	---------

OnBrd/Ext VGA Select	Select a VGA. Options: • Auto • Onboard	Auto
Parameter	Description	Default
	• External	
VGA Slot	This parameter is displayed when OnBrd/Ext VGA Select is set to External . Select the slot number of the enabled external VGA.	1

3.2.7 AMD CBS

The **AMD CBS** screen includes the [DF](#), [UMC](#), [NBIO](#), and [FCH](#) common options, and provides the information about [CPUs](#), memory, [PCIe](#) interfaces and [SATA](#) interfaces. [Figure 3-17](#) shows the **AMD CBS** screen.

Figure 3-17 AMD CBS Screen



For a description of the parameters on the **AMD CBS** screen, refer to [Table 3-12](#).

Table 3-12 Parameter Descriptions for the AMD CBS Screen

Parameter	Description
CPU Common Options	Sets general CPU option parameters. For details, refer to 3.2.7.1 CPU Common Options .
Parameter	Description
DF Common Options	Sets general DF option parameters. For details, refer to 3.2.7.2 DF Common Options .
UMC Common Options	Provides UMC common options. For details, refer to 3.2.7.3 UMC Common Options .
NBIO Common Options	Sets general NBIO option parameters. For details, refer to 3.2.7.4 NBIO Common Options .
FCH Common Options	Sets general bridge chip option parameters. For details, refer to 3.2.7.5 FCH Common Options .
Soc Miscellaneous Control	Sets chip miscellaneous control parameters. For details, refer to 3.2.7.6 Soc Miscellaneous Control .
CXL Common Options	Sets general CXL parameters. For details, refer to 3.2.7.7 CXL Common Options .

3.2.7.1 CPU Common Options

CPU Common Options

[Figure 3-18](#) through [Figure 3-20](#) show the **CPU Common Options** screen.

Figure 3-18 CPU Common Options Screen—1

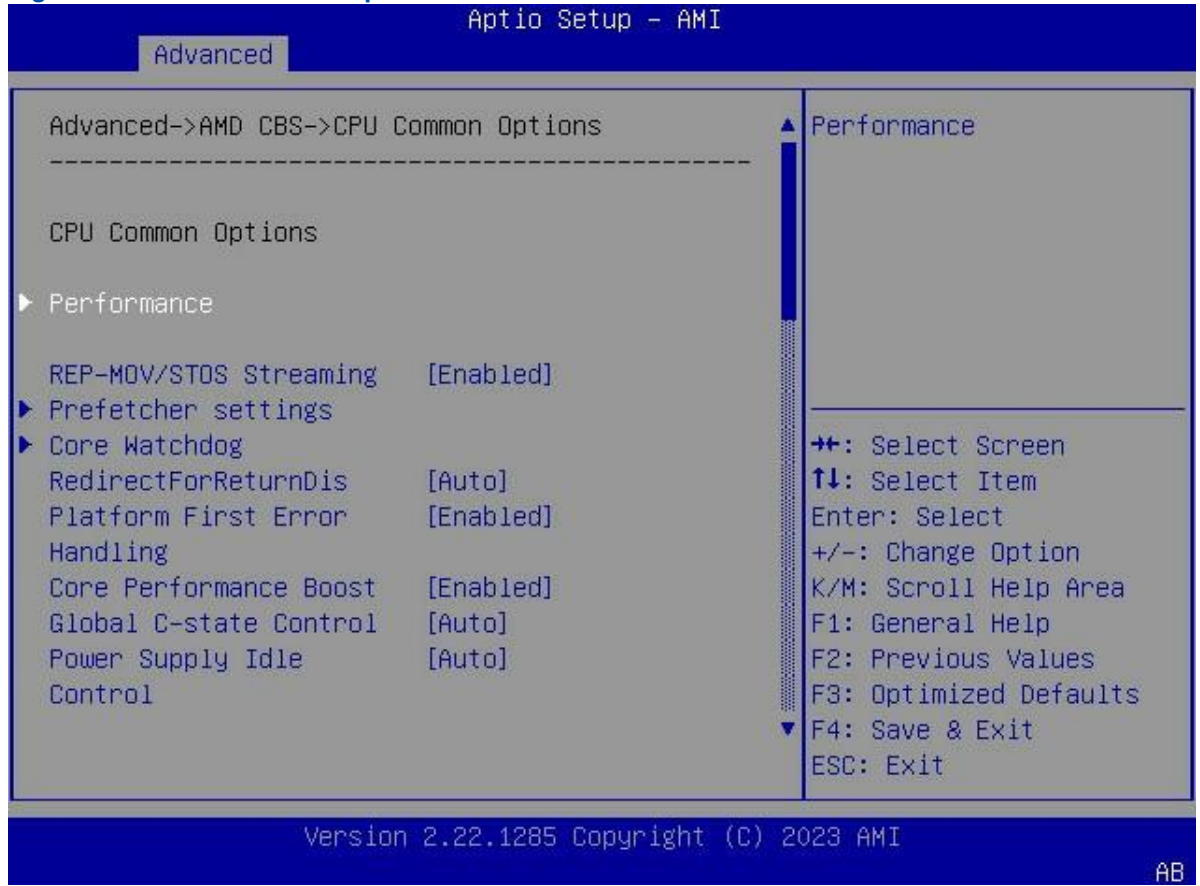


Figure 3-19 CPU Common Options Screen—2

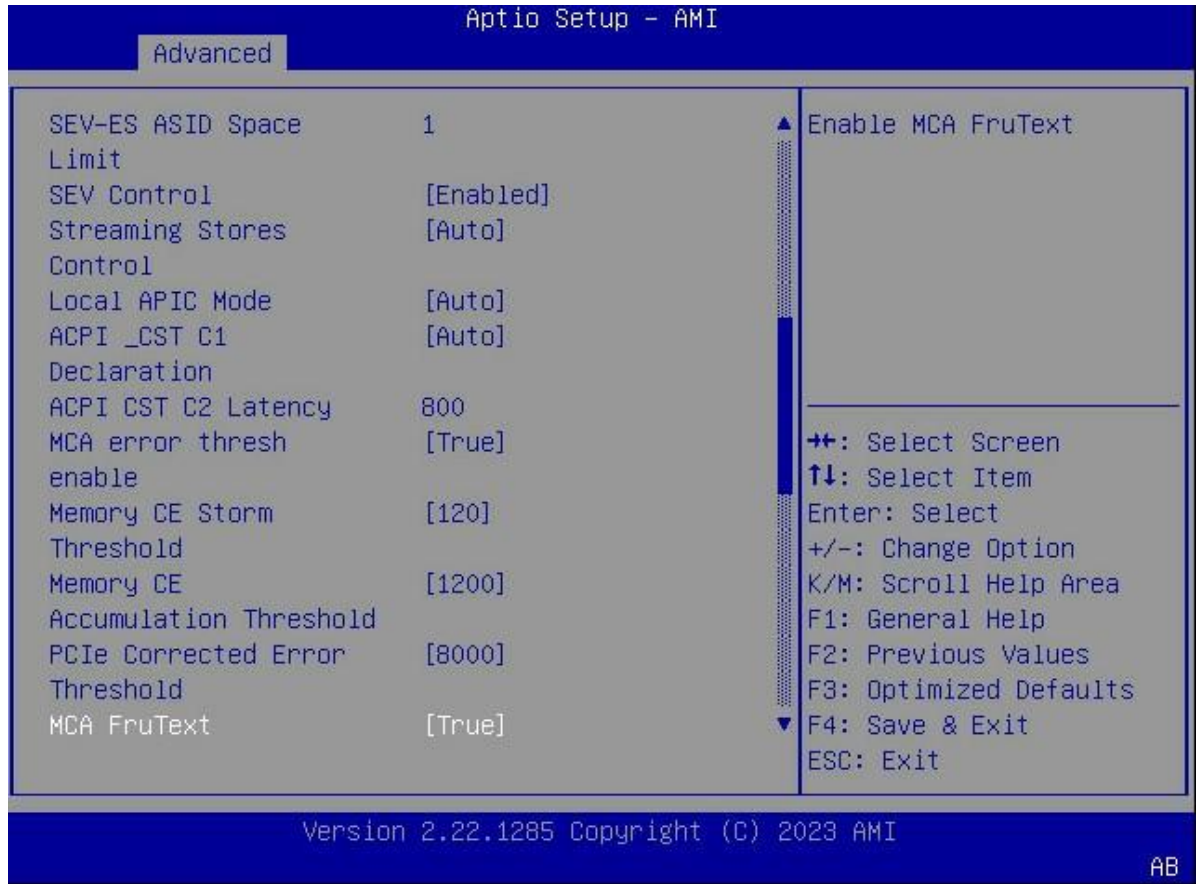
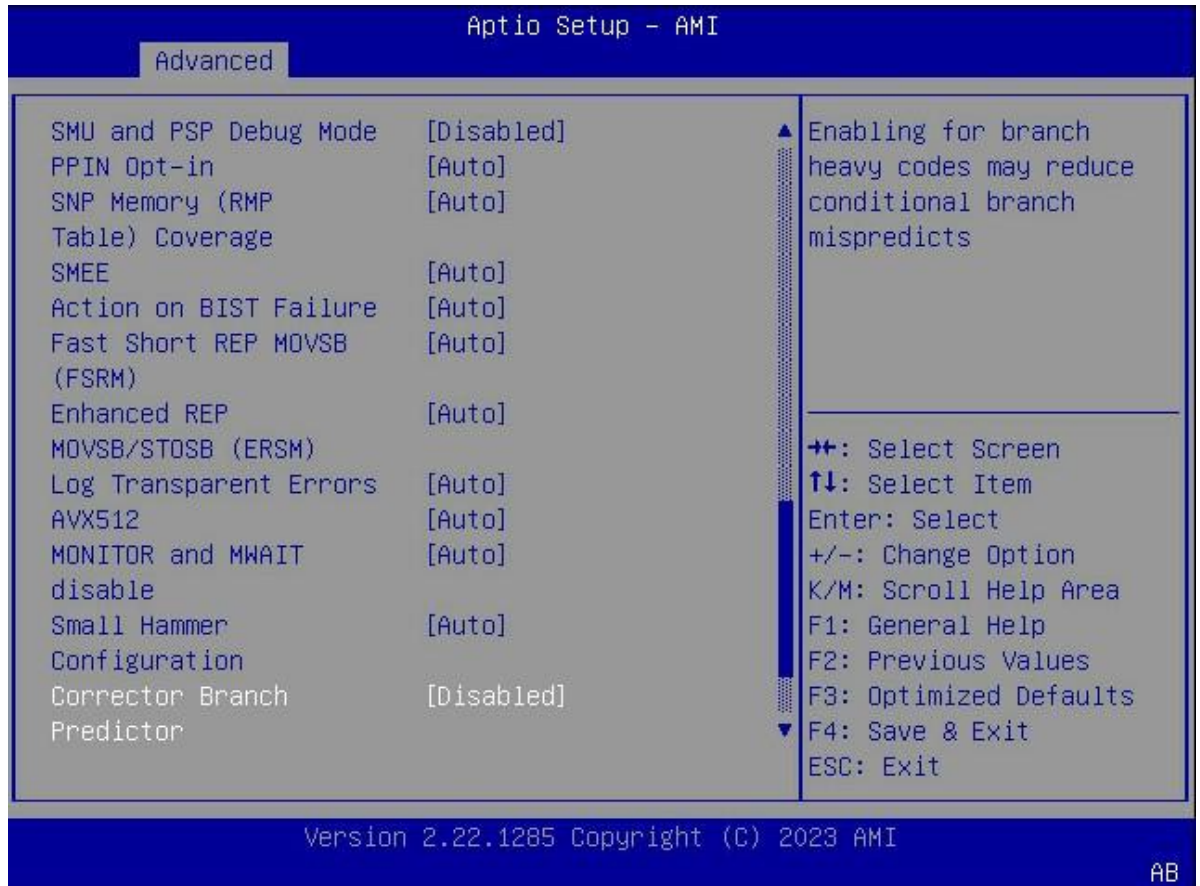


Figure 3-20 CPU Common Options Screen—3



For a description of the parameters on the **CPU Common Options** screen, refer to [Table 3-13](#).

Table 3-13 Parameter Descriptions for the CPU Common Options Screen

Parameter	Description	Default
Performance	Sets the performance parameters. For details, refer to Performance .	-
REP-MOV/STOS Streaming	Enables or disables the REP-MOV/STOS streaming feature to use non-cached streaming storage to provide larger capacity. - Enabled: enables the REP-MOV/STOS streaming feature. - Disabled: disables the REP-MOV/STOS streaming feature.	Enabled
Prefetcher settings	Sets prefetcher parameters. For details, refer to Prefetcher Settings .	-
Core Watchdog	Sets the core watchdog parameters. For details, refer to Core Watchdog .	-

Parameter	Description	Default
RedirectForReturnDis	To solve the GCC/C000005 problem for XV Core on CZ A0, set DecfgNoRdrctForReturns for MSRC001_1029 Decode Configuration (DE_CFG) bit 14. Options: ● Auto. ● 1: sets DecfgNoRdrctForReturns to 1. ● 0: sets DecfgNoRdrctForReturns to 0.	Auto
Platform First Error Handling	Enables or disables the platform firmware precedence feature. Options: ● Auto. ● Enabled: enables the platform firmware precedence feature. ● Disabled: disables the platform firmware precedence feature.	Enabled
Core Performance Boost	Enables or disables the CPB feature. Options: ● Enabled: enables the CPB feature. ● Disabled: disables the CPB feature.	Enabled
Global C-state Control	Enables or disables CPU C-state power saving mode. Options: ● Auto. ● Enabled: enables CPU C-state power saving mode. ● Disabled: disables CPU C-state power saving mode.	Auto
Power Supply Idle Control	Enables or disables power supply idleness control. Options: ● Auto ● Typical Current Idle ● Low Current Idle	Auto

SEV-ES ASID Space Limit	Sets the SEV-ES ASID space limit. SEV VMs using ASIDs below the SEV-ES ASID Space Limit must enable the SEV-ES feature. Hexadecimal notation, range: 0x1–0x10. When the parameter is set to 1, all are SEV guests and there are no SEV-ES or SNPs guests.	1
-------------------------	---	---

Parameter	Description	Default
SEV Control	Enables or disables the SEV feature. Options: ● Enabled: enables the SEV feature. ● Disabled: disables the SEV feature.	Enabled
Streaming Stores control	Enables or disables the streaming storage feature. Options: ● Auto. ● Enabled: enables the streaming storage feature. ● Disabled: disables the streaming storage feature.	Auto
Local APIC Mode	Select Local APIC Mode. Options: ● Compatibility ● xAPIC ● x2APIC ● Auto	x2APIC
ACPI _CST C1 Declaration	Enables or disables the ACPI _CST C1 declaration. Options: ● Auto. ● Enabled: enables the ACPI _CST C1 declaration. ● Disabled: disable the ACPI _CST C1 declaration.	Auto

MCA error thresh enable	Enables or disables the MCA error threshold. Options: ● Auto. ● Enabled: enables the MCA error threshold. ● Disabled: disables the MCA error threshold.	Auto
Memory CE Storm Threshold	Sets the threshold for the accumulated number of memory CEs .	120
Memory CE Accumulation Threshold	Sets the 24-hour memory CE accumulation threshold.	1200
PCIe Corrected Error Threshold	Sets the PCIe CE accumulation threshold.	8000
MCA Fru Text	Enables or disables the MCA Fru text feature. Options:	Enabled

Parameter	Description	Default
	● Enabled: enables the MCA Fru text feature. ● Disabled: disables the MCA Fru text feature.	
SMU and PSP debug Mode	Enables or disables SMU and PSP debugging mode. Options: ● Auto. ● Enabled: enables SMU and PSP debugging mode. ● Disabled: disable SMU and PSP debugging mode.	Disabled
PPIN Opt-in	Enables or disables the PPIN retrieval feature. Options: ● Auto. ● Enabled: enables the PPIN retrieval feature. ● Disabled: disables the PPIN retrieval feature.	Auto

SNP Memory (RMP Table)Coverage	Enables or disables the coverage of the entire system memory. Options: ● Auto. ● Enabled: enables the coverage of the entire system memory. ● Disabled: disables the coverage of the entire system memory. ● Custom.	Auto
SMEE	Enables or disables the secure memory encryption feature. Options: ● Auto. ● Enabled: enables the secure memory encryption feature. ● Disabled: disables the secure memory encryption feature.	Auto
Action on BIST Failure	Select the action to take when a BIST fault is detected. Options: ● Auto ● Down-CCD	Auto

Parameter	Description	Default
	● Do nothing	
Fast Short REP MOVSB (FSRM)	Enables or disables the FSRM feature. Options: ● Auto. ● Enabled: enables the FSRM feature. ● Disabled: disables the FSRM feature.	Auto
Enhanced REP MOVSB/STOSB(ERSM)	Enables or disables the ERSM feature. Options: ● Enabled: enables the ERSM feature. ● Disabled: disables the ERSM feature.	Auto

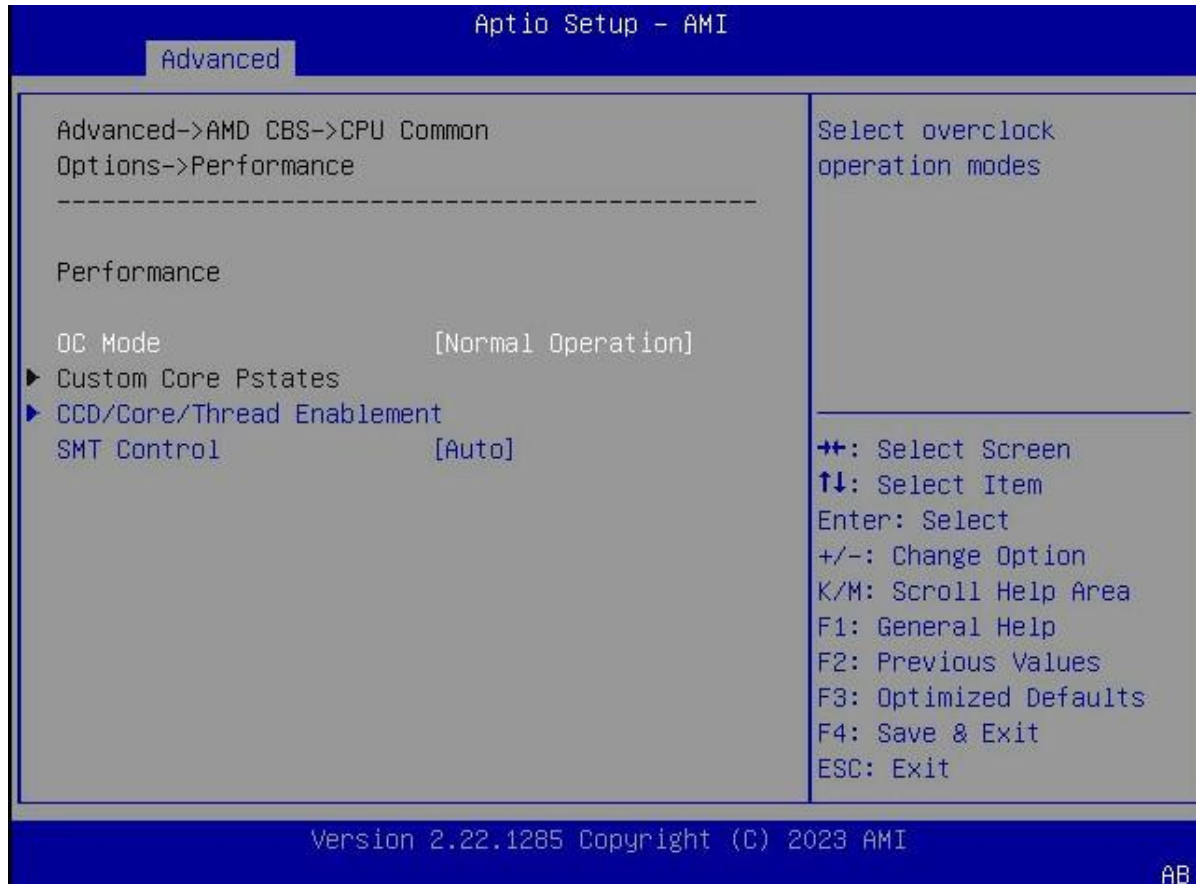
Log Transparent Errors	Enables or disables the logging of transparent errors in the MCA. Options: ● Auto. ● Enabled: enables the logging of transparent errors in the MCA. ● Disabled: disables the logging of transparent errors in the MCA.	Auto
AVX512	Enables or disables AVX512. Options: ● Auto. ● Enabled: enables AVX512. ● Disabled: disables AVX512.	Auto
MONITOR and MWAIT disable	Enables or disables the disablement of MONITOR and MWAIT. Options: ● Auto. ● Enabled: disables MONITOR and MWAIT. When this parameter is set to Enabled, the MONITOR, MWAIT, MONITOR X, and MWAIT X opcodes become invalid. ● Disabled: enables MONITOR and MWAIT.	Auto
Small Hammer Configuration	Enables or disables the Small Hammer configuration. Options: ● Auto. ● Enabled: enables the Small Hammer configuration. ● Disabled: disables the Small Hammer configuration.	Auto
Parameter	Description	Default
Corrector Branch Predictor	Enables or disables the corrector branch predictor. Options: ● Enabled: enables the corrector branch predictor. ● Disabled: disables the corrector branch predictor.	Disabled

PAUSE Delay	Enables or disables the pause delay feature. Options: ● Auto. ● Disabled: disables the pause delay feature. ● 16 Cycles: After the PAUSE command is executed, the thread is idle for 16 cycles. ● 32 Cycles: After the PAUSE command is executed, the thread is idle for 32 cycles. ● 64 Cycles: After the PAUSE command is executed, the thread is idle for 64 cycles. ● 128 Cycles: After the PAUSE command is executed, the thread is idle for 128 cycles.	Auto
CPU Speculative Store Modes	Select the CPU speculative storage mode. Options: ● Balanced ● More Speculative ● Less Speculative ● Auto	Auto
Prefetch/Request Throttle	Enables or disables the prefetch/request throttling feature. Options: ● Auto. ● Enabled: enables the prefetch/request throttling feature. ● Disabled: disables the prefetch/request throttling feature.	Auto

Performance

Figure 3-21 shows the **Performance** screen.

Figure 3-21 Performance Screen



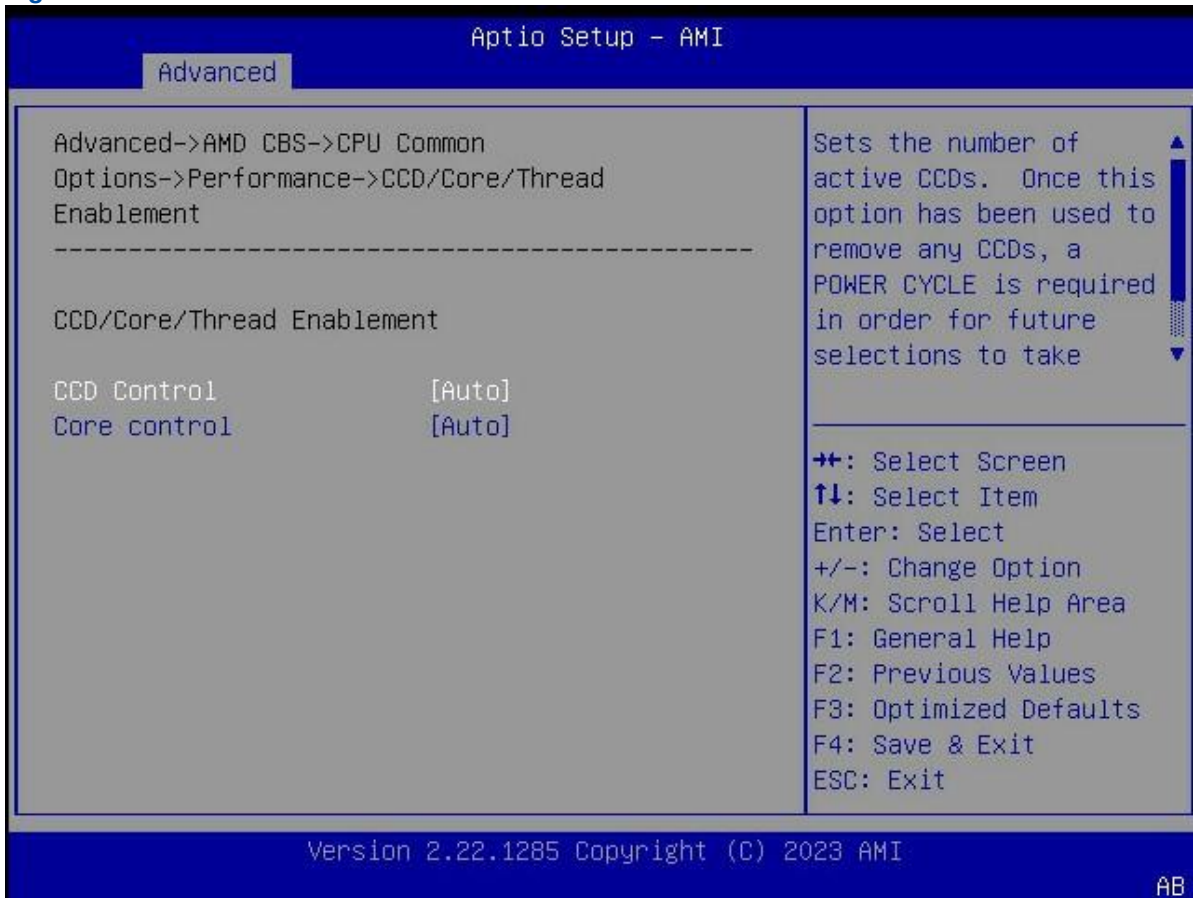
For a description of the parameters on the **Performance** screen, refer to [Table 3-14](#).

Table 3-14 Parameter Descriptions for the Performance Screen

Parameter	Description	Default
OC Mode	Select an OC mode. Options: - Normal Operation - Customized	Normal Operation
Custom Core Pstates	This parameter can be configured when OC Mode is set to Customized . Select the core P state configuration mode. Press Enter to unfold the settings. - Decline: prevents you from setting the core P state. - Accept: allows you to set the core P state.	-

CCD/Core/Thread Enablement	Sets the CCD/core/thread status. Press the Enter key. The CCD/Core/Thread Enablement screen is displayed, as shown in Figure 3-22 .	-
Parameter	Description	Default
SMT Control	Enables or disables the SMT control feature. • Auto. • Enabled: enables the SMT control feature. • Disabled: disables the SMT control feature.	Auto

Figure 3-22 CCD/Core/Thread Enablement Screen



For a description of the parameters on the **CCD/Core/Thread Enablement** screen, refer to [Table 3-14](#).

Table 3-15 Parameter Descriptions for the CCD/Core/Thread Enablement Screen

Parameter	Description	Default
-----------	-------------	---------

CCD Control	Select the number of CCDs to use. Options: ● Auto ● 2 CCDs ● 4 CCDs ● 6 CCDs ● 8 CCDs ● 10 CCDs	Auto
Parameter	Description	Default
Core Control	Select the number of cores to use. Options: ● Auto ● ONE (1 + 0) ● TWO (2 + 0) ● THREE (3 + 0) ● FOUR (4 + 0) ● FIVE (5 + 0) ● SIX (6 + 0) ● SEVEN (7 + 0)	Auto

Prefetcher Settings

Figure 3-23 shows the **Prefetcher settings** screen.

Figure 3-23 Prefetcher Settings Screen



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

Table 3-16 Parameter Descriptions for the Prefetcher Settings Screen

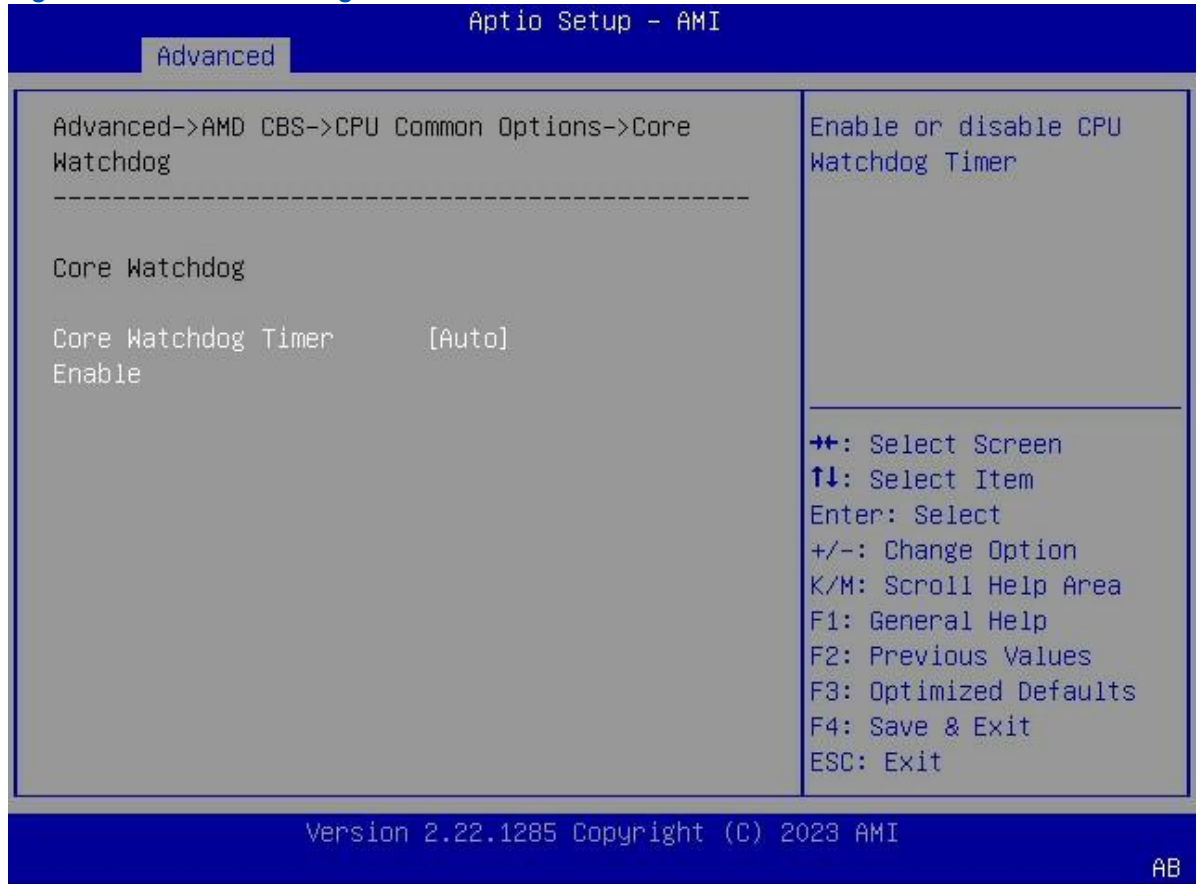
Parameter	Description	Default
L1 Stream HW Prefetcher	Enables or disables the L1-cache stream hardware prefetcher. Options: ● Auto. ● Enabled: enables the L1-cache stream hardware prefetcher. ● Disabled: disables the L1-cache stream hardware prefetcher.	Auto

L1 Stride Prefetcher	Enables or disables the L1 stride prefetcher feature. Options: ● Auto. ● Enabled: enables the L1 stride prefetcher feature. ● Disabled: disables the L1 stride prefetcher feature.	Auto
L1 Region Prefetcher	Enables or disables the L1 region prefetcher feature. Options: ● Auto. ● Enabled: enables L1 region prefetch. ● Disabled: disables the XPT prefetch feature.	Auto
L2 Stream HW Prefetcher	Enables or disables the L2-cache stream hardware prefetcher. Options: ● Auto. ● Enabled: enables the L2-cache stream hardware prefetcher. ● Disabled: disables the L2-cache stream hardware prefetcher.	Auto
L2 Up/Down Prefetcher	Enables or disables the L2 Up/Down prefetcher feature. Options: ● Auto. ● Enabled: enables the L2 Up/Down prefetcher feature. ● Disabled: disables the L2 Up/Down prefetcher feature.	Auto
Parameter	Description	Default
L1 Burst Prefetcher Mode	Enables or disables the L1 burst prefetcher feature. Options: ● Auto. ● Enabled: enables the L1 burst prefetcher feature. ● Disabled: disables the L1 burst prefetcher feature.	Auto

Core Watchdog

Figure 3-24 shows the **Core Watchdog** screen.

Figure 3-24 Core Watchdog Screen



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

Table 3-17 Parameter Descriptions for the Core Watchdog Screen

Parameter	Description	Default
Core Watchdog Timer Enable	Enables or disables the core watchdog timer.	Auto
Parameter	Description	Default
	Options: • Auto. • Enabled: enables the core watchdog timer. • Disabled: disables the core watchdog timer.	

3.2.7.2 DF Common Options

DF Common Options

Figure 3-25 shows the **DF Common Options** screen.

Figure 3-25 DF Common Options Screen—1

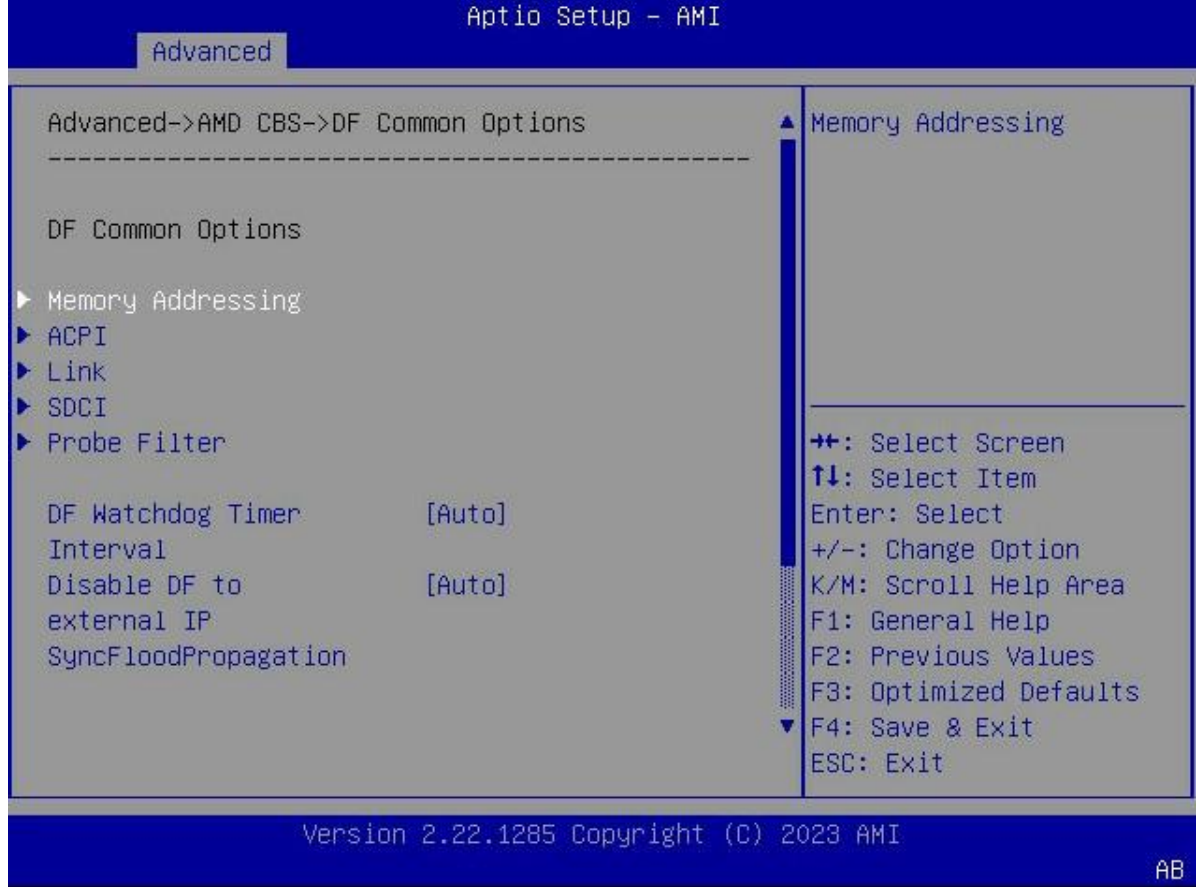
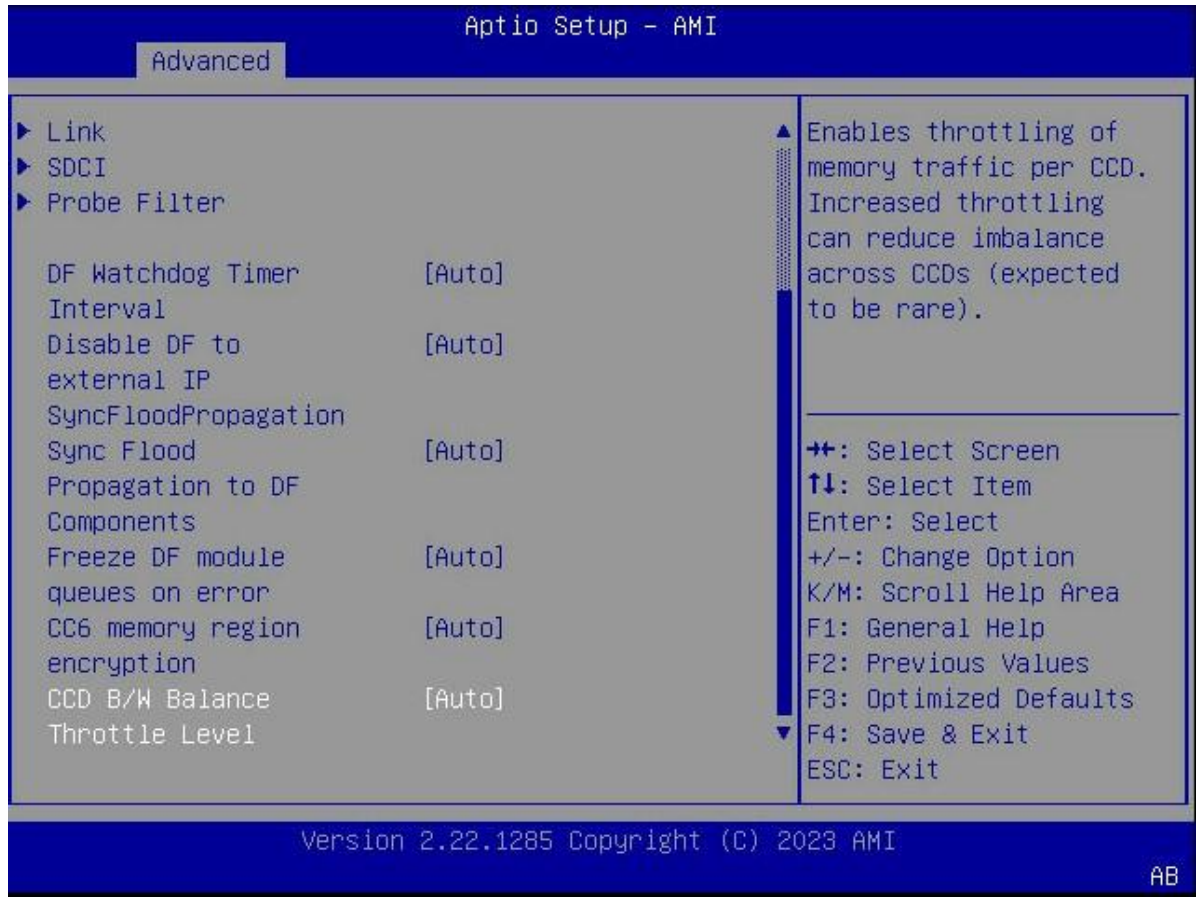


Figure 3-26 DF Common Options Screen—2



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

Table 3-18 Parameter Descriptions for the DF Common Options Screen

Parameter	Description	Default
Memory Addressing	Sets memory address management parameters. For details, refer to Memory Addressing .	-
ACPI	Sets advanced power interface configuration parameters. For details, refer to ACPI .	-
Link	Sets link parameters. For details, refer to Link .	-
SDCI	Sets SDCI parameters. For details, refer to SDCI .	-
Probe Filter	Sets probe filter parameters. For details, refer to Probe Filter .	-

DF Watchdog Timer Interval	Select an interval for the DF watchdog timer.	Auto
----------------------------	---	------

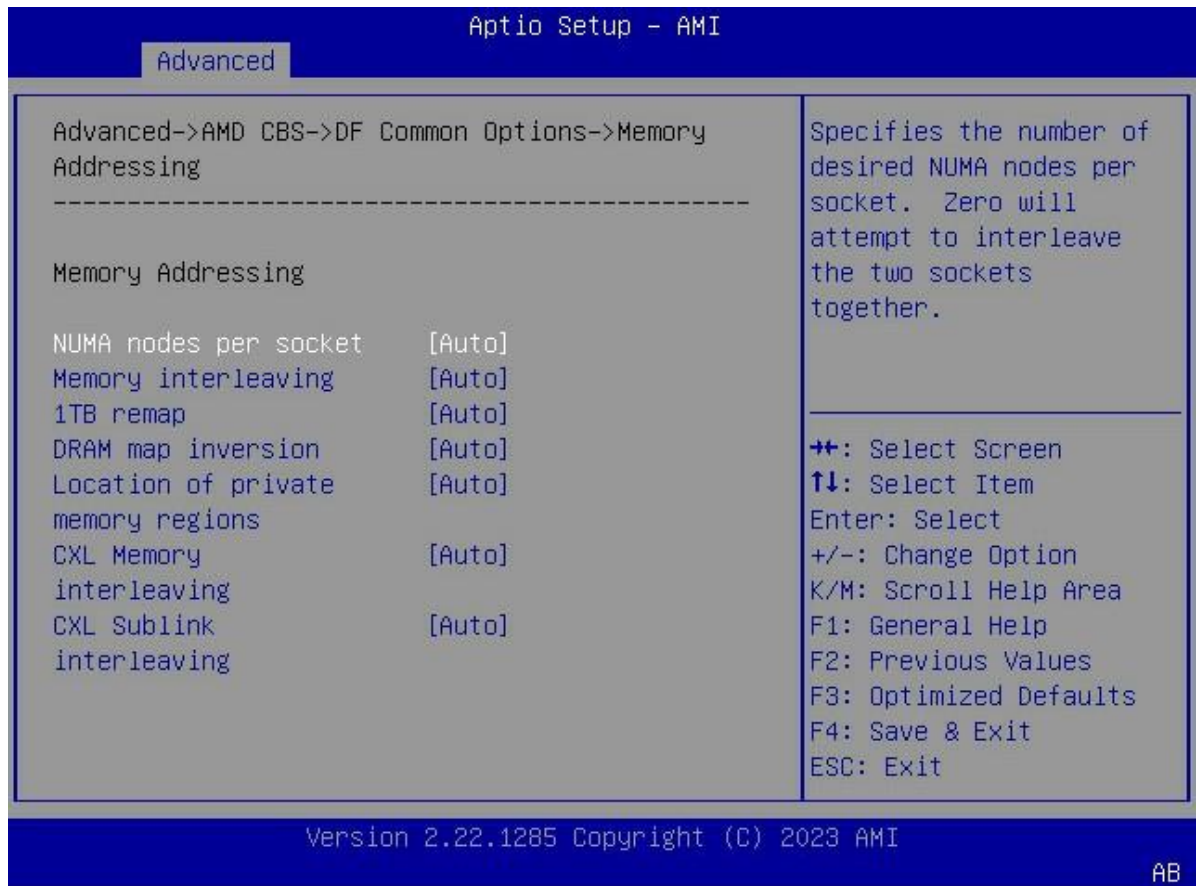
Parameter	Description	Default
	Options: ● Auto ● 41 ms ● 166 ms ● 334 ms ● 669 ms ● 1.34 s ● 2.68 s ● 5.36 s	
Disable DF to external IP SyncFloodPropagation	Enables or disables batch synchronization between the DF and its downstream subordinate components. Options: ● Auto ● Sync Flood disabled: disables batch synchronization between the DF and its downstream subordinate components. ● Sync Flood enabled: enables batch synchronization between the DF and its downstream subordinate components.	Auto
Sync Flood Propagation to DF Components	Enables or disables SYNC flood propagation to DF components. Options: ● Auto. ● Sync Flood enabled: enables SYNC flood propagation to DF components. ● Sync Flood disabled: disables SYNC flood propagation to DF components.	Auto
Freeze DF module queues on error	Enables or disables DF module queue freezing upon an error. Options: ● Auto. ● Enabled: enables DF module queue freezing upon an error. ● Disabled: disables DF module queue freezing upon an error.	Auto

CC6 memory region encryption	Enables or disables CC6 memory region encryption. Options: ● Auto.	Auto
Parameter	Description	Default
	● Enabled: enables CC6 memory region encryption. ● Disabled: disables CC6 memory region encryption.	
CCD B/W Balance Throttle Level	Select the CCD B/W throttling level. ● Auto ● Level 0 ● Level 1 ● Level 2 ● Level 3 ● Level 4	Auto

Memory Addressing

Figure 3-27 shows the **Memory Addressing** screen.

Figure 3-27 Memory Addressing Screen



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

Table 3-19 Parameter Descriptions for the Memory Addressing Screen

Parameter	Description	Default
NUMA nodes per socket	Select the number of NUMA nodes required per socket. Options: ● Auto ● NPS0 ● NPS1 ● NPS2 ● NPS4	Auto

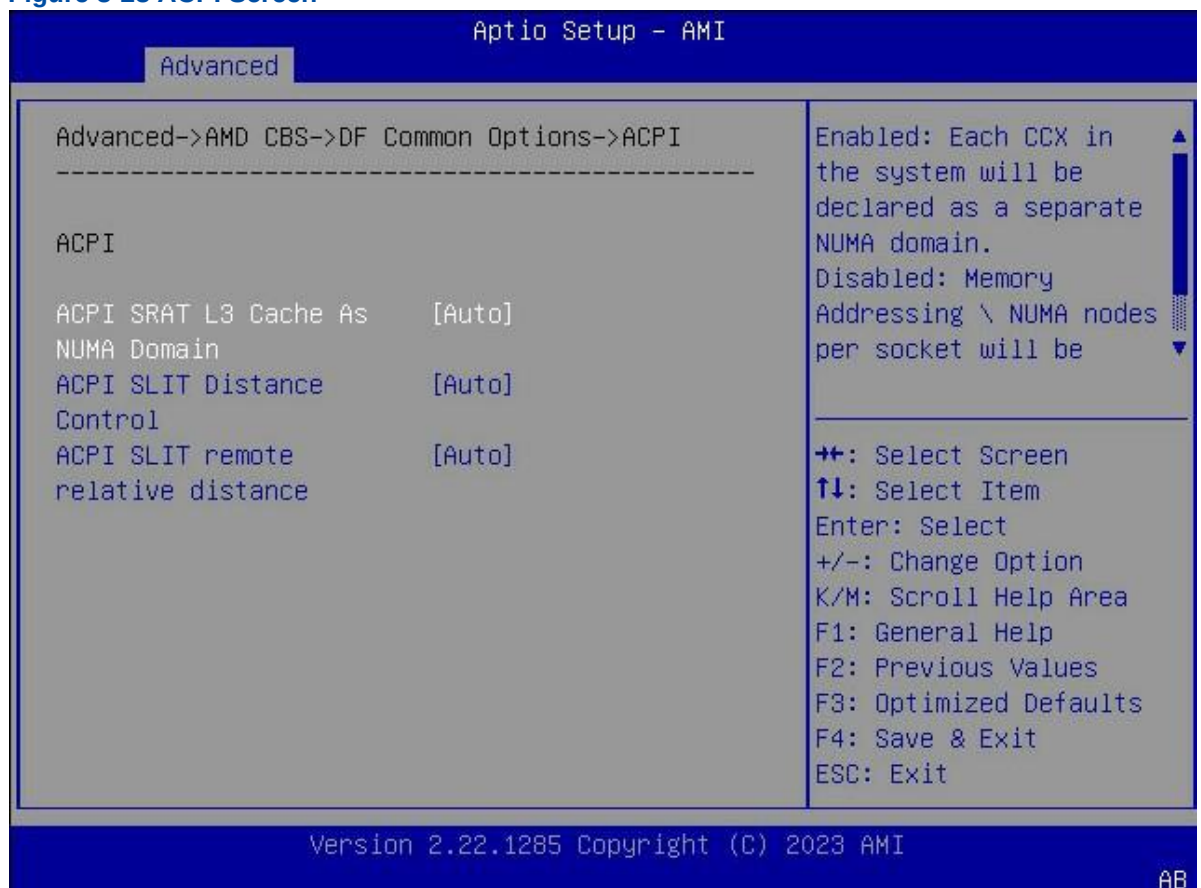
Memory interleaving	Enables or disables the memory interleaving feature. Options: ● Auto. ● Enabled: enables the memory interleaving feature. ● Disabled: disables the memory interleaving feature.	Auto
1TB remap	Enables or disables the 1TB remapping feature. ● Auto. ● Attempt to remap: enables the 1TB remapping feature. ● Do not remap: disables the 1TB remapping feature.	Auto
DRAM map Inversion	Enables or disables DRAM mapping inversion. Options: ● Auto. ● Enabled: enables DRAM mapping inversion. ● Disabled: disables DRAM mapping inversion.	Auto
Location of private memory regions	Select the location of the dedicated memory area in DRAM. Options: ● Auto ● Distributed ● Consolidated	Auto
CXL Memory interleaving	Enables or disables the CXL memory interleaving feature. Options: ● Auto. ● Enabled: enables the CXL memory interleaving feature.	Auto
Parameter	Description	Default
	● Disabled: disables the CXL memory device interleaving feature.	

CXL Sublink interleaving	Enables or disables the CXL sub-link interleaving feature. Options: • Auto. • Enabled: enables the CXL sub-link interleaving feature. • Disabled: disables the CXL sub-link interleaving feature.	Auto
--------------------------	---	------

ACPI

Figure 3-28 shows the **ACPI** screen.

Figure 3-28 ACPI Screen



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

Table 3-20 Parameter Descriptions for the ACPI Screen

Parameter	Description	Default
-----------	-------------	---------

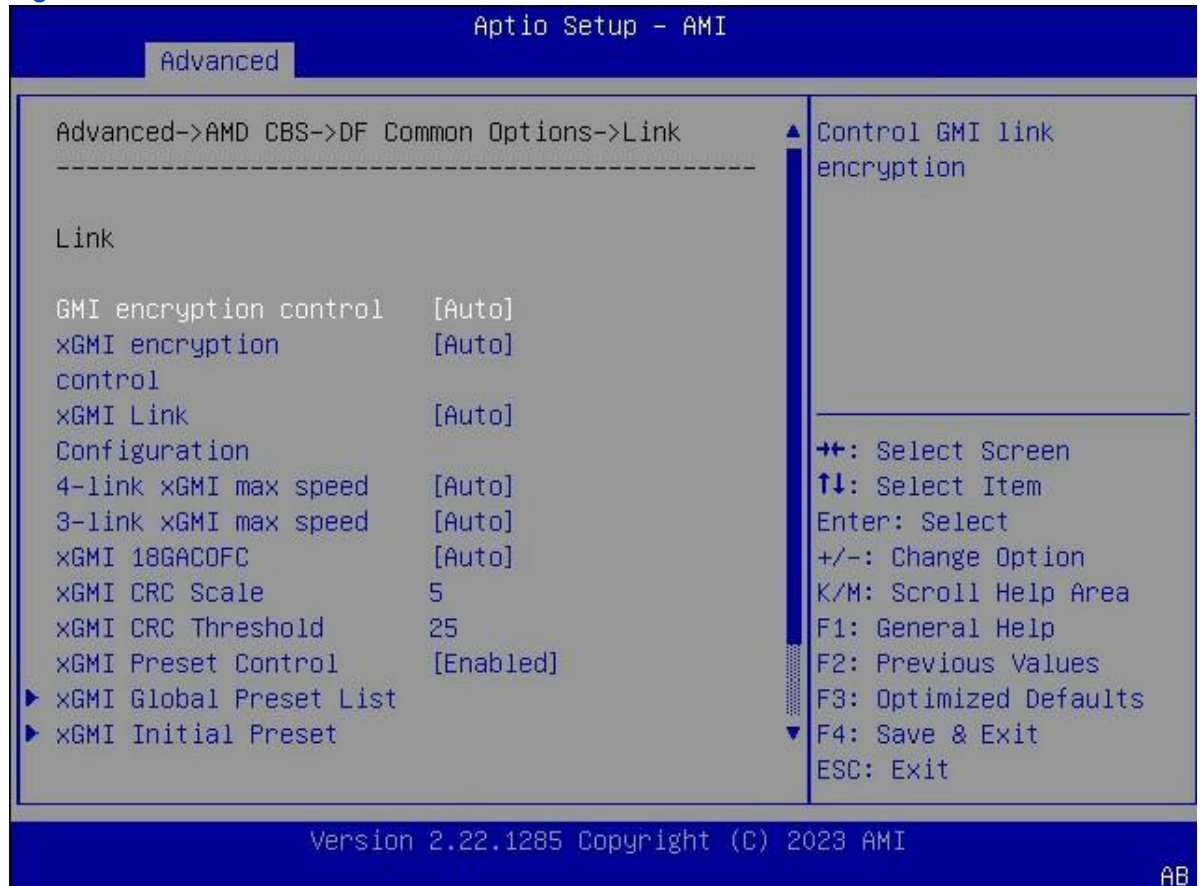
ACPI SRAT L3 Cache As NUMA Domain	Enables or disables the ACPI SRAT L3 cache as a NUMA domain. Options: ● Auto. ● Enabled: enables the ACPI SRAT L3 cache as a NUMA domain. ● Disabled: disables ACPI SRAT L3 cache as a NUMA domain.	Auto
CPI SLIT Distance Control	Select a declaration mode for ACPI SLIT distance control. Options: ● Auto ● Manual	Auto
ACPI SLIT same socket distance	This parameter is displayed when CPI SLIT Distance Control is set to Manual. Sets the distance to other physical domains within the same socket.	12
ACPI SLIT remote socket distance	This parameter is displayed when CPI SLIT Distance Control is set to Manual. Sets the distance to other physical domains on the remote socket.	32
ACPI SLIT local CXL distance	This parameter is displayed when CPI SLIT Distance Control is set to Manual. Sets the distance to a CXL domain on the same socket.	50
ACPI SLIT remote CXL distance	This parameter is displayed when CPI SLIT Distance Control is set to Manual. Sets the distance to a CXL domain on the other socket.	60
ACPI SLIT local inter-CXL distance	Displays the distance between the local CXLs in the ACPI SLIT.	255
ACPI SLIT remote inter-CXL distance	Displays the distance between remote Slinks in the ACPI SLIT.	255

ACPI SLIT remote relative distance	This parameter is displayed when CPI SLIT Distance Control is set to Auto . Select the remote relative distance in the ACPI SLIT. Options:	Auto
Parameter	Description	Default
	• Auto • Near • Far	

Link

Figure 3-29 shows the **Link** screen.

Figure 3-29 Link Screen



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

Table 3-21 Parameter Descriptions for the Link Screen

Parameter	Description	Default
-----------	-------------	---------

GMI encryption control	Enables or disables GMI link encryption. Options: ● Auto. ● Enabled: enables GMI link encryption. ● Disabled: disables GMI link encryption.	Auto
xGMI encryption control	Enables or disables xGMI link encryption. Options:	Auto

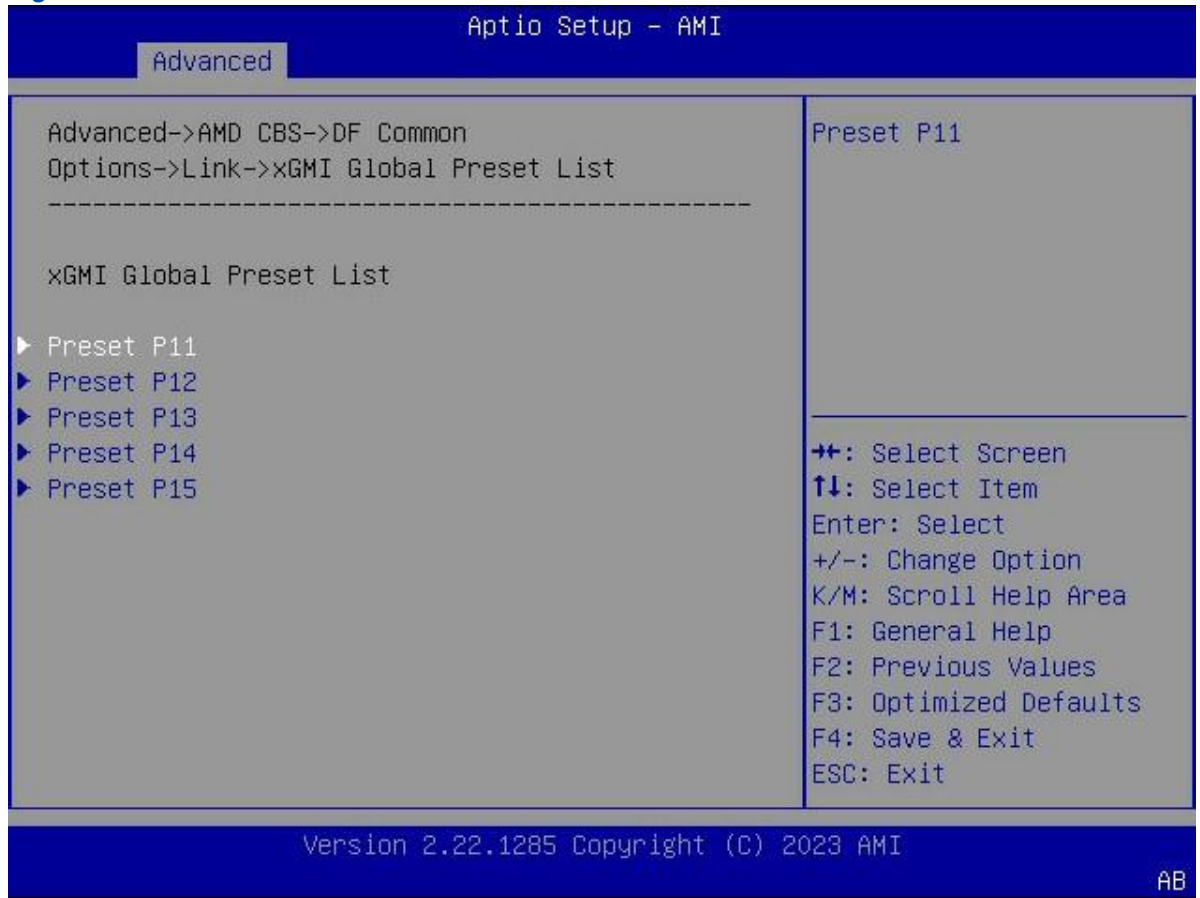
Parameter	Description	Default
	● Auto. ● Enabled: enables xGMI link encryption. ● Disabled: disables xGMI link encryption.	
xGMI Link Configuration	Sets the number of xGMI links used on a multi-core system. Options: ● Auto ● 3 xGMI Links ● 4 xGMI Links ● 2 xGMI Links + 2 PCI Links	Auto
4-link xGMI max speed	Select the maximum speed for a 4-link xGMI. Options: ● Auto ● 12 Gbps ● 16 Gbps ● 17 Gbps ● 18 Gbps ● 20 Gbps ● 22 Gbps ● 23 Gbps ● 24 Gbps ● 25 Gbps ● 26 Gbps ● 27 Gbps ● 30 Gbps ● 32 Gbps	Auto

3-link xGMI max speed	Sets the maximum speed for a 3-link xGMI. Options: ● Auto ● 12 Gbps ● 16 Gbps ● 17 Gbps ● 18 Gbps ● 20 Gbps ● 22 Gbps ● 23 Gbps ● 24 Gbps ● 25 Gbps ● 26 Gbps ● 27 Gbps ● 30 Gbps	Auto
-----------------------	--	------

Parameter	Description	Default
	● 32 Gbps	
xGMI 18GACOFc	Enables or disables the xGMI 18GACOFc feature. ● Auto. ● Enabled: enables the xGMI 18GACOFc feature. ● Disabled: disables the xGMI 18GACOFc feature.	Auto
xGMI CRC Scale	Sets leaky bucket scale for xGMI and WAFL CRC errors.	5
xGMI CRC Threshold	Sets the leaky bucket threshold for xGMI and WAFL CRC errors.	25
xGMI Preset Control	Enables or disables the xGMI preset control feature. Options: ● Auto. ● Enabled: enables the xGMI preset control feature. ● Disabled: disables the xGMI preset control feature.	Enabled
xGMI Global Preset List	Sets XGMI global preset list parameters. Press the Enter key. The xGMI Global Preset List screen is displayed, as shown in Figure 3-30 .	-

xGMI Initial Preset	Sets xGMI initial preset parameters. Press Enter . The xGMI Initial Preset screen is displayed, as shown in Figure 3-31 .	-
xGMI TXEQ Search Mask	Sets the parameters for the xGMI TXEQ search mask. Press the Enter key. The xGMI TXEQ Search Mask screen is displayed, as shown in Figure 3-32 .	-
xGMI AC/DC Coupled Link	Sets the parameters for xGMI AC/DC-coupled link technology. Press the Enter key. The xGMI AC/DC Coupled Link screen is displayed, as shown in Figure 3-33 through Figure 3-34 .	-
xGMI Channel Type	Sets xGMI channel type parameters. Press the Enter key. The xGMI Channel Type screen is displayed, as shown in Figure 3-35 through Figure 3-36 .	-

Figure 3-30 xGMI Global Preset List Screen



For a description of the parameters on the **xGMI Global Preset List** screen, refer to [Table 3-22](#).

Table 3-22 Parameter Descriptions for the xGMI Global Preset List Screen

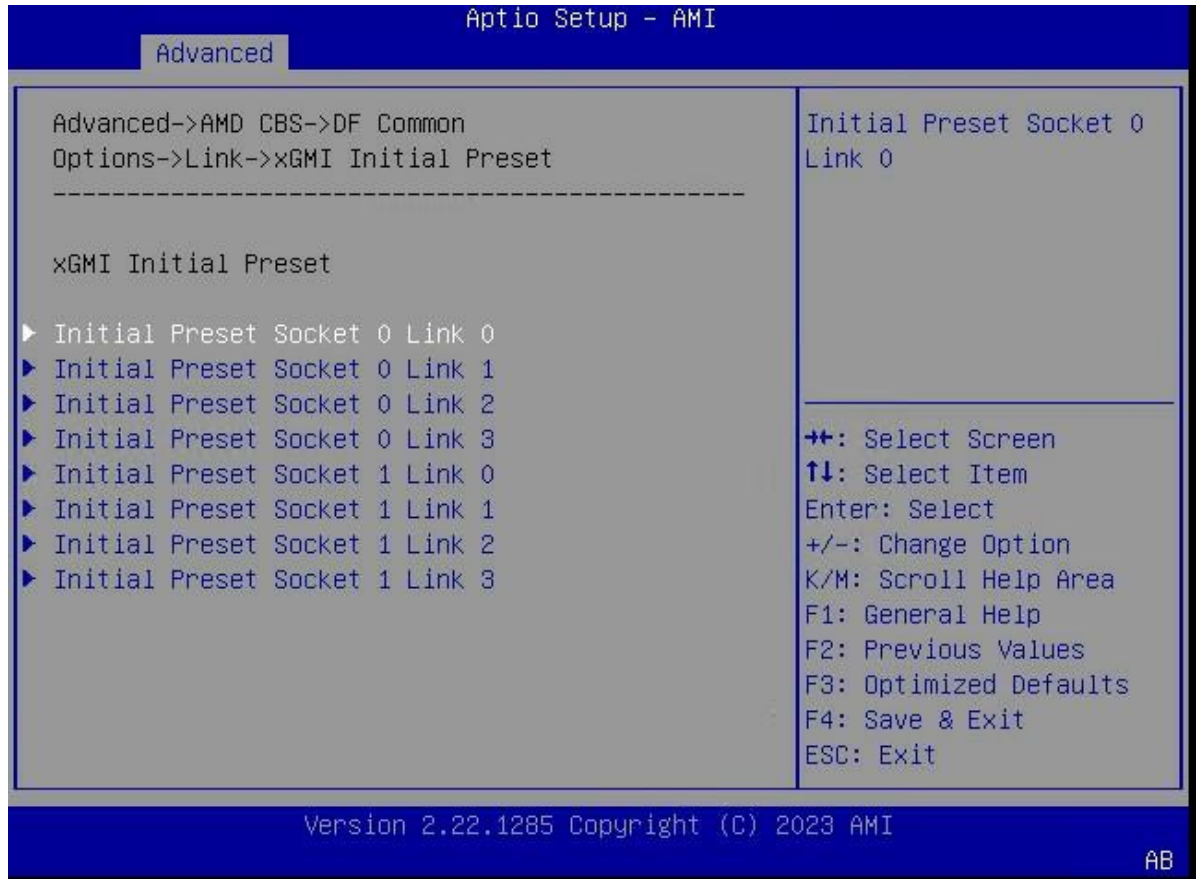
Parameter	Description
Preset P11	Sets preset P11 parameters. Press Enter . The Preset P11 screen is displayed. You can set the following parameters: ● Preset p11 (APCB). Default: 3000. ● Preset p11 Cmn1. Default: 0. ● Preset p11 Cn. Default: 30. ● Preset p11 Cmp1. Default: 0.
Preset P12	Sets preset P12 parameters.
Preset P13	Sets preset P13 parameters.
Preset P14	Sets preset P14 parameters.
Preset P15	Sets preset P15 parameters.



Note

The parameters of **Preset P12** and **Preset P12** are the same as those of **Preset P11**.

Figure 3-31 xGMI Initial Preset Screen



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

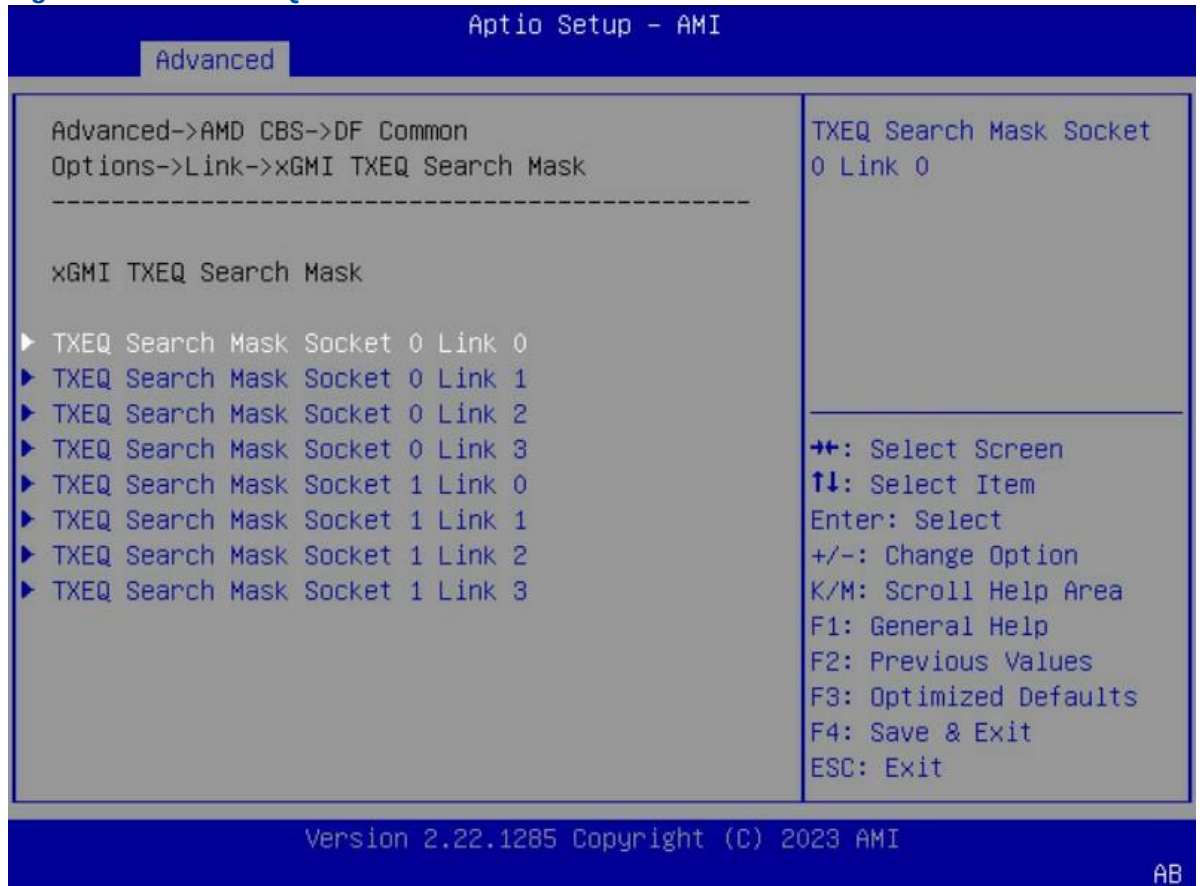
Table 3-23 Parameter Descriptions for the xGMI Initial Preset Screen

Parameter	Description
Initial Preset Socket 0 Link 0	Configure the parameters for initial preset socket 0 link 0. Press Enter . The Initial Preset Socket 0 Link 0 screen is displayed. You can set the following parameters: - Initial Preset Socket 0 Link 0 Pstate0/1/2/3 (APCB). Default: 4444. - Initial Preset Socket 0 Link 0 Pstate0. Default: Four. - Initial Preset Socket 0 Link 0 Pstate1. Default: Four. - Initial Preset Socket 0 Link 0 Pstate2. Default: Four. - Initial Preset Socket 0 Link 0 Pstate3. Default: Four.
Initial Preset Socket 0 Link 1	Sets the parameters for initial preset socket 0 link 1.
Initial Preset Socket 0 Link 2	Sets the parameters for initial preset socket 0 link 2.
Initial Preset Socket 0 Link 3	Sets the parameters for initial preset socket 0 link 3.
Parameter	Description

Initial Preset Socket 1 Link 0	Sets the parameters for initial preset socket 1 link 0.
Initial Preset Socket 1 Link 1	Sets the parameters for initial preset socket 1 link 1.
Initial Preset Socket 1 Link 2	Sets the parameters for initial preset socket 1 link 2.
Initial Preset Socket 1 Link 3	Sets the parameters for initial preset socket 1 link 3.

**Note**

The parameters of **Initial Preset Socket 0 Link 1** and **Initial Preset Socket 0 Link 2** are the same as those of **Initial Preset Socket 0 Link 0**.

Figure 3-32 xGMI TXEQ Search Mask Screen

For a description of the parameters on the **xGMI TXEQ Search Mask** screen, refer to [Table 3-24](#).

Table 3-24 Parameter Descriptions for the xGMI TXEQ Search Mask Screen

Parameter	Description
-----------	-------------

TEXQ Search Mask Socket 0 Link 0	Sets the parameters for TEXQ Search Mask Socket 0 Link 0.
Parameter	Description
	Press Enter. The TEXQ Search Mask Socket 0 Link 0 screen is displayed. You can set the following parameters: ● TEXQ Search Mask Socket 0 Link 0 Pstate 0. Default: 7A. ● TEXQ Search Mask Socket 0 Link 0 Pstate 1. Default: 7A. ● TEXQ Search Mask Socket 0 Link 0 Pstate 2. Default: 7A. ● TEXQ Search Mask Socket 0 Link 0 Pstate 3. Default: 7A.
TEXQ Search Mask Socket 0 Link 1	Sets the parameters for TEXQ Search Mask Socket 0 Link 1.
TEXQ Search Mask Socket 0 Link 2	Sets the parameters for TEXQ Search Mask Socket 0 Link 2.
TEXQ Search Mask Socket 0 Link 3	Sets the parameters for TEXQ Search Mask Socket 0 Link 3.
TEXQ Search Mask Socket 1 Link 0	Sets the parameters for TEXQ Search Mask Socket 1 Link 0.
TEXQ Search Mask Socket 1 Link 1	Sets the parameters for TEXQ Search Mask Socket 1 Link 1.
TEXQ Search Mask Socket 1 Link 2	Sets the parameters for TEXQ Search Mask Socket 1 Link 2.
TEXQ Search Mask Socket 1 Link 3	Sets the parameters for TEXQ Search Mask Socket 1 Link 3.

**Note**

Parameters of **TEXQ Search Mask Socket 0 Link 1** and **TEXQ Search Mask Socket 0 Link 2** are the same as those of **TEXQ Search Mask Socket 0 Link 0**.

Figure 3-33 xGMI AC/DC Coupled Link Screen—1

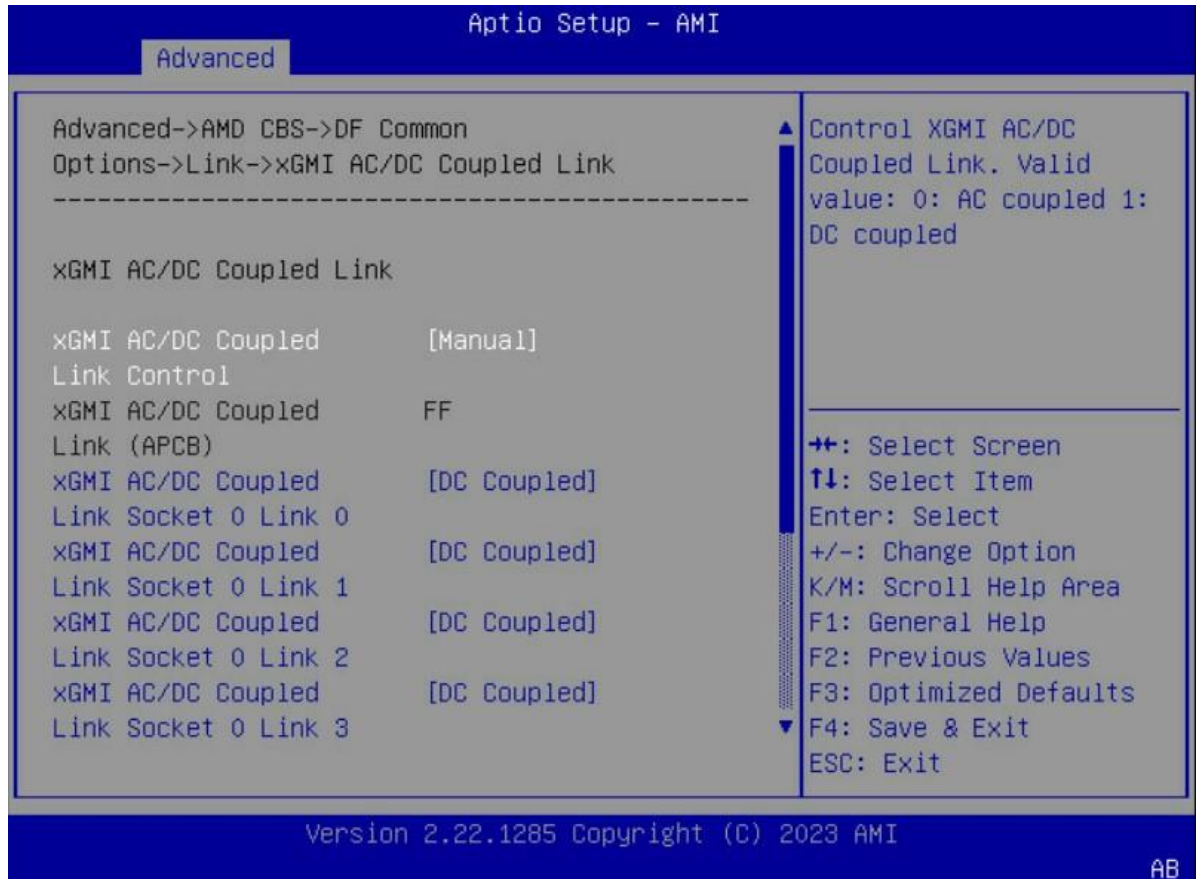
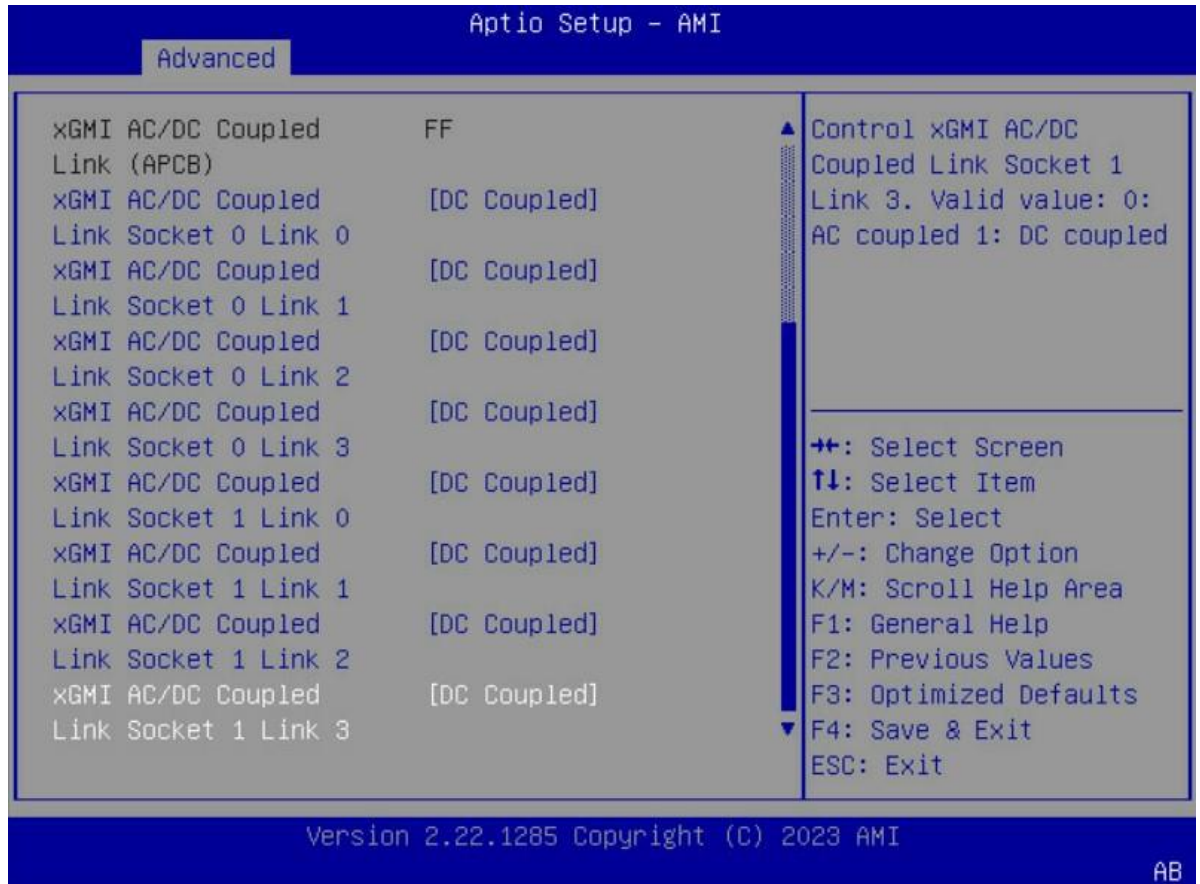


Figure 3-34 xGMI AC/DC Coupled Link Screen—2



For a description of the parameters on the **xGMI AC/DC Coupled Link** screen, refer to [Table 3-25](#).

Table 3-25 Parameter Descriptions for the xGMI AC/DC Coupled Link Screen

Parameter	Description	Default
xGMI AC/DC Coupled Link Control	Select xGMI AC/DC-coupled link control mode. Options: ● Auto ● Manual	Auto
xGMI AC/DC Coupled Link Socket 0 Link 0	This parameter is displayed when xGMI AC/DC Coupled Link Control is set to Manual . Select the coupling mode for xGMI AC/DC-coupled link Socket 0 Link 0. Options: ● DC Coupled ● AC Coupled	DC Coupled
xGMI AC/DC Coupled Link Socket 0 Link 1	This parameter is displayed when xGMI AC/DC Coupled Link Control is set to Manual .	DC Coupled

Parameter	Description	Default
	Select the coupling mode for xGMI AC/DC-coupled link Socket 0 Link 1. Options: ● DC Coupled ● AC Coupled	
xGMI AC/DC Coupled Link Socket 0 Link 2	This parameter is displayed when xGMI AC/DC Coupled Link Control is set to Manual . Select the coupling mode for xGMI AC/DC-coupled link Socket 0 Link 2. Options: ● DC Coupled ● AC Coupled	DC Coupled
xGMI AC/DC Coupled Link Socket 0 Link 3	This parameter is displayed when xGMI AC/DC Coupled Link Control is set to Manual . Select the coupling mode for xGMI AC/DC-coupled link Socket 0 Link 3. Options: ● DC Coupled ● AC Coupled	DC Coupled
xGMI AC/DC Coupled Link Socket 1 Link 0	This parameter is displayed when xGMI AC/DC Coupled Link Control is set to Manual . Select the coupling mode for xGMI AC/DC-coupled link Socket 1 Link 0. Options: ● DC Coupled ● AC Coupled	DC Coupled
xGMI AC/DC Coupled Link Socket 1 Link 1	This parameter is displayed when xGMI AC/DC Coupled Link Control is set to Manual . Select the coupling mode for xGMI AC/DC-coupled link Socket 1 Link 1. Options: ● DC Coupled ● AC Coupled	DC Coupled

xGMI AC/DC Coupled Link Socket 1 Link 2	This parameter is displayed when xGMI AC/DC Coupled Link Control is set to Manual . Select the coupling mode for xGMI AC/DC-coupled link Socket 1 Link 2. Options: • DC Coupled • AC Coupled	DC Coupled
Parameter	Description	Default
xGMI AC/DC Coupled Link Socket 1 Link 3	This parameter is displayed when xGMI AC/DC Coupled Link Control is set to Manual . Select the coupling mode for xGMI AC/DC-coupled link Socket 1 Link 3. Options: • DC Coupled • AC Coupled	DC Coupled

Figure 3-35 xGMI Channel Typet Screen—1

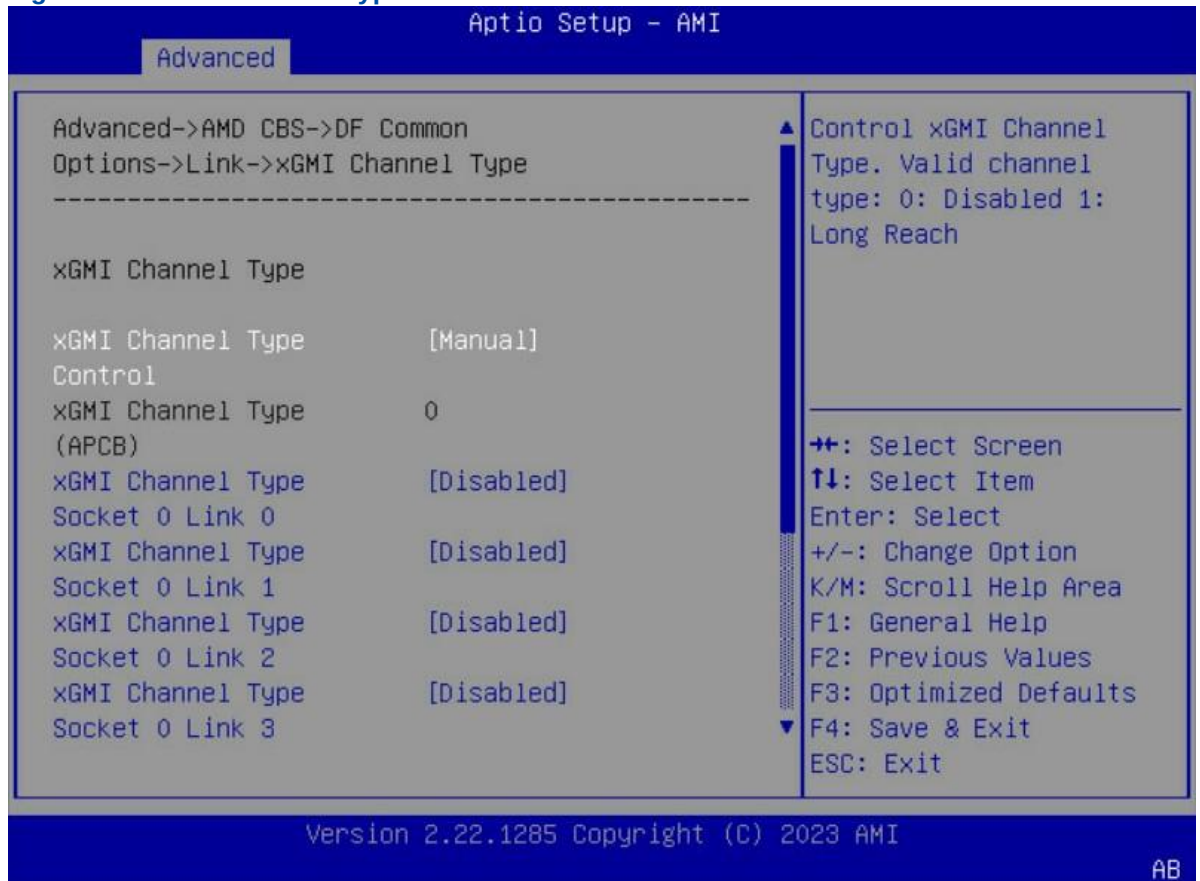
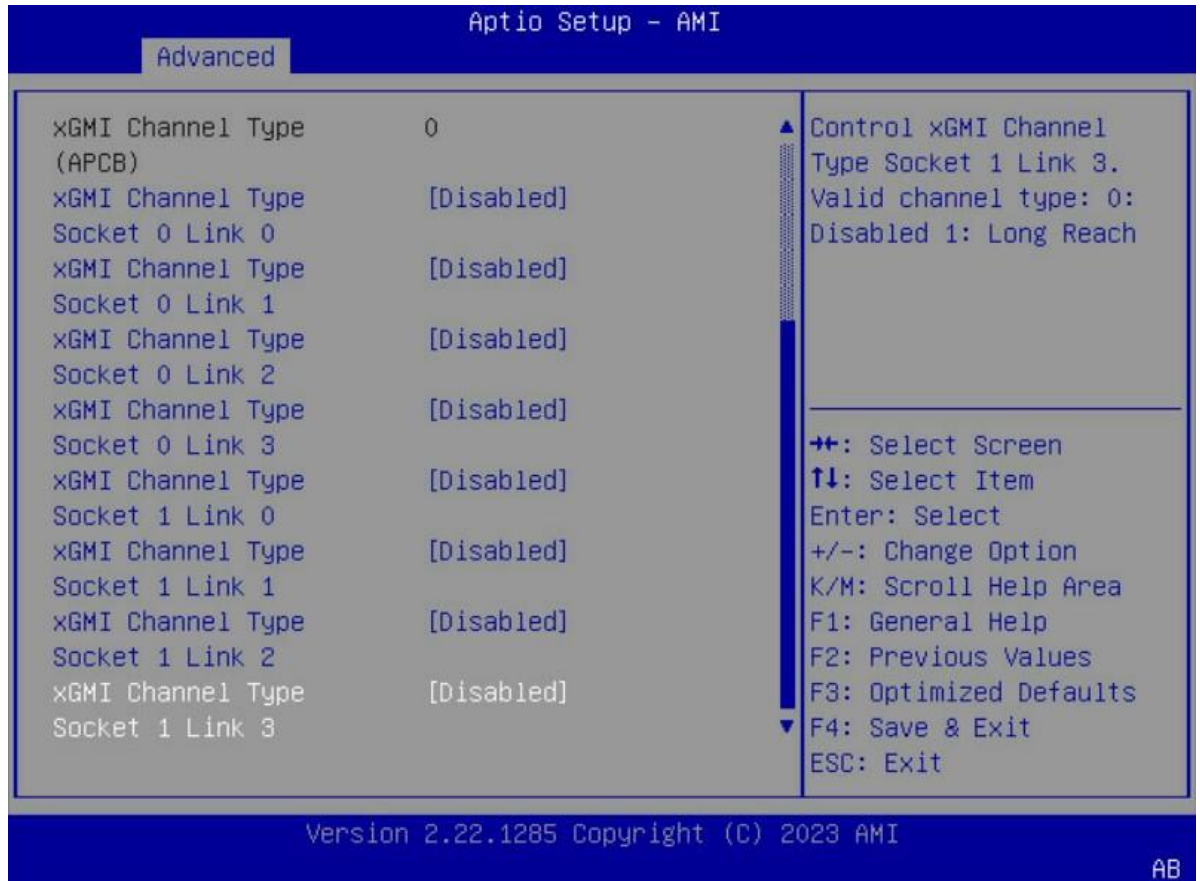


Figure 3-36 xGMI Channel Typet Screen—2



For a description of the parameters on the **xGMI Channel Typet** screen, refer to [Table 3-25](#).

Table 3-26 Parameter Descriptions for the xGMI Channel Typet Screen

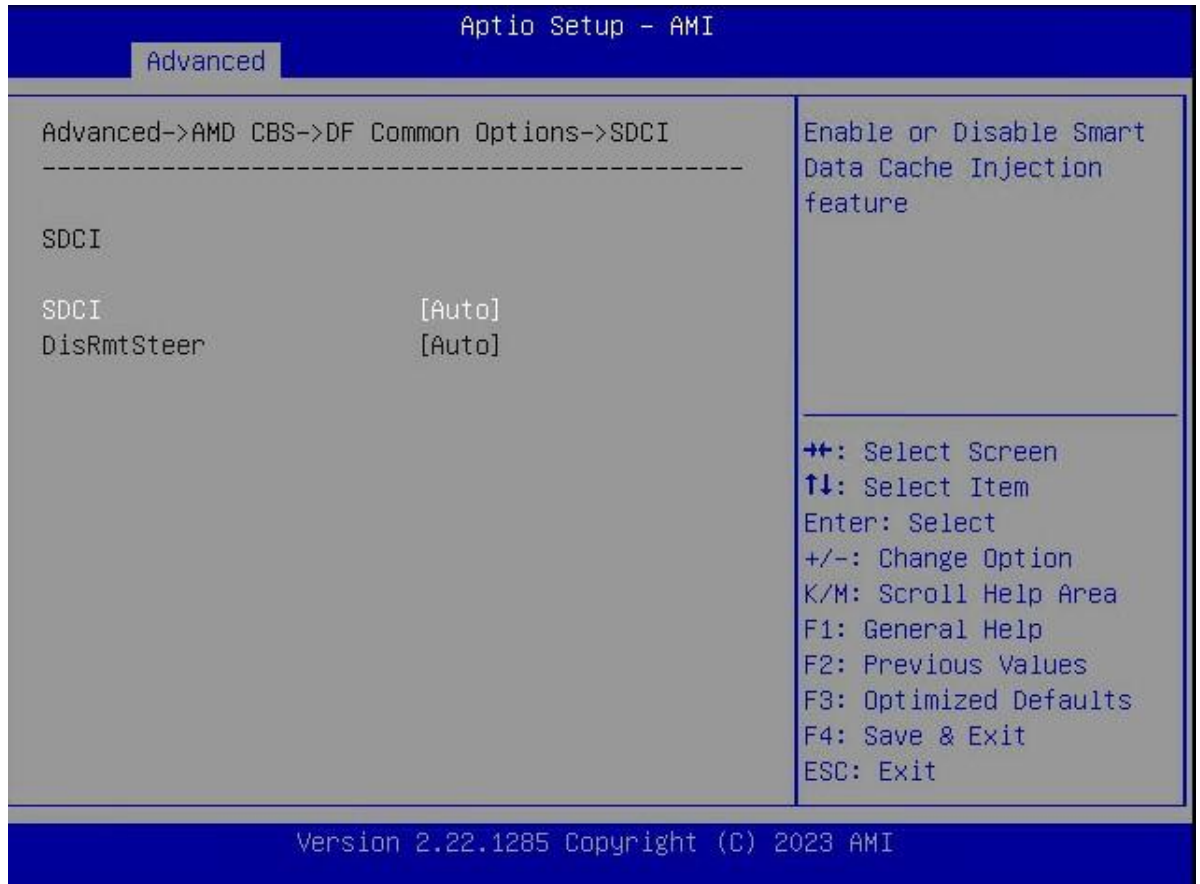
Parameter	Description	Default
xGMI Channel Type Control	Select the xGMI channel type. Options: • Auto • Manual	Auto
xGMI Channel Type (APCB)	Displays xGMI channel type (APCB) information.	0
xGMI Channel Type Socket 0 Link 0	Select a valid xGMI channel type for Socket 0 Link 0. Options: • Disabled • Long Reach	Disabled
xGMI Channel Type Socket 0 Link 1	Select the xGMI channel type for Socket 0 Link 1. Options: • Disabled • Long Reach	Disabled

Parameter	Description	Default
xGMI Channel Type Socket 0 Link 2	Select the xGMI channel type for Socket 0 Link 2. Options: ● Disabled ● Long Reach	Disabled
xGMI Channel Type Socket 0 Link 3	Select the xGMI channel type for Socket 0 Link 3. Options: ● Disabled ● Long Reach	Disabled
xGMI Channel Type Socket 1 Link 0	Select the xGMI channel type for Socket 1 Link 0. Options: ● Disabled ● Long Reach	Disabled
xGMI Channel Type Socket 1 Link 1	Select a valid xGMI channel type for Socket 1 Link 1. Options: ● Disabled ● Long Reach	Disabled
xGMI Channel Type Socket 1 Link 2	Select the xGMI channel type for Socket 1 Link 2. Options: ● Disabled ● Long Reach	Disabled
xGMI Channel Type Socket 1 Link 3	Select a valid xGMI channel type for Socket 1 Link 1. Options: ● Disabled ● Long Reach	Disabled

SDCI

Figure 3-37 shows the **SDCI** screen.

Figure 3-37 SDCI Screen



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

Table 3-27 Parameter Descriptions for the SDCI Screen

Parameter	Description	Default
SDCI	Enables or disables smart data cache injection. Options: ● Auto. ● Enabled: enables smart data cache injection. ● Disabled: disables smart data cache injection.	Auto
DisRmtSteer	This parameter can be configured when SDCI is set to Enabled . Enables or disables steering probe transmission to remote slots. Options: ● Auto. ● Enabled: disables steering probe transmission to remote slots. ● Disabled: enables steering probe transmission to remote slots.	Auto

Probe Filter

Figure 3-38 shows the **Probe Filter** screen.

Figure 3-38 Probe Filter Screen



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

Table 3-28 Parameter Descriptions for the Probe Filter Screen

Parameter	Description	Default
Organization	Select whether multiple memory/CXL channels share the probe filter storage. Options: ● Auto ● Dedicated ● Shared	Dedicated

Periodic Directory Rinse (PDR) Tuning	Select an option to control the performance-affected PDR settings by workload and/or processor. Options: ● Auto	Auto
Parameter	Description	Default
	● Memory-Sensitive ● Cache-Bound ● Neutral ● Adaptive	

3.2.7.3 UMC Common Options

UMC Common Options

Figure 3-39 shows the **UMC Common Options** screen.

Figure 3-39 UMC Common Options Screen



For a description of the parameters on the **UMC Common Options** screen, refer to [Table 3-29](#).

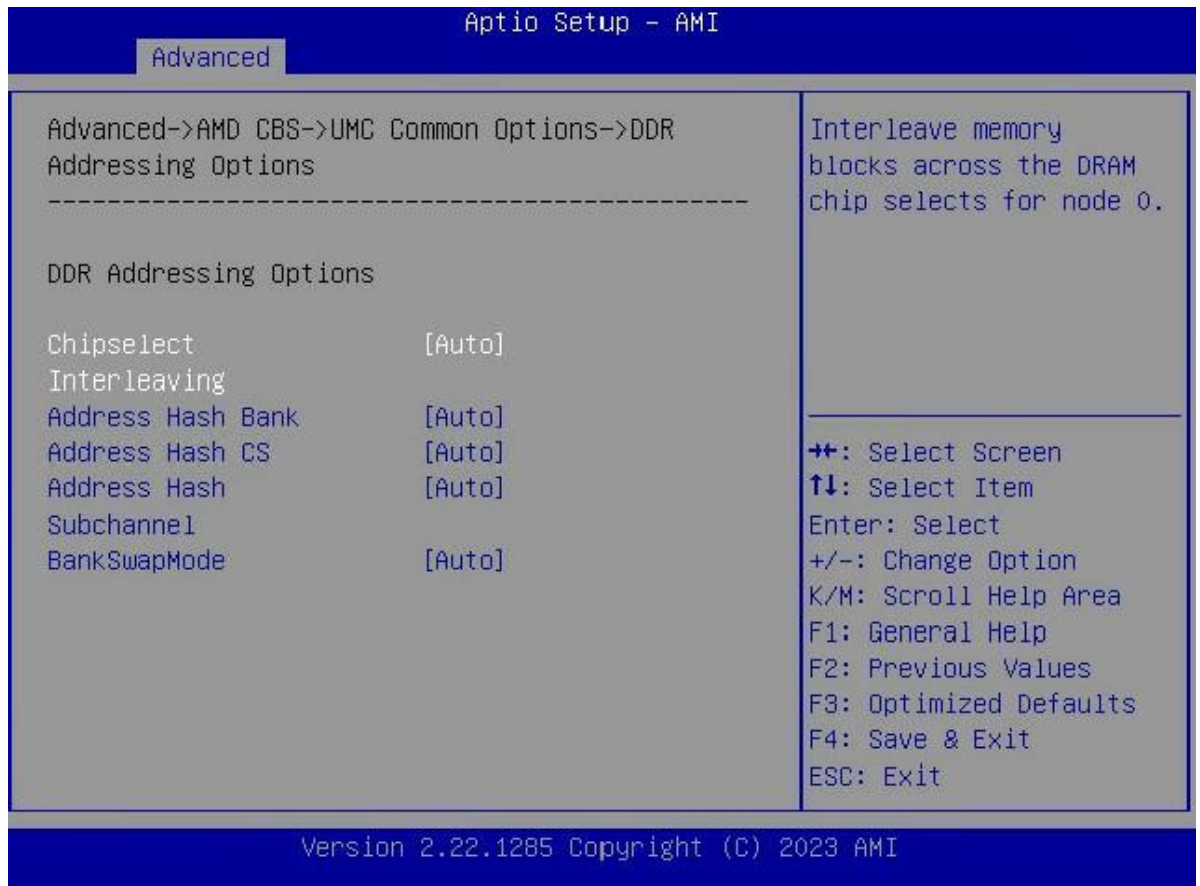
Table 3-29 Parameter Descriptions for the UMC Common Options Screen

Parameter	Description
DDR Addressing Options	Sets parameters for DDR addressing options. For details, refer to DDR Addressing Options .
DDR Controller Configuration	Sets DDR controller parameters. For details, refer to DDR Controller Configuration .
Parameter	Description
DDR MBIST Options	Sets parameters for DDR MBIST options. For details, refer to DDR MBIST Options .
DDR RAS	Sets DDR RAS parameters. For details, refer to DDR RAS .
DDR Bus Configuration	Sets DDR bus parameters. For details, refer to DDR Bus Configuration .
DDR Timing Configuration	Sets DDR timing parameters. For details, refer to DDR Timing Configuration .
DDR Training Options	Sets parameters for DDR training options. For details, refer to DDR Training Options .
DDR Security	Sets the HDD security parameters. For details, refer to DDR Security .
DDR PMIC Configuration	Sets DDR PMIC parameters. For details, refer to DDR PMIC Configuration .
DDR Miscellaneous	Sets other DDR parameters. For details, refer to DDR Miscellaneous .
DDR PHY (CMN)	Sets DDR PHY (CMN) parameters. For details, refer to DDR PHY (CMN) .

DDR Addressing Options

[Figure 3-40](#) shows the **DDR Addressing Options** screen.

[Figure 3-40 DDR Addressing Options Screen](#)



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

Table 3-30 Parameter Descriptions for the DDR Addressing Options Screen

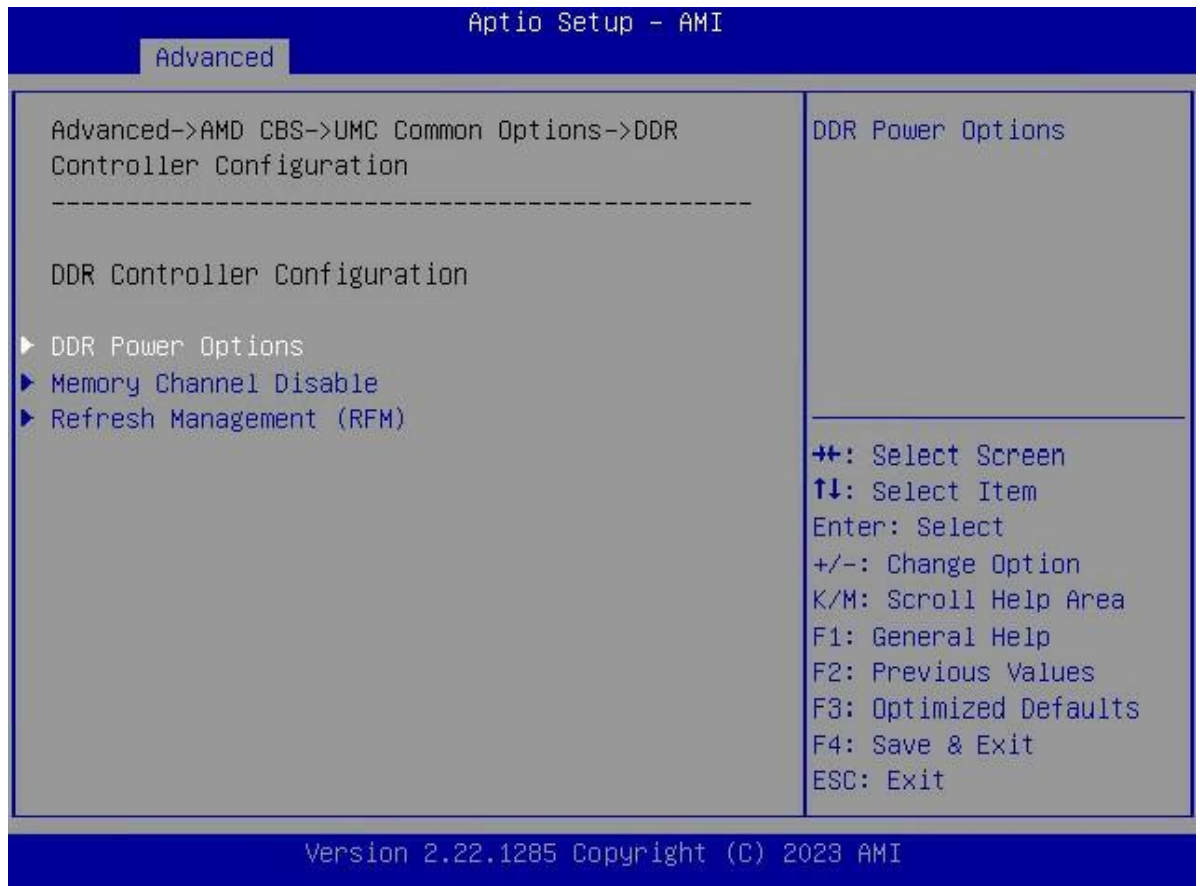
Parameter	Description	Default
Chipselect Interleaving	Enables or disables interleaved memory block selection for Node 0 across DRAM chips. Options: ● Auto: enables interleaved memory block selection for Node 0 across DRAM chips. ● Disabled: disables interleaved memory block selection for Node 0 across DRAM chips.	Disabled
Address Hash Bank	Enables or disables the address hash bank. Options: ● Auto.	Auto

Parameter	Description	Default
	● Enabled: enables the address hash bank. ● Disabled: disables the address hash bank.	
Address Hash CS	Enables or disables address hash CS. Options: ● Auto. ● Enabled: enables address hash CS. ● Disabled: disables address hash CS.	Auto
Address Hash Subchannel	Enables or disables the address hash subchannel. Options: ● Auto. ● Enabled: enables the address hash subchannel. ● Disabled: disables the address hash subchannel.	Auto
BankSwapMode	Sets the bank swapping mode. Options: ● Auto ● Disabled ● Swap CPU	Auto

DDR Controller Configuration

Figure 3-41 shows the **DDR Controller Configuration** screen.

Figure 3-41 DDR Controller Configuration Screen

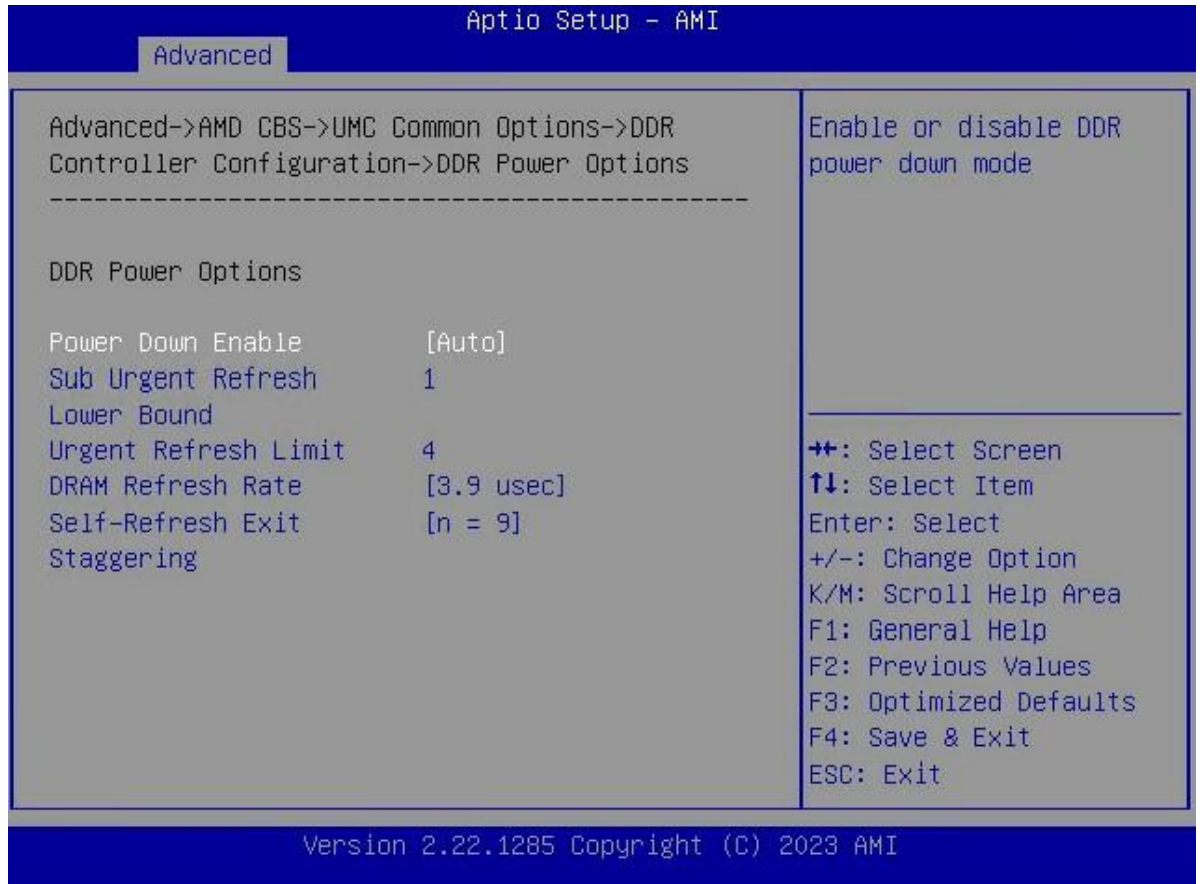


For a description of the parameters on the **DDR Controller Configuration** screen, refer to [Table 3-31](#).

Table 3-31 Parameter Descriptions for the DDR Controller Configuration Screen

Parameter	Description
DDR Power Options	Sets parameters for DDR power options. Press Enter . The DDR Power Options screen is displayed, as shown in Figure 3-42 .
Memory Channel Disable	Sets parameters for disabling a memory channel. Press the Enter key. The Memory Channel Disable screen is displayed, as shown in Figure 3-43 through Figure 3-44 .
Refresh Management (RFM)	Sets refresh management parameters. Press the Enter key. The Refresh Management (RFM) screen is displayed, as shown in Figure 3-45 .

Figure 3-42 DDR Power Options Screen



For a description of the parameters on the **DDR Power Options** screen, refer to [Table 3-32](#).

Table 3-32 Parameter Descriptions for the DDR Power Options Screen

Parameter	Description	Default
Power Down Enable	Enables or disables DDR power-down mode. Options: • Auto. • Enabled: enables DDR power-down mode. • Disabled: disables DDR power-down mode.	Auto
Sub Urgent Refresh Lower Bound	Sets the storage refresh limit required to enter sub-emergency refresh mode.	1
Urgent Refresh Limit	Sets the storage refresh limit required to enter emergency refresh mode.	4
DRAM Refresh Rate	Sets the DRAM refresh rate.	3.9 usec

Self-Refresh Exit Staggering	Sets the self-refresh exit staggering parameters. Options: • Disabled • n = 1	n = 9
Parameter	Description	Default
	• n = 2 • n = 3 • n = 4 • n = 5 • n = 6 • n = 7 • n = 8 • n = 9	

Figure 3-43 Memory Channel Disable Screen—1

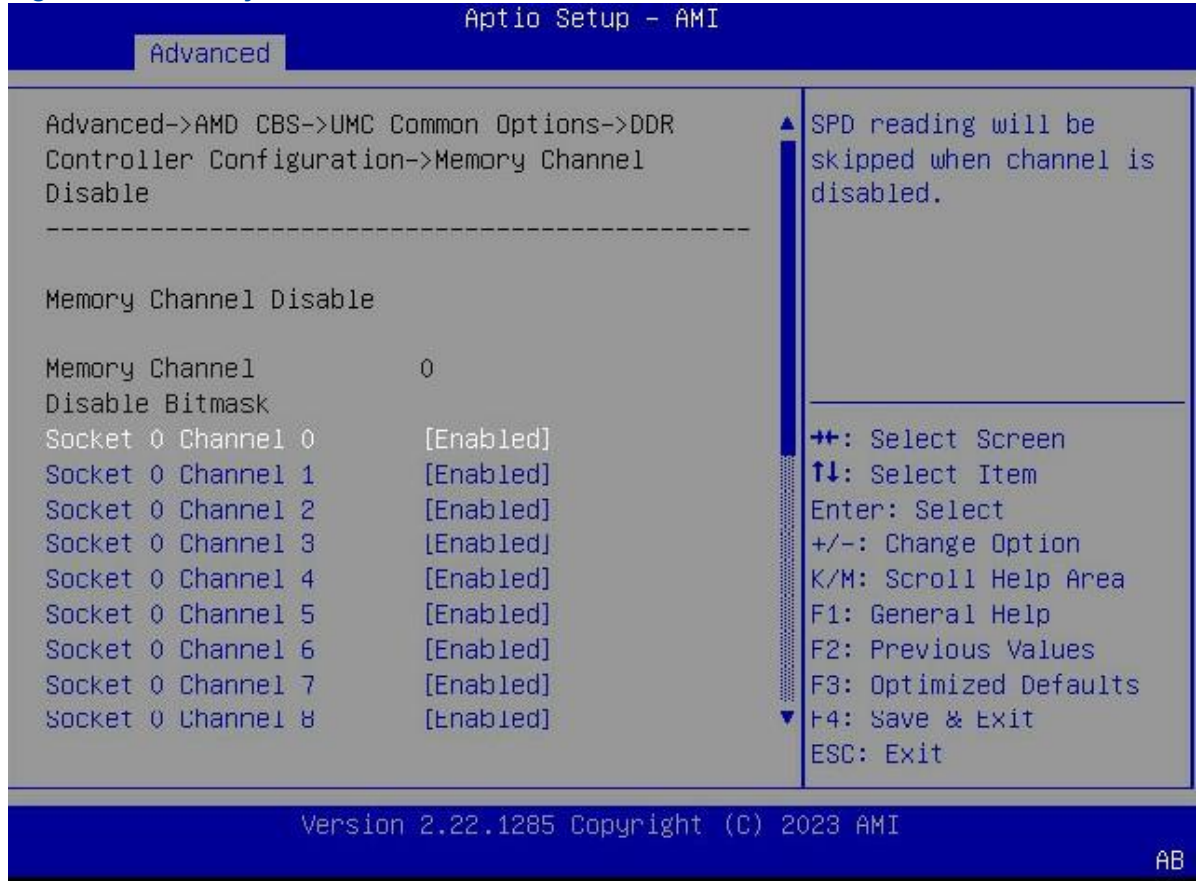
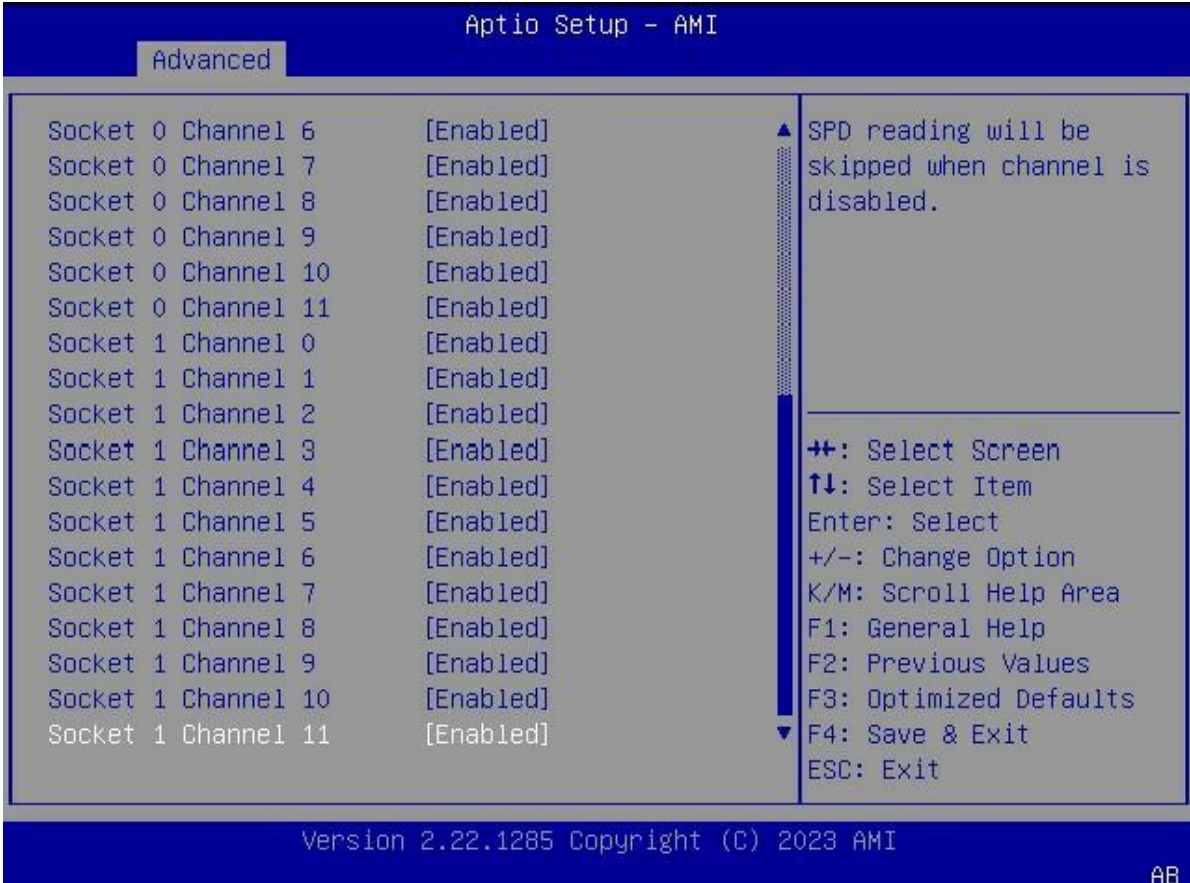


Figure 3-44 Memory Channel Disable Screen—2



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

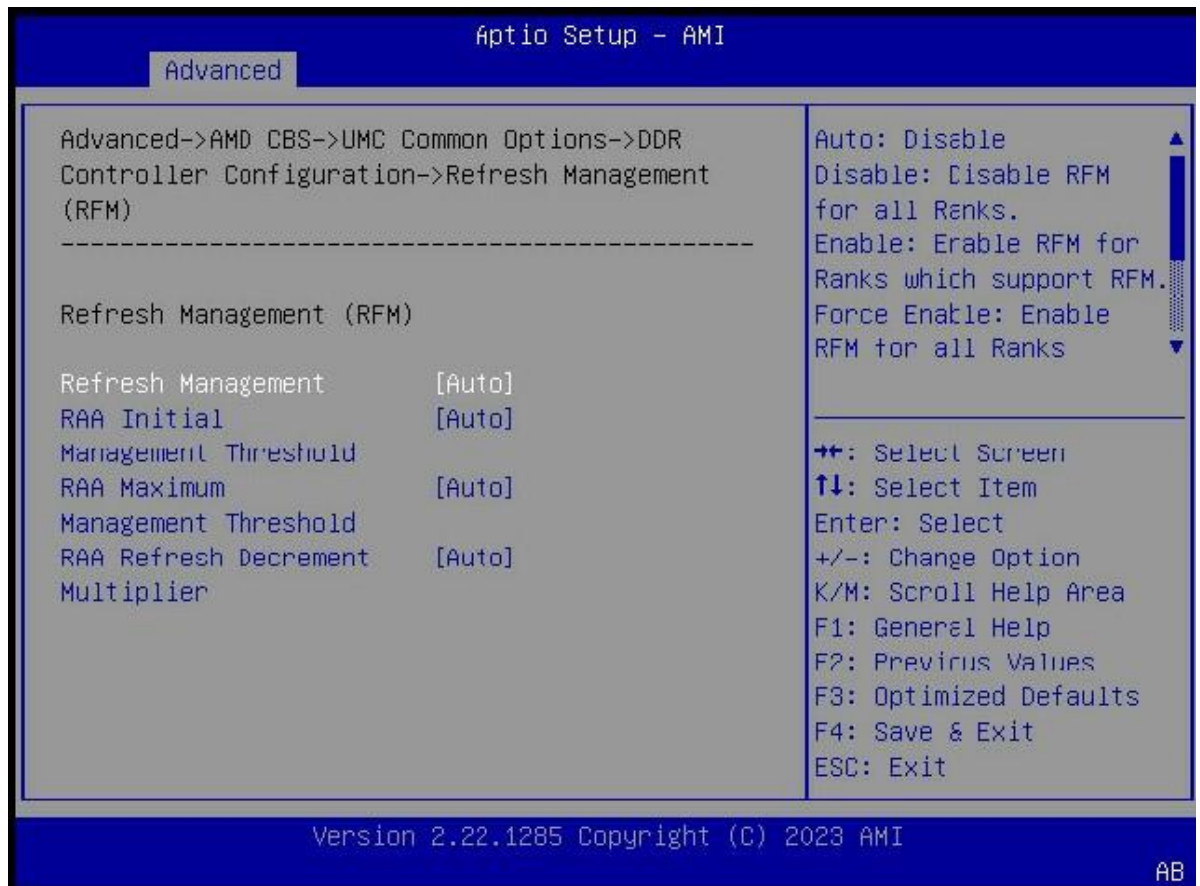
 Note

Socket 0 Channel 0 is used as an example.

Table 3-33 Parameter Descriptions for the Memory Channel Disable Screen

Parameter	Description	Default
Socket 0 Channel 0	Enables or disables the channel. Options: - Enabled: enables the channel. - Disabled: disables the channel. When this parameter is set to Disabled, the channel skips the reading of SPD information.	Enabled

Figure 3-45 Refresh Management (RFM) Screen



For a description of the parameters on the **Refresh Management (RFM)** screen, refer to [Table 3-34](#).

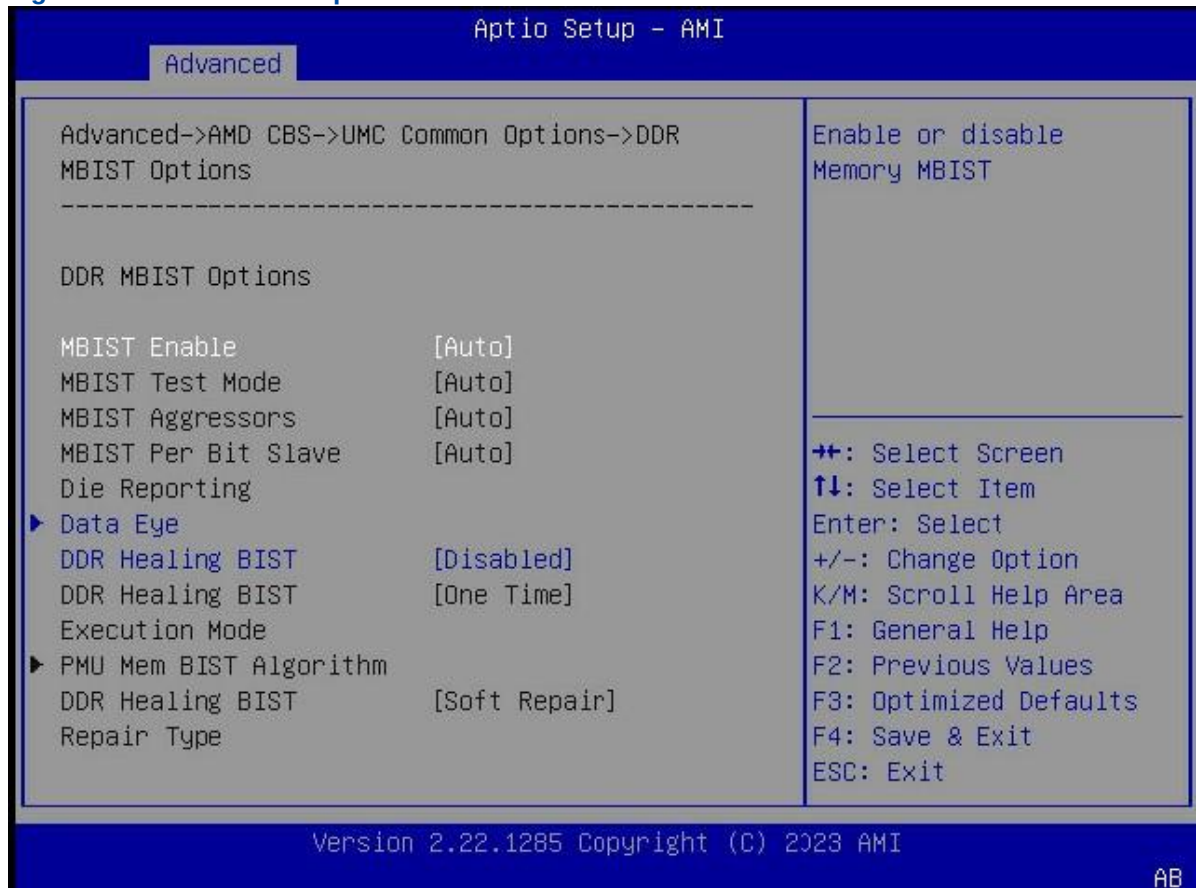
Table 3-34 Parameter Descriptions for the Refresh Management (RFM) Screen

Parameter	Description	Default
Refresh Management	Select the refresh management mode. Options: ● Auto Calls: disables refresh management. ● Disable: disables RFM for all rankings. ● Enable: enables RFM for RFM-enabled rankings. ● Force Enable: enables RFM for all rankings forcibly.	Auto
RAA Initial Management Threshold	Select the initial RAA management threshold. Options: ● Auto: The BIOS selects the minimum supported value from the SPD. ● 32 ● 40 ● 48 ● 56	Auto

Parameter	Description	Default
	● 64 ● 72 ● 80	
RAA Maximum Management Threshold	Select the highest RAA management threshold. Options: ● Auto: The BIOS selects the minimum supported value from the SPD. ● 3X ● 4X ● 5X ● 6X	Auto
RAA Refresh Decrement Multiplier	Select the RAA refresh decrement multiplier. Options: ● Auto ● 0.5 ● 1	Auto

DDR MBIST Options

Figure 3-46 shows the **DDR MBIST Options** screen.

Figure 3-46 DDR MBIST Options Screen

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

Table 3-35 Parameter Descriptions for the DDR MBIST Options Screen

Parameter	Description	Default
MBIST Enable	Enables or disables the MBIST feature. - Auto. - Enabled: enables the MBIST feature. - Disabled: disables the MBIST feature.	Auto
MBIST Test Mode	This parameter can be configured when MBIST Enable is set to Enabled . Select the MBIST mode. Options: - Auto - Interface Mode - Data Eye Mode - Both	Auto
MBIST Aggressors	This parameter can be configured when MBIST Enable is set to Enabled .	Auto

Parameter	Description	Default
	Enables or disables the MBIST Aggressors test feature. Options: ● Auto. ● Enabled: enables the MBIST Aggressors test feature. ● Disabled: disables the MBIST Aggressors test feature.	
MBIST Per Bit Slave Die Reporting	This parameter can be configured when MBIST Enable is set to Enabled. Enables or disables the reporting of 2D Data Eye results in ABL log for each DQ, Chipselect, and channel. Options: ● Auto. ● Enabled: enables the reporting of 2D Data Eye results in ABL log for each DQ, Chipselect, and channel. ● Disabled: disables the reporting of 2D Data Eye results in ABL log for each DQ, Chipselect, and channel.	Auto
Data Eye	Sets data eye parameters. Press Enter. The Data Eye screen is displayed, as shown in Figure 3-47 through Figure 3-49.	-
DDR Healing BIST	Select the memory healing BIST mode. Options: ● Disabled ● PMU Mem BIST ● Self-Healing Mem BIST ● PMU and Self-Healing Mem BIST	Disabled

DDR Healing BIST Execution Mode	This parameter can be configured when DDR Healing BIST is set to PMU Mem BIST, SelfHealing Mem BIST, or PMU and Self-Healing Mem BIST. Select the execution mode for DDR healing BIST. Options: ● One Time: only executes DDR healing BIST once. ● Every Boot: executes DDR healing BIST during each boot process.	One Time
Parameter	Description	Default
PMU Mem BIST Algorithm	This parameter can be configured when DDR Healing BIST is set to PMU Mem BIST or PMU and Self-Healing Mem BIST. This parameter sets the parameters for the PMU MEM BIST algorithm. Press the Enter key. The PMU Mem BIST Algorithm screen is displayed, as shown in Figure 3-50.	-
DDR Healing BIST Repair Type	This parameter can be configured when DDR Healing BIST is set to PMU Mem BIST or PMU and Self-Healing Mem BIST. Select the execution mode for DDR healing BIST. Options: ● Soft Repair ● Hard Repair ● No Repair - Test only	Soft Repair

Figure 3-47 Data Eye Screen—1



Figure 3-48 Data Eye Screen—2

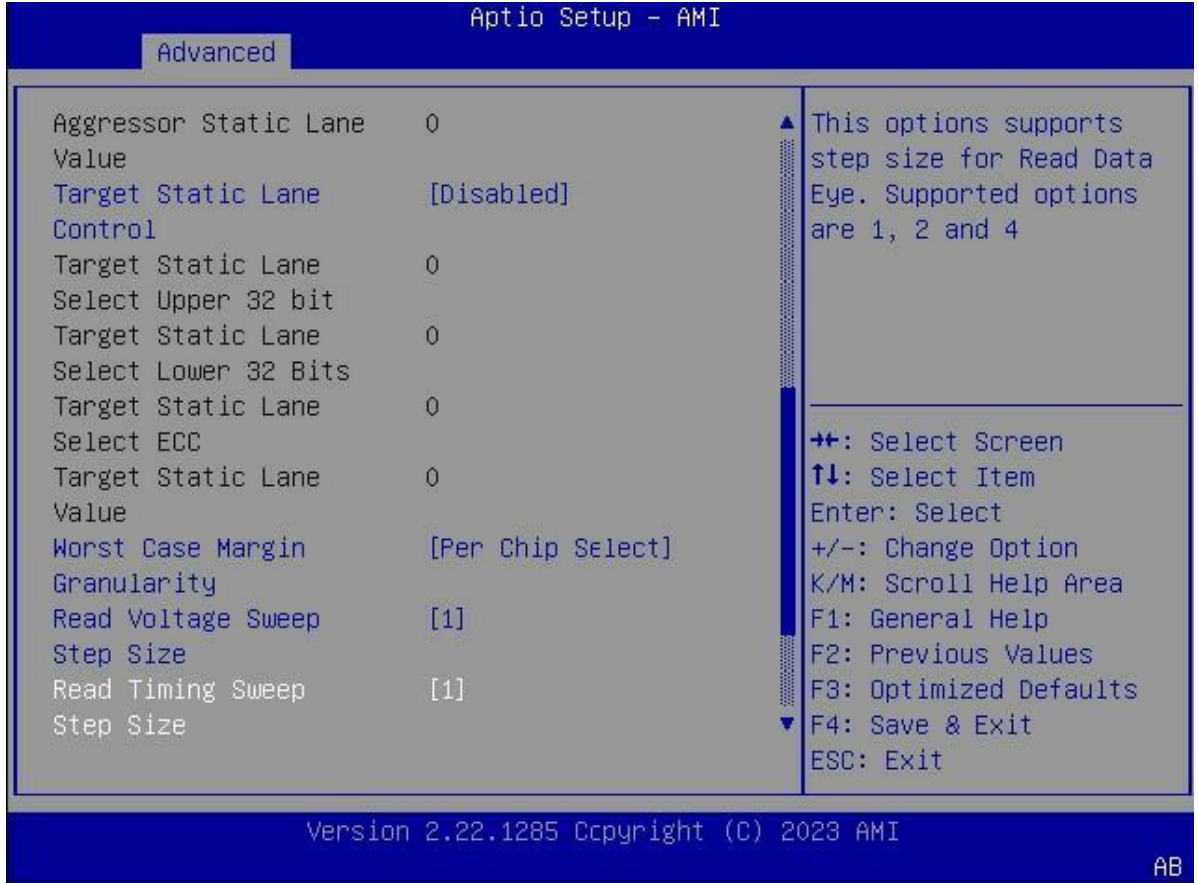


Figure 3-49 Data Eye Screen—3



For a description of the parameters on the **Data Eye** screen, refer to [Table 3-36](#).

Table 3-36 Parameter Descriptions for the Data Eye Screen

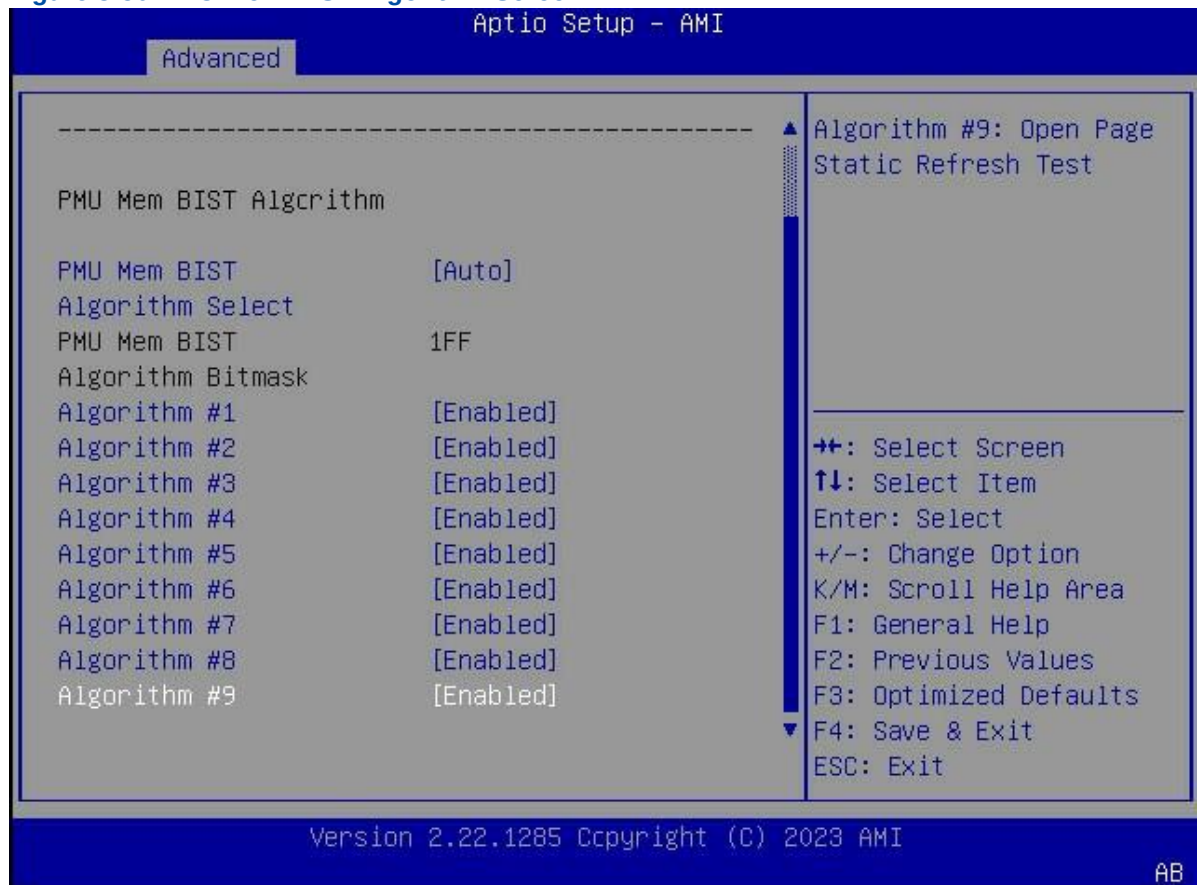
Parameter	Description	Default
Pattern Select	Select a pattern. Options: ● PRBS ● SSO ● Both	PRBS
Pattern Length	Sets the pattern length.	3
Aggressor Channel	Select the Aggressor channel. Options: ● One Sub-Channel ● Half Channels ● All Channels	All Channels
Aggressor Static Lane Control	Enables or disables the Aggressor Static Lane Control feature. Options:	Disabled

Parameter	Description	Default
	- Enabled: enables the Aggressor Static Lane Control feature. - Disabled: disables the Aggressor Static Lane Control feature.	
Aggressor Static Lane Select Upper 32 bit	This parameter can be configured when Aggressor Static Lane Control is set to Enabled . This parameter sets the upper 32 bits for Aggressor Static Lane Selection. The bit mask represents the bits to be read.	0
Aggressor Static Lane Select Lower 32 bit	This parameter can be configured when Aggressor Static Lane Control is set to Enabled . This parameter sets the lower 32 bits for Aggressor Static Lane Selection. The bit mask represents the bits to be read.	0
Aggressor Static Lane Select ECC	This parameter can be configured when Aggressor Static Lane Control is set to Enabled . This parameter sets Aggressor Static Lane Selection for the ECC channel. The bit mask represents the bits to be read.	0
Aggressor Static Lane Value	This parameter can be configured when Aggressor Static Lane Control is set to Enabled . This parameter sets the Aggressor Static Lane value. The bit mask represents the bits to be read.	0
Target Static Lane Control	Enables or disables the Target Static Lane Control feature. Options: - Enabled: enables the Target Static Lane Control feature. - Disabled: disables the Target Static Lane Control feature.	Disabled
Target Static Lane Select Upper 32 bit	This parameter can be configured when Target Static Lane Control is set to Enabled. This parameter sets the upper 32 bits for Target Static Lane Selection. The bit mask indicates the bit to be read.	0

Target Static Lane Select Lower 32 bit	This parameter can be configured when Target Static Lane Control is set to Enabled .	0
--	--	---

Parameter	Description	Default
	This parameter sets the lower 32 bits for Target Static Lane Selection. The bit mask indicates the bit to be read.	
Target Static Lane Select ECC	This parameter can be configured when Target Static Lane Control is set to Enabled . This parameter sets Target Static Lane Selection for the ECC channel. The bit mask indicates the bit to be read.	0
Target Static Lane Value	This parameter can be configured when Target Static Lane Control is set to Enabled . This parameter sets the target static lane value. The bit mask indicates the bit to be read.	0
Worst Case Margin Granularity	Select the worst-case margin granularity. Options: ● Per Chip Select ● Per Nibble	Per Chip Select
Read Voltage Sweep Step Size	Select the step size for Read Data Eye voltage sweep. Options: ● 1 ● 2 ● 4	1
Read Timing Sweep Step Size	Select the step size for Read Data Eye. Options: ● 1 ● 2 ● 4	1
Write Voltage Sweep Step Size	Select the step size for Write Data Eye voltage sweep. Options: ● 1 ● 2 ● 4	1

Write Timing Sweep Step Size	Select the step size for Write Data Eye. Options: • 1 • 2 • 4	1
Silent Execution	Enables or disables the silent execution feature.	Disabled
Parameter	Description	Default
	Options: • Enabled: enables the silent execution feature. • Disabled: disables the silent execution feature.	

Figure 3-50 PMU Mem BIST Algorithm Screen

For a description of the parameters on the **PMU Mem BIST Algorithm** screen, refer to [Table 3-37](#).

Table 3-37 Parameter Descriptions for the PMU Mem BIST Algorithm Screen

Parameter	Description	Default
-----------	-------------	---------

PMU Mem BIST Algorithm Select	Select a PMU Mem BIST algorithm configuration mode. Options: ● Auto ● By User: The PMU Mem BIST algorithm is configured in accordance with the user-configured parameters.	Auto
-------------------------------	---	------

Parameter	Description	Default
	● By Vendor: The PMU Mem BIST algorithm is configured in accordance with the parameters configured by the vendor. After PMU Mem BIST Algorithm Select is set to By Vendor, the parameters below are hidden.	
PMU Mem BIST Algorithm Bitmask	Displays the bitmask for the PMU Mem BIST algorithm.	1FF
Algorithm #1	Enables or disables the Write-Pause-Read feature. Options: ● Enabled: enables the Write-Pause-Read feature. ● Disabled: disables the Write-Pause-Read feature.	Enabled
Algorithm #2	Enables or disables the Write-Pause-Read-ShorttWR feature. Options: ● Enabled: enables the Write-Pause-Read-ShorttWR feature. ● Disabled: disables the Write-Pause-ReadShorttWR feature.	Enabled
Algorithm #3	Enables or disables the Row Victim Aggressor feature. Options: ● Enabled: enables the Row Victim Aggressor feature. ● Disabled: disables the Row Victim Aggressor feature.	Enabled

Algorithm #4	Enables or disables the Write-Pause-Read-PageClosure feature. Options: ● Enabled: enables the Write-Pause-Read-ClosePage feature. ● Disabled: disables the Write-Pause-ReadClose-Page feature.	Enabled
Algorithm #5	Enables or disables the stress test during page closure. Options: ● Enabled: enables the stress test during page closure.	Enabled
Parameter	Description	Default
	● Disabled: disables the stress test during page closure.	
Algorithm #6	Enables or disables the Double Row Victim Aggressor feature. Options: ● Enabled: enables the Double Row Victim Aggressor feature. ● Disabled: disables the Double Row Victim Aggressor feature.	Enabled
Algorithm #7	Enables or disables the Checkerboard RMW feature when a page is open. Options: ● Enabled: enables the Checkerboard RMW feature when a page is open. ● Disabled: disables the Checkerboard RMW feature when a page is open.	Enabled
Algorithm #8	Enables or disables the tWR stress feature during page closure. Options: ● Enabled: enables the tWR stress feature during page closure. ● Disabled: disables the tWR stress feature during page closure.	Enabled

Algorithm #9	Enables or disables the static refresh test when a page is open. Options: • Enabled: enables the static refresh test when a page is open. • Disabled: disables the static refresh test when a page is open.	Enabled
--------------	--	---------

DDR RAS

Figure 3-51 through Figure 3-52 show the **DDR RAS** screen.

Figure 3-51 DDR RAS Screen—1

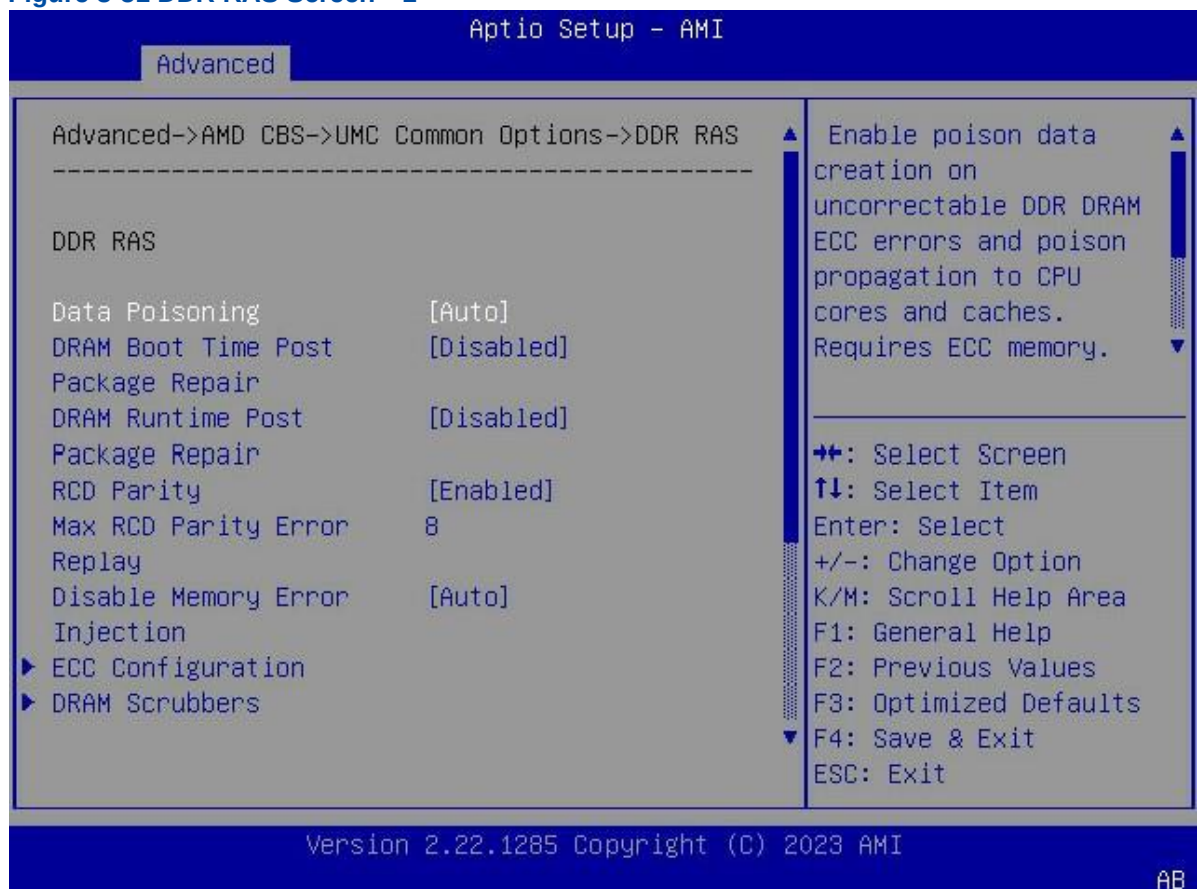
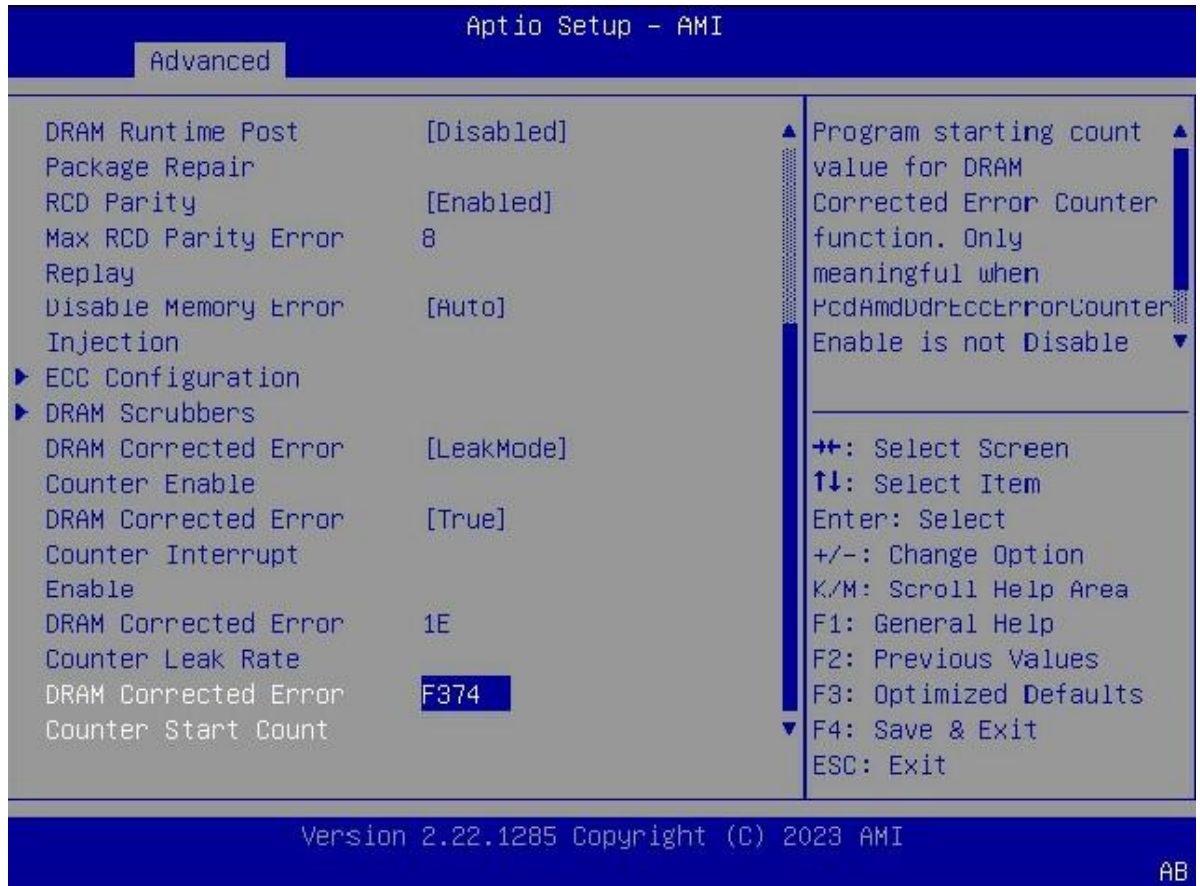


Figure 3-52 DDR RAS Screen—2



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

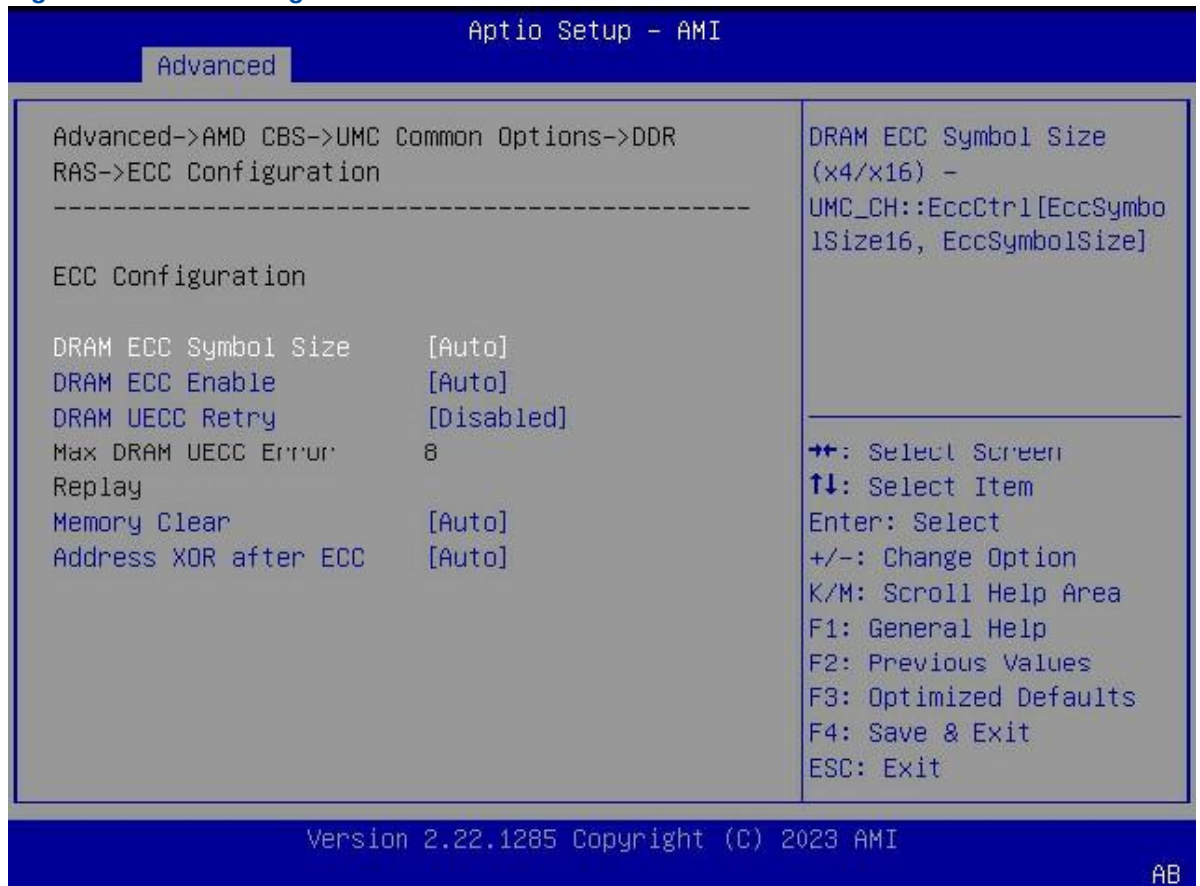
Table 3-38 Parameter Descriptions for the DDR RAS Screen

Parameter	Description	Default
Data Poisoning	Enables or disables the data poisoning feature. Options: - Auto. - Enabled: enables the data poisoning feature. - Disabled: disables the data poisoning feature.	Auto
DRAM Boot Time Post Package Repair	Enables or disables DRAM post package repair at the boot time. Options: - Enabled: enables DRAM post package repair at the boot time. - Disabled: disables DRAM post package repair at the boot time.	Disabled

Parameter	Description	Default
DRAM Runtime Post Package Repair	Enables or disables DRAM runtime post package repair. Options: - Enabled: enables DRAM runtime post package repair. - Disabled: disables DRAM runtime post package repair.	Disabled
RCD Parity	Enables or disables RCD parity check. Options: - Enabled: enables RCD parity check. - Disabled: disables RCD parity check.	Enabled
Max RCD Parity Error Replay	Sets the maximum number of replays of RCD parity check errors. Range: 0x01–0x3F.	8
Disable Memory Error Injection	Enables or disables the memory error injection feature. Options: - Auto. - Enabled: enables the memory error injection feature. - Disabled: disables the memory error injection feature.	Auto
ECC Configuration	Sets ECC parameters. Press Enter . The Login page is displayed, as shown in Figure 3-53 .	-
DRAM Scrubbers	Sets DRAM cleanup parameters. Press Enter . The Submit screen is displayed, as shown in Figure 3-54 .	-
DRAM Corrected Error Counter Enable	Select the mode for the corrected error counter of the DRAM. Options: - Disabled - NoLeakMode - LeakMode	LeakMode

DRAM Corrected Error Counter Interrupt Enable	Enables or disables the interrupt feature of the corrected error counter of the DRAM. Options: Enabled: enables the interrupt feature of the corrected error counter of the DRAM.	Enabled
Parameter	Description	Default
	Disabled: disables the interrupt feature of the corrected error counter of the DRAM.	
DRAM Corrected Error Counter Leak Rate	Sets the leak rate of the corrected error counter of the DRAM, range: 0x00–0x1F.	1E
DRAM Corrected Error Counter Start Count	Sets the program start value for the corrected error counter of the DRAM, range: 0x0000–0xFFFF.	F374

Figure 3-53 ECC Configuration Screen



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

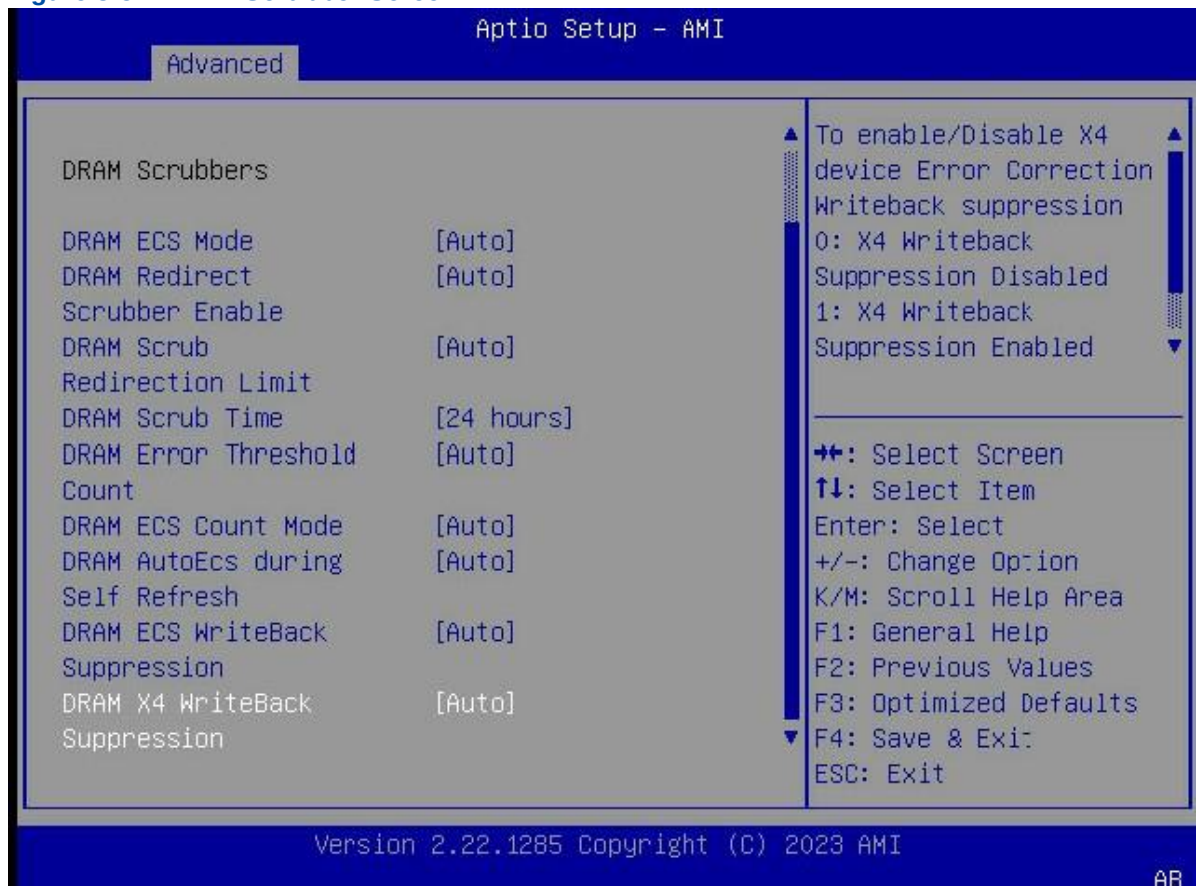
Table 3-39 Parameter Descriptions for the ECC Configuration Screen

Parameter	Description	Default
-----------	-------------	---------

DRAM ECC Symbol Size	Select the DRAM ECC symbol size. Options: ● Auto ● x4 ● x16	Auto
DRAM ECC Enabled	Enables or disables the DRAM ECC feature.	Auto

Parameter	Description	Default
	Options: ● Auto. ● Enabled: enables the DRAM ECC feature. ● Disabled: disables the DRAM ECC feature.	
DRAM UECC Retry	Enables or disables the DRAM UECC retry feature. Options: ● Auto. ● Enabled: enables the DRAM UECC retry feature. ● Disabled: disables the DRAM UECC retry feature.	Auto
Max DRAM UECC Error Replay	This parameter can be configured when DRAM UECC Retry is set to Enabled . This parameter sets the maximum number of DRAM UECC error replays, range: 0x01–0x3F.	8
Memory Clear	Enables or disables the memory clearing feature. Options: ● Auto. ● Enabled: enables the memory clearing feature. ● Disabled: disables the memory clearing feature. When this parameter is set to Disabled, memory is not cleared after training.	Auto

Address XOR after ECC	Enables or disables address XOR after ECC is enabled. Options: ● Auto. ● Enabled: enables address XOR after ECC is enabled. ● Disabled: disables address XOR after ECC is enabled.	Auto
-----------------------	--	------

Figure 3-54 DRAM Scrubber Screen

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

Table 3-40 Parameter Descriptions for the DRAM Scrubbers Screen

Parameter	Description	Default
DRAM ECS Mode	Select the DRAM ECS mode. Options: ● Auto ● DisableECS ● AutomaticECS ● ManualECS	Auto

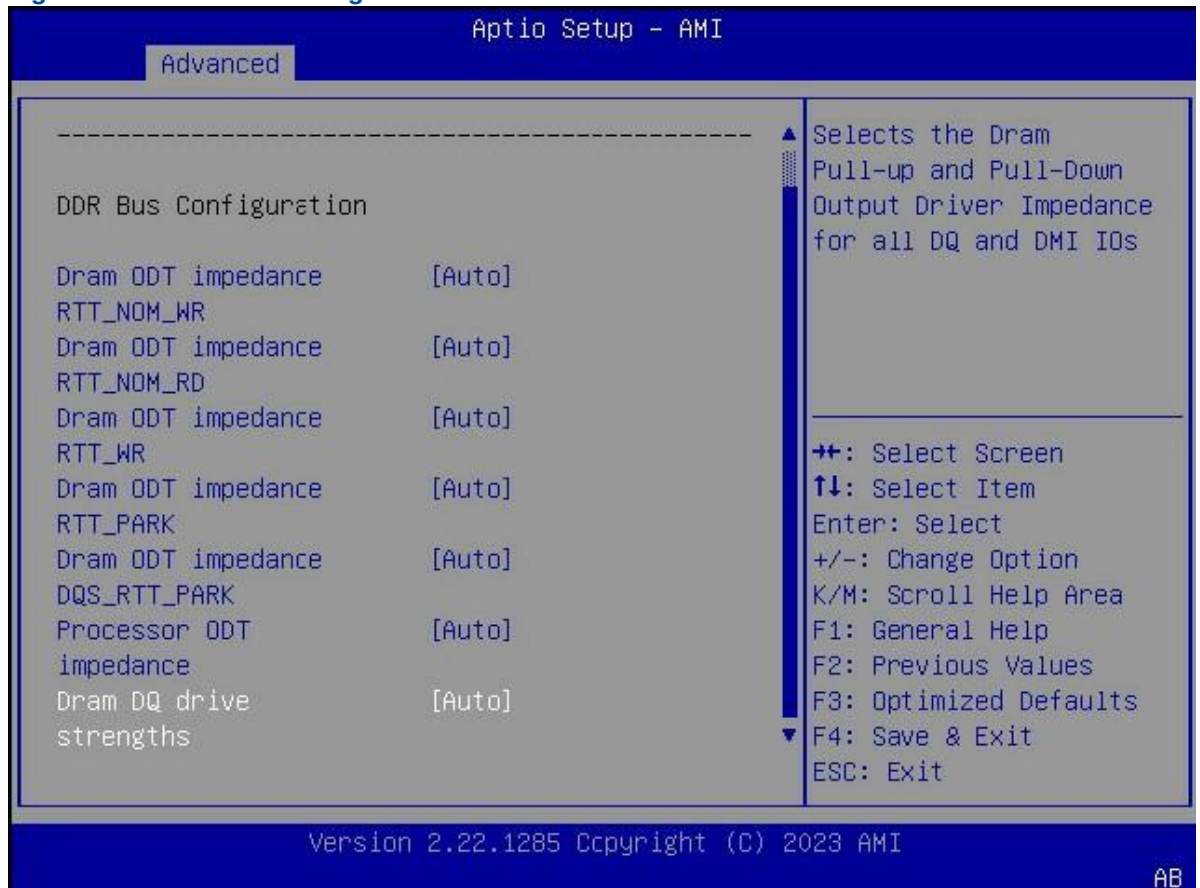
DRAM Redirect Scrubber Enable	Enables or disables the DRAM redirection scrubbing program. Options: ● Auto. ● Enabled: enables the DRAM redirection scrubbing program. ● Disabled: disables the DRAM redirection scrubbing program.	Auto
-------------------------------	--	------

Parameter	Description	Default
DRAM Scrub Redirection Limit	Select the maximum number of DRAM scrubs with redirection. Options: ● Auto ● 8 Scrubs ● 4 Scrubs ● 2 Scrubs ● 1 Scrubs	Auto
DRAM Scrub Time	Select the DRAM scrubbing duration. Options: ● Disabled ● 1 hour ● 4 hours ● 6 hours ● 7 hours ● 12 hours ● 16 hours ● 24 hours ● 48 hours	24 hours
DRAM Error Threshold Count	Select the DRAM error threshold count. Options: ● Auto ● ETC_4 ● ETC_16 ● ETC_64 ● ETC_256 ● ETC_1024 ● ETC_4096	Auto

DRAM ECS Count Mode	Select the DRAM ECS count mode. Options: ● Auto ● Row Count Mode ● Code Word Count Mode	Auto
DRAM AutoEcs during Self Refresh	Select the DRAM AutoEcs mode during self-refresh. Options: ● Auto ● AutoEcs Disabled ● AutoEcs Enabled	Auto
Parameter	Description	Default
DRAM ECS WriteBack Suppression	Enables or disables DRAM ECS writeback suppression. Options: ● Auto. ● Enabled: enables DRAM ECS writeback suppression. ● Disabled: disables DRAM ECS writeback suppression.	Auto
DRAM X4 WriteBack Suppression	Enables or disables DRAM X4 Writeback Suppression. Options: ● Auto. ● Enabled: enables DRAM X4 Writeback Suppression. ● Disabled: disables DRAM X4 Writeback Suppression.	Auto

DDR Bus Configuration

Figure 3-55 shows the **DDR Bus Configuration** screen.

Figure 3-55 DDR Bus Configuration Screen

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

Table 3-41 DDR Bus Configuration Screen

Parameter	Description	Default
Dram ODT impedance RTT_NOM_WR	Select the terminal impedance of the RTT_NOM_WR on the Dram chip. Options: • Auto • RTT_OFF • RZQ (240) • RZQ/2 (120) • RZQ/3 (80) • RZQ/4 (60) • RZQ/5 (48) • RZQ/6 (40) • RZQ/7 (34)	Auto

Dram ODT impedance RT-T_NOM_RD	Select the terminal impedance of the RTT_NOM_RD on the Dram chip. Options:	Auto
--------------------------------	---	------

Parameter	Description	Default
	● Auto ● RTT_OFF ● RZQ (240) ● RZQ/2 (120) ● RZQ/3 (80) ● RZQ/4 (60) ● RZQ/5 (48) ● RZQ/6 (40) ● RZQ/7 (34)	
Dram ODT impedance RTT_WR	Select the terminal impedance of the RTT_WR on the Dram chip. Options: ● Auto ● RTT_OFF ● RZQ (240) ● RZQ/2 (120) ● RZQ/3 (80) ● RZQ/4 (60) ● RZQ/5 (48) ● RZQ/6 (40) ● RZQ/7 (34)	Auto
Dram ODT impedance RT-T_PERK	Select the terminal impedance of the RTT_PERK on the Dram chip. Options: ● Auto ● RTT_OFF ● RZQ (240) ● RZQ/2 (120) ● RZQ/3 (80) ● RZQ/4 (60) ● RZQ/5 (48) ● RZQ/6 (40) ● RZQ/7 (34)	Auto

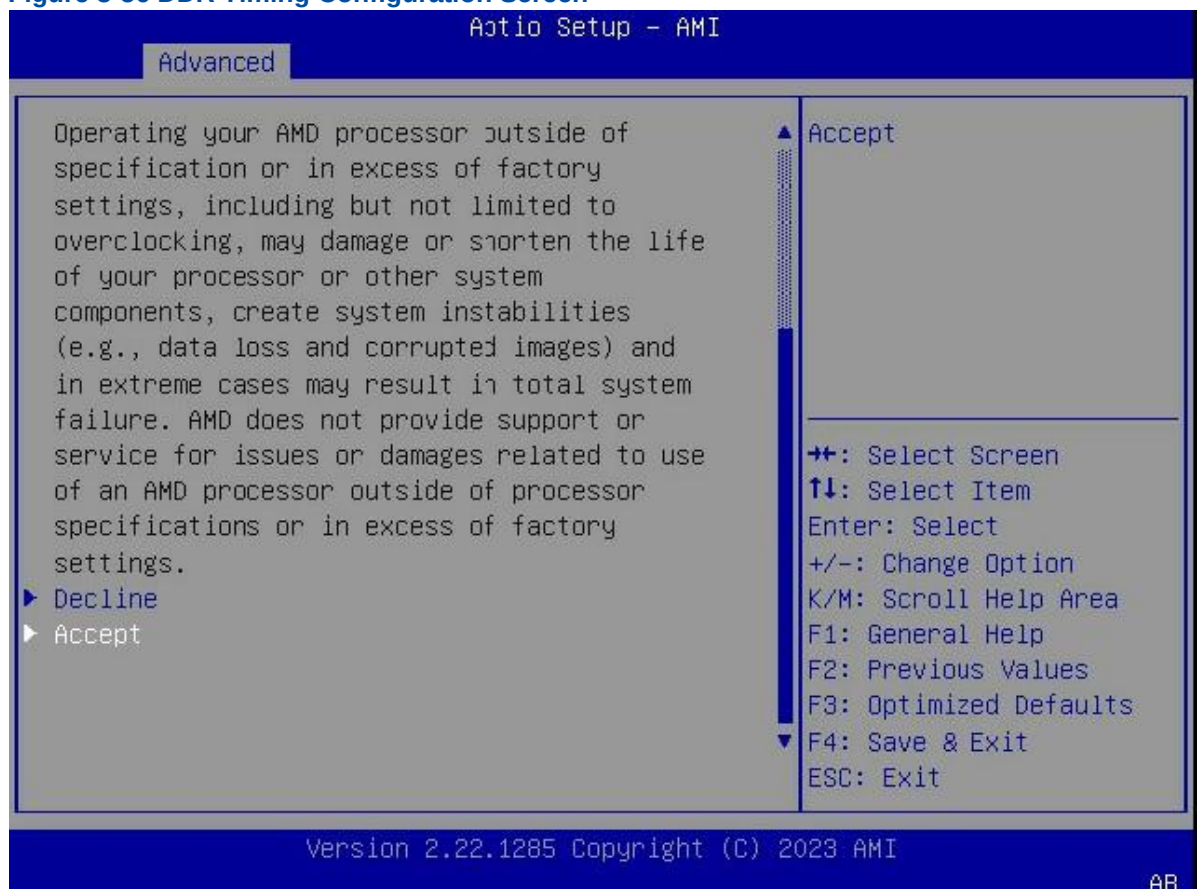
Dram ODT impedance DQS_RT-T_PARK	Select the terminal impedance of the DQS_RTT_PARK on the Dram chip. Options: ● Auto ● RTT_OFF ● RZQ (240) ● RZQ/2 (120) ● RZQ/3 (80) ● RZQ/4 (60)	Auto
Parameter	Description	Default
	● RZQ/5 (48) ● RZQ/6 (40) ● RZQ/7 (34)	
Processor ODT impedance	Selects the ODT impedance of the processor. Options: ● Auto ● High Impedance ● 480 ohm ● 240 ohm ● 160 ohm ● 120 ohm ● 96 ohm ● 80 ohm ● 68.6 ohm ● 60 ohm ● 53.3 ohm ● 48 ohm ● 43.6 ohm ● 40 ohm ● 36.9 ohm ● 34.3 ohm ● 32 ohm ● 30 ohm ● 28.2 ohm ● 26.7 ohm ● 25.3 ohm	Auto

Dram DQ drive strengths	Select the impedance of the Dram pull-up and pull-down output drivers. Options: • Auto • 48 ohm • 40 ohm • 34 ohm	Auto
-------------------------	---	------

DDR Timing Configuration

Figure 3-56 shows the **DDR Timing Configuration** screen.

Figure 3-56 DDR Timing Configuration Screen



For a description of the parameters on the **DDR Timing Configuration** screen, refer to [Table 3-42](#).

Table 3-42 Parameter Descriptions for the DDR Timing Configuration Screen

Parameter	Description
Decline	Rejects the alarms displayed on the page. Press Enter . The UMC Common Options screen is displayed.

Accept	Accepts the alarms displayed on the page. Press Enter . The Accept screen is displayed, as shown in Figure 3-57 .
--------	--

Figure 3-57 Accept Screen



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

Table 3-43 Parameter Descriptions for the Accept Screen

Parameter	Description	Default
Active Memory Timing Settings	Enables or disables active memory timing settings. - Auto - Enabled: enables active memory timing settings.	Enabled

Memory Target Speed	Select the target memory speed. Options: ● Auto ● DDR3200 ● DDR3600 ● DDR4000 ● DDR4400 ● DDR4800 ● DDR5200 ● DDR5600	Auto
SPD Timing	Sets SPD timing parameters.	-

Parameter	Description	Default
	Press Enter. The SPD Timing screen is displayed. You can set the parameters. ● TcI Ctrl: Select a configuration mode for the CAS Delay Time. Default: Auto. ● Trcd Ctrl: Select a configuration mode for the RAS# Active to CAS# Read Delay Time. Default: Auto. ● Trp Ctrl: Select a configuration mode for the Row Precharge Delay Time. Default: Auto. ● Tras Ctrl: Select a configuration mode for the minimum duration from the activation command to the precharge command. Default: Auto. ● Trc Ctrl: Select a configuration mode for the Active to Active/Refresh Delay Time. Default: Auto. ● Twr Ctrl: Select a configuration mode for the Minimum Write Recovery Time. Default: Auto. ● Trfc1 Ctrl: Select a configuration mode for the Refresh Recovery Delay Time (tRFC1). Default: Auto. ● Trfc2 Ctrl: Select a configuration mode for the Refresh Recovery Delay Time (tRFC2). Default: Auto. ● TrfcSb Ctrl: Select a configuration mode for the Refresh Recovery Delay Time (tRFCsb). Default: Auto.	

Non-SPD Timing	Sets non-SPD timing parameters. Press Enter. The Non-SPD Timing screen is displayed. You can set the parameters. ● Tcwl Ctrl: Select a configuration mode for the CAS Write Delay Time. Default: Auto. ● Trtp Ctrl: Select a configuration mode for the Read CAS# to Precharge command delay time. Default: Auto. ● TrrdL Ctrl: Select a configuration mode for the Activate to Activate Delay Time in the same bank group (tRRD_L). Default: Auto. ● TeedS Ctrl: Select a configuration mode for the Activate to Activate Delay Time in a different bank group (tRRD_S). Default: Auto. ● Tfaw Ctrl: Select a configuration mode for the Four Activate Window Time. Default: Auto.	-
Parameter	Description	Default

	● Twtrl Ctrl: Select a configuration mode for the Minimum Write to Read Time in the same bank group. Default: Auto. ● TwtrS Ctrl: Select a configuration mode for the Minimum Write to Read Time in a different bank group. Default: Auto. ● TrdScL Ctrl: Select a configuration mode for the CAS to CAS delay time in the same bank group. Default: Auto. ● TrdrdSc Ctrl: Select a configuration mode for the Read to Read turnaround timing in the same chipselect. Default: Auto. ● TrdrdSd Ctrl: Select a configuration mode for the Read to Read turnaround timing in the same DIMM. Default: Auto. ● TrdrdDd Ctrl: Select a configuration mode for the Read to Read turnaround timing in a different DIMM. Default: Auto. ● TwrwrScL Ctrl: Select the configuration mode for the CAS to CAS Delay Time in the same bank group. Default: Auto. ● TrdrdSc Ctrl: Select a configuration mode for the Write to Write turnaround timing in the same chipselect. Default: Auto. ● TwrwrSd Ctrl: Select a configuration mode for the Write to Write turnaround timing in the same DIMM. Default: Auto. ● TwrwrDd Ctrl: Select a configuration mode for the Write to Write turnaround timing in a different DIMM. Default: Auto. ● Twrrd Ctrl: Select a configuration mode for the Write to Read turnaround timing. Default: Auto. ● Tedwr Ctrl: Select a configuration mode for the Read to Write turnaround timing. Default: Auto.	
--	---	--

DDR Training Options

Figure 3-58 shows the **DDR Training Options** screen.

Figure 3-58 DDR Training Options Screen



For a description of the parameters on the **DDR Training Options** screen, refer to [Table 3-44](#).

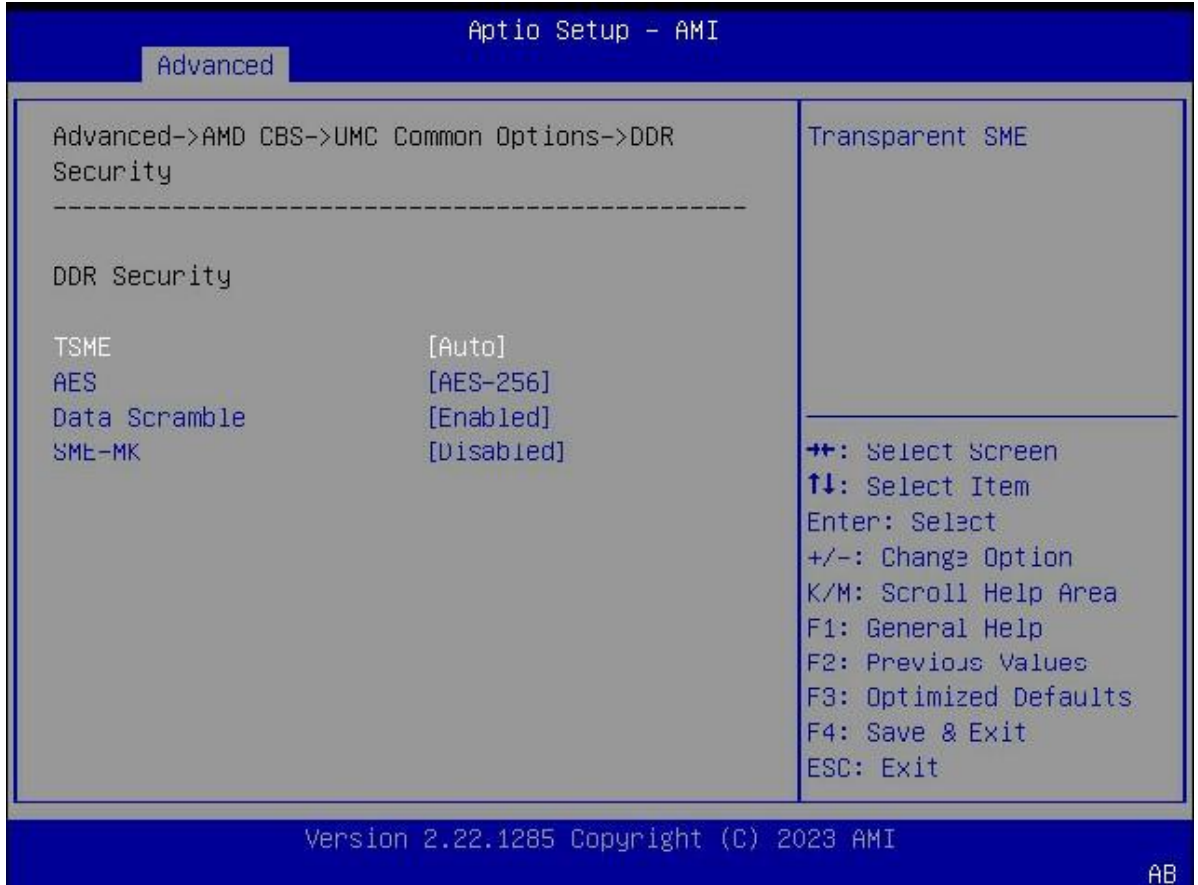
Table 3-44 Parameter Descriptions for the DDR Training Options Screen

Parameter	Description	Default
DRAM PDA Enumerate ID Programming Mode	Select PDA enumeration mode. Options: • Auto • Toggling PDA enumeration mode • Legacy PDA enumeration mode	Auto

DDR Security

[Figure 3-59](#) shows the **DDR Security** screen.

Figure 3-59 DDR Security Screen



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

Table 3-45 Parameter Descriptions for the DDR Security Screen

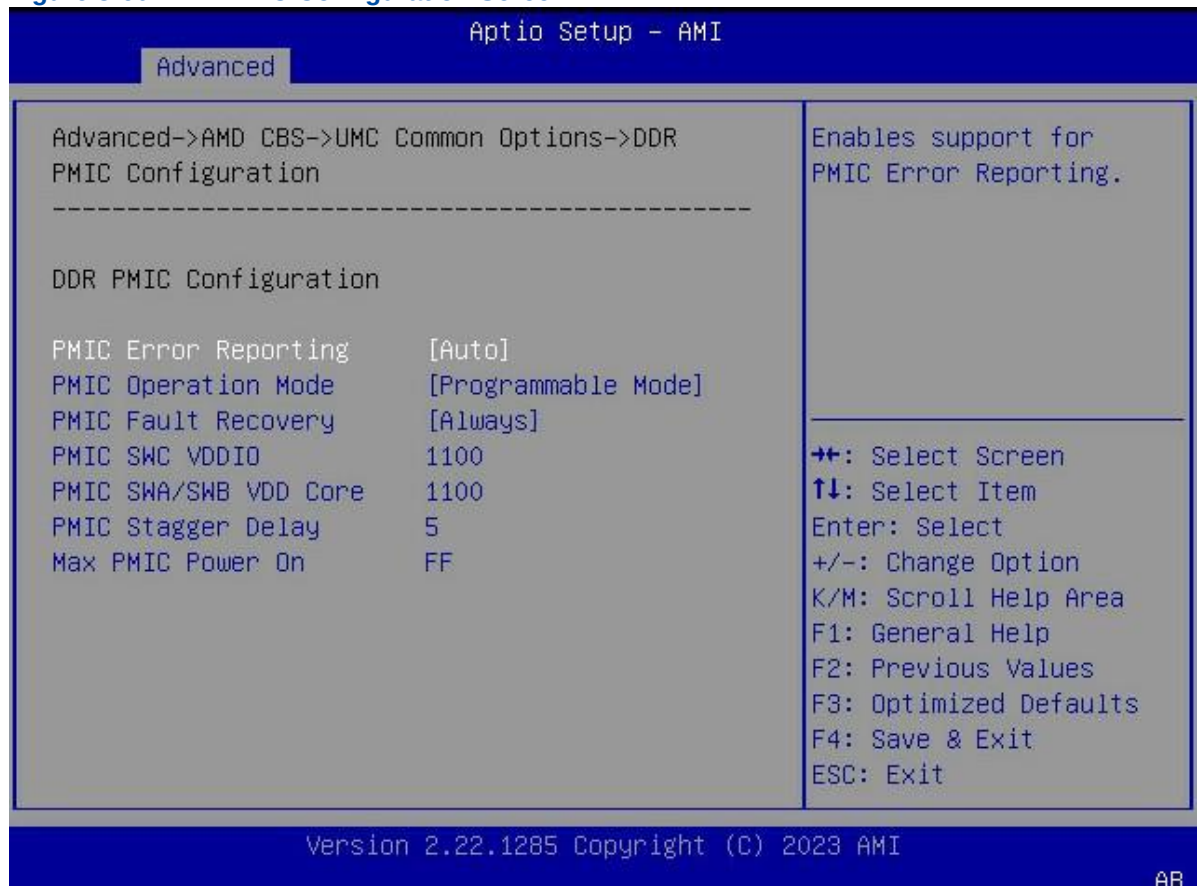
Parameter	Description	Default
TSME	Enables or disables TSME. Options: - Auto. - Enabled: enables TSME. - Disabled: disables TSME.	Auto
AES	Select an AES mode. Options: - AES-128 - AES-256	AES-256
Data Scramble	Enables or disables the data scrambling feature. Options: Enabled: enables the data scrambling feature.	Enabled

Parameter	Description	Default
	Disabled: disables the data scrambling feature.	
SME-MK	Enables or disables SME-MK encryption mode. Options: - Enabled: enables SME-MK encryption mode. - Disabled: disables SME-MK encryption mode.	Disabled

DDR PMIC Configuration

Figure 3-60 shows the **DDR PMIC Configuration** screen.

Figure 3-60 DDR PMIC Configuration Screen



For a description of the parameters on the **DDR PMIC Configuration** screen, refer to [Table 3-46](#).

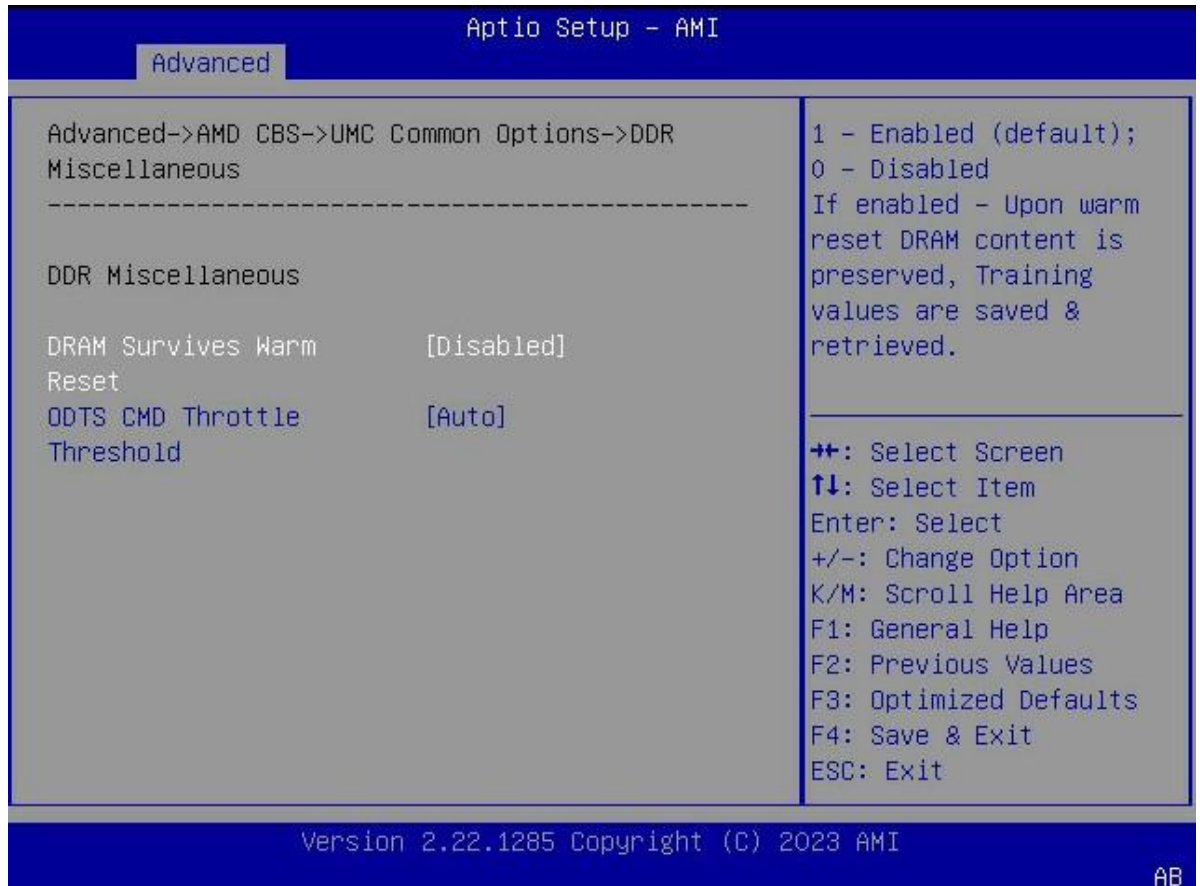
Table 3-46 Parameter Descriptions for DDR PMIC Configuration

Parameter	Description	Default
PMIC Error Reporting	Enables or disables PMIC error reporting. Options: ● Auto. ● Enabled: enables PMIC error reporting. ● Disabled: disables PMIC error reporting.	Auto
PMIC Operation Mode	Select a PMIC operation mode. Options: ● Secure Mode ● Programmable Mode	Programmable Mode
PMIC Fault Recovery	Select the PMIC fault recovery mode: Options: ● Always ● Never ● Once	Always
PMIC SWC VDDIO	Sets the PMIC SWC VDDIO, range: 1000–1200, unit: millivolts.	1100
PMIC SWA/SWB VDD Core	Sets the PMIC SWA/SWB VDD core, range: 1000–1200, unit: millivolts.	1100
PMIC Stagger Delay	Sets the amount of time to wait between power-on of DIMMs, range: 0–99, unit: milliseconds.	5
Max PMIC Power On	Sets the maximum number of DIMMs that can be powered on at the same time, range: 0x00–0xFF.	FF

DDR Miscellaneous

Figure 3-61 shows the **DDR Miscellaneous** screen.

Figure 3-61 DDR Miscellaneous Screen



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

Table 3-47 Parameter Descriptions for the DDR Miscellaneous Screen

Parameter	Description	Default
DRAM Survives Warm Reset	Enables or disables the DRAM warm reset keep-alive feature. Options: - Enabled: enables the DRAM warm reset keep-alive feature. - Disabled: disables the DRAM warm reset keep-alive feature.	Disabled
PMIC CMD Operation Mode	Select the PMIC CMD operation mode. Options: - Auto > 85' C > 90' C > 95' C	Auto

DDR PHY (CMN)

Figure 3-62 shows the **DDR PHY (CMN)** screen.

Figure 3-62 DDR PHY (CMN) Screen



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

Table 3-48 DDR PHY (CMN) Screen

Parameter	Description	Default
Periodic Training	Enables or disables periodic training. Options: • Auto. • Enabled: enables periodic training. • Disabled: disables periodic training.	Auto

3.2.7.4 NBIO Common Options

NBIO Common Options

Figure 3-63 through Figure 3-65 show the **NBIO Common Options** screen.

Figure 3-63 NBIO Common Options Screen—1

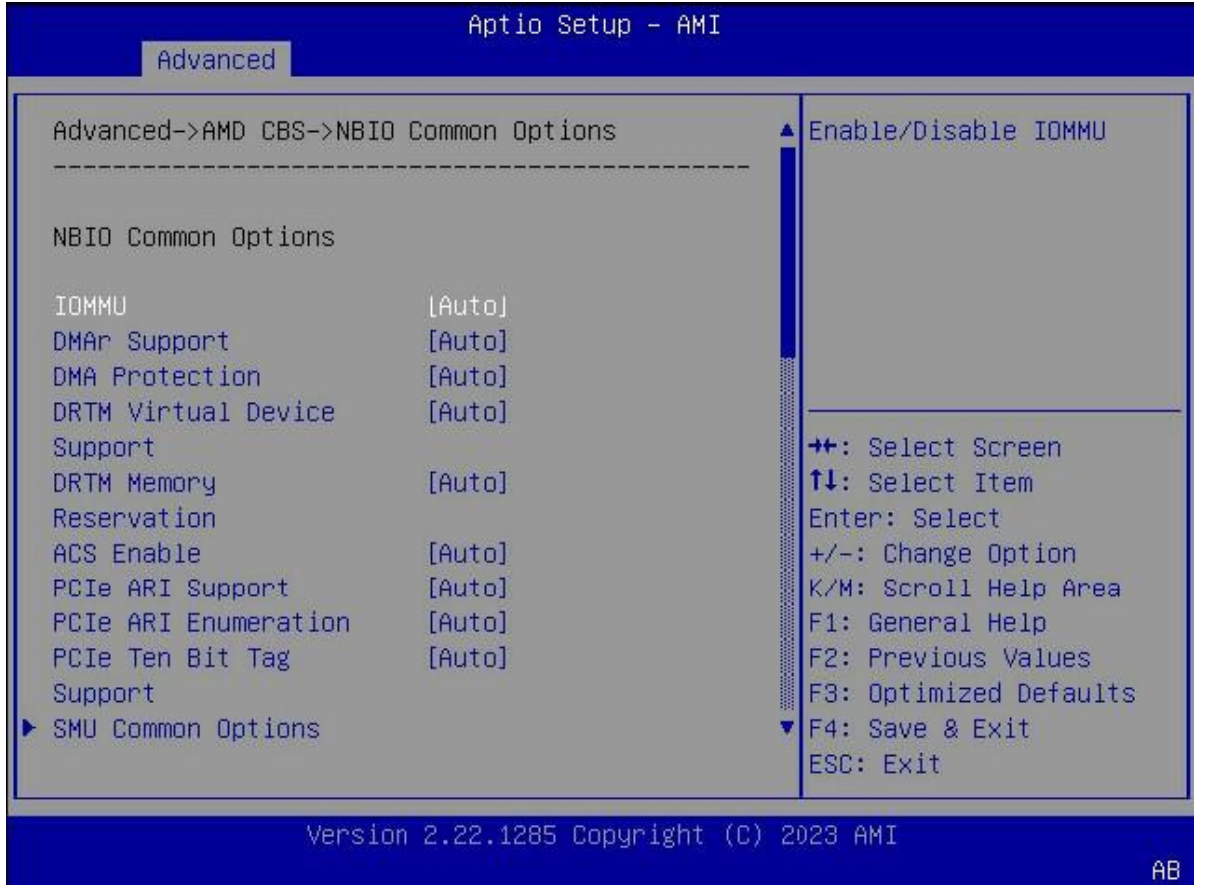


Figure 3-64 NBIO Common Options Screen—2

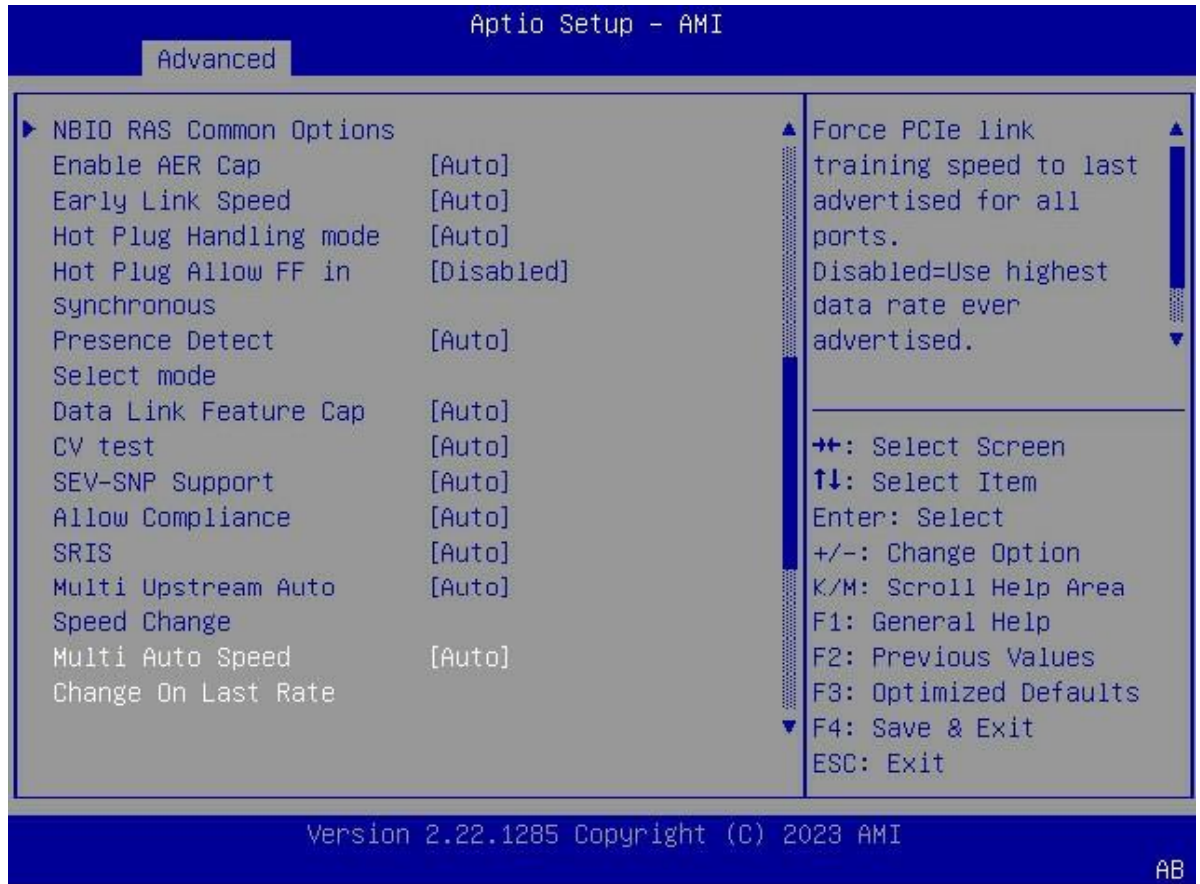


Figure 3-65 NBIO Common Options Screen—3



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

Table 3-49 Parameter Descriptions for the NBIO Common Options Screen

Parameter	Description	Default
IOMMU	Enables or disables the IO memory management unit. Options: ● Auto. ● Enabled: enables the IO memory management unit. ● Disabled: disables the IO memory management unit.	Auto
DMAr Support	Enables or disables DMAr support. Options: ● Auto. ● Enabled: enables DMAr support. ● Disabled: disables DMAr support.	Auto

DMA Protection	Enables or disables the DMA protection feature.	Auto
----------------	---	------

Parameter	Description	Default
	Options: ● Auto. ● Enabled: enables the DMA protection feature. ● Disabled: disables the DMA protection feature.	
DRTM Virtual Device Support	Enables or disables DRTM virtual device support. Options: ● Auto. ● Enabled: enables DRTM virtual device support. ● Disabled: disables DRTM virtual device support.	Auto
DRTM Memory Reservation	Enables or disables the DRTM memory reservation feature. Options: ● Auto. ● Enabled: enables the DRTM memory reservation feature. ● Disabled: disables the DRTM memory reservation feature.	Auto
ACS Enable	Enables or disables the ACS feature. Options: ● Auto. ● Enabled: enables the ACS feature. Before enabling ACS, you must enable AER first. ● Disabled: disables the ACS feature.	Auto
PCIe ARI Support	Enables or disables PCIe ARI support. Options: ● Auto. ● Enabled: enables PCIe ARI support. ● Disabled: disables PCIe ARI support.	Auto

PCIe ARI Enumeration	Enables or disables PCIe ARI enumeration. Options: ● Auto. ● Enabled: enables PCIe ARI enumeration. ● Disable: disables PCIe ARI enumeration.	Auto
PCIe Ten Bit Tag Support	Enables or disables PCIe Ten Bit Tag support.	Auto

Parameter	Description	Default
	Options: ● Auto. ● Enabled: enables PCIe Ten Bit Tag support. ● Disabled: disables PCIe Ten Bit Tag support.	
SMU Common Options	Sets general SMU parameters. For details, refer to SMU Common Options .	-
NBIO RAS Common Options	Sets general NBIO RAS parameters. For details, refer to NBIO RAS Common Options .	-
EnabledAER Cap	Enables or disables the AER feature. Options: ● Auto. ● Enabled: enables the AER feature. ● Disabled: disables the AER feature.	Auto
Early Link Speed	Select the early link speed. Options: ● Auto ● Gen1 ● Gen2	Auto
Hot Plug Handling mode	Select the hot swapping processing mode. Options: ● Auto ● OS First ● Firmware First/EDR if OS supports ● Firmware First but allow OS first ● System Firmware Intermediary	Auto

Hot Plug Allow FF in Synchronous	Enables or disables Firmware First Hot Plug mode in mode A and mode B synchronous mappings. Options: ● Enabled: enables Firmware First Hot Plug mode in mode A and mode B synchronous mappings. ● Disabled: disables Firmware First Hot Plug mode in mode A and mode B synchronous mappings.	Disabled
Presence Detect Select mode	Select the signal presence detection mode. Options: ● Auto ● OR	Auto

Parameter	Description	Default
	● AND ● In-Band Only ● Out-of-Band Only	
Data Link Feature Cap	Enables or disables data link feature cap. Options: ● Auto. ● Enabled: enables data link feature cap. ● Disabled: disables data link feature cap.	Auto
CV test	Enables or disables the CV test feature. Options: ● Auto. ● Enabled: enables the CV test feature. ● Disabled: disables the CV test feature.	Auto
SEV-SNP Support	Enables or disables SEV-SNP support. Options: ● Enabled: enables SEV-SNP support. ● Disabled: disables SEV-SNP support.	Disabled
SRIS	Enables or disables the SRIS feature. Options: ● Auto. ● Enabled: enables the SRIS feature. ● Disabled: disables the SRIS feature.	Auto

Multi Upstream Auto Speed Change	Enables or disables the uplink rate auto-change feature for all PCIe devices. Options: ● Auto. ● Enabled: enables the uplink rate auto-change feature for all PCIe devices. ● Disabled: disables the uplink rate auto-change feature for all PCIe devices.	Auto
Multi Auto Speed Change On Last Rate	Sets the PCIe link training speed. Options: ● Auto: uses the default value. ● Enabled: uses the last value. ● Disabled: uses the maximum value.	Auto
PCIE Link Speed Capability	Select the link speed capability for all PCIe ports. Options: ● Auto ● Maximum speed	Auto

Parameter	Description	Default
	● Gen1 ● Gen2 ● Gen3 ● Gen4 ● Gen5	
RTM Margining Support	Enables or disables the RTM margining feature. Options: ● Auto. ● Enabled: enables the RTM margining feature. ● Disabled: disables the RTM margining feature.	Auto

EQ Bypass To Highest Rate	Enables or disables the EQ bypass to maximum rate. Options: ● Auto. ● Enabled: enables the EQ bypass to maximum rate. ● Disabled: disables the EQ bypass to maximum rate.	Auto
Non-PCIe Compliant Support	Enables or disables non-PCIe compliance. Options: ● Auto. ● Enabled: enables non-PCIe compliance. ● Disabled: disables non-PCIe compliance.	Auto
PCIe Idle Power Setting	Select the PCIe idle power policy. Options: ● Optimize for Latency ● Optimize for Perf/Power	Optimize for Latency
nBif Common Option	Sets general nBif parameters. For details, refer to nBif Common Option .	-
Link EQ Preset Options	Sets link EQ presetting parameters. For details, refer to Link EQ Preset Options .	-
Enabled2 SPC (Gen 4)	Enables or disables the Enabled2 SPC (Gen 4) feature. Options: ● Auto. ● Enabled: enables the Enabled2 SPC (Gen 4) feature.	Auto
Parameter	Description	Default
	When this feature is enabled, two symbols can be used per clock for devices with the Gen 4 speed.	

SMU Common Options

Figure 3-66 through Figure 3-67 show the **SMU Common Options** screen.

Figure 3-66 SMU Common Options Screen—1

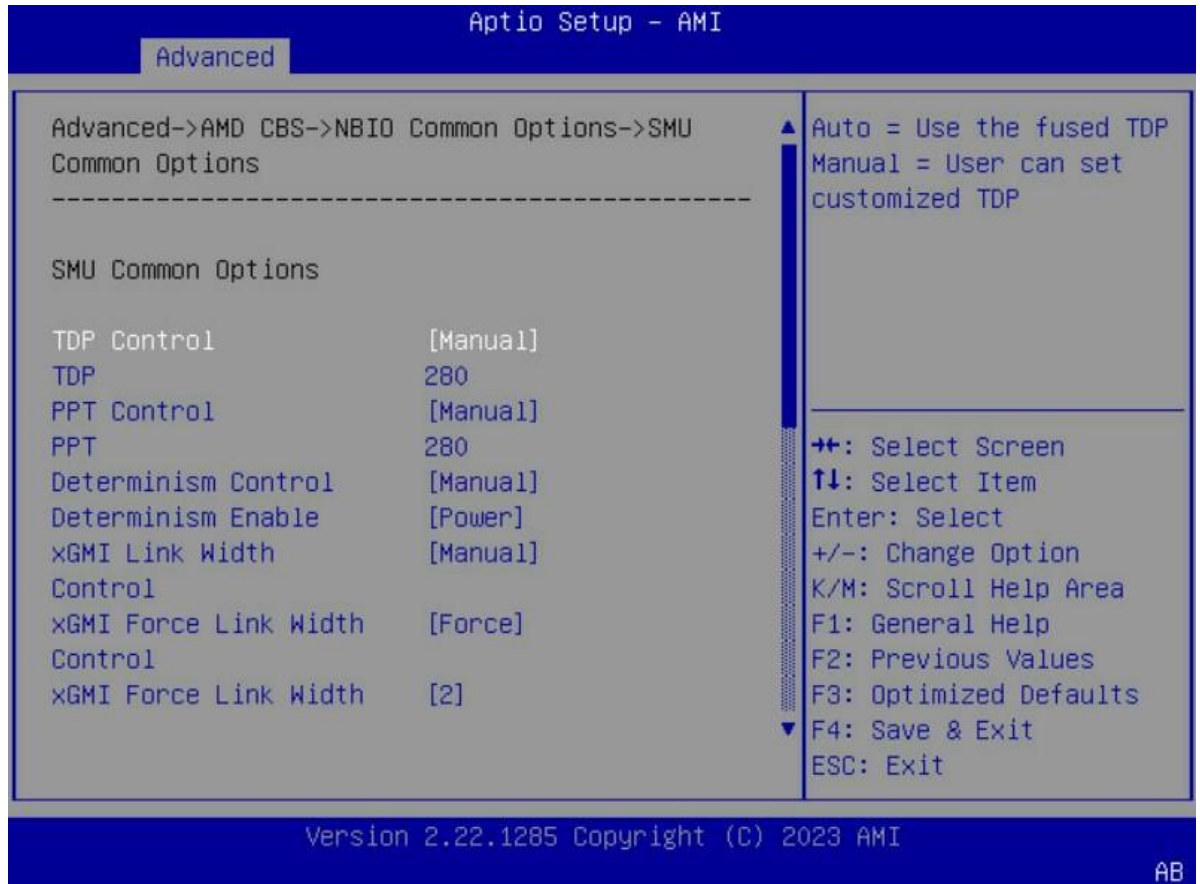
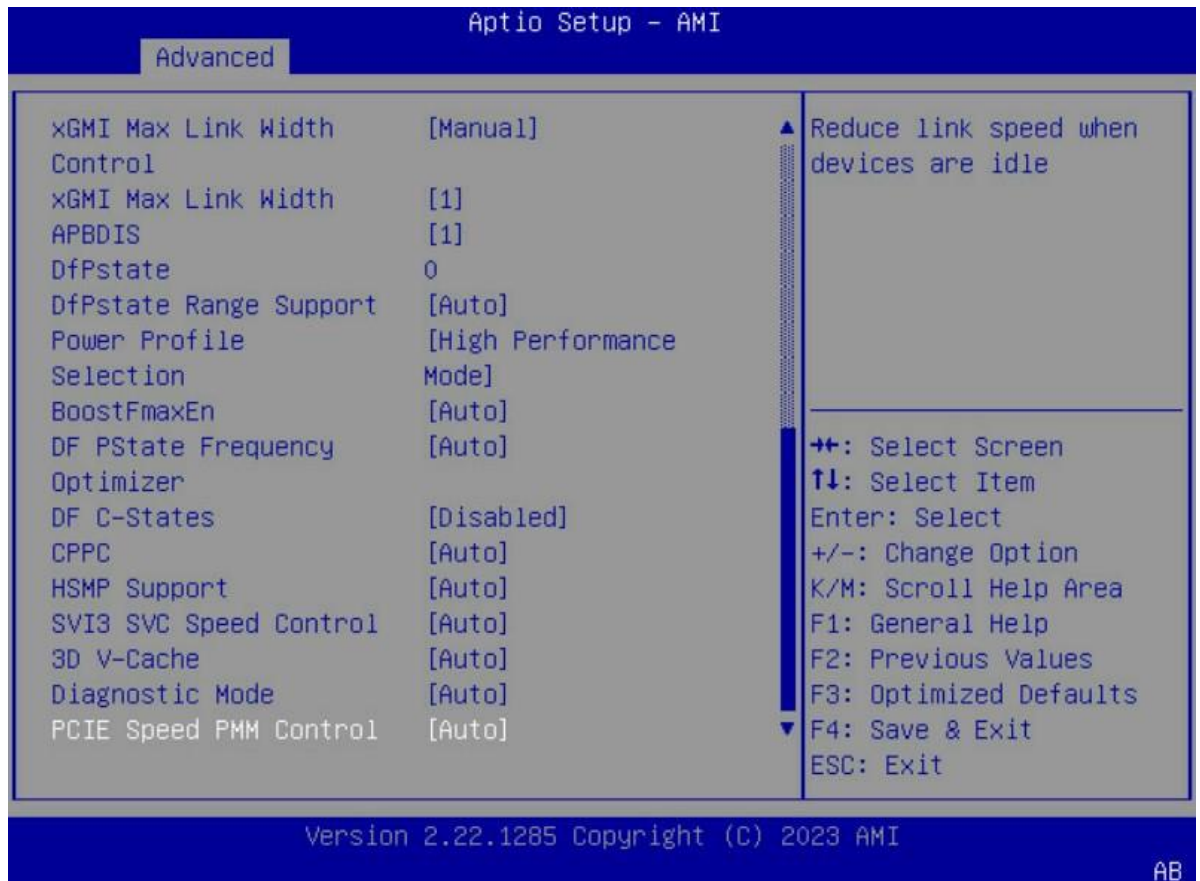


Figure 3-67 SMU Common Options Screen—2



For a description of the parameters on the **SMU Common Options** screen, refer to [Table 3-50](#).

Table 3-50 Parameter Descriptions for the SMU Common Options Screen

Parameter	Description	Default
TDP Control	Select a TDP control mode. Options: ● Auto ● Manual	Auto
PPT Control	Select a PPT control mode. Options: ● Auto ● Manual	Auto
Determinism Control	Select a Determinism control mode. Options: ● Auto ● Manual	Auto

Determinism Enable	This parameter is displayed when Determinism Control is set to Manual . Sets the DetermininiEnabled mode.	Performance
--------------------	--	-------------

Parameter	Description	Default
	Options: ● Power ● Performance	
xGMI Link Width Control	Sets the mode for xGMI link width control. Options: ● Auto ● manual	Auto
xGMI Force Link Width Control	This parameter is displayed when xGMI Link Width Control is set to Manual . Select whether the xGMI link width is forcibly controlled. Options: ● Auto ● Force ● Unforce	Auto
xGMI Force Link Width	This parameter is displayed when xGMI Force Link Width Control is set to Force . Select the xGMI forced link width. Options: ● Auto ● 2 ● 1 ● 0	Auto
xGMI Max Link Width Control	Select the mode for xGMI link max-width control. Options: ● Auto ● Manual	Auto

xGMII Max Link Width	This parameter is displayed when xGMI Max Link Width Control is set to Manual . Select the xGMI maximum link width. Options: ● Auto ● 2 ● 1 ● 0	Auto
APBDIS	Select an APBDIS mode. Options: ● Auto. ● 0: APBDIS.	Auto

Parameter	Description	Default
	● 1: Non-APBDIS (task mode).	
DfPstate	This parameter is displayed when APBDIS is set to 1 . Sets the Df P state index.	0
DfPstate Range Support	Enables or disables DfPstate range support. Options: ● Auto. ● Enabled: enables DfPstate range support. ● Disabled: disables DfPstate range support.	Auto
Power Profile Selection	Select the mode for xGMI link max-width control. Options: ● High Performance Mode ● Efficiency Mode ● Maximum IO Performance Mode	High Performance Mode
BoostFmaxEn	Select a BoostFmaxEn mode. Options: ● Auto: uses the default Fmax. ● manual: uses the user-defined Fmax.	Auto

DF PState Frequency Optimizer	Enables or disables the DF P state frequency optimizer. Options: ● Auto. ● Enabled: enables DF P state frequency optimizer. ● Disabled: disables DF P state frequency optimizer.	Auto
DF Cstates	Enables or disables the DF C state. Options: ● Auto. ● Enabled: enables the DF C state. ● Disabled: disables the DF C state.	Auto
CPPC	Enables or disables the CPPC feature. Options: ● Auto. ● Enabled: enables the CPPC feature.	Auto
Parameter	Description	Default
	● Disabled: disables the CPPC feature.	
HSMP Support	Enables or disables HSMP support. Options: ● Auto. ● Enabled: supports HSMP. ● Disabled: HSMP is not supported.	Auto
SVI3 SVC Speed Control	Select an SVI3 SVC speed control mode. Options: ● Auto ● Manual	Auto
SVI3 SVC Speed	This parameter is displayed when SVI3 SVC Speed Control is set to Manual . Select the SVI3 SVC speed. Options: ● 20.00 MHz ● 13.33 MHz ● 5.00 MHz	20.00 MHz

3D V-Cache	Select a 3D V-Cache mode. Options: ● Auto ● Disabled ● 1 stack	Auto
Diagnostic Mode	Enables or disables diagnostic mode. Options: ● Auto. ● Enabled: enables diagnostic mode. ● Disabled: disables diagnostic mode.	Auto
PCIe Speed PMM Control	Select the mode for PCIe speed PMM control. Options: ● Auto ● Dynamic link speed determined by Power Management functionality ● Static Target Link Speed (GEN4) ● Static Target Link Speed (GEN5)	Auto

NBIO RAS Common Options

Figure 3-68 shows the **NBIO RAS Common Options** screen.

Figure 3-68 NBIO RAS Common Options Screen—1

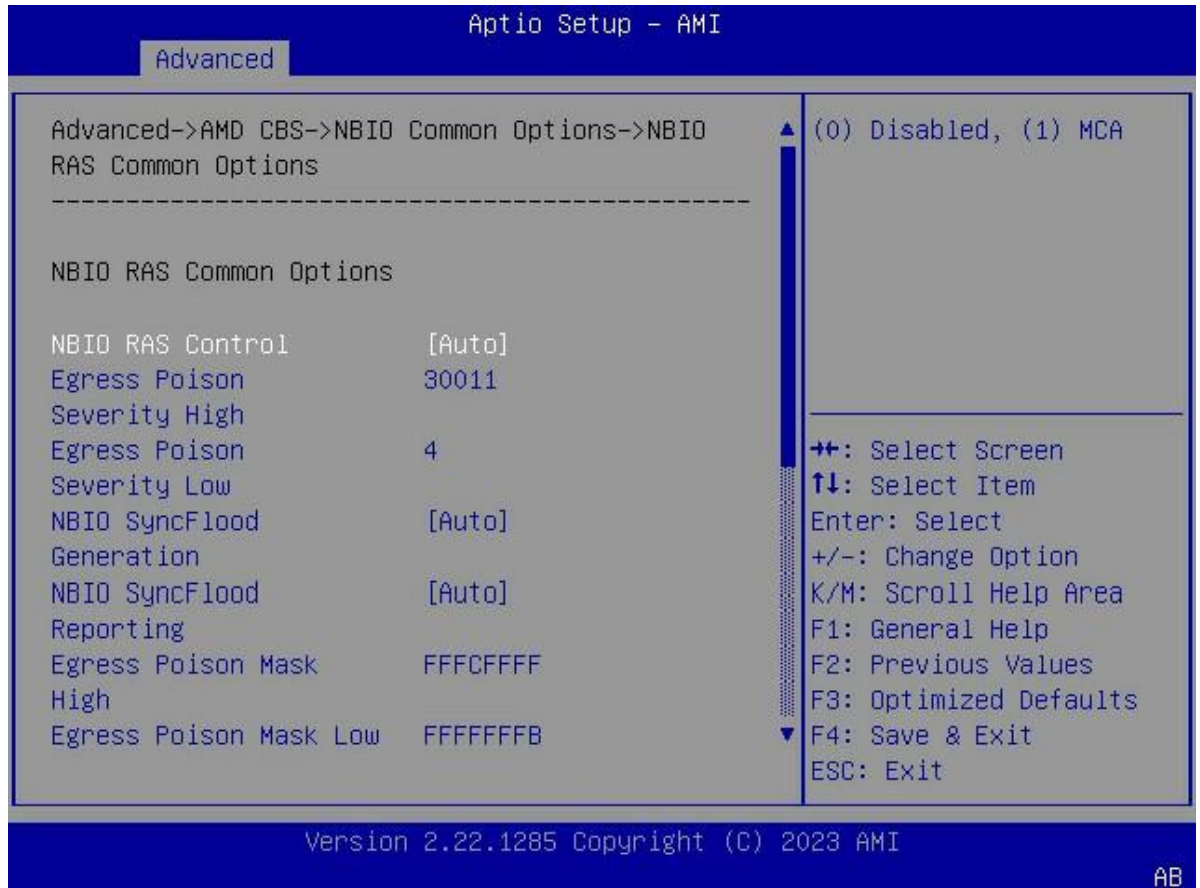
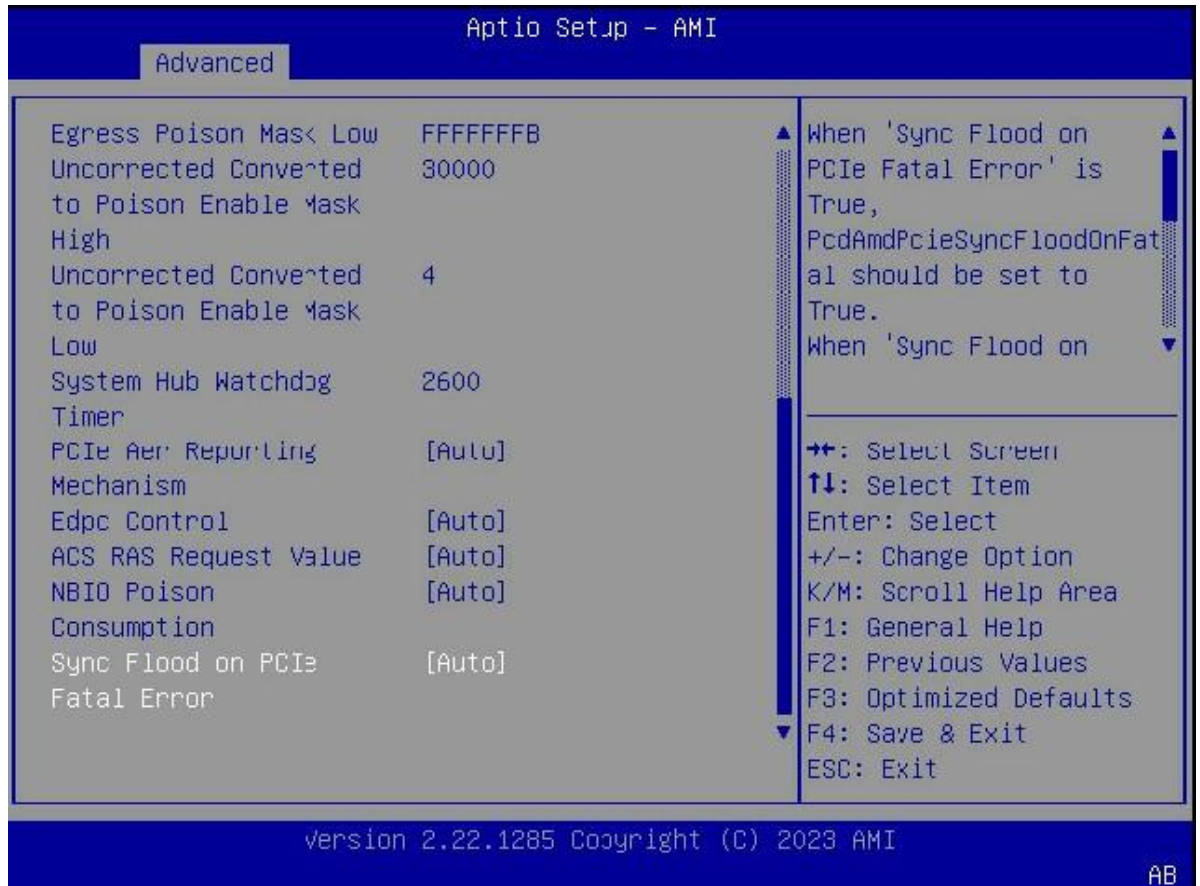


Figure 3-69 NBIO RAS Common Options Screen—2



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

Table 3-51 Parameter Descriptions for the NBIO RAS Common Options Screen

Parameter	Description	Default
NBIO RAS Control	Select the NBIO RAS control mode. Options: ● Auto ● Disabled ● MCA	Auto
Egress Poison Severity High	Sets the highest 32 bits for the Egress Poison severity.	0x30011
Egress Poison Severity Low	Sets the lowest 32 bits for the Egress Poison severity.	0x4
NBIO SyncFlood Generation	Enables or disables NBIO SYN flood generation. Options: ● Auto.	Auto

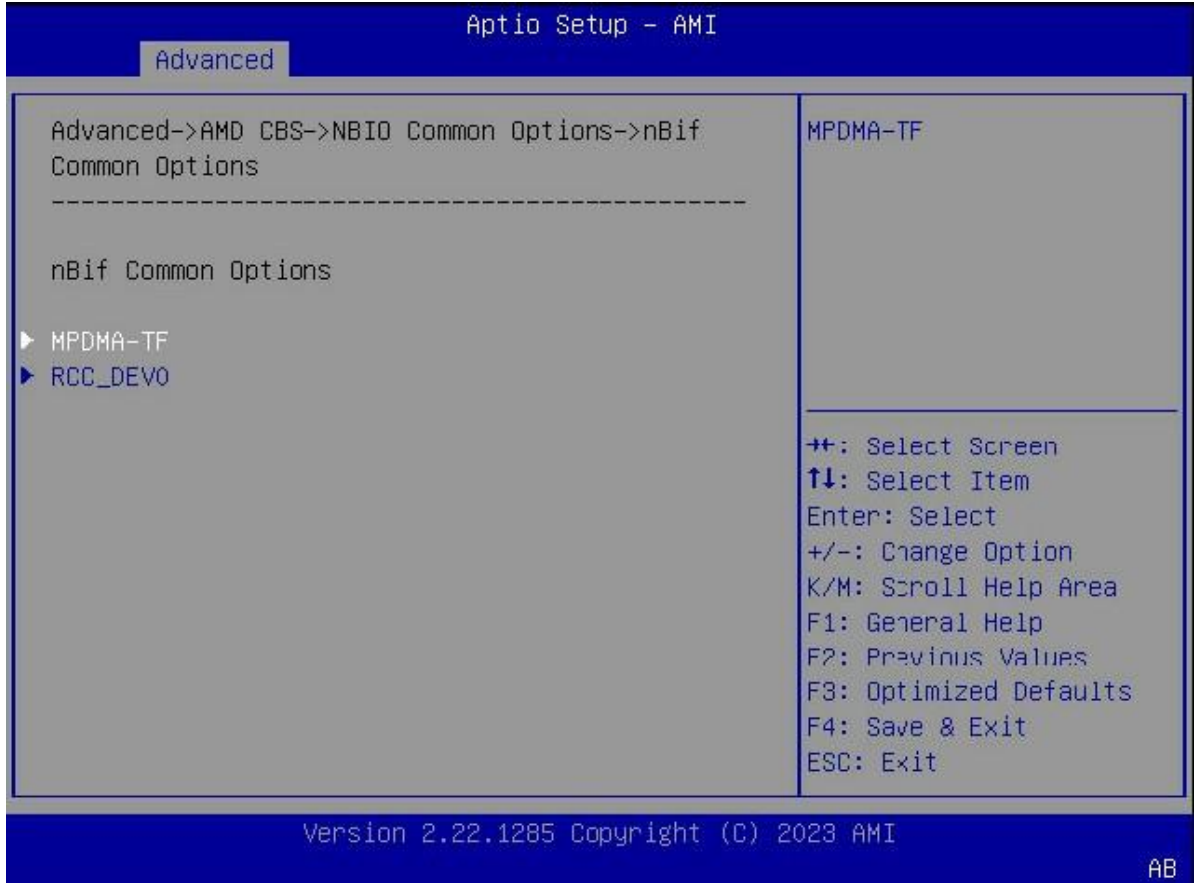
Parameter	Description	Default
	● Enabled: enables NBIO SYN flood generation. ● Disabled: disables NBIO SYN flood generation.	
NBIO SyncFlood Reporting	Enables or disables NBIO SYN flood reporting. Options: ● Auto. ● Enabled: enables NBIO SYN flood reporting. ● Disabled: disables NBIO SYN flood reporting.	Auto
Egress Poison Mask High	Sets the highest 32 bits for the Egress Poison mask.	0xFFFFCFFF
Egress Poison Mask Low	Sets the lowest 32 bits for the Egress Poison mask.	0xFFFFFFFFB
Uncorrected Converted to Poison Enable Mask High	Sets the highest 32 bits of data that can be converted to an uncorrected Poison-enabled mask.	0x30000
Uncorrected Converted to Poison Enable Mask Low	Sets the lowest 32 bits of data that can be converted to an uncorrected Poison-enabled mask.	0x4
System Hub Watchdog Timer	Sets the interval (in milliseconds) of the system hub watchdog timer.	2600
PCIe Aer Reporting Mechanism	Select a PCIe Aer reporting mechanism. Options: ● Auto ● Firmware First ● Firmware First but allow OS First ● OS First	Auto
Edpc Control	Enables or disables the EDPC control feature. Options: ● Auto. ● Enabled: enables the EDPC control feature. ● Disabled: disables the EDPC control feature.	Auto

ACS RAS Request Value	Select an ACS RAS request value. Options: ● Auto ● Direct Request Access Enabled ● Request Blocking Enabled	Auto
Parameter	Description	Default
	● Request Redirect Enabled	
NBIO Poison consumption	Enables or disables the NBIO Poison consumption feature. Options: ● Auto. ● Enabled: enables the NBIO Poison consumption feature. ● Disabled: disables the NBIO Poison consumption feature.	Auto
Sync Flood on PCIe Fatal Error	Enables or disables SYNC flood upon a fatal PCIe error. Options: ● Auto. ● Enabled: enables SYNC flood upon a fatal PCIe error. ● Disabled: disables SYNC flood upon a fatal PCIe error.	Auto

nBif Common Option

Figure 3-70 shows the **nBif Common Option** screen.

Figure 3-70 nBif Common Option Screen

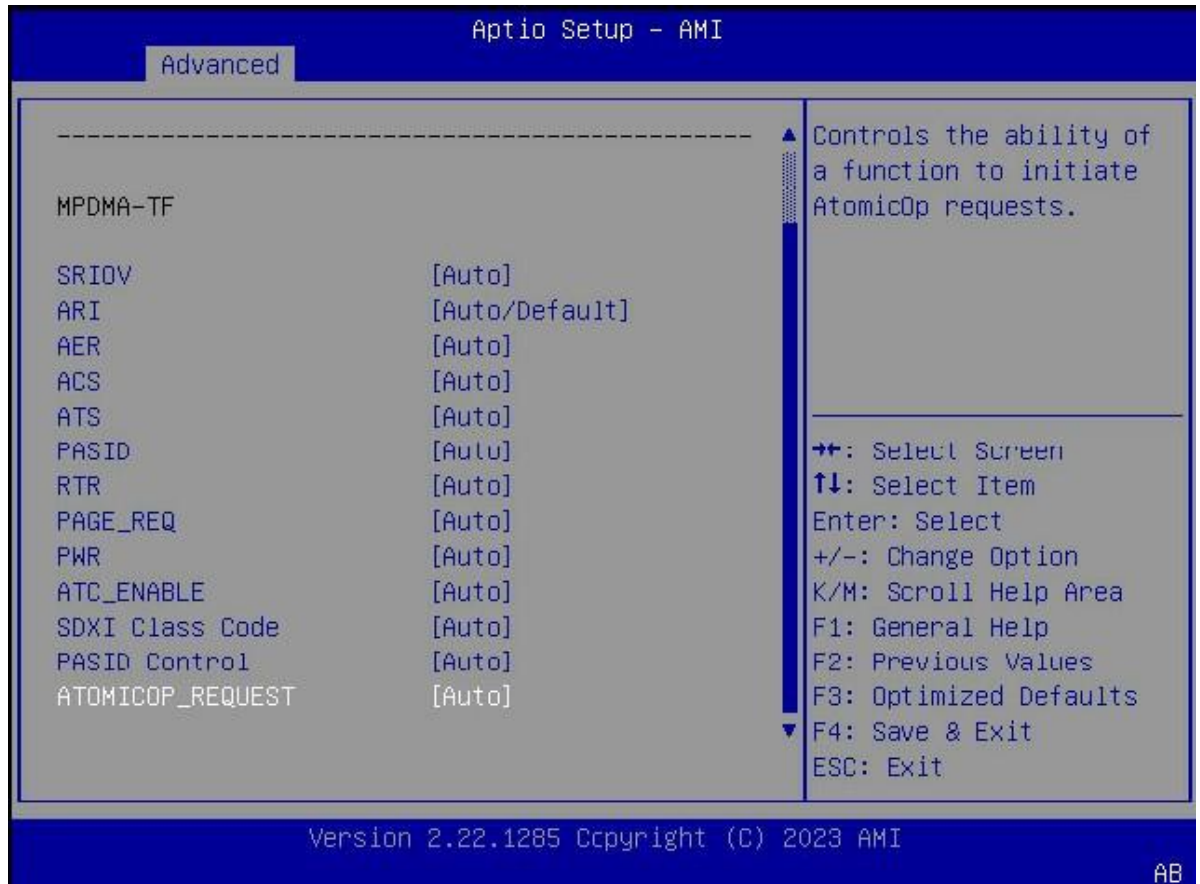


For a description of the parameters on the **nBif Common Option** screen, refer to [Table 3-52](#).

Table 3-52 Parameter Descriptions for the nBif Common Option Screen

Parameter	Description
MPDMA-TF	Sets MPDMA-TF parameters. Press Enter . The MPDMA-TF screen is displayed, as shown in Figure 3-71 .
RCC_DEVO	Sets RCC_DEVO parameters. Press Enter . The RCC_DEVO screen is displayed, as shown in Figure 3-72 through Figure 3-73 .

Figure 3-71 MPDMA-TF Screen



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

Table 3-53 Parameter Descriptions for the MPDMA-TF Screen

Parameter	Description	Default
SRIOV	Enables or disables the SRIOV feature. Options: ● Auto. ● Enabled: enables the SRIOV feature. ● Disabled: disables the SRIOV feature.	Auto
ARI	Enables or disables the ARI upper limit. Options: ● Auto: default. ● Enabled: enables the ARI upper limit. ● Disabled: disables the ARI upper limit.	Auto: default.

AER	Enables or disables the AER upper limit. Options: ● Auto. ● Enabled: enables the AER upper limit. ● Disabled: disables the AER upper limit.	Auto
-----	---	------

Parameter	Description	Default
ACS	Enables or disables the ACS upper limit. Options: ● Auto. ● Enabled: enables the ACS upper limit. ● Disabled: disables the ACS upper limit.	Auto
ATS	Enables or disables the ATS upper limit. Options: ● Auto. ● Enabled: enables the ATS upper limit. ● Disabled: disables the ATS upper limit.	Auto
PASID	Enables or disables the PASID feature. Options: ● Auto. ● Enabled: enables the PASID feature. ● Disabled: disables the PASID feature.	Auto
RTR	Enables or disables the RTR feature. Options: ● Auto. ● Enabled: enables the RTR feature. ● Disabled: disables the RTR feature.	Auto
PAGE_REQ	Enables or disables the page request feature. Options: ● Auto. ● Enabled: enables the page request feature. ● Disabled: disables the page request feature.	Auto

PWR	Enables or disables the PWR budget capability. Options: ● Auto. ● Enabled: enables the PWR budget capability. ● Disabled: disables the PWR budget capability.	Auto
ATC_ENABLE	Enables or disables the ATC_ENABLE feature. Options: ● Auto.	Auto

Parameter	Description	Default
	● Enabled: enables the ATC_ENABLE feature. ● Disabled: disables the ATC_ENABLE feature.	
SDXI Class Code	Enables or disables SDXI class codes. Options: ● Auto. ● Enabled: enables SDXI class codes. ● Disabled: disable SDXI class codes.	Auto
PASID Control	Enables or disables the PASID control feature. Options: ● Auto. ● Enabled: enables the PASID control feature. ● Disabled: disables the PASID control feature.	Auto
ATOMICOP_REQUEST	Enables or disables the ATOMICOP_REQUEST feature. Options: ● Auto. ● Enabled: enables the ATOMICOP_REQUEST feature. ● Disabled: disables the ATOMICOP_REQUEST feature.	Auto

Figure 3-72 RCC_DEV0 Screen—1

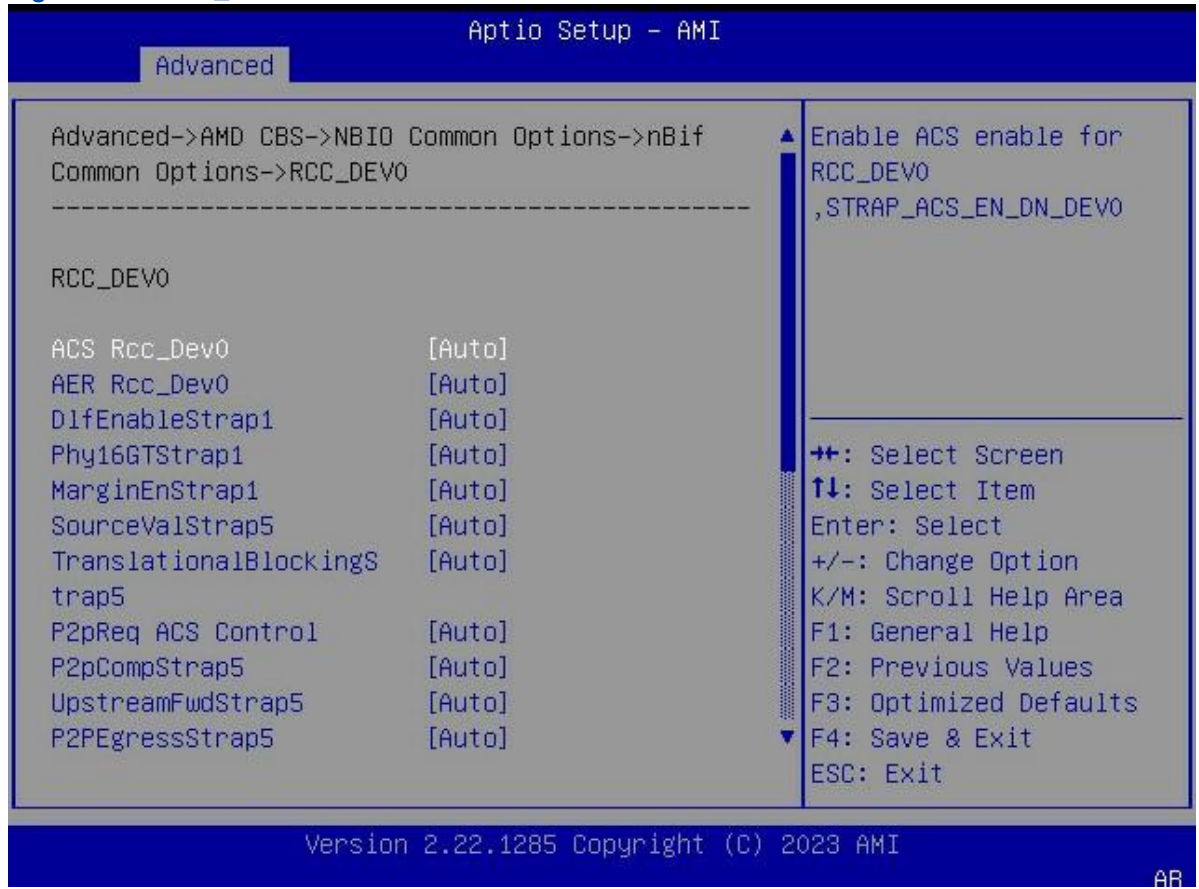
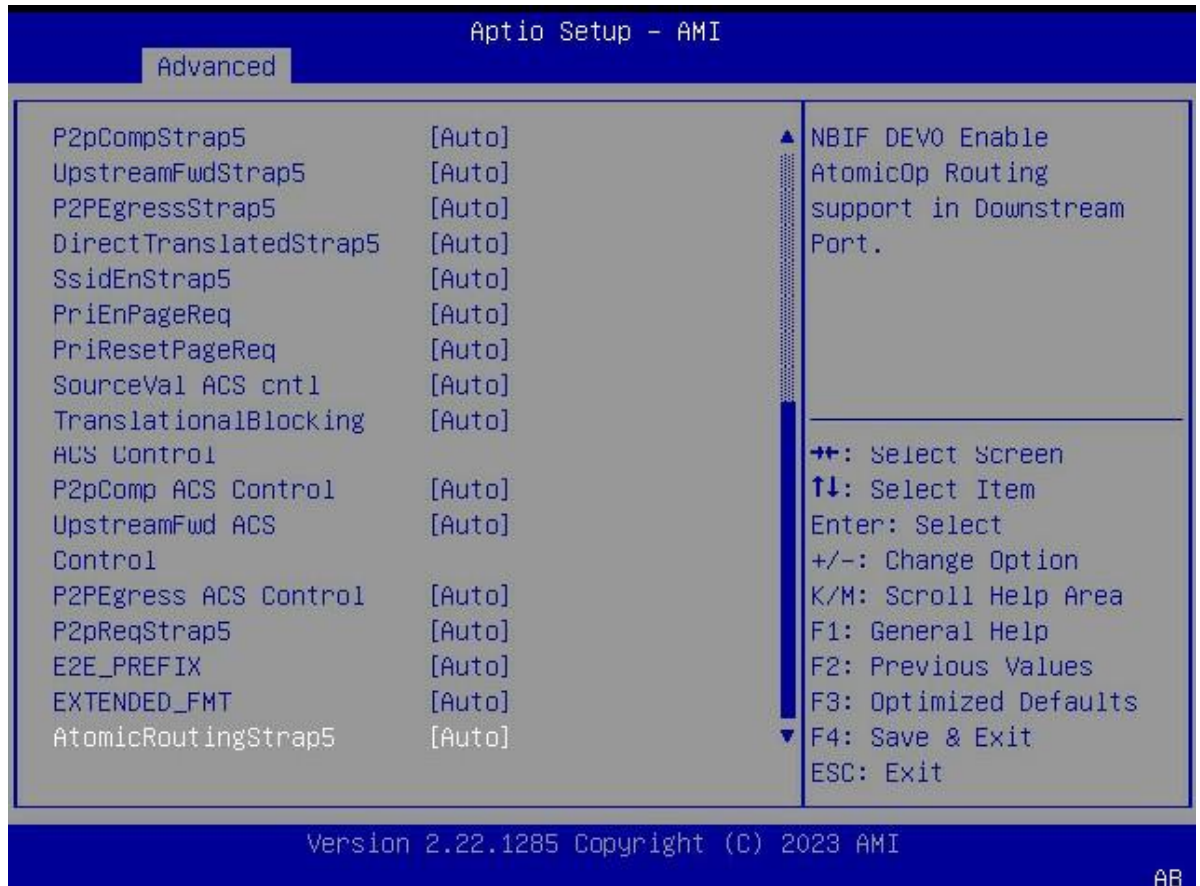


Figure 3-73 RCC_DEV0 Screen—2



For a description of the parameters on the **RCC_DEV0** screen, refer to [Table 3-54](#).

Table 3-54 Parameter Descriptions for the RCC_DEV0 Screen

Parameter	Description	Default
ACS Rcc_Dev0	Enables or disables ACS. Options: ● Auto. ● Enabled: enables ACS. ● Disabled: disables ACS.	Auto
AER Rcc_Dev0	Enables or disables AER. Options: ● Auto. ● Enabled: enables AER. ● Disabled: disables AER.	Auto
DlfEnableStrap1	Enables or disables the DlfEnableStrap1 feature. Options: ● Auto	Auto

Parameter	Description	Default
	● Enabled: enables the DIfEnableStrap1 feature. ● Disabled: disables the DIfEnableStrap1 feature.	
Phy16GTStrap1	Enables or disables the Phy16GTStrap1 feature. Options: ● Auto ● Enabled: enables the Phy16GTStrap1 feature. ● Disabled: disables the Phy16GTStrap1 feature.	Auto
MarginEnStrap1	Enables or disables the MarginEnStrap1 feature. Options: ● Auto. ● Enabled: enables the MarginEnStrap1 feature. ● Disabled: disables the MarginEnStrap1 feature.	Auto
SourceValStrap5	Enables or disables the SourceValStrap5 feature. Options: ● Auto. ● Enabled: enables the SourceValStrap5 feature. ● Disabled: disables the SourceValStrap5 feature.	Auto
TranslationalBlockingStrap5	Enables or disables the TranslationalBlockingStrap5 feature. Options: ● Auto. ● Enabled: enables the TranslationalBlockingStrap5 feature. ● Disabled: disables the TranslationalBlockingStrap5 feature.	Auto

P2pReq ACS Control	Enables or disables the P2pReq ACS control feature. Options: ● Auto.	Auto
--------------------	--	------

Parameter	Description	Default
	● Enabled: enables the P2pReq ACS control feature. ● Disabled: disables the P2pReq ACS control feature.	
P2pCompStrap5	Enables or disables the P2pCompStrap5 feature. Options: ● Auto: automatic mode. ● Enabled: enables the P2pCompStrap5 feature. ● Disabled: disables the P2pCompStrap5 feature.	Auto
UpstreamFwdStrap5	Enables or disables the UpstreamFwdStrap5 feature. ● Auto. ● Enabled: enables the UpstreamFwdStrap5 feature. ● Disabled: disables the UpstreamFwdStrap5 feature.	Auto
P2PEgressStrap5	Enables or disables the P2PEgressStrap5 feature. Options: ● Auto. ● Enabled: enables the P2PEgressStrap5 feature. ● Disabled: disables the P2PEgressStrap5 feature.	Auto

DirectTranslatedStrap5	Enables or disables the DirectTranslatedStrap5 feature. Options: ● Auto: automatic mode. ● Enabled: enables the DirectTranslatedStrap5 feature. ● Disabled: disables the DirectTranslatedStrap5 feature.	Auto
SsidEnStrap5	Enables or disables the SsidEnStrap5 feature. Options: ● Auto. ● Enabled: enables the SsidEnStrap5 feature.	Auto

Parameter	Description	Default
	● Disabled: disables the SsidEnStrap5 feature.	
PriEnPageReq	Enables or disables the PriEnPageReq feature. Options: ● Auto. ● Enabled: enables the PriEnPageReq feature. ● Disabled: disables the PriEnPageReq feature.	Auto
PriResetPageReq	Enables or disables the PriResetPageReq feature. Options: ● Auto. ● Enabled: enables the PriResetPageReq feature. ● Disabled: disables the PriResetPageReq feature.	Auto

SourceVal ACS cntl	Enables or disables the SourceVal ACS control feature. Options: ● Auto. ● Enabled: enables the SourceVal ACS control feature. ● Disabled: disables the SourceVal ACS control feature.	Auto
TranslationalBlocking ACS Control	Enables or disables the TranslationalBlocking ACS control feature. Options: ● Auto. ● Enabled: enables the TranslationalBlocking ACS control feature. ● Disabled: disables the TranslationalBlocking ACS control feature.	Auto
P2pComp ACS Control	Enables or disables the P2pComp ACS control feature. Options: ● Auto. ● Enabled: enables the P2pComp ACS control feature.	Auto

Parameter	Description	Default
	● Disabled: disables the P2pComp ACS control feature.	
UpstreamFwd ACS Control	Enables or disables UpstreamFwd ACS control. Options: ● Auto. ● Enabled: Enable UpstreamFwd ACS control. ● Disabled: Disable UpstreamFwd ACS control.	Auto

P2PEgress ACS Control	Enables or disables the P2PEgress ACS control feature. Options: ● Auto. ● Enabled: enables the P2PEgress ACS control feature. ● Disabled: disables the P2PEgress ACS control feature.	Auto
P2pReqStrap5	Enables or disables the P2pReqStrap5 feature. Options: ● Auto. ● Enabled: enables the P2pReqStrap5 feature. ● Disabled: disables the P2pReqStrap5 feature.	Auto
E2E_PREFIX	Enables or disables the E2E_PREFIX feature. Options: ● Auto. ● Enabled: enables the E2E_PREFIX feature. ● Disabled: disables the E2E_PREFIX feature.	Auto
EXTENDED_FMT	Enables or disables the EXTENDED_FMT feature. Options: ● Auto. ● Enabled: enables the EXTENDED_FMT feature.	Auto
Parameter	Description	Default
	● Disabled: disables the EXTENDED_FMT feature.	

AtomicRoutingStrap5	Enables or disables the AtomicOp routing support for downlink ports. Options: • Auto. • Enabled: enables the AtomicOp routing support for downlink ports. • Disabled: disables the AtomicOp routing support for downlink ports.	Auto
---------------------	---	------

Link EQ Preset Options

Figure 3-74 shows the **Link EQ Preset Options** screen.

Figure 3-74 Link EQ Preset Options Screen

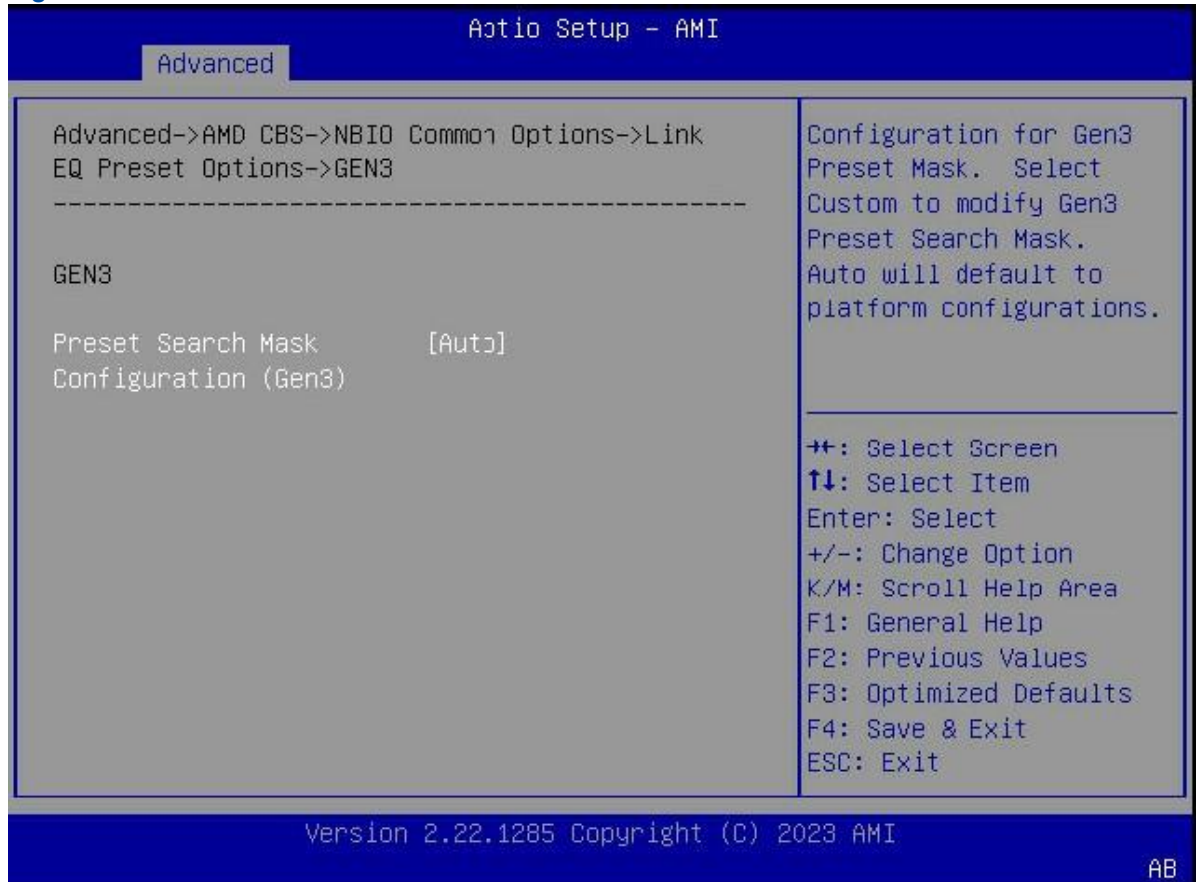


For a description of the parameters on the **Link EQ Preset Options** screen, refer to [Table 3-55](#).

Table 3-55 Parameter Descriptions for the Link EQ Preset Options Screen

Parameter	Description
-----------	-------------

GEN3	Sets the GEN3 presetting parameter. Press Enter . The GEN3 screen is displayed, as shown in Figure 3-75 .
GEN4	Sets the GEN4 presetting parameter.
GEN5	Sets the GEN5 presetting parameter.

Figure 3-75 GEN3 Screen

For a description of the parameters on the **GEN3** screen, refer to [Table 3-56](#).

Table 3-56 Parameter Descriptions for the GEN3 Screen

Parameter	Description	Default
Preset Search Mask Configuration (Gen3)	Sets the search mask presetting mode for Gen3. Options: ● Auto: The search mask presetting of Gen3 is automatically configured by the platform. ● Custom: The search mask presetting of Gen3 is customized by the user.	Auto

**Note**

The parameter for **GEN4** and **GEN5** is the same as that for **GEN3**.

3.2.7.5 FCH Common Options

FCH Common Options

Figure 3-76 shows the **FCH Common Options** screen.

Figure 3-76 FCH Common Options Screen



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

Table 3-57 Parameter Descriptions for the FCH Common Options Screen

Parameter	Description
I3C/I2C Configuration Options	Sets I3C/I2C parameters. For details, refer to I3C/I2C Configuration Options .
SATA Configuration Options	Sets SATA parameters. For details, refer to SATA Configuration Options .

USB Configuration Options	Sets USB parameters.
Parameter	Description
	For details, refer to USB Configuration Options .
Uart Configuration Options	Configure Uart parameters. For details, refer to Uart Configuration Options .
ESPI Configuration Options	Sets ESPI parameters. For details, refer to ESPI Configuration Options .
FCH RAS Options	Sets FCHRAS parameters. For details, refer to FCH RAS Options .
Miscellaneous Options	Set other parameters. For details, refer to Miscellaneous Options .

I3C/I2C Configuration Options

Figure 3-77 through Figure 3-78 show the **I3C/I2C Configuration Options** screen.

Figure 3-77 I3C/I2C Configuration Options—1

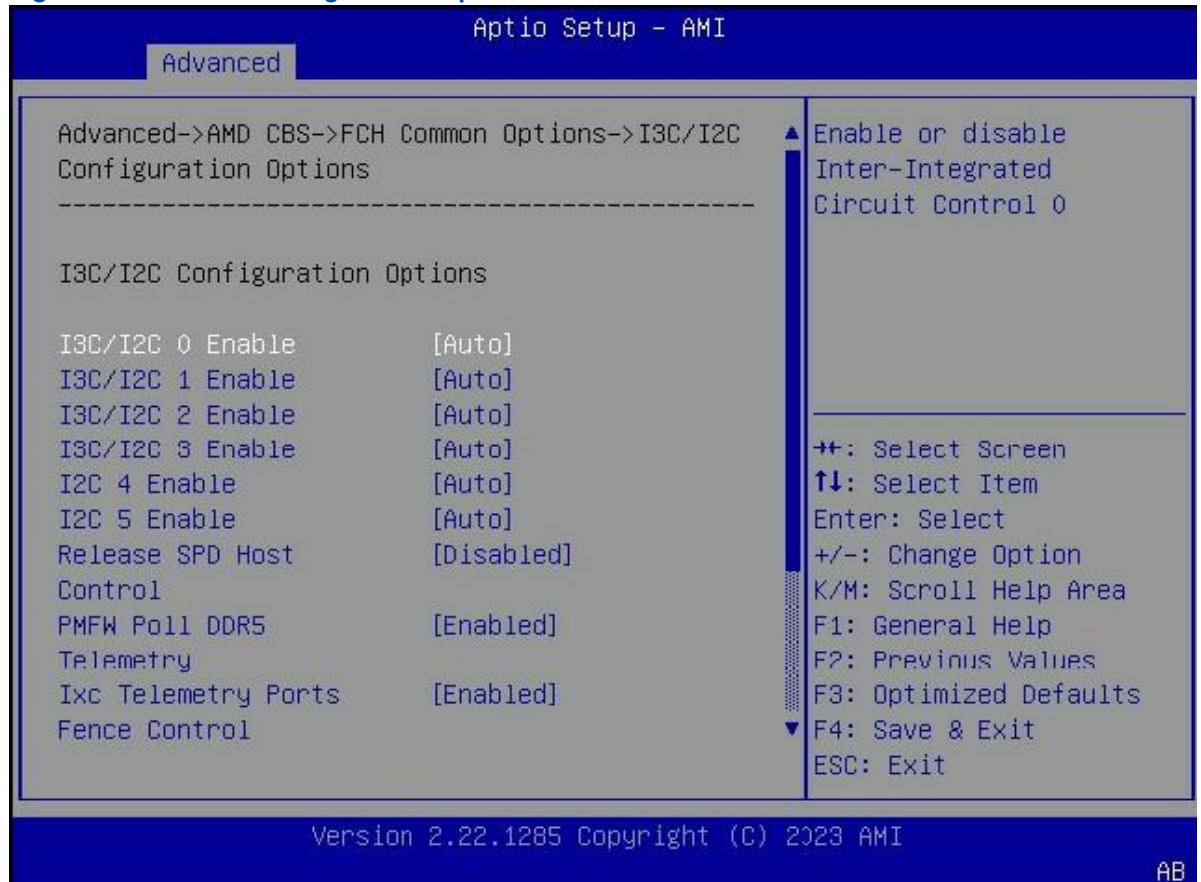
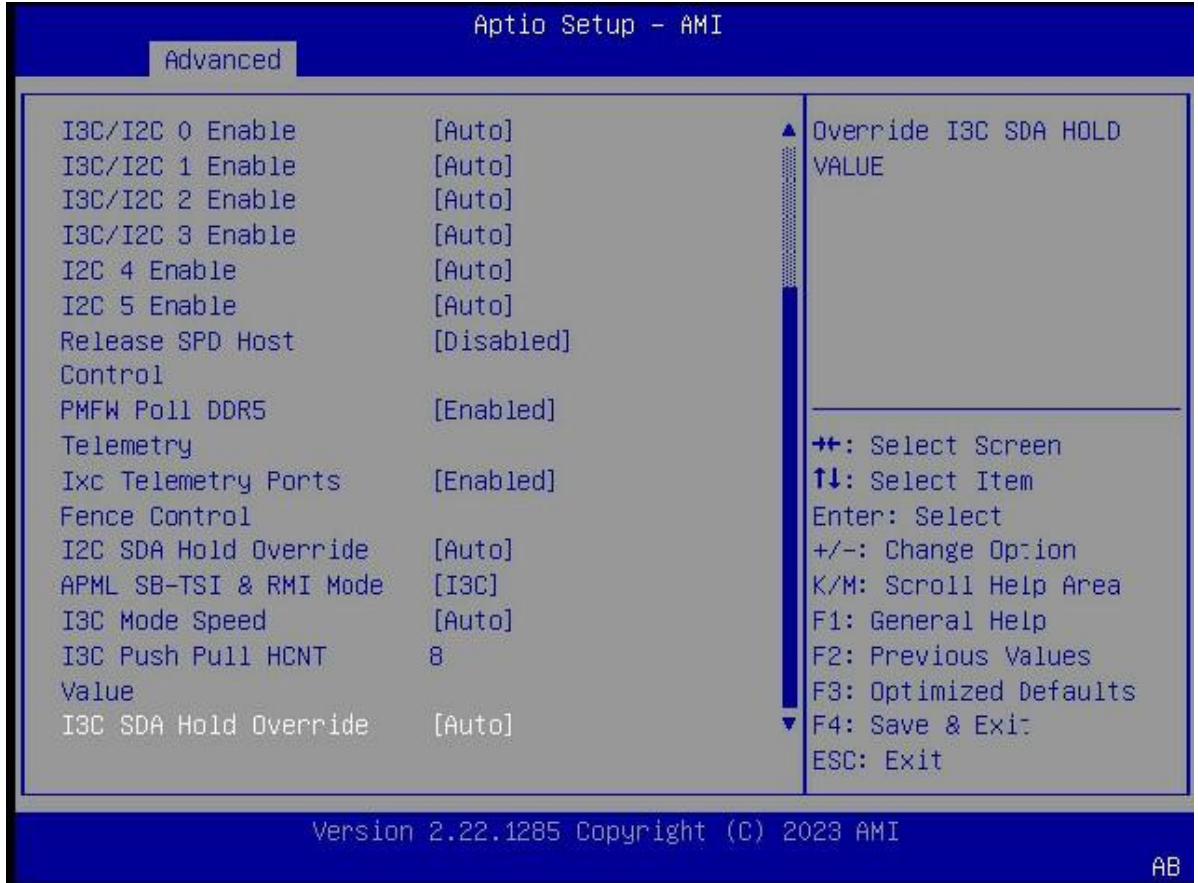


Figure 3-78 I3C/I2C Configuration Options—2



For a description of the parameters on the **I3C/I2C Configuration Options** screen, refer to [Table 3-58](#).

Table 3-58 Parameter Descriptions for the I3C/I2C Configuration Options Screen

Parameter	Description	Default
I3C/I2C 0 Enable	Enables or disables the internal integrated circuit control 0. Options: • Auto. • Enabled: enables internal integrated circuit control 0. • Disabled: disables internal integrated circuit control 0.	Auto
I3C/I2C 1 Enable	Enables or disables the internal integrated circuit control 1. Options: • Auto. • Enabled: enables internal integrated circuit control 1.	Auto

Parameter	Description	Default
	● Disabled: disables internal integrated circuit control 1.	
I3C/I2C 2 Enable	Enables or disables the internal integrated circuit control 2. Options: ● Auto. ● Enabled: enables internal integrated circuit control 2. ● Disabled: disables internal integrated circuit control 2.	Auto
I3C/I2C 3 Enable	Enables or disables the internal integrated circuit control 3. Options: ● Auto. ● Enabled: enables internal integrated circuit control 3. ● Disabled: disables internal integrated circuit control 3.	Auto
I2C 4 Enable	Enables or disables the internal integrated circuit control 4. Options: ● Auto. ● Enabled: enables internal integrated circuit control 4. ● Disabled: disables internal integrated circuit control 4.	Auto
I2C 5 Enable	Enables or disables the internal integrated circuit control 5. Options: ● Auto. ● Enabled: enables internal integrated circuit control 5. ● Disabled: disables internal integrated circuit control 5.	Auto

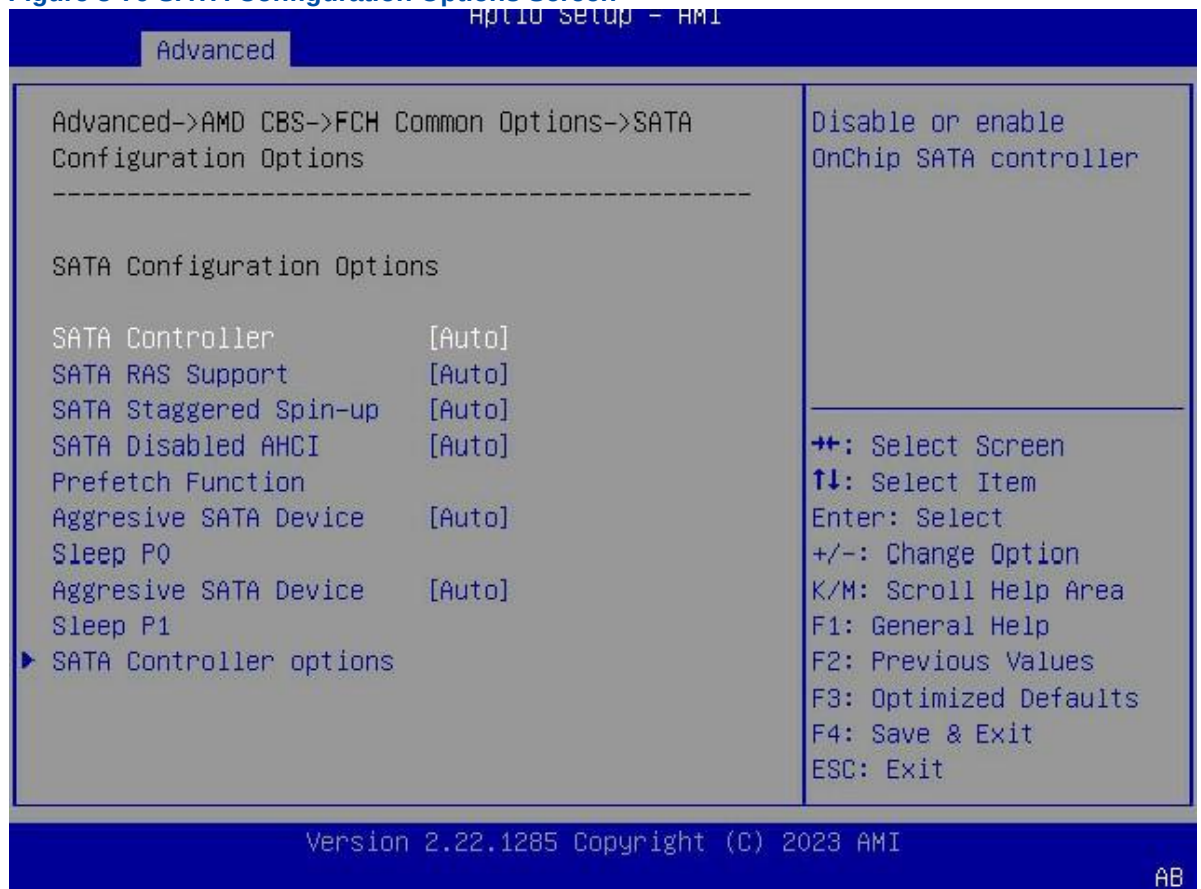
Release SPD Host Control	Enables or disables SPD host control release. Options: - Enabled: enables SPD host control release. - Disabled: disables SPD host control release.	Disabled
PMFW Poll DDR5 Telemetry	Enables or disables PMFW polling DDR5 telemetry. Options:	Enabled
Parameter	Description	Default
	- Enabled: enables PMFW polling DDR5 telemetry. - Disabled: disables PMFW polling DDR5 telemetry.	
Ixc Telemetry Ports Fence Control	Enables or disables the control on the Ixc telemetry port fence. Options: - Enabled: enables the control on the Ixc telemetry port fence. - Disabled: disables the control on the Ixc telemetry port fence.	Enabled
I2C SDA Hold Override	Enables or disables the Override I2C SDA_TX_HOLD and SDA_RX_HOLD features. Options: - Auto. - Enabled: enables the Override I2C SDA_TX_HOLD and SDA_RX_HOLD features. - Disabled: disables the Override I2C SDA_TX_HOLD and SDA_RX_HOLD features.	Auto
APML SB-TSI & RMI Mode	Select the APML SB -TSI and RMI modes. Options: - I3C - I2C	I3C
I3C Mode Speed	Select the I3C mode speed. Options: - Auto - SDR2 (6 MHz) - SDR0 (12.5 MHz)	Auto
I3C Push Pull HCNT Value	Sets the I3C push-pull HCNT value.	8

I3C SDA Hold Override	Enables or disables the I3C SDA Hold Override feature. Options: • Auto. • Enabled: enables the I3C SDA Hold Override feature. • Disabled: disables the I3C SDA Hold Override feature.	Auto
-----------------------	---	------

SATA Configuration Options

Figure 3-79 shows the **SATA Configuration Options** screen.

Figure 3-79 SATA Configuration Options Screen



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

Table 3-59 Parameter Descriptions for the SATA Configuration Options Screen

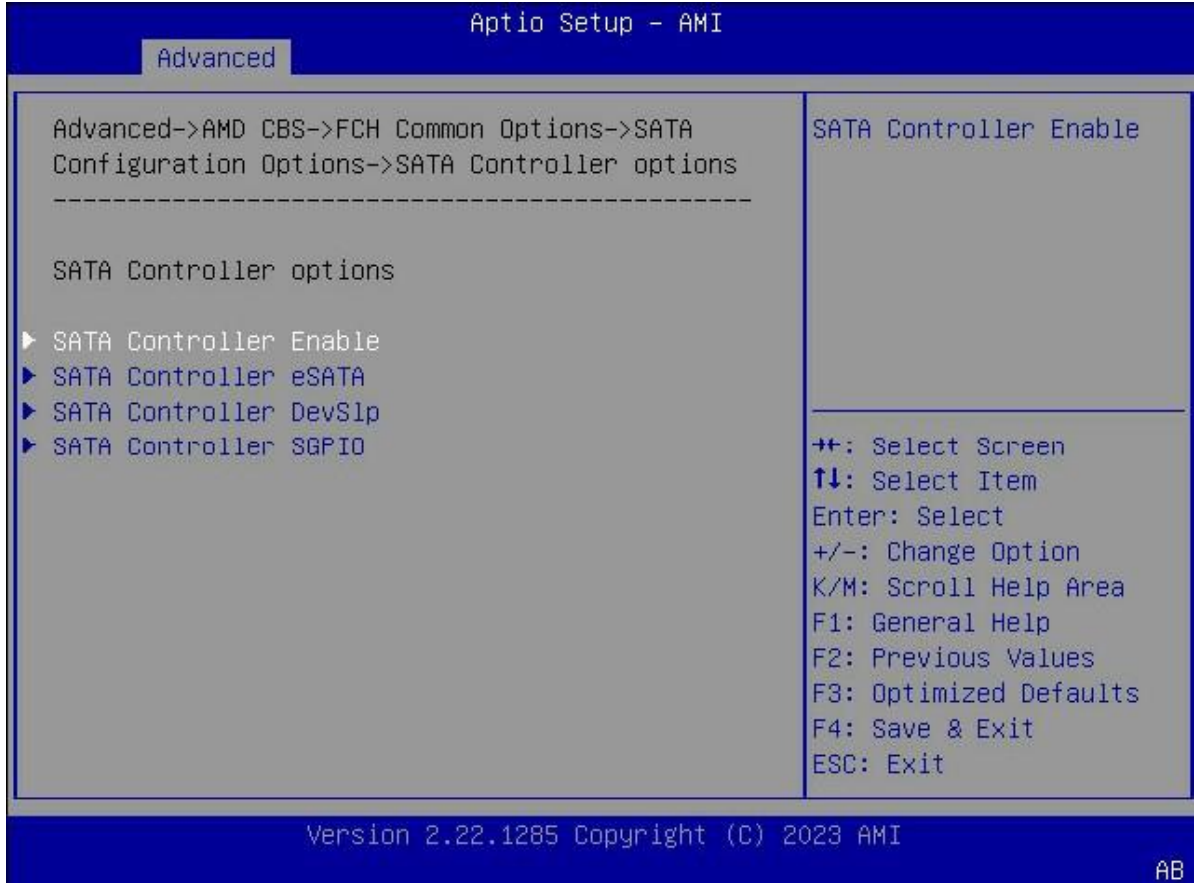
Parameter	Description	Default
-----------	-------------	---------

SATA Controller	Enables or disables SATA controllers. Options: ● Auto. ● Enabled: enables SATA controllers. ● Disabled: disables SATA controllers.	Auto
SATA RAS Support	Enables or disables SATA RAS support. Options: ● Auto. ● Enabled: enables SATA RAS support. ● Disabled: disables SATA RAS support.	Auto
SATA Staggered Spin-up	Enables or disables the staggered SATA spin-up feature. Options:	Auto

Parameter	Description	Default
	● Auto. ● Enabled: enables the staggered SATA spin-up feature. ● Disabled: disables the staggered SATA spin-up feature.	
SATA Disabled AHCI Prefetch Function	Enables or disables the AHCI prefetching feature for SATA devices. Options: ● Auto. ● Enabled: enables the AHCI prefetching feature for SATA devices. ● Disabled: disables the AHCI prefetching feature for SATA devices.	Auto

Aggressive SATA Device Sleep P0	Enables or disables aggressive sleep mode for SATA devices connected to port P0. Options: ● Auto. ● Enabled: enables aggressive sleep mode for SATA devices connected to port P0. ● Disabled: disables aggressive sleep mode for SATA devices connected to port P0.	Auto
Aggressive SATA Device Sleep P1	Enables or disables aggressive sleep mode for SATA devices connected to port P1. Options: ● Auto. ● Enabled: enables aggressive sleep mode for SATA devices connected to port P1. ● Disabled: disables aggressive sleep mode for SATA devices connected to port P1.	Auto
SATA Controller options	Sets the SATA controller parameters. Press the Enter . The SATA Controller options screen is displayed, as shown in Figure 3-80 .	-

Figure 3-80 SATA Controller Options Screen



For a description of the parameters on the **SATA Controller options** sheet, refer to [Table 3-60](#).

Table 3-60 Parameter Descriptions for the SATA Controller Options Screen

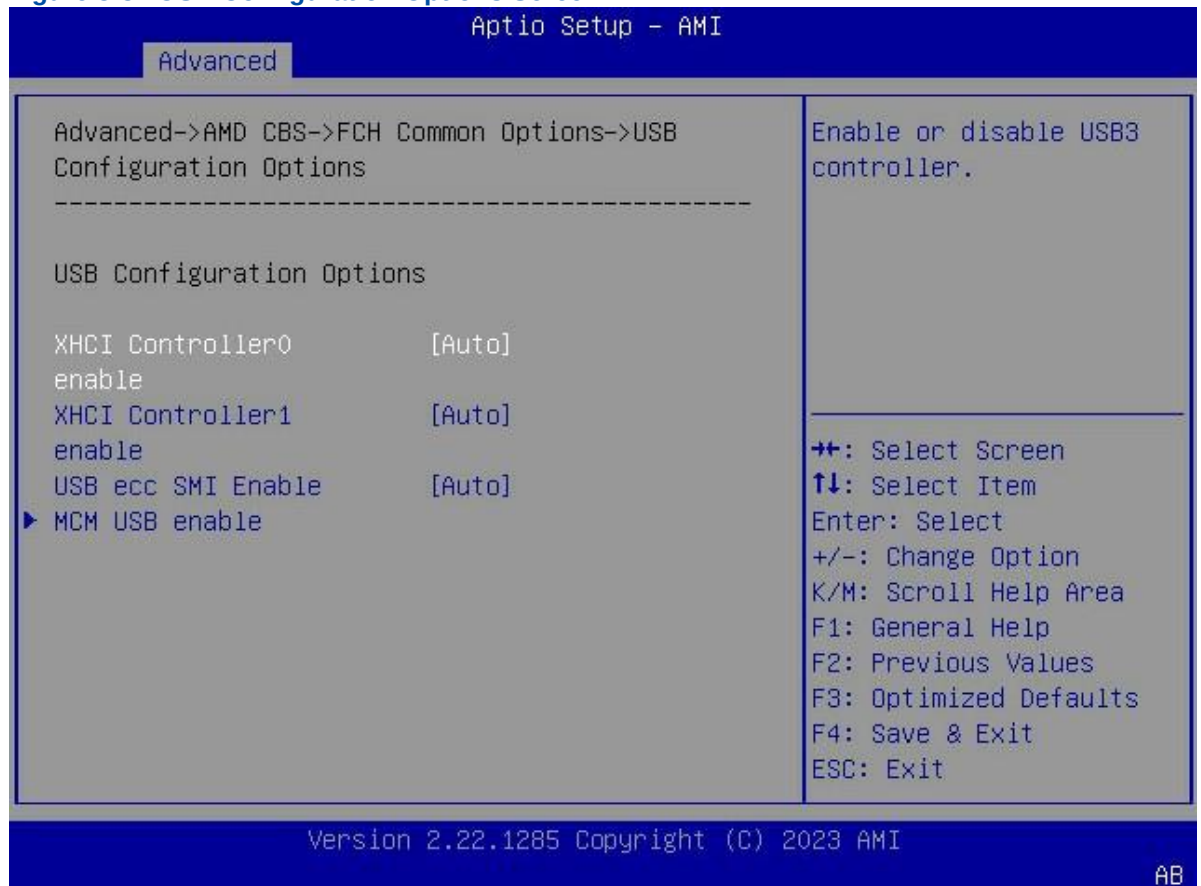
Parameter	Description
SATA Controller Enable	Configure Enabled parameters. Press the Enter key. The SATA Controller Enable screen is displayed. You can set the following parameters: ● Sata0Enabled: enables or disables Sata0. Default: Auto. ● Sata1Enabled: enables or disables Sata1. Default: Auto. ● Sata2Enabled: enables or disables Sata2. Default: Auto. ● Sata3Enabled: enables or disables Sata3. Default: Auto. ● Sata4 (Socket1) Enable ● Sata5 (Socket1) Enable ● Sata6 (Socket1) Enable ● Sata7 (Socket1) Enable
SATA Controller eSATA	Sets SATA controller eSATA parameters.
SATA Controller DevSlp	Sets SATA controller DevSlp parameters.
SATA Controller SGPIO	Sets SATA controller SGPIO parameters.

Parameter	Description
	Press the Enter key. The SATA Controller SGPIO screen is displayed. You can set the parameters. ● SATA0 SGPIO: enables or disables PSata0 SGPIO. Default: Auto. ● SATA1 SGPIO: enables or disables SATA1 SGPIO. Default: Auto. ● SATA2 SGPIO: enables or disables SATA2 SGPIO. Default: Auto. ● SATA3 SGPIO: enables or disables SATA3 SGPIO. Default: Auto. ● SATA4 SGPIO: enables or disables SATA4 SGPIO. Default: Auto. ● SATA5 SGPIO: enables or disables SATA5 SGPIO. Default: Auto. ● SATA6 SGPIO: enables or disables SATA6 SGPIO. Default: Auto. ● SATA7 SGPIO: enables or disables SATA7 SGPIO. Default: Auto.

USB Configuration Options

Figure 3-81 shows the **USB Configuration Options** screen.

Figure 3-81 USB Configuration Options Screen

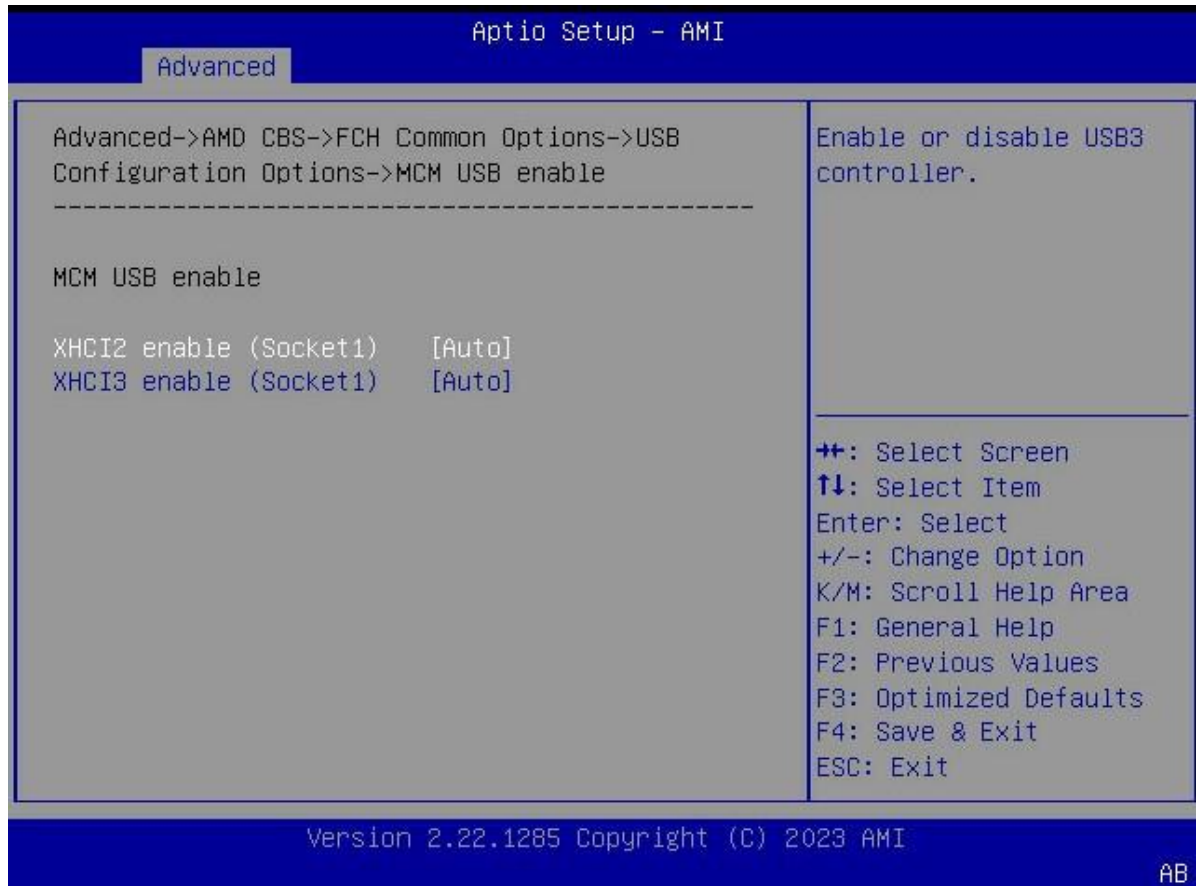


For a description of the parameters on the **USB Configuration Options** screen, refer to [Table 3-61](#).

Table 3-61 Parameter Descriptions for the USB Configuration Options Screen

Parameter	Description	Default
XHCI Controller0 enable	Enables or disables XHCI controller0. Options: ● Auto. ● Enabled: enables XHCI controller0. ● Disabled: disables XHCI controller0.	Auto
XHCI Controller1 enable	Enables or disables XHCI controller1. Options: ● Auto. ● Enabled: enables XHCI controller1. ● Disabled: disables XHCI controller1.	Auto
USB ecc SMI Enable	Enables or disables the USB ECC SMI feature. Options: ● Auto. ● Enabled: Enables the USB ECC SMI feature. ● Disabled: Disables the USB ECC SMI feature.	Auto
MCM USB enable	Sets MCM USB enable parameters. Press Enter . The MCM USB Enable screen is displayed, as shown in Figure 3-82 .	-

Figure 3-82 MCM USB Enable Screen



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

Table 3-62 Parameter Descriptions for the MCM USB Enable Screen

Parameter	Description	Default
XHCI2 enable (Socket1)	Enables or disables XHCI2. Options: ● Auto. ● Enabled: enables XHCI2. ● Disabled: disables XHCI2.	Auto
XHCI3 enable (Socket1)	Enables or disables XHCI3. Options: ● Auto. ● Enabled: enables XHCI3. ● Disabled: disables XHCI3.	Auto

Uart Configuration Options

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

Figure 3-83 Uart Configuration Options Screen



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

Table 3-63 Parameter Descriptions for the Uart Configuration Options Screen

Parameter	Description	Default
Uart 0 enable	Enables or disables the Uart 0 feature. Options: ● Auto. ● Enabled: enables the Uart 0 feature. ● Disabled: disables the Uart 0 feature.	Auto
Uart 1 enable	Enables or disables the Uart 1 feature. Options: ● Auto. ● Enabled: enables the Uart 1 feature. ● Disabled: disables the Uart 1 feature.	Auto
Uart 2 enable	Enables or disables the Uart 2 feature. Options: ● Auto. ● Enabled: enables the Uart 2 feature.	Auto

Parameter	Description	Default
	When this parameter is set to Enabled , Uart 0 does not monitor hardware traffic. Disabled: disables the Uart 2 feature.	
Uart 3 enable	Enables or disables the Uart 3 feature. Options: - Auto. - Enabled: enables the Uart 3 feature. - Disabled: disables the Uart 3 feature.	Auto

ESPI Configuration Options

Figure 3-84 shows the **ESPI Configuration Options** screen.

Figure 3-84 ESPI Configuration Options Screen



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

Table 3-64 Parameter Descriptions for the ESPI Configuration Options Screen

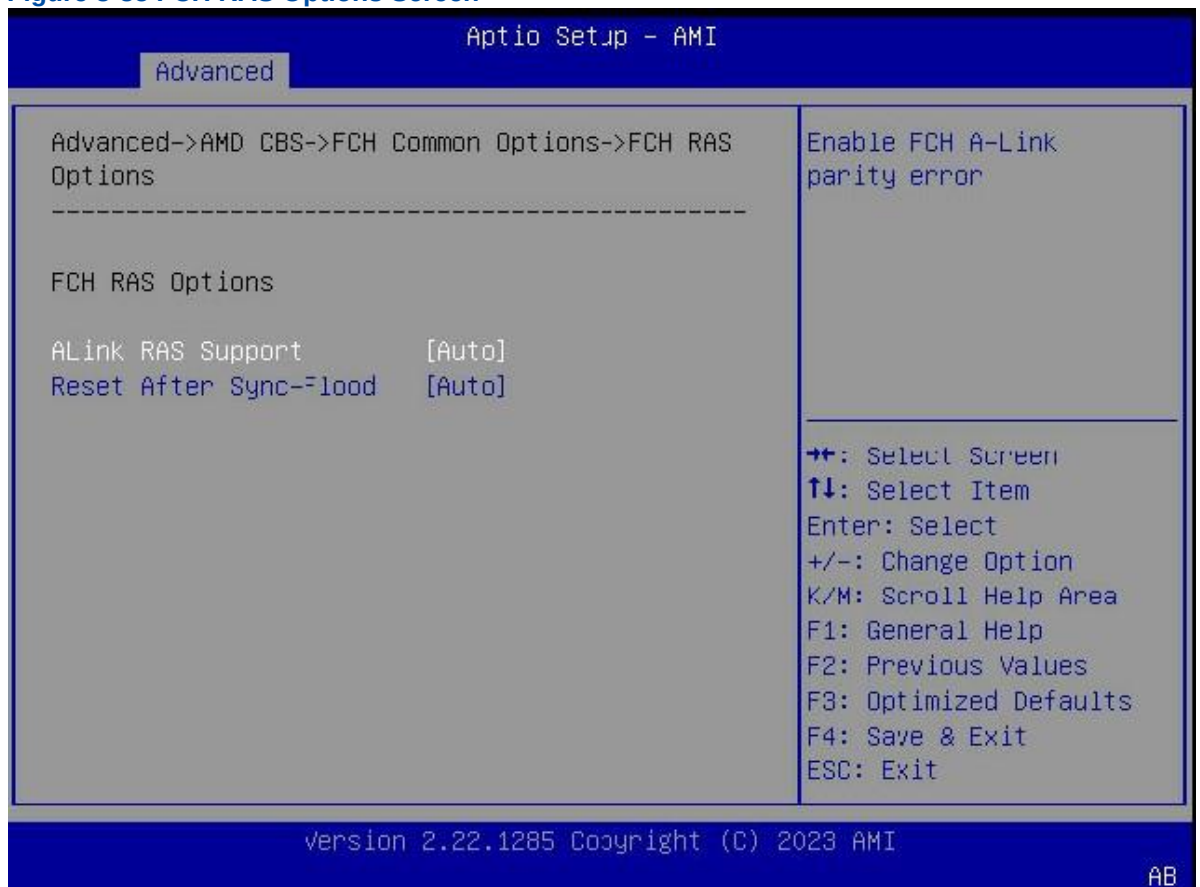
Parameter	Description	Default
-----------	-------------	---------

ESPI Enable	Enables or disables ESPI.	Auto
Parameter	Description	Default
	Options: • Auto. • Enabled: enables ESPI. • Disabled: disables ESPI.	

FCH RAS Options

Figure 3-85 shows the **FCH RAS Options** screen.

Figure 3-85 FCH RAS Options Screen



For a description of the parameters on the **FCH RAS Options** screen, refer to [Table 3-65](#).

Table 3-65 Parameter Descriptions for the FCH RAS Options Screen

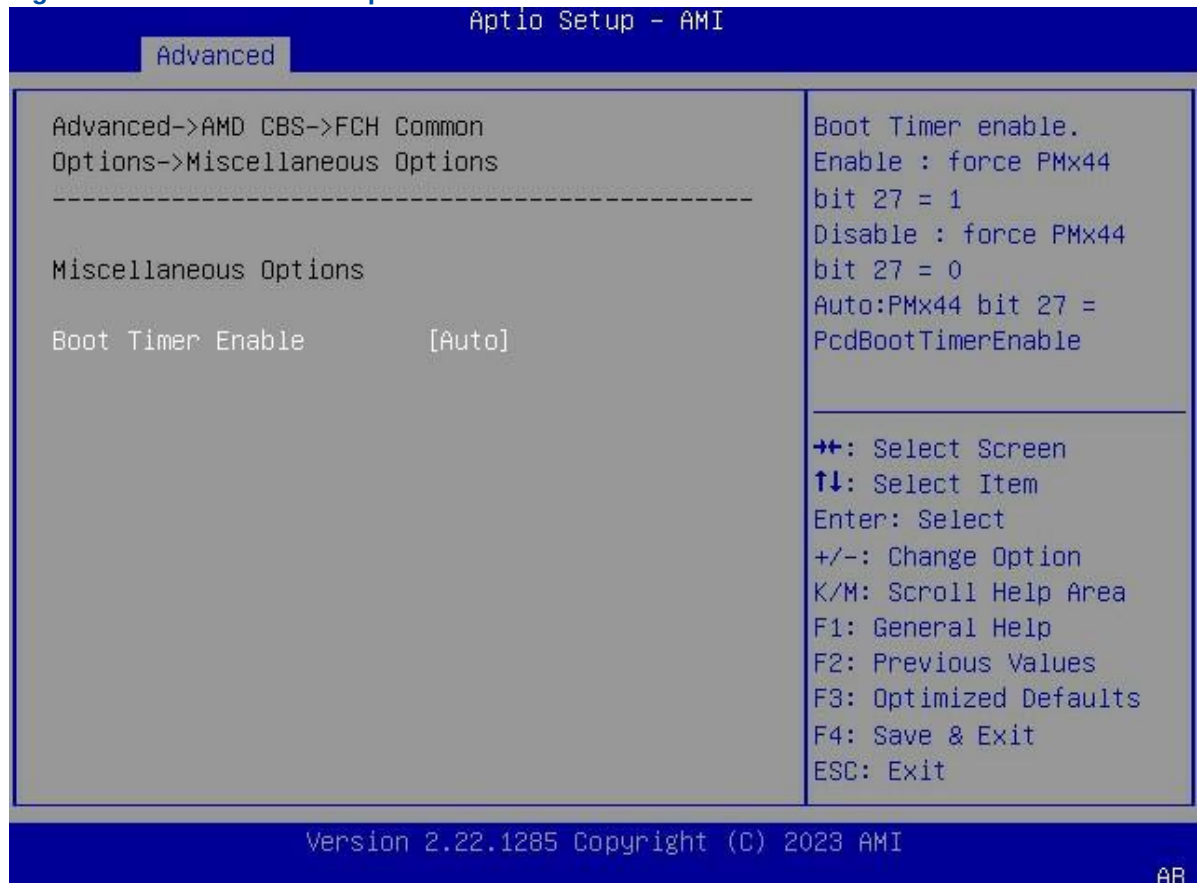
Parameter	Description	Default
-----------	-------------	---------

ALink RAS Support	Enables or disables A-Link parity. Options: ● Auto. ● Enabled: enables A-Link parity. ● Disabled: disables A-Link parity.	Auto
Reset After Sync-Flood	Enables or disables reset after sync-flood.	Auto
Parameter	Description	Default
	Options: ● Auto. ● Enabled: enables reset after sync-flood. ● Disabled: disables reset after sync-flood.	

Miscellaneous Options

Figure 3-86 shows the **Miscellaneous Options** screen.

Figure 3-86 Miscellaneous Options Screen



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

Table 3-66 Parameter Descriptions for the Miscellaneous Options Screen

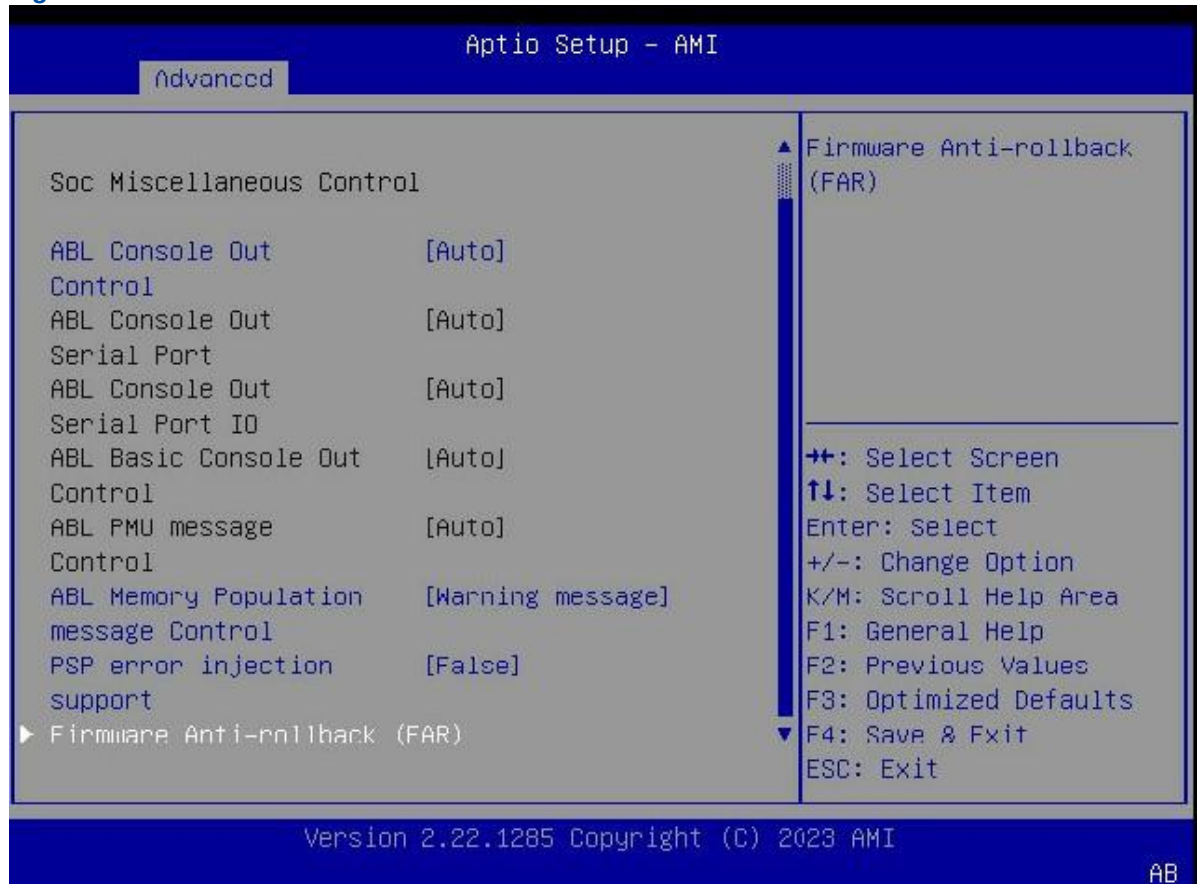
Parameter	Description	Default
Boot Time Enable	Enables or disables the boot time counter. Options: ● Auto: PMx44 bit 27 = PcdBootTimerEnable. ● Enabled: forcibly sets PMx44 bit 27 to 1. ● Disabled: forcibly sets PMx44 bit 27 to 0.	Auto

3.2.7.6 Soc Miscellaneous Control

Soc Miscellaneous Control

Figure 3-87 shows the **Soc Miscellaneous Control** screen.

Figure 3-87 Soc Miscellaneous Control Screen



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

Table 3-67 Parameter Descriptions for the Soc Miscellaneous Control Screen

Parameter	Description	Default
-----------	-------------	---------

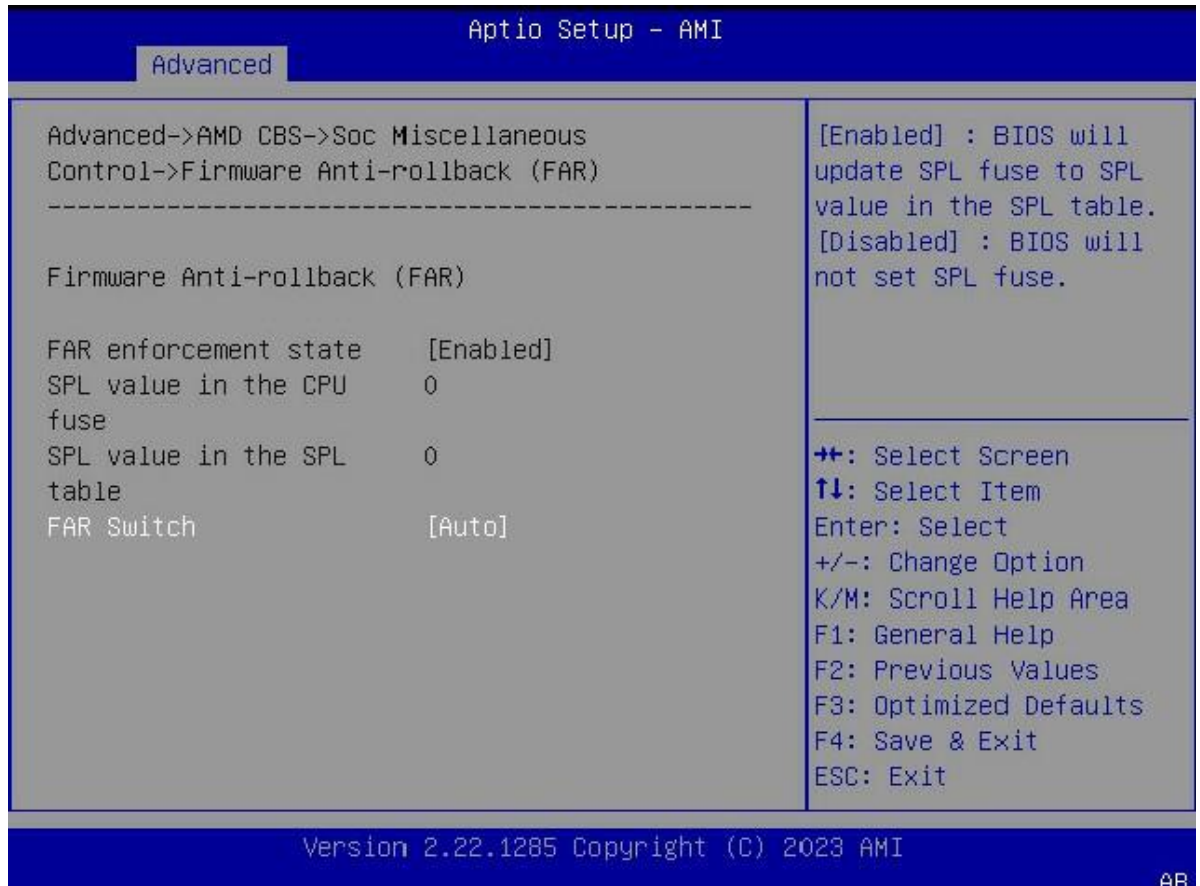
ABL Console Out Control	Enables or disables the ABL console output feature. Options: ● Auto. ● Enabled: enables the ABL console output feature. ● Disabled: disables the ABL console output feature.	Auto
ABL Console Out Serial Port	This parameter can be set when ABL Console Out Control is set to Enabled .	Auto

Parameter	Description	Default
	Select the serial port for ABL console output. Options: ● Auto ● eSPI UART ● SOC UART0 ● SOC UART1	
ABL Console Out Serial Port IO	This parameter can be set when ABL Console Out Serial Port is set to eSPI UART . Select serial port I/O for ABL console output. Options: ● Auto ● 0x3F8 ● 0x2F8 ● 0x3E8 ● 0x2E8	Auto
ABL Basic Console Out Control	This parameter can be set when ABL Console Out Control is set to Enabled . Enables or disables the basic console output feature for the ABL. Options: ● Auto. ● Enabled: enables the basic console output feature for the ABL. ● Disabled: disables the basic console output feature for the ABL.	Auto

ABL PMU Message Control	This parameter can be set when ABL Console Out Control is set to Enabled. Select the total number of PMU debugging messages. Options: ● Auto ● Detailed debug message ● Coarse debug message ● Stage completion ● Assertion messages ● Firmware completion message only	Auto
ABL Memory Population message Control	Select the ABL Memory population message. Options: ● Warning message ● Fatal error	Warning message
PSP error injection support	Enables or disables PSP error injection support.	Disabled
Parameter	Description	Default
	Options: ● Enabled: enables PSP error injection support. ● Disabled: disables PSP error injection support.	
Firmware Anti-rollback (FAR)	Sets firmware anti-rollback (FAR) parameters. For details, refer to Firmware Anti-rollback (FAR).	-
Firmware Anti-rollback (FAR)		

Figure 3-88 shows the **Firmware Anti-rollback (FAR)** screen.

Figure 3-88 Firmware Anti-rollback (FAR) Screen



For a description of the parameters on the **Firmware Anti-rollback (FAR)** screen, refer to [Table 3-68](#).

Table 3-68 Parameter Descriptions for the Firmware Anti-rollback (FAR) Screen

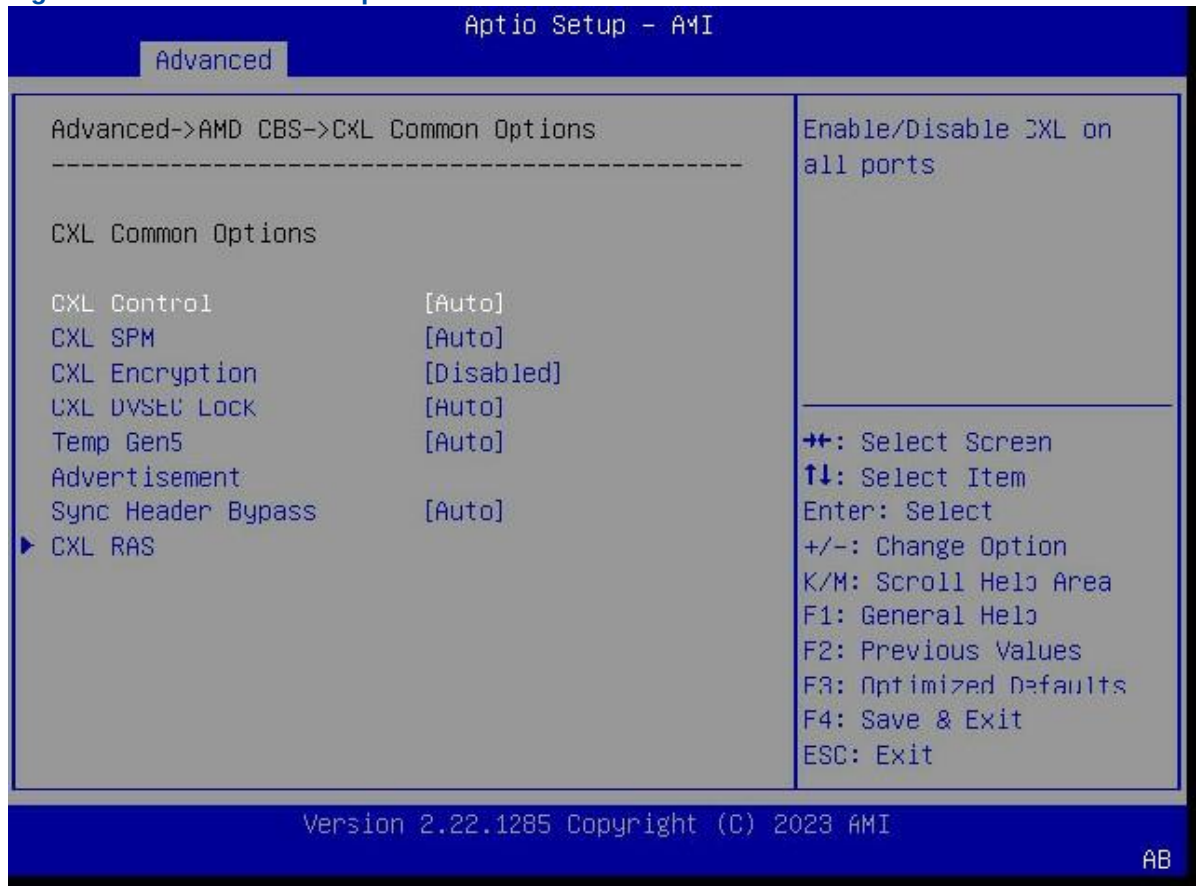
Parameter	Description	Default
FAR enforcement state	Enables or disables the FAR enforcement state.	Enabled
Parameter	Description	Default
	Options: - Enabled: enables the FAR enforcement state. - Disabled: disables the FAR enforcement state.	
SPL value in the CPU fuse	Sets the SPL value in the CPU fuse.	0
SPL value in the SPL table	Sets the SPL value in the SPL table.	0

FAR Switch	Enables or disables the FAR feature. Options: • Auto. • Enabled: updates the SPL fuse to the SPL value in the SPL table. • Disabled: No SPL fuse is set.	Auto
------------	---	------

3.2.7.7 CXL Common Options

CXL Common Options

Figure 3-89 shows the **CXL Common Options** screen.

Figure 3-89 CXL Common Options Screen

For a description of the parameters on the **CXL Common Options** screen, refer to [Table 3-69](#).

Table 3-69 Parameter Descriptions for the CXL Common Options Screen

Parameter	Description	Default
CXL Control	Enable or disable CXL on all ports. Options: ● Auto. ● Enabled: enables CXL on all ports. ● Disabled: disables CXL on all ports.	Auto
CXL SPM	Enables or disables the CXL SPM feature. Options: ● Auto. ● Enabled: enables the CXL SPM feature. ● Disabled: disables the CXL SPM feature.	Auto

CXL Encryption	Enables or disables CXL encryption. Options: Enabled: enables CXL encryption.	Disabled
Parameter	Description	Default
	Disabled: disables CXL encryption.	
CXL DVSEC Lock	Enables or disables the CXL DVSEC locking feature. Options: - Auto. - Enabled: enables the CXL DVSEC locking feature. - Disabled: disables the CXL DVSEC locking feature.	Auto
Temp Gen5 Advertisementk	Enables or disables the Temp Gen5 broadcast feature. Options: - Auto. - Enabled: enables the Temp Gen5 broadcast feature. - Disabled: disables the Temp Gen5 broadcast feature.	Auto
Sync Header Bypass	Enables or disables the Sync Header Bypass feature. Options: - Auto. - Enabled: enables the Sync Header Bypass feature. - Disabled: disables the Sync Header Bypass feature.	Auto
CXL RAS	Sets CXL RAS parameters. For details, refer to CXL RAS .	-

CXL RAS

[Figure 3-90](#) shows the **CXL RAS** screen.

Figure 3-90 CXL RAS Screen



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

Table 3-70 Parameter Descriptions for the CXL RAS Screen

Parameter	Description	Default
CXL Protocol Error Reporting	Select the reporting mechanism for CXL protocol errors. Options: ● Disabled ● SameAsPcieAer ● ForceAerFwFirstIfCxlPresent	SameAsPcieAer
CXL Component Error Reporting	Select the reporting mechanism for CXL component errors. Options: ● OS First ● FW-First	FW-First

3.2.8 UEFI Variables Protection

[Figure 3-91](#) shows the **UEFI Variables Protection** screen.

Figure 3-91 UEFI Variables Protection Screen



For a description of the parameters on the **UEFI Variables Protection** screen, refer to [Table 3-71](#).

Table 3-71 Parameter Descriptions for the UEFI Variables Protection Screen

Parameter	Description	Default
Password protection of Runtime Variables	Enables or disables the password protection feature for runtime variables. Options: - Enabled: enables the password protection feature for runtime variables. - Disabled: disables the password protection feature for runtime variables.	Disabled

3.2.9 Serial Port Console Redirection

[Figure 3-92](#) through [Figure 3-93](#) show the **Serial Port Console Redirection** screen.

Figure 3-92 Serial Port Console Redirection Screen—1

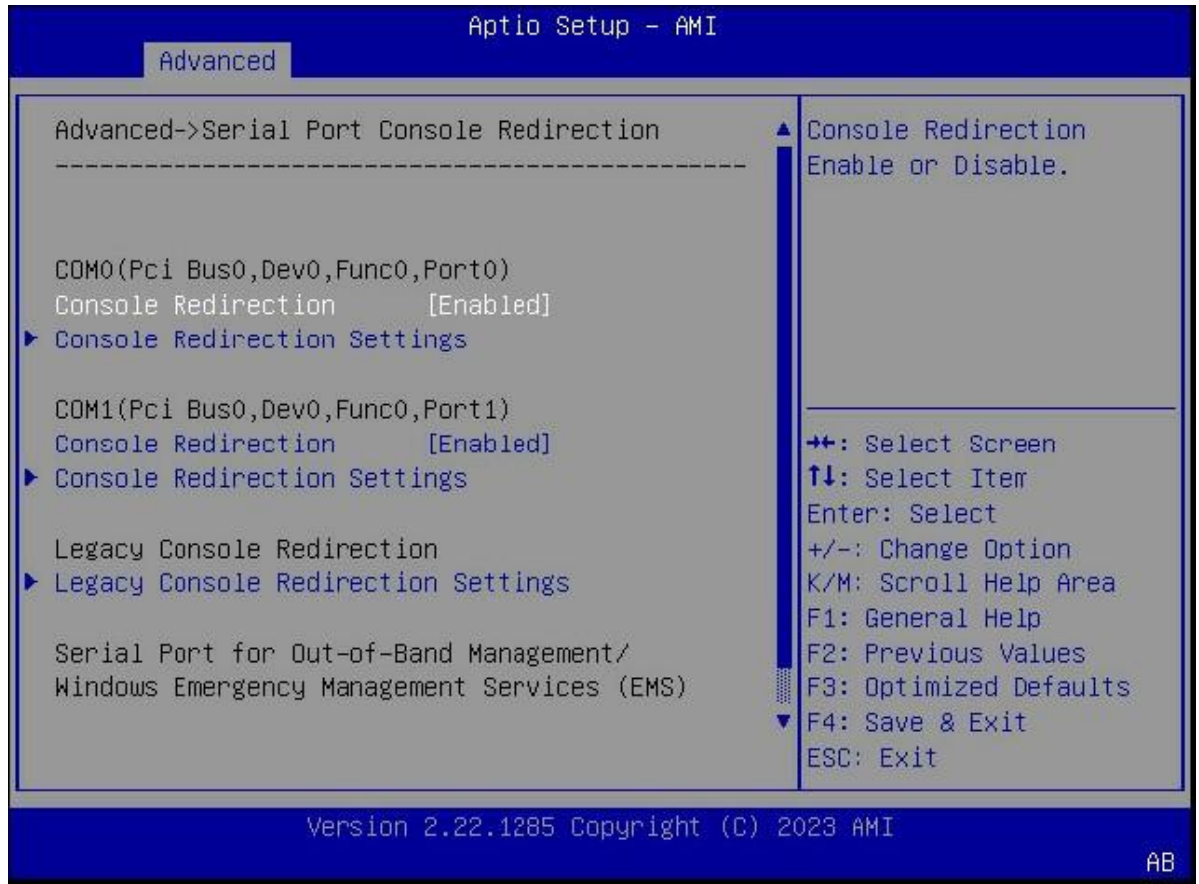
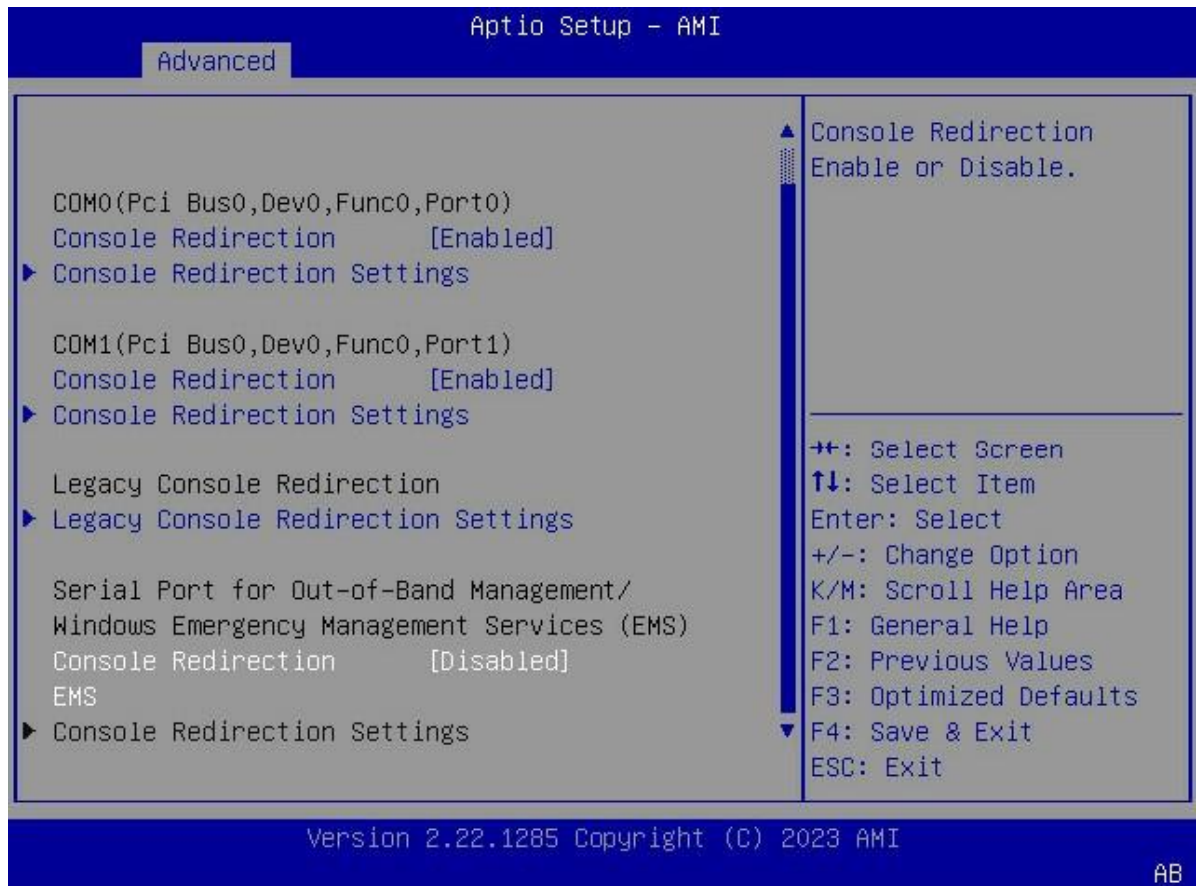


Figure 3-93 Serial Port Console Redirection Screen—2



For a description of the parameters on the **Serial Port Console Redirection** screen, refer to [Table 3-72](#).

Table 3-72 Parameter Descriptions for the Serial Port Console Redirection Screen

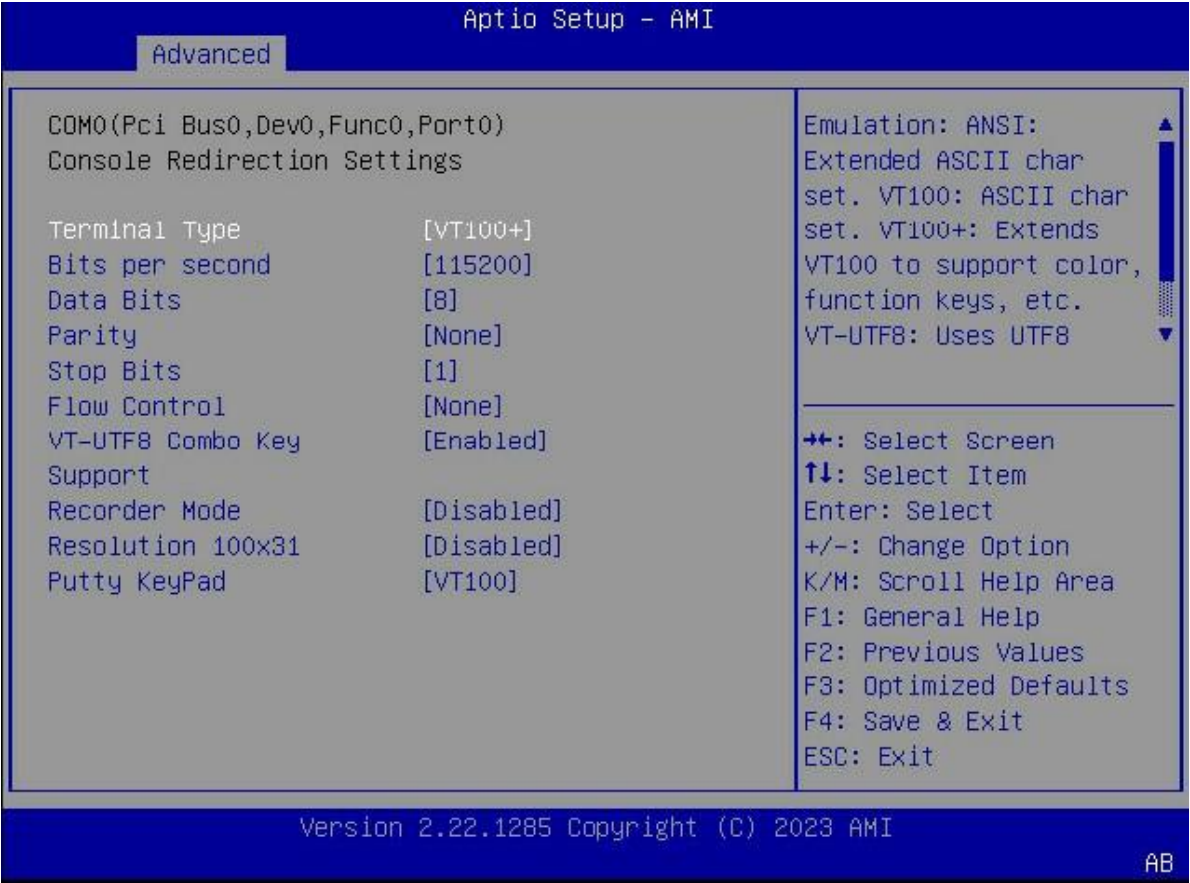
Parameter	Description	Default
Console Redirection	Enables or disables the serial port redirection feature. Options: ● Enabled: enables the serial port redirection feature. ● Disabled: disables the serial port redirection feature. When this parameter is set to Disabled, the Console Redirection Settings item below becomes non-configurable.	Enabled
Console Redirection Settings	Sets serial port redirection parameters to specify how the host and the remote computer exchange data. The host and the remote computer should have the same or compatible settings.	-

Parameter	Description	Default
	For details, refer to 3.2.9.1 Console Redirection Settings .	
Legacy Console Redirection Settings	Sets serial port redirection parameters in Legacy mode. For details, refer to 3.2.9.2 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 , the Console Redirection Settings item below becomes non-configurable.	Disabled
Console Redirection Settings	Sets console redirection parameters for the EMS. For details, refer to 3.2.9.3 Console Redirection Settings .	-

3.2.9.1 Console Redirection Settings

[Figure 3-94](#) shows the **Console Redirection Settings** screen.

[Figure 3-94 Console Redirection Settings Screen](#)



For a description of the parameters on the **Console Redirection Settings** screen, refer to [Table 3-73](#).

Table 3-73 Parameter Descriptions for the Console Redirection Settings Screen

Parameter	Description	Default
Terminal Type	Select the terminal type. Options: • ANSI: extended ASCII character set. • VT100: ASCII character set. • VT100+: extended VT100 for support for color display and functional keys. • VT-UTF8: maps unicode characters to one or more bytes.	VT100+

Bits per Second	Select the number of bits transmitted per second. The transmission speed must match the serial port, and very long lines or lines with noise may need lower speeds. Options: ● 9600	115200
-----------------	--	--------

Parameter	Description	Default
	● 19200 ● 38400 ● 57600 ● 115200	
Data Bits	Select the number of bits used by the actual data in a byte. Options: ● 7 ● 8	8
Parity	Select the 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. Error detection is not performed for Mark and Space, each of which can be used as an additional data bit.	None
Stop Bits	Stop bit, which indicates the end 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.	None
Parameter	Description	Default
	Hardware flow control uses two lines. One is used to send the "stop" signal and the other is used to send the "start" signal.	
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
--------------	---	-------

3.2.9.2 Legacy Console Redirection Settings

Figure 3-95 shows the **Legacy Console Redirection Settings** screen.

Figure 3-95 Legacy Console Redirection Settings Screen



For a description of the parameters on the **Legacy Console Redirection Settings** screen, refer to [Table 3-74](#).

Table 3-74 Parameter Descriptions for the Legacy Console Redirection Settings Screen

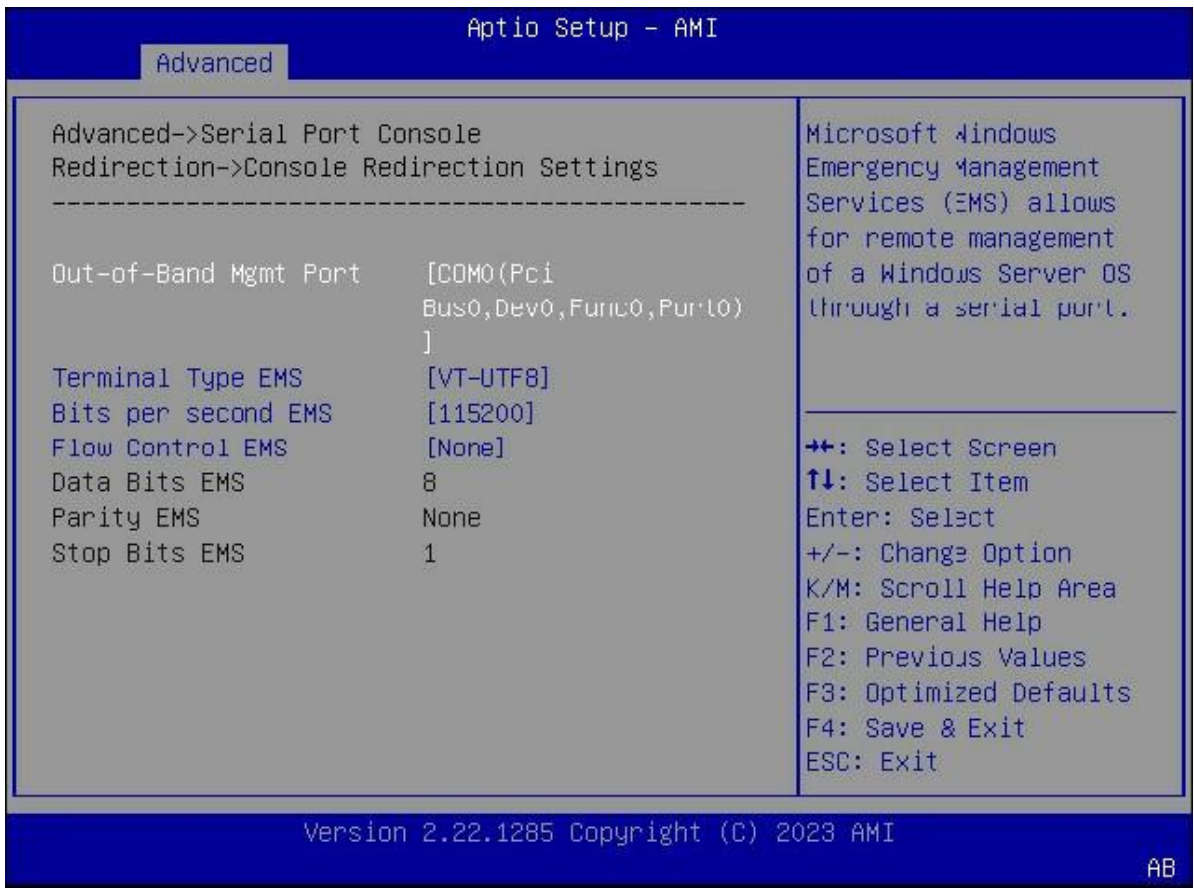
Parameter	Description	Default
-----------	-------------	---------

Redirection COM Port	Select the COM port for redirection of OS , Option, and ROM information in Legacy mode. Options: • COM0 • COM1	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
Parameter	Description	Default
	• Always Enable: enables legacy console redirection for the legacy OS. • BootLoader: disables legacy console redirection before the legacy OS is loaded.	

3.2.9.3 Console Redirection Settings

Figure 3-96 shows the **Console Redirection Settings** screen.

Figure 3-96 Console Redirection Settings Screen



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

Table 3-75 Parameter Descriptions for the Console Redirection Settings Screen

Parameter	Description	Default
Out-of-Band Mgmt Port	Select an out-of-band management serial port. Options: - COM0 - COM1	COM0
Terminal Type EMS	Select an EMS terminal type.	VT-UTF8
Parameter	Description	Default

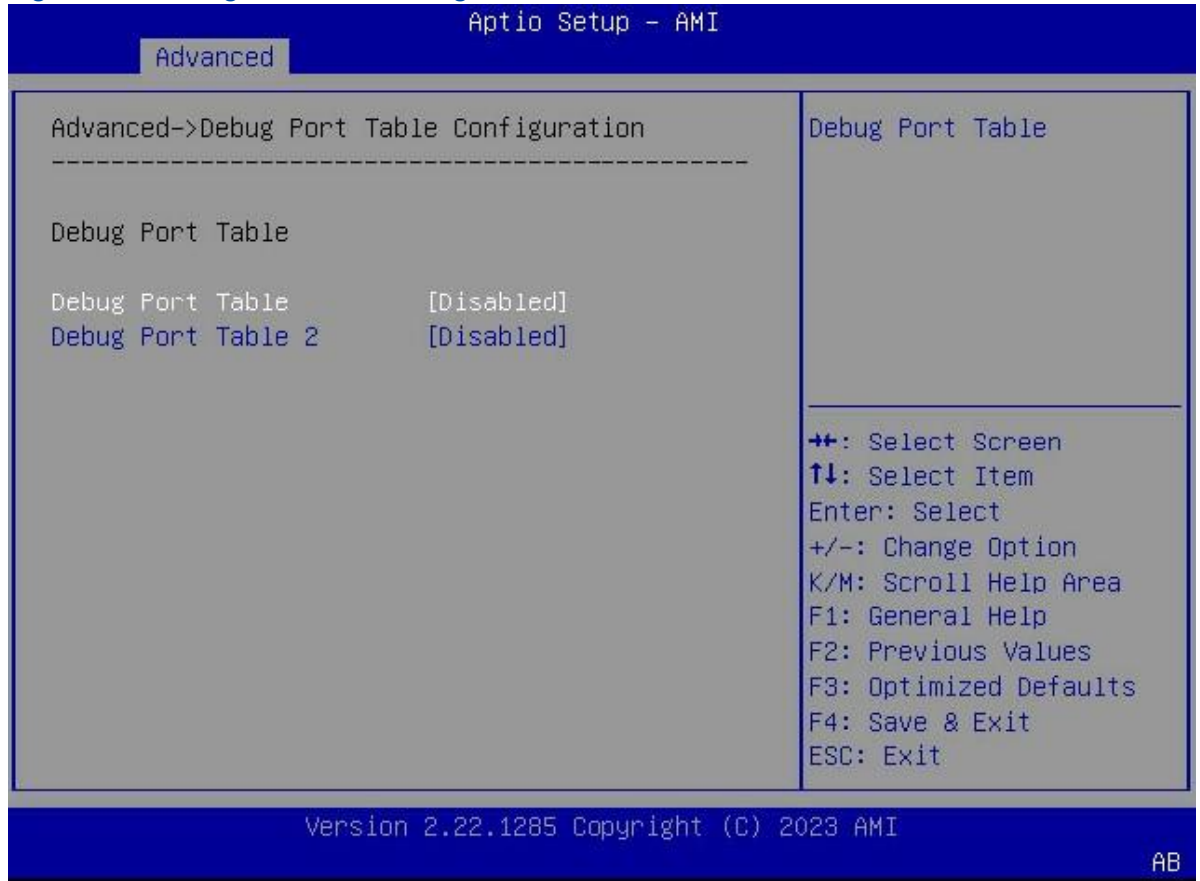
	Options: ● VT100: ASCII character set. ● VT100+: extension of VT100, which is used to support color display and functional keys. ● VT-UTF8: UTF8 is used to map unicode characters to one or more bytes. ● ANSI: extended ASCII character set. EMS terminal types are sorted as follows: ● VT-UTF8 ● VT100+ ● 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 need 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. 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 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
Data Bits EMS	Displays the number of bits used by each actual byte of data in the EMS.	8
Parity EMS	Displays the parity of the EMS.	None

Parameter	Description	Default
Stop Bits EMS	Displays the stop bit of the EMS.	1

3.2.10 Debug Port Table Configuration

Figure 3-97 shows the **Debug Port Table Configuration** screen.

Figure 3-97 Debug Port Table Configuration Screen



For a description of the parameters on the **Debug Port Table Configuration** screen, refer to [Table 3-76](#).

Table 3-76 Parameter Descriptions for the Debug Port Table Configuration Screen

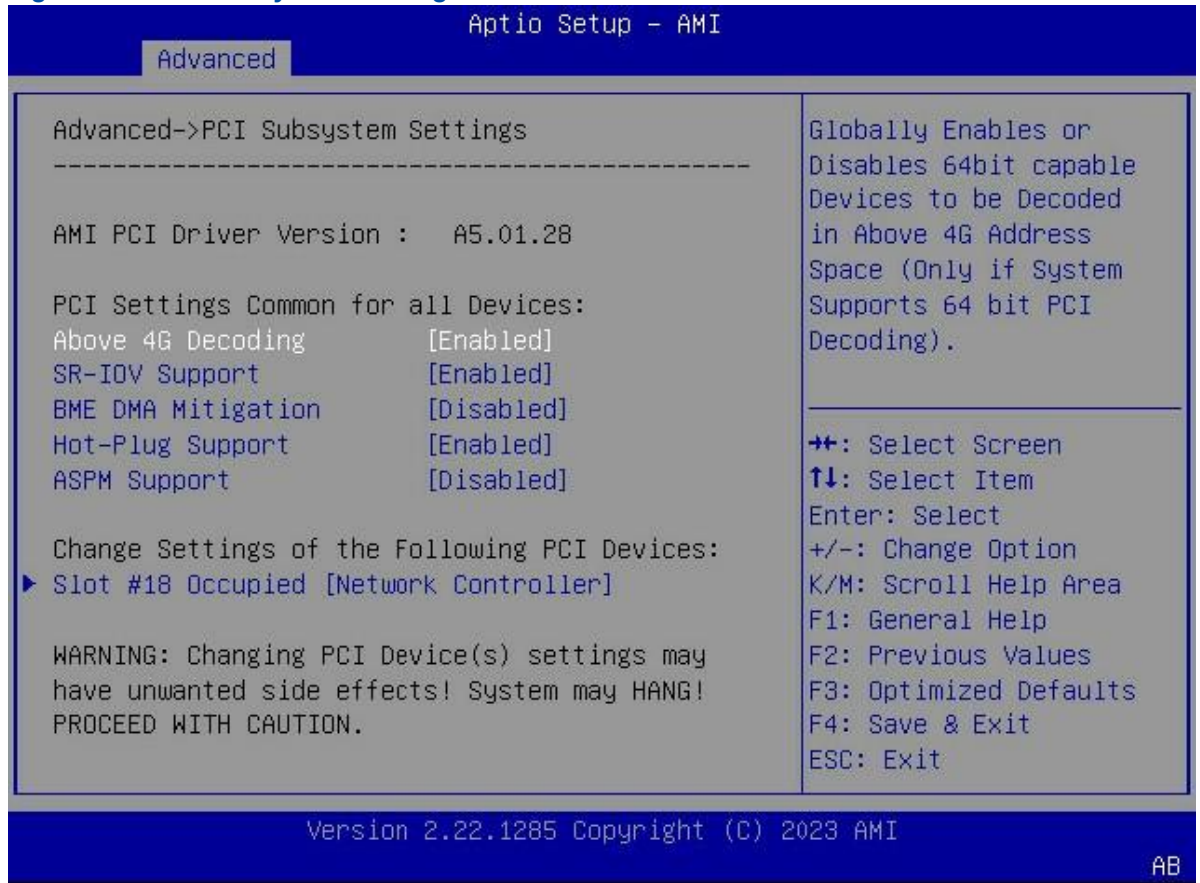
Parameter	Description	Default
Debug Port Table	Enables or disables the port debugging table. Options: - Enabled: enables the port debugging table. - Disabled: disables the port debugging table.	Disabled

Parameter	Description	Default
Debug Port Table 2	Enables or disables the port debugging table 2. Options: - Enabled: enables the port debugging table 2. - Disabled: disables the port debugging table 2.	Disabled

3.2.11 PCI Subsystem Settings

Figure 3-98 shows the **PCI Subsystem Settings** screen.

Figure 3-98 PCI Subsystem Settings Screen



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

Table 3-77 Parameter Descriptions for the PCI Subsystem Settings Screen

Parameter	Description	Default
-----------	-------------	---------

PCI Bus Driver Version	Displays the version number of the AMI PCI bus driver software.	A5.01.28
------------------------	--	----------

Parameter	Description	Default
Above 4G Decoding	Enables or disables decoding of 64-bit devices in the address space above 4GB (only when the system supports 64-bit PCI decoding). Options: - Enabled: enables decoding of 64-bit devices in the address space above 4GB. - Disabled: disables decoding of 64-bit devices in the address space above 4GB.	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
BME DMA Mitigation	Enables or disables BME DMA mitigation. Options: - Enabled: enables BME DMA mitigation. - Disabled: disables BME DMA mitigation.	Disabled
Hot-Plug Support	Enables or disables hot swapping support of the entire system. Options: - Enabled: enables hot swapping support of the entire system. When this parameter is set to Enabled, if the system has hot-swappable slots, a setup page is provided for you to configure the hot-swappable PCI resource parameters. - Disabled: disables hot swapping support of the entire system.	Enabled
ASPM Support	Enables or disables ASPM support. Options: - Enabled: enables ASPM support. - Disabled: disables ASPM support.	Disabled

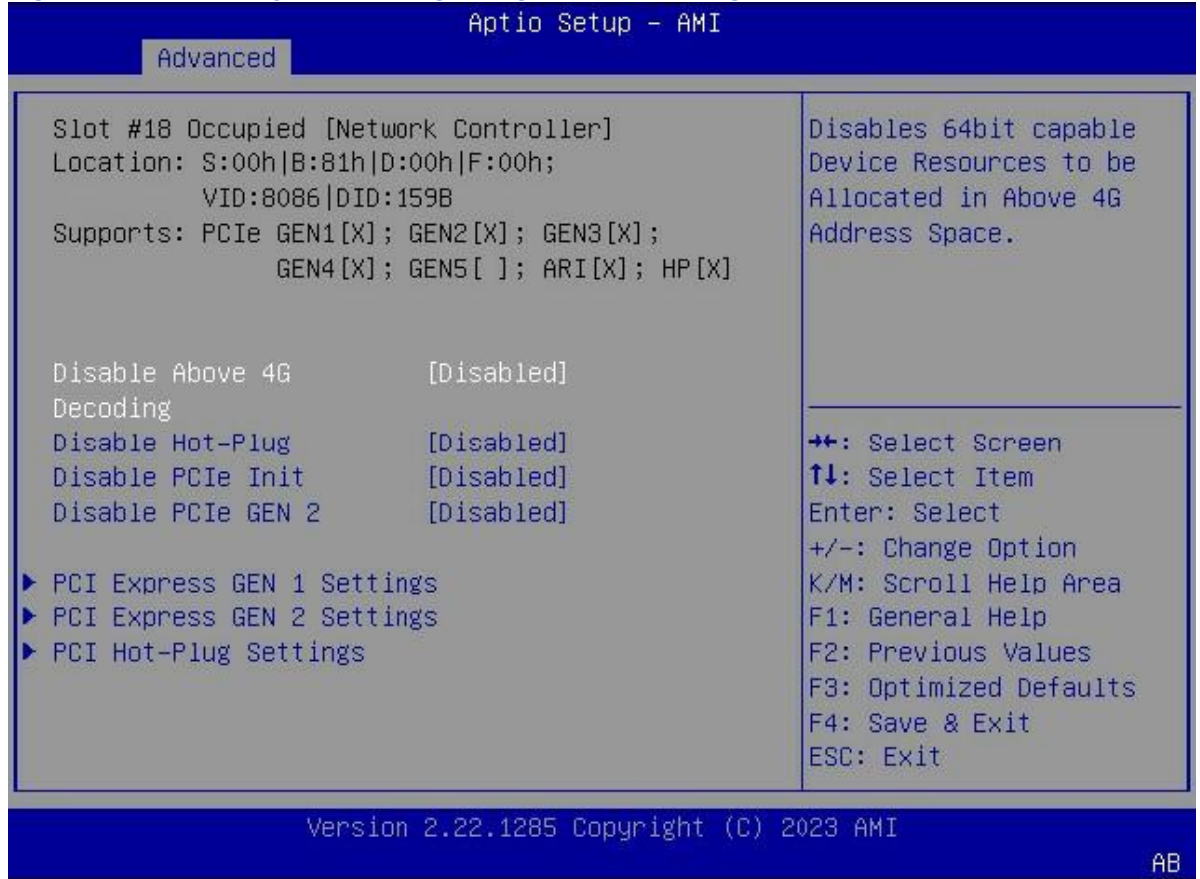
Slot #18 Occupied[Network Controller]	Modifies the parameters of the on-board PCI device or PCI slot. This parameter is related to system devices. Slot #18 Occupied[Network Controller] is used as an example. For details, refer to	-
Parameter	Description	Default
	3.2.11.1 PCI Subsystem Settings-Single Device Setting.	

3.2.11.1 PCI Subsystem Settings-Single Device Setting

PCI Subsystem Settings-Single Device Setting

Figure 3-99 shows the **PCI Subsystem Settings-Single Device Setting** screen.

Figure 3-99 PCI Subsystem Settings-Single Device Setting Screen



For a description of the parameters on the **PCI Subsystem Settings-Single Device Setting** screen, refer to [Table 3-78](#).

Table 3-78 Parameter Descriptions for the PCI Subsystem Settings-Single Device Setting Screen

Parameter	Description	Default
Location	Displays the location, VID , and DID of the PCI device.	S: 00hIB: 81h I D:00h I F:00h ; VID : 8086IDID : 159B

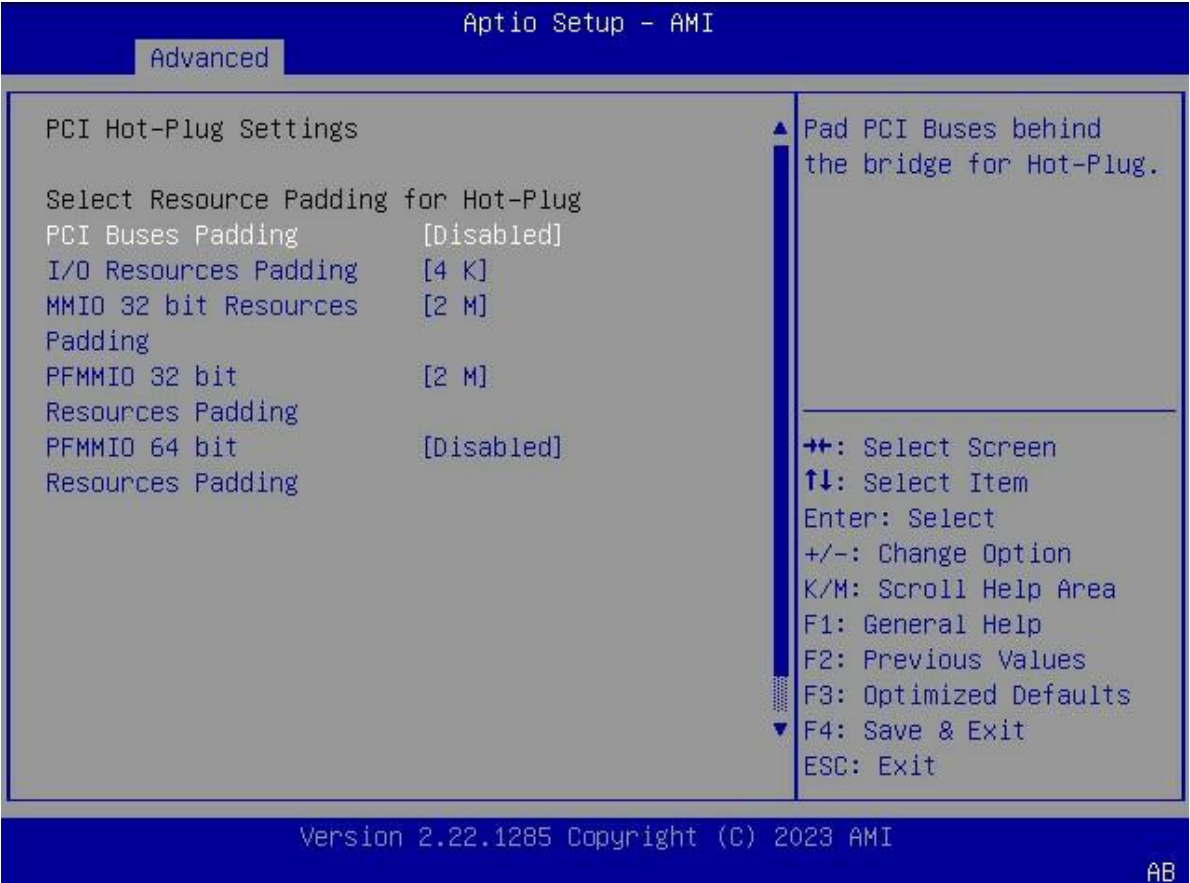
Parameter	Description	Default
Supports	Displays the features supported by the PCI device.	PCIe GEN1[X]; GEN2[X]; GEN3[X]; GEN4[X]; GEN5[]; ARI[X]; HP[X]
Disable Above 4G Decoding	Enables or disables the decoding feature of 64bit devices in the address space above 4G. Options: - Enabled: enables the decoding feature of 64bit devices in the address space above 4G. - Disabled: disables the decoding feature of 64-bit devices in the address space above 4G.	Disabled
Disable Hot-Plug	Enables or disables BIOS-based hot-swapping support on the selected device or slot. Options: - Enabled: enables BIOS-based hot-swapping support on the selected device or slot. - Disabled: disables BIOS-based hot-swapping support on the selected device or slot.	Disabled
Disable PCIe Init	Enables or disables the BIOS-based PCIe initialization feature on the selected device and its subordinate PCIe devices. Options: - Enabled: enables the BIOS-based PCIe initialization feature on the selected device and its subordinate PCIe devices. - Disabled: disables the BIOS-based PCIe initialization feature on the selected device and its subordinate PCIe devices.	Disabled

Disable PCIe GEN 2	Enables or disables the BIOS-based PCIe GEN2 initialization feature on the selected device and its subordinate PCIe devices. Options: ● Enabled: enables the BIOS-based PCIe GEN2 initialization feature on the selected device and its subordinate PCIe devices. ● Disabled: disables the BIOS-based PCIe GEN2 initialization feature on the selected device and its subordinate PCIe devices.	Disabled
PCI Express GEN 1 Settings	Sets PCIe GEN 1 parameters.	-
Parameter	Description	Default
PCI Express GEN 2 Settings	Sets PCIe GEN 2 parameters.	-
PCI Hot-Plug Settings	Sets PCI hot swapping parameters. For details, refer to PCI Hot-Plug Settings.	-

PCI Hot-Plug Settings

[Figure 3-100](#) shows the **PCI Hot-Plug Settings** screen.

Figure 3-100 PCI Hot-Plug Settings Screen



For a description of the parameters on the **PCI Hot-Plug Settings** screen, refer to [Table 3-79](#).

Table 3-79 Parameter Descriptions for the PCI Hot-Plug Settings Screen

Parameter	Description	Default
PCI Buses Padding	Select the PCI bus padding for hot swapping. Options: ● Disabled ● 1 ● 2	Disabled

Parameter	Description	Default
-----------	-------------	---------

	• 3 • 4 • 5 • 6 • 7 • 8 • 9 • 10	
I/O Resources Padding	Select the I/O resource padding for hot swapping. Options: • Disabled • 4K • 8K • 16K • 32K	4K
MMIO 32 bit Resources Padding	Select MMIO 32-bit resource padding for hot swapping. Options: • Disabled • 1M • 2M • 4M • 8M • 16M • 32M • 64M • 128M • 256M • 512M	2M
PFMMIO 32 bit Resources Padding	Select the PFMMIO 32-bit resource padding for hot swapping. Options: • Disabled • 1M • 2M • 4M • 8M • 16M • 32M • 64M • 128M	2M

Parameter	Description	Default
	• 256M • 512M	
PFMMIO 64 bit Resources Padding	Select the PFMMIO 64-bit resource padding for hot swapping. Options: • Disabled • 1M • 2M • 4M • 8M • 16M • 32M • 64M • 128M • 256M • 512M • 1G • 2G • 4G • 8G	Disabled

3.2.12 USB Configuration

Figure 3-101 through Figure 3-102 show the **USB Configuration** screen.

Figure 3-101 USB Configuration Screen—1

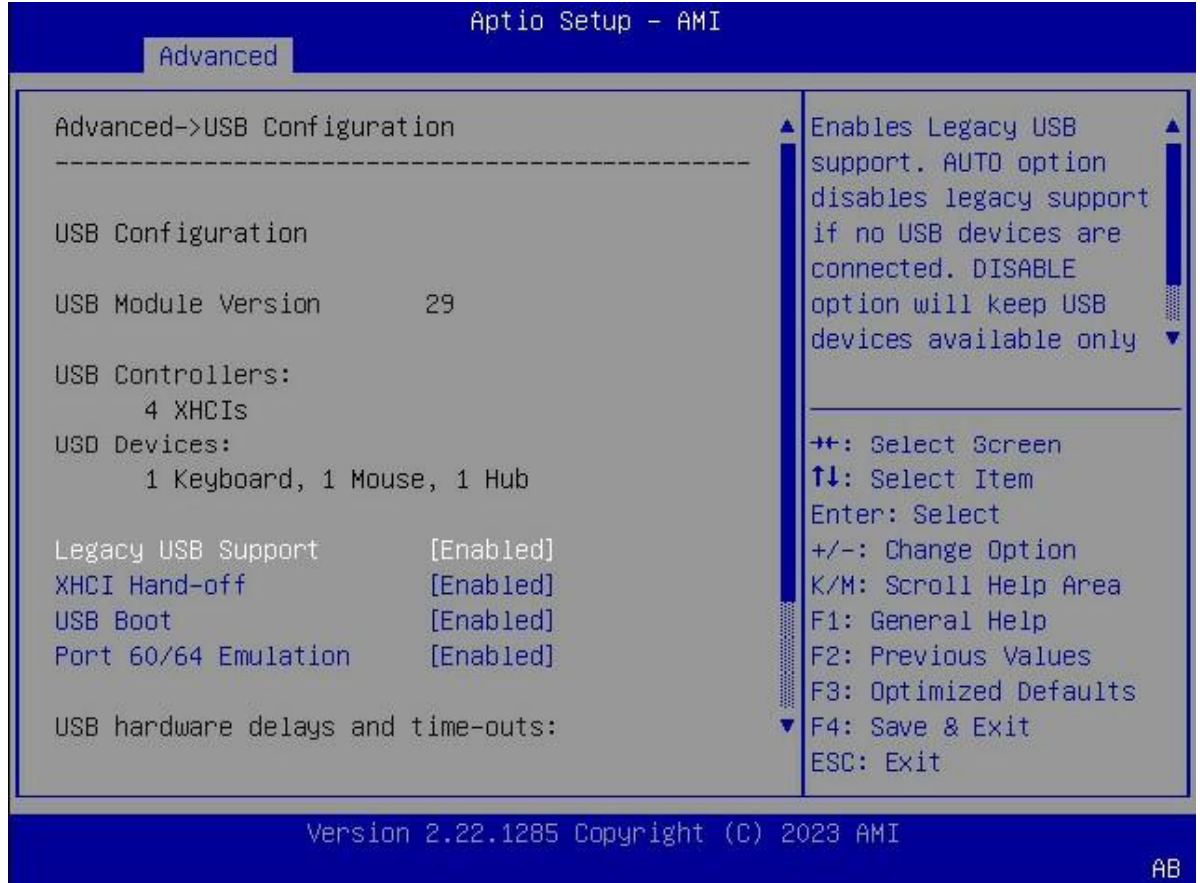
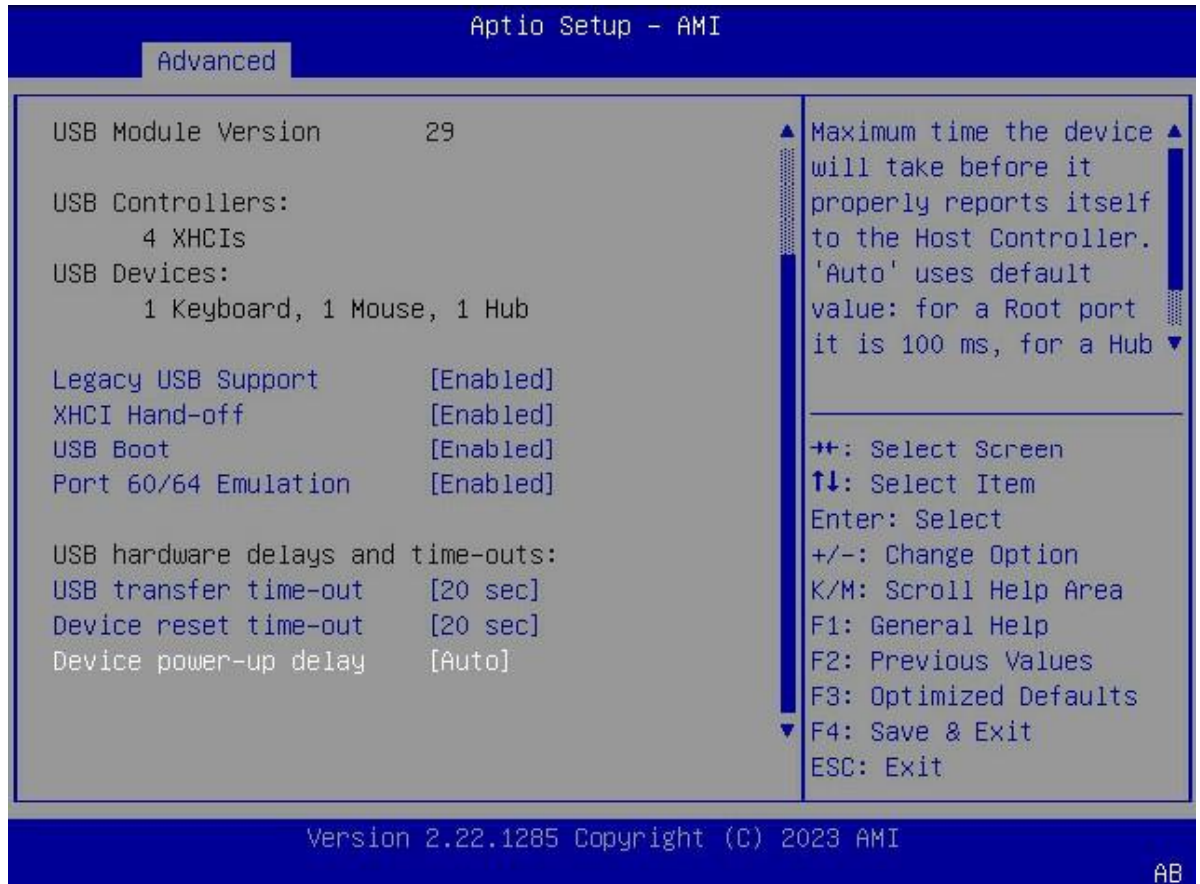


Figure 3-102 USB Configuration Screen—2



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

Table 3-80 Parameter Descriptions for the USB Configuration Screen

Parameter	Description	Default
USB Module Version	Displays the USB module version number.	-
USB Controllers	Displays the USB controller.	-
USB Devices	Displays the USB device.	-

Legacy USB Support	Enables or disables USB support in Legacy mode. Options: ● Auto: If there are no USB devices, USB support in Legacy mode is disabled. ● 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.	Enabled
--------------------	---	---------

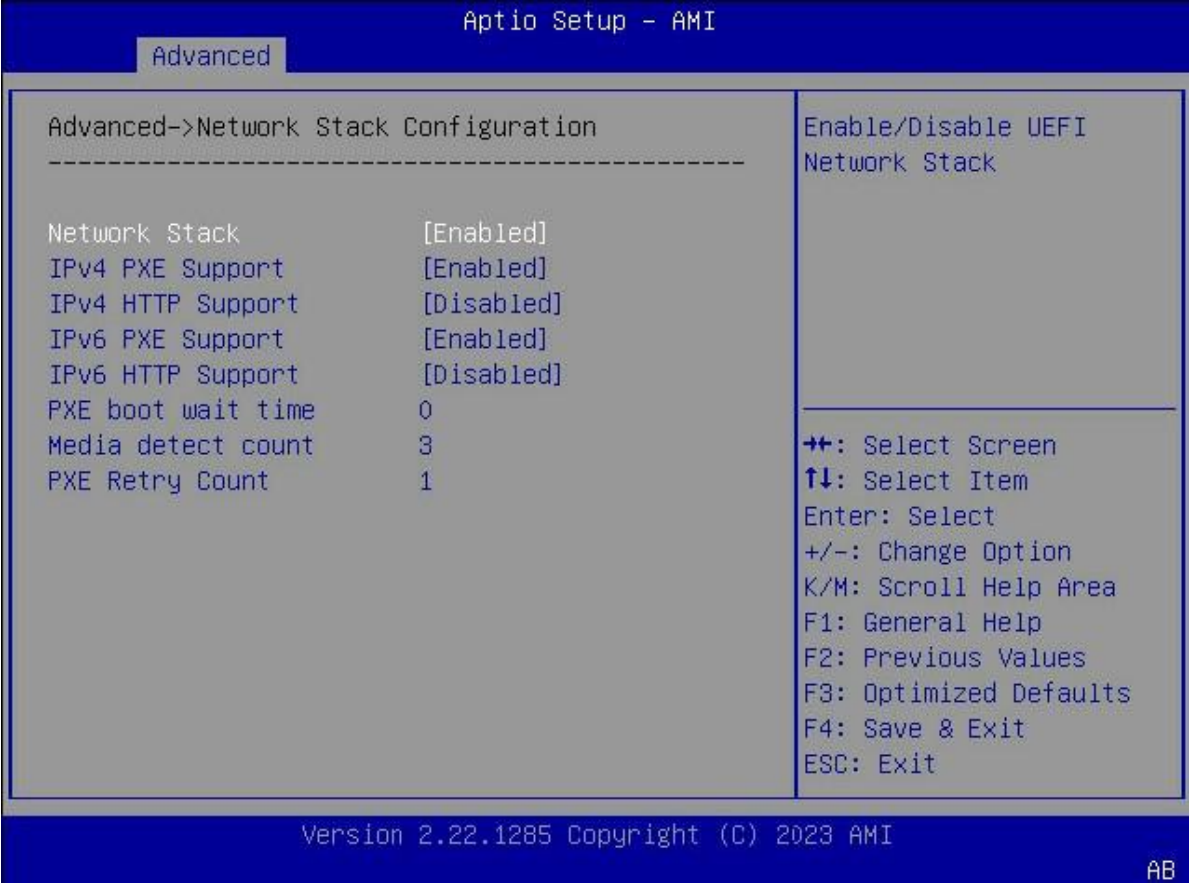
Parameter	Description	Default
XHCI Handoff	Enables or disables the XHCI handoff feature, which provides a viable solution for an operating system that does not support XHCI. XHCI ownership changes shall be declared by the XHCI driver. Enables or disables the XHCI handoff feature. Options: ● Enabled: enables the XHCI handoff feature. ● Disabled: disables the XHCI handoff feature.	Enabled
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
Port 60/64 Emulation	Enables or disables the port 60/64 emulation feature. Options: ● Enabled: enables the port 60/64 emulation feature. ● Disabled: disables the port 60/64 emulation feature.	Enabled

USB hardware delays and timeouts	Select the USB transfer timeout period. Options: • 1 sec • 5 sec • 10 sec • 20 sec	20 sec
USB transfer time-out	Select the device reset delay time. Options: • 10 sec • 20 sec • 30 sec • 40 sec	20 sec
Device reset time-out	Sets the device power-on delay time. Options:	Auto
Parameter	Description	Default
	• Auto: uses the default setting. • Manual: requires manual configuration.	

3.2.13 Network Stack Configuration

Figure 3-103 shows the **Network Stack Configuration** screen.

Figure 3-103 Network Stack Configuration Screen



For a description of the parameters on the **Network Stack Configuration** screen, refer to [Table 3-81](#).

Table 3-81 Parameter Descriptions for the Network Stack Configuration Screen

Parameter	Description	Default
Network Stack	Enables or disables the UEFI network protocol stack. Options: ● Enabled: enables the UEFI network protocol stack. ● Disabled: disables the UEFI network protocol stack.	Enabled

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 PXE boot feature. Options: ● Enabled: enables the IPv4 HTTP boot feature. ● Disabled: disables the IPv4 HTTP boot feature.	Disabled
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	Sets the number of media device detection times to check the number of times that a media device is present, range: 1–50. ● To increase the value by one, press +. ● To decrease the value by one, press -.	3

Parameter	Description	Default
	To specify a value, press the corresponding number key.	
PXE Retry Count	Sets the number of PXE retries. - To increase the value by one, press +. - To decrease the value by one, press -. - To specify a value, press the corresponding number key.	1

3.2.14 CSM Configuration

Figure 3-104 shows the **CSM Configuration** screen.

Figure 3-104 CSM Configuration Screen



For a description of the parameters on the **CSM Configuration** screen, refer to [Table 3-82](#).

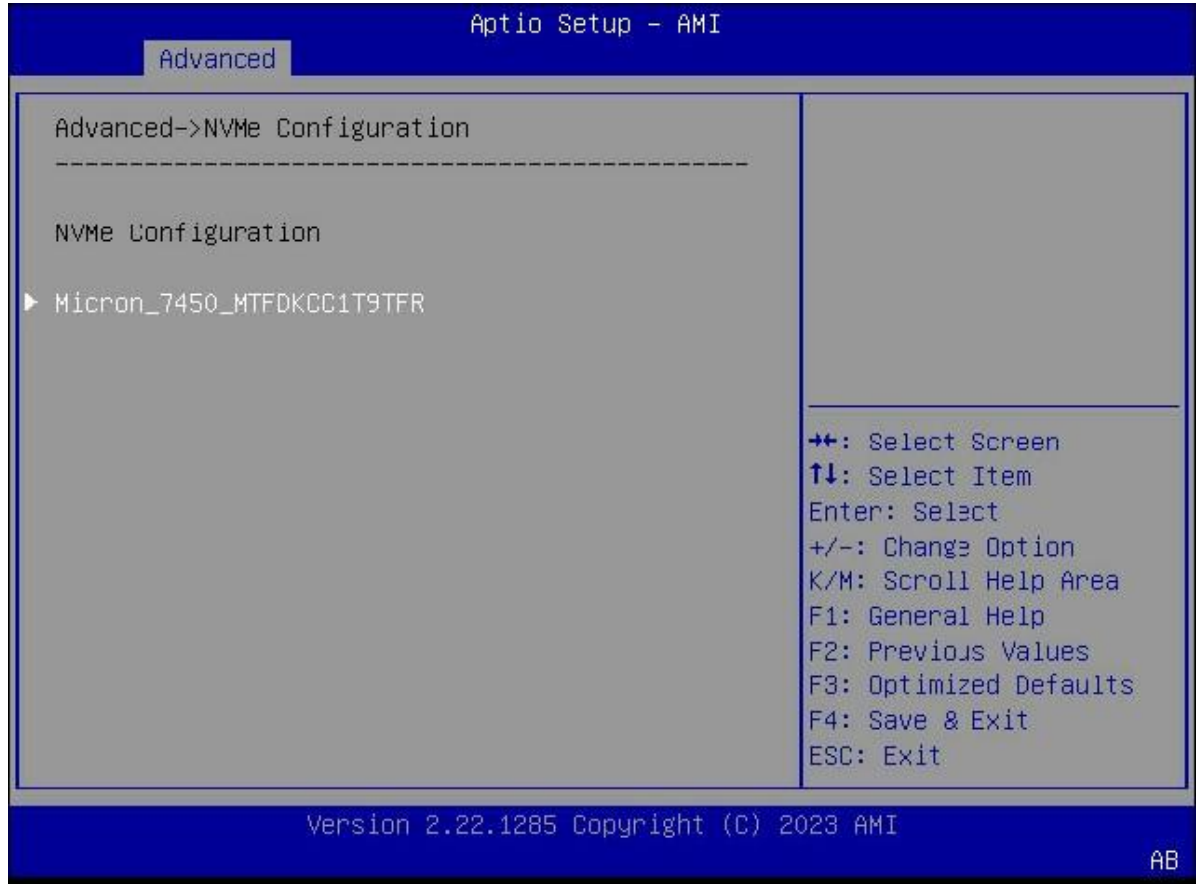
Table 3-82 Parameter Descriptions for the CSM Configuration Screen

Parameter	Description	Default
-----------	-------------	---------

CSM Support	Enables or disables CSM support. Options: Enabled: enables CSM support.	Enabled
Parameter	Description	Default
	Disabled: disables CSM support. When this parameter is set to Disabled, the parameters below are hidden.	
CSM16 Module Version	Displays the version number of the CSM16 module.	07.84
GateA20 Active	Select a GateA20 State. Options: - Upon Request: GA20 can be disabled by using the BIOS service. - Always: Disabling GA20 is not allowed. The Always option is useful when any RT code is executed above 1MB.	Upon Request
INT19 Trap Response	Sets the mode in which the Option Rom responds to the INT19 Trap. Options: - Immediate: executes the trap immediately. - Postponed: executes the trap during legacy boot.	Immediate

3.2.15 NVMe Configuration

Figure 3-105 shows the **NVMe Configuration** screen.

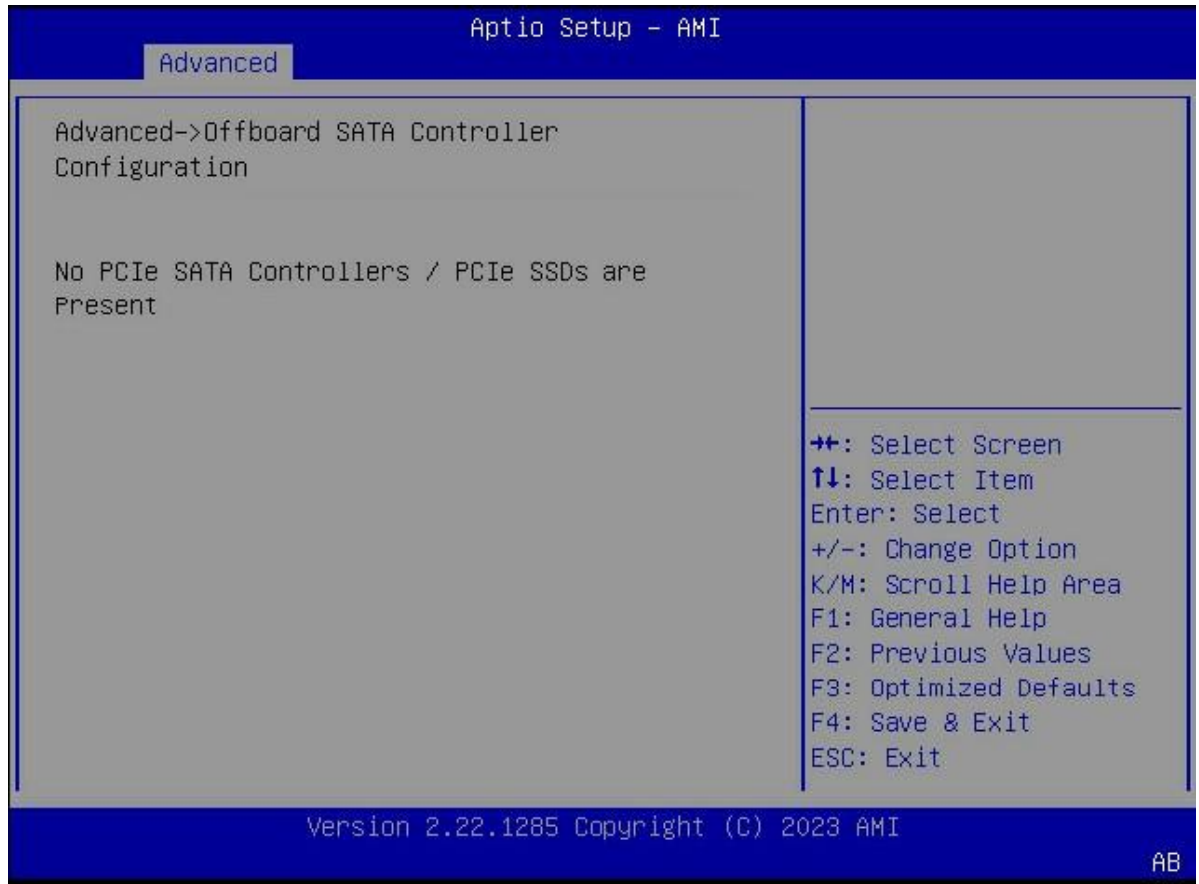
Figure 3-105 NVMe Configuration Screen**Note**

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

3.2.16 Offboard SATA Controller Configuration

[Figure 3-106](#) shows the **Offboard SATA Controller Configuration** screen.

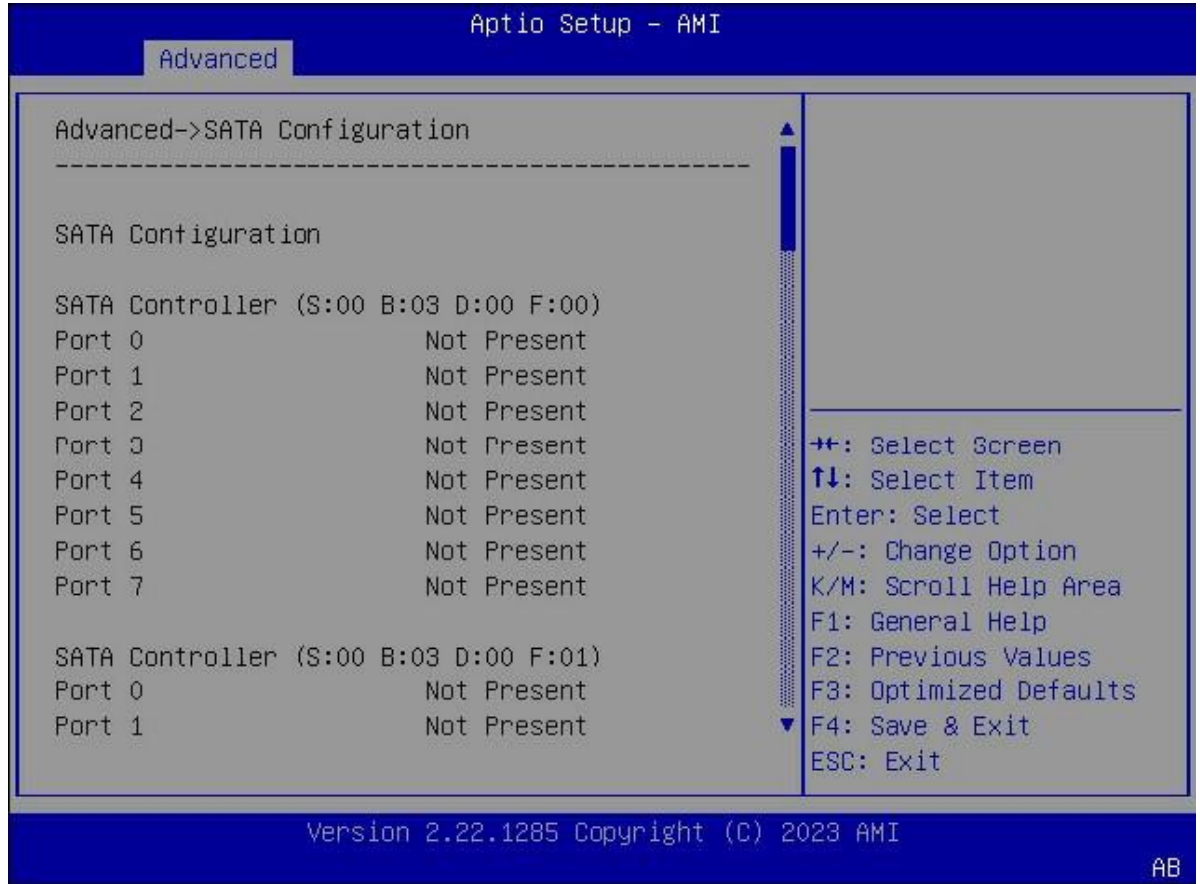
Figure 3-106 Offboard SATA Controller Configuration Screen

**Note**

If an offline [SATA](#) drive is mounted on the mainboard, the offline SATA drive information is displayed.

3.2.17 SATA Configuration

[Figure 3-107](#) shows the **SATA Configuration** screen.

Figure 3-107 SATA Configuration Screen

Note

The **SATA Configuration** screen displays the position and presence information about SATA controllers. The information is described as follows:

- If a SATA controller is present, the information about the SATA controller is displayed.
- If a SATA controller is not present, **Not Present** is displayed.

3.2.18 CPU Configuration

Figure 3-108 shows the **CPU Configuration** screen.

Figure 3-108 CPU Configuration Screen



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

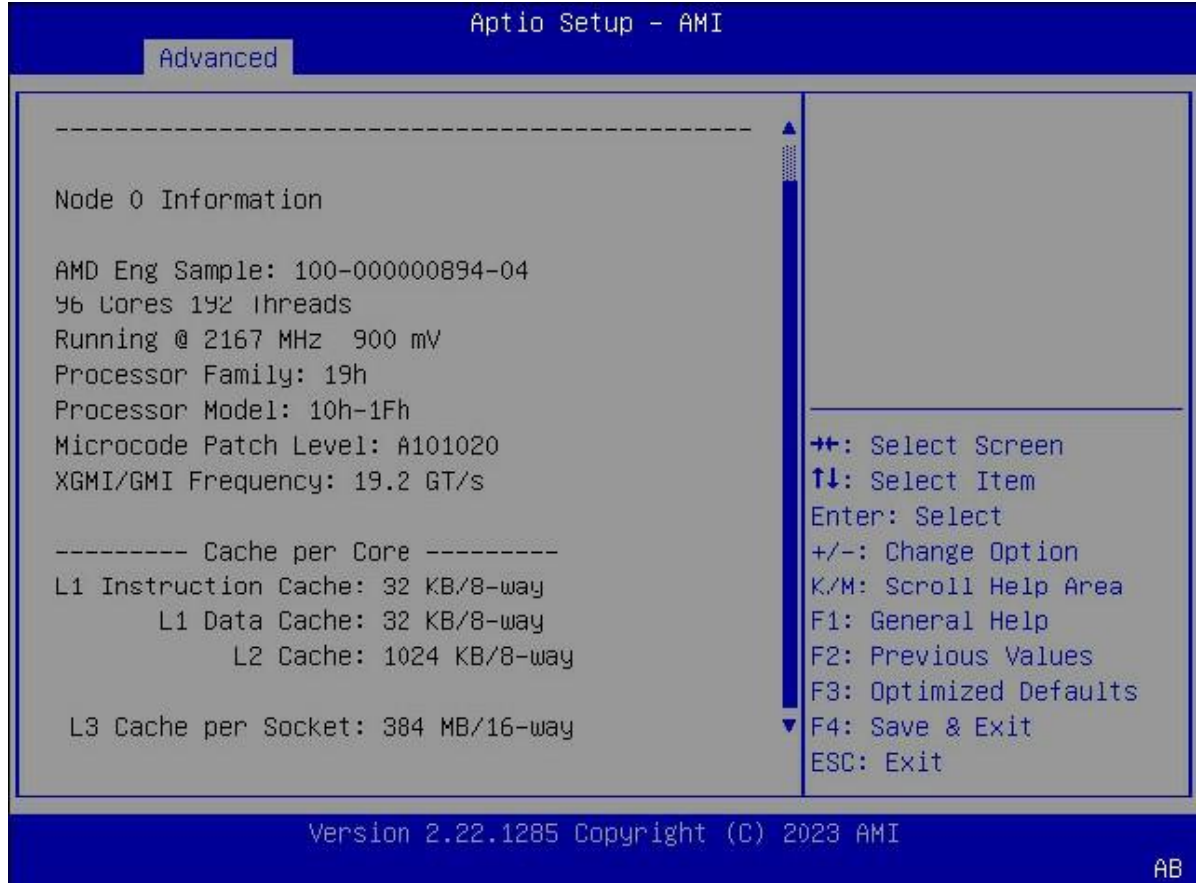
Table 3-83 Parameter Descriptions for the CPU Configuration Screen

Parameter	Description	Default
SVM Mode	Enables or disables the CPU virtualization feature. Options: - Enabled: enables the CPU virtualization feature. - Disabled: disables the CPU virtualization feature.	Enabled
Node 0 Information	Displays the information about node 0. For details, refer to 3.2.18.1 Node 0 Information .	-
Node 1 Information	Displays the information about node 1. For details, refer to 3.2.18.1 Node 0 Information .	-

3.2.18.1 Node 0 Information

Figure 3-109 shows the **Node 0 Information** screen.

Figure 3-109 Node 0 Information Screen

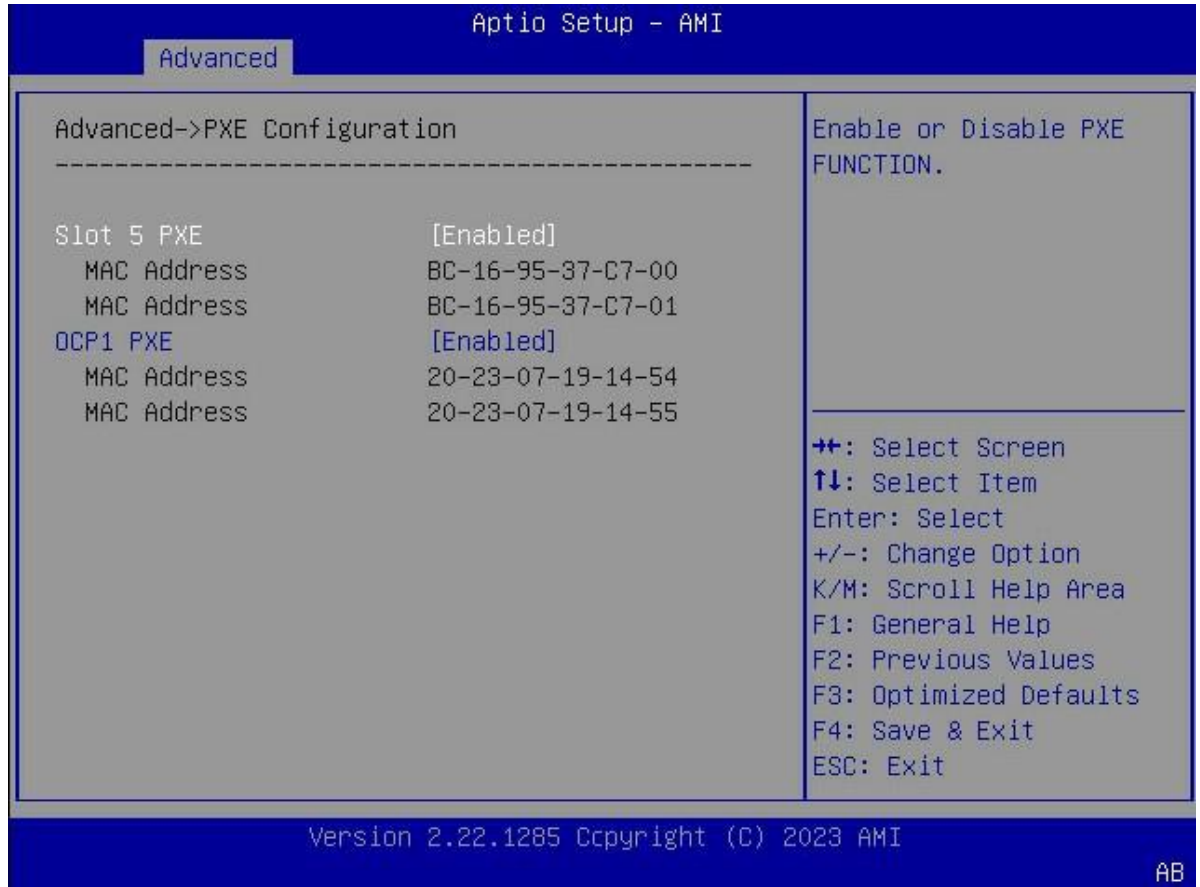


Note

The parameters on the **Node 0 Information** screen are the same as those on the **Node 1 Information** screen. This procedure uses the **Node 0 Information** screen as an example.

3.2.19 PXE Configuration

Figure 3-110 shows the **PXE Configuration** screen.

Figure 3-110 PXE Configuration Screen

Note

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

For a description of the parameters on the **PXE Configuration** screen, refer to [Table 3-84](#).

Table 3-84 Parameter Descriptions for the PXE Configuration Screen

Parameter	Description	Default
Slot 5 PXE	Enables or disables the PXE feature of the standard NIC in slot 5. Options: - Enabled: enables the PXE feature of the standard NIC in slot 5. - Disabled: disables the PXE feature of the standard NIC in slot 5.	Enabled

OCP 1 PXE	Enables or disables the PXE feature of the OCP NIC 1 . Options: Enabled: enables the PXE feature of the OCP NIC 1.	Enabled
Parameter	Description	Default
	Disabled: disables the PXE feature of the OCP NIC 1.	

3.2.20 AMD Mem Configuration Status

Figure 3-111 through Figure 3-112 show the **AMD Mem Configuration Status** screen.

Figure 3-111 AMD Mem Configuration Status Screen—1

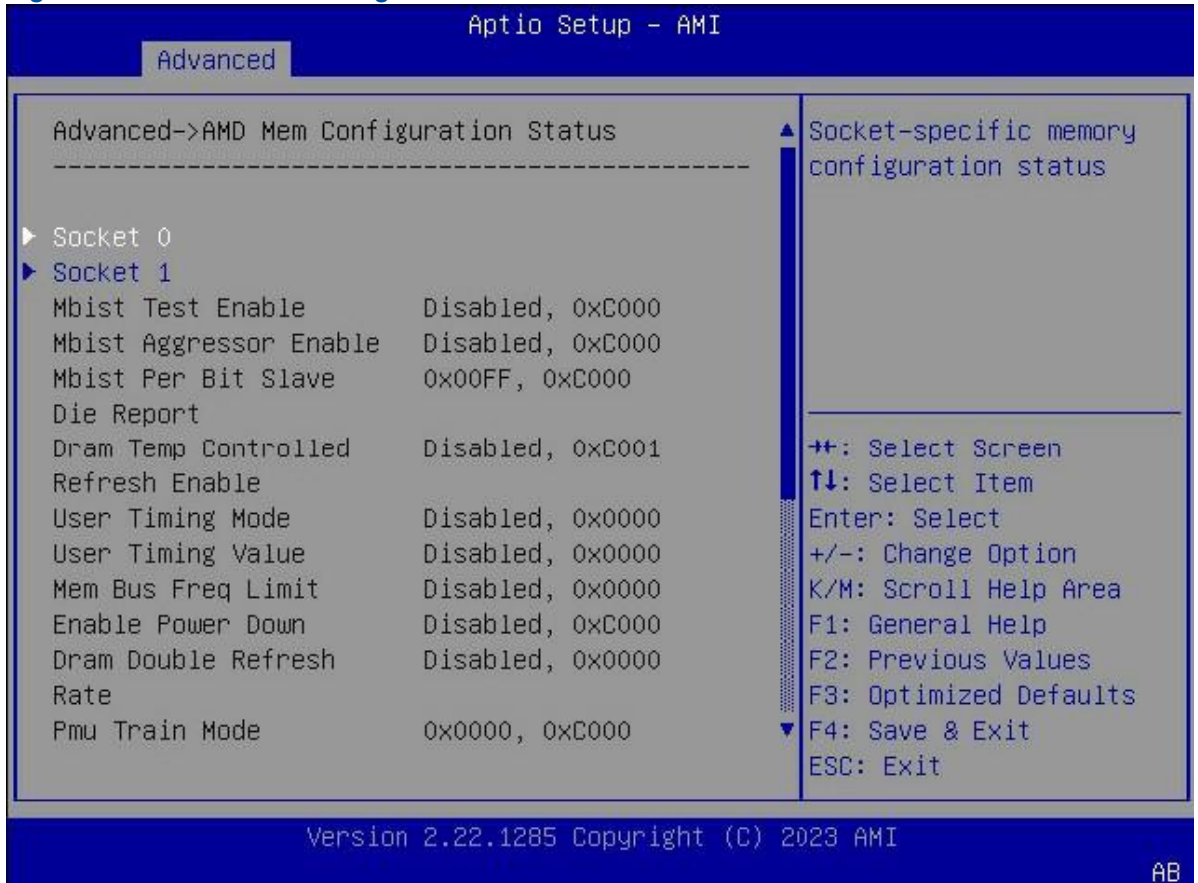
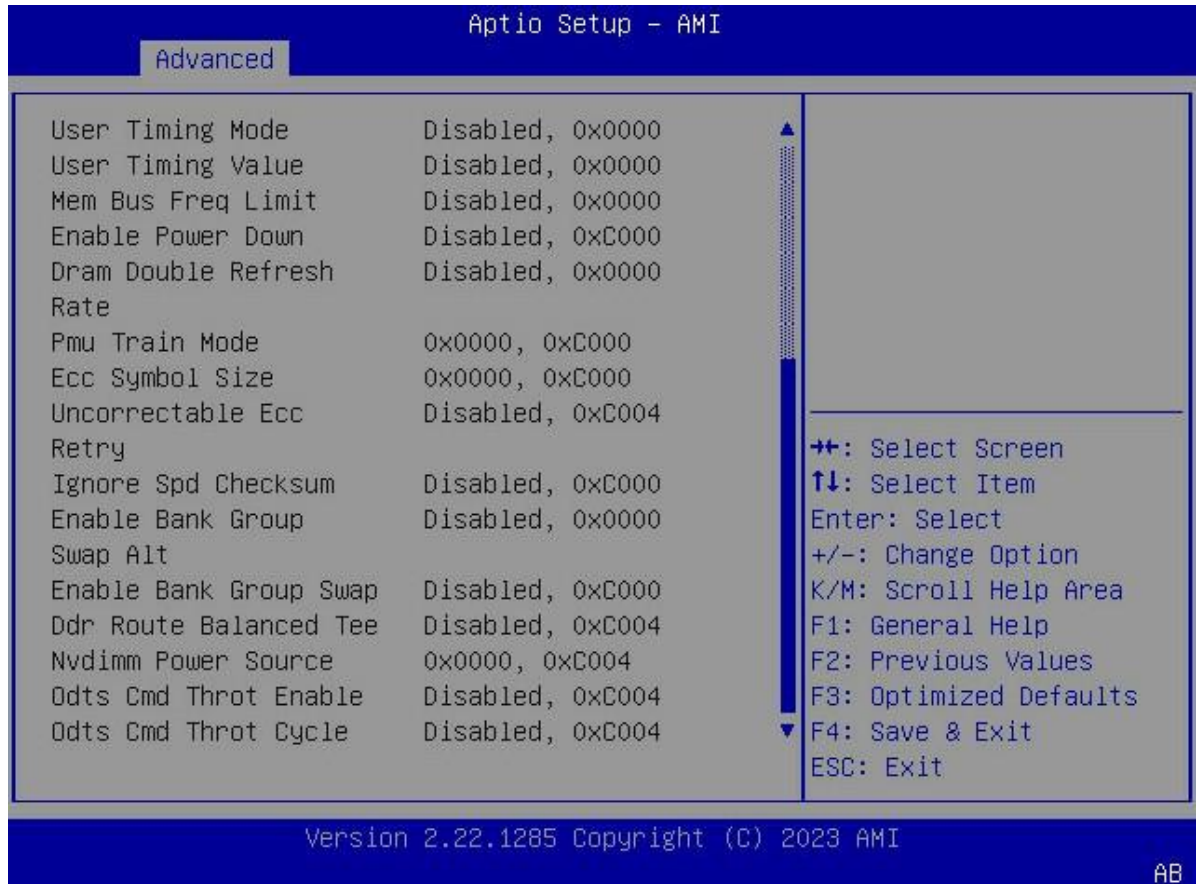


Figure 3-112 AMD Mem Configuration Status Screen—2



For a description of the parameters on the **AMD Mem Configuration Status** screen, refer to [Table 3-85](#).

Table 3-85 Parameter Descriptions for the AMD Mem Configuration Status Screen

Parameter	Description
Socket 0	Sets the memory configuration status of the Socket 0. For details, refer to 3.2.20.1 Socket 0 .
Socket 1	Sets the memory configuration status of the Socket 1. For details, refer to 3.2.20.1 Socket 0 .
Mbist Test Enable	Displays the Mbist test enabling information.
Mbist Aggressor Enable	Displays Mbist Aggressor enabling information.
Mbist Per Bit Slave Die Report	Displays the number of per bit slave die result reports from the MBIST.
Dram Temp Controlled Refresh Enable	Displays the enabling information about the temperature-controlled refresh feature in DRAM.
User Timing Mode	Displays user timing mode.

User Timing Value	Displays user timing value.
Parameter	Description
Mem Bus Freq Limit	Displays the memory Bus frequency limit.
Enable Power Down	Displays the enabling information about the power-down feature.
Dram Double Refresh Rate	Displays the DRAM double refresh rate information.
Pmu Train Mode	Displays PMU train mode information.
Ecc Symbol Size	Displays the ECC symbol size information.
Uncorrectable Ecc Retry	Displays uncorrectable ECC retry information.
Ignore Spd Checksum	Displays the SPD check ignorance setting and information.
Enable Bank Group Swap Alt	Displays the enabling information about Alt in Bank Group Swap.
Enable Bank Group Swap	Displays the enabling information about Bank Group Swap.
Ddr Route Balanced Tee	Displays DDR route balanced tee information.
Nvdimmm Power Source	Displays NVDIMM power information.
Odts Cmd Throt Enable	Displays the enabling information about the ODTS CMD throttling feature.
Odts Cmd Throt Cycle	Displays the cycle information about the ODTS CMD throttling feature.

3.2.20.1 Socket 0

Socket 0

Figure 3-113 shows the **Socket 0** screen.

Figure 3-113 Socket 0 Screen—1

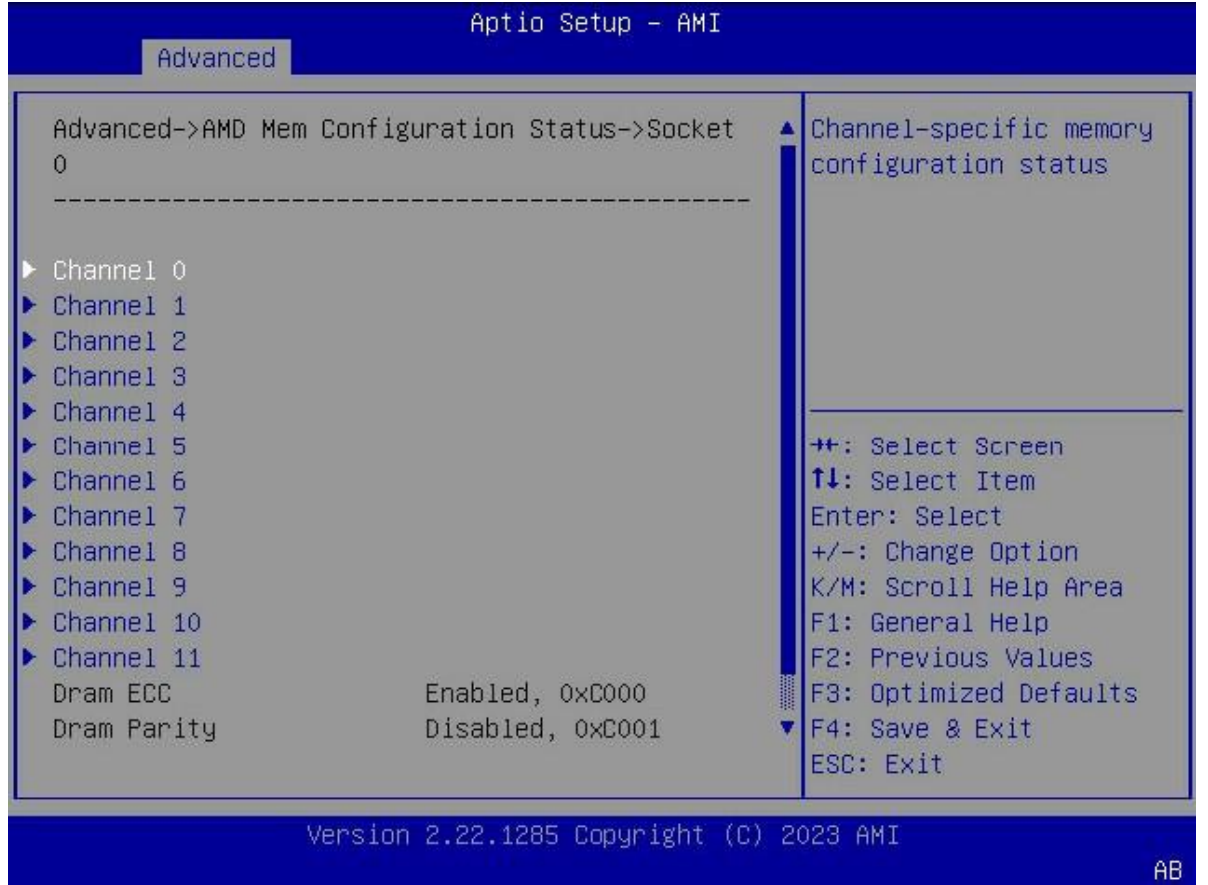
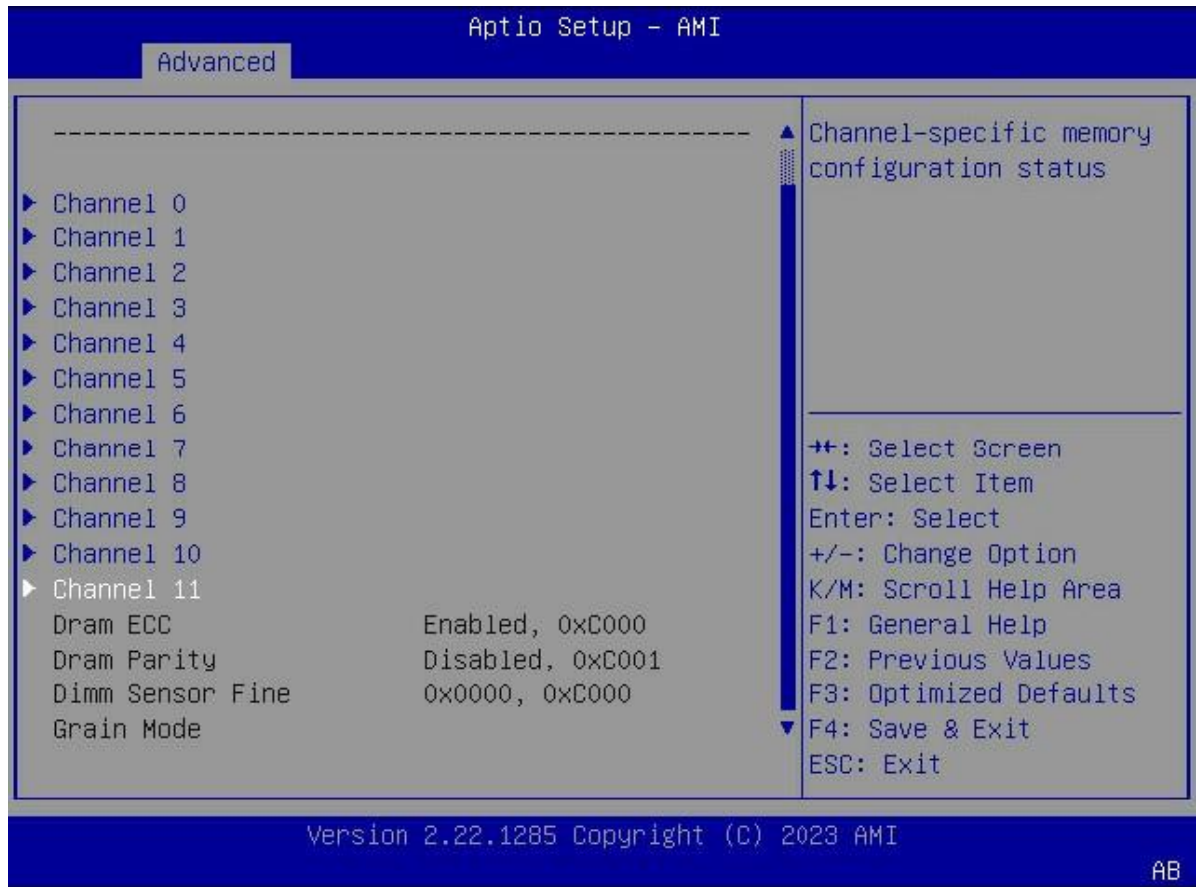


Figure 3-114 Socket 0 Screen—2

Note

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

For a description of the parameters on the **Socket 0** screen, refer to [Table 3-86](#).

Table 3-86 Parameter Descriptions for the Socket 0 Screen

Parameter	Description
Channel 0	Sets memory configuration status for Channel 0. For details, refer to Channel 0 .
Dram ECC	Displays DRAM ECC information.
Dram Parity	Displays DRAM Parity information.
Dimm Sensor Fine Grain Mode	Displays the information about the DIMM sensor Fine Grain mode.

**Note**

The settings of **Channel 1** and **Channel 2** are the same as those of **Channel 0**.

Channel 0

Figure 3-115 shows the **Channel 0** screen.

Figure 3-115 Channel 0 Screen

**Note**

Channel 0 is used as an example.

For a description of the parameters on the **Channel 0** screen, refer to [Table 3-87](#).

Table 3-87 Parameter Descriptions for the Channel 0 Screen

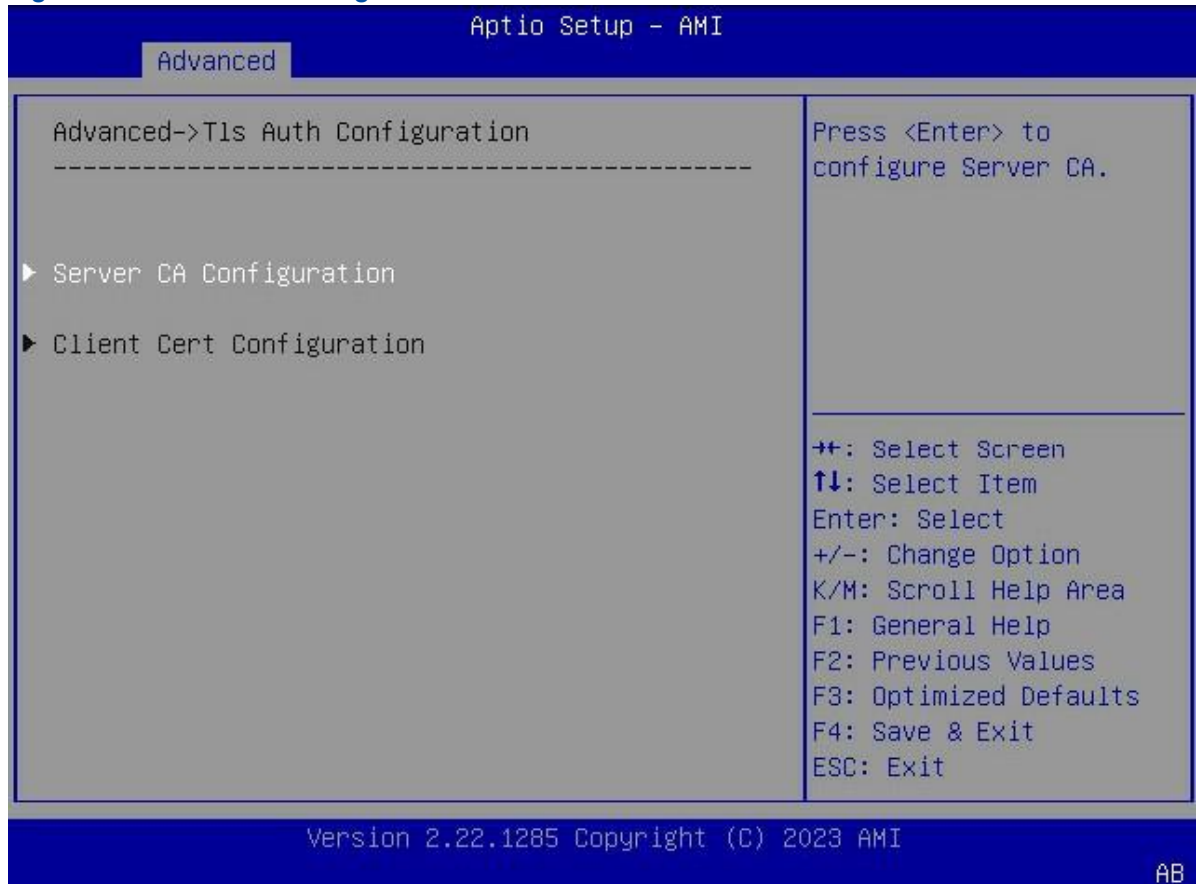
Parameter	Description
DIMM0 Presence	Displays the presence information about DIMM0. Absent: DIMM0 is not present.

Chipset/Bank Interleave	Displays Chipset-bank interaction information.
-------------------------	--

3.2.21 Tls Auth Configuration

Figure 3-116 shows the **Tls Auth Configuration** screen.

Figure 3-116 Tls Auth Configuration Screen



For a description of the parameters on the **Tls Auth Configuration** screen, refer to [Table 3-88](#).

Table 3-88 Parameter Descriptions for the Tls Auth Configuration Screen

Parameter	Description
Server CA Configuration	Sets server CA parameters. For details, refer to 3.2.21.1 Server CA Configuration .
Client Cert Configuration	Sets client certification parameters. This parameter cannot be configured.

3.2.21.1 Server CA Configuration

Server CA Configuration

Figure 3-117 shows the **Server CA Configuration** screen.

Figure 3-117 Server CA Configuration Screen



For a description of the parameters on the **Server CA Configuration** screen, refer to [Table 3-89](#).

Table 3-89 Parameter Descriptions for the Server CA Configuration Screen

Parameter	Description
Enroll Cert	Registers certificates. For details, refer to Enroll Cert .
Delete Cert	Deletes certificates. For details, refer to Delete Cert .

Enroll Cert

[Figure 3-118](#) shows the **Enroll Cert** screen.

Figure 3-118 Enroll Cert Screen



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

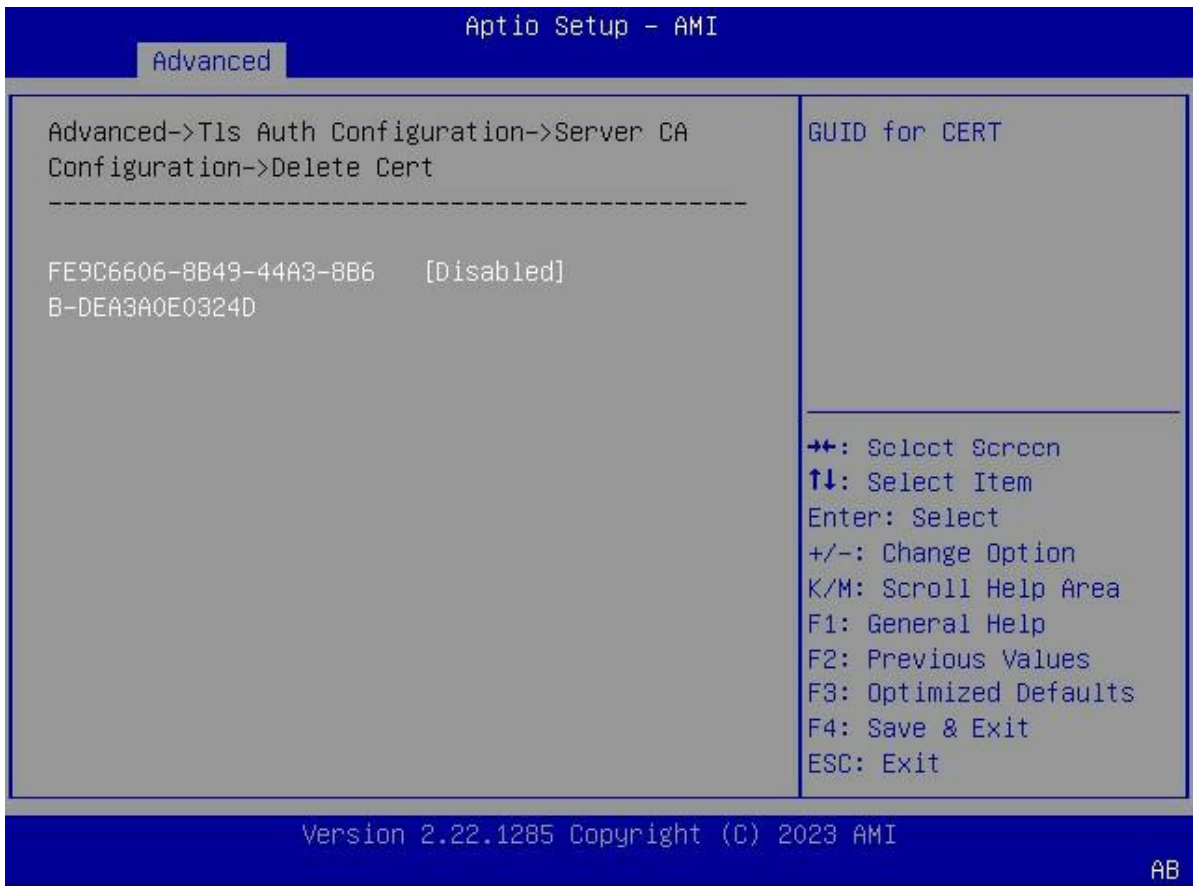
Table 3-90 Parameter Descriptions for the Enroll Cert Screen

Parameter	Description
Enroll Cert Using File	Registers 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: 11111111-2222-3333-4444-1234567890ab.
Commit Changes and Exit	Submits the changes and exits.
Discard Changes and Exit	Discards the changes and exits.

Delete Cert

[Figure 3-119](#) shows the **Delete Cert** screen.

Figure 3-119 Delete Cert Screen



For a description of the parameters on the **Delete Cert** screen, refer to [Table 3-91](#).

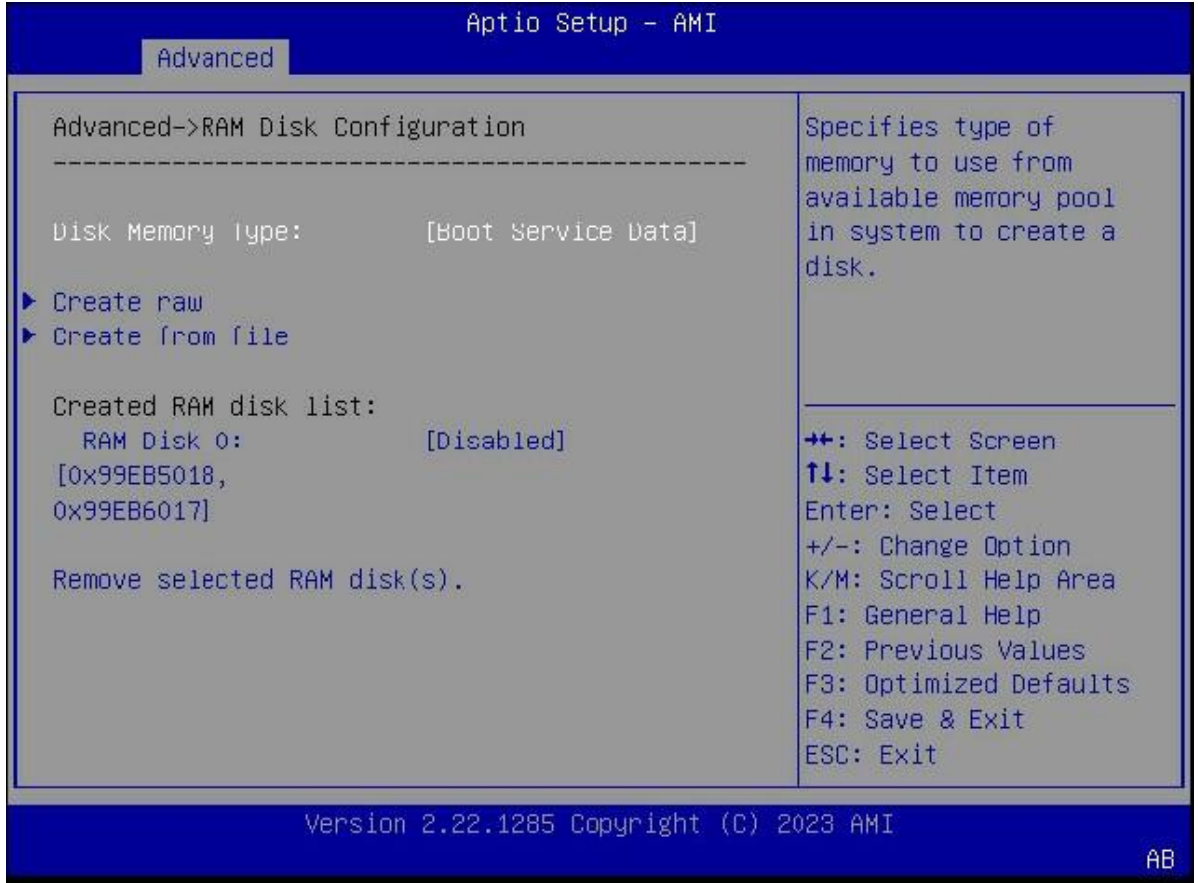
Table 3-91 Parameter Descriptions for the Delete Cert Screen

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

3.2.22 RAM Disk Configuration

[Figure 3-120](#) shows the **RAM Disk Configuration** screen.

Figure 3-120 RAM Disk Configuration Screen



For a description of the parameters on the **RAM Disk Configuration** screen, refer to [Table 3-92](#).

Table 3-92 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 3.2.22.1 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:	Disabled

Parameter	Description	Default
	- Enabled: deletes the selected RAM disk. - Disabled: disables deletion of the selected RAM disk.	
Remove selected RAM disk(s)	Deletes the enabled disks from the list of created RAM disks.	-

3.2.22.1 Create raw

Figure 3-121 shows the **Create raw** screen.

Figure 3-121 Create Raw Screen



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

Table 3-93 Parameter Descriptions for the Create Raw Screen

Parameter	Description	Default
Size(Hex)	Sets the disk size.	1
Create & Exit	Creates the raw disk and exits.	-

Discard & Exit	Discards raw disk creation and exits.	-
----------------	---------------------------------------	---

3.2.23 AMD PBS

Figure 3-122 shows the **AMD PBS** screen.

Figure 3-122 AMD CBS Screen



For a description of the parameters on the **AMD PBS** screen, refer to [Table 3-94](#).

Table 3-94 Parameter Descriptions for the AMD PBS Screen

Parameter	Description	Default
RAS	Sets AMD CPM RAS parameters. For details, refer to 3.2.23.1 RAS .	-
SPI Locking	Enables or disables the SPI locking feature. Options: - Enabled: enables the SPI locking feature. - Disabled: disables the SPI locking feature.	Disabled

HBA	Enables or disables the HBA feature of the standard backplane. Options:	Disabled
Parameter	Description	Default
	- Enabled: enables the HBA feature of the standard backplane. - Disabled: disable the HBA feature of the standard backplane.	
iLA TraceMemoryEn	Enables or disables the iLA TraceMemoryEn feature. Options: - Enabled: enables the iLA TraceMemoryEn feature. - Disabled: disables the iLA TraceMemoryEn feature.	Disabled
iLA TraceMemoryEn reserved MMIO	Displays the reserved MMIO information about iLA TraceMemoryEn.	0
CXL Range Encryption	Sets the parameters for AMD CXL range encryption. For details, refer to 3.2.23.2 CXL Range Encryption .	-

3.2.23.1 RAS

[Figure 3-123](#) through [Figure 3-124](#) show the **RAS** screen.

Figure 3-123 RAS Screen—1

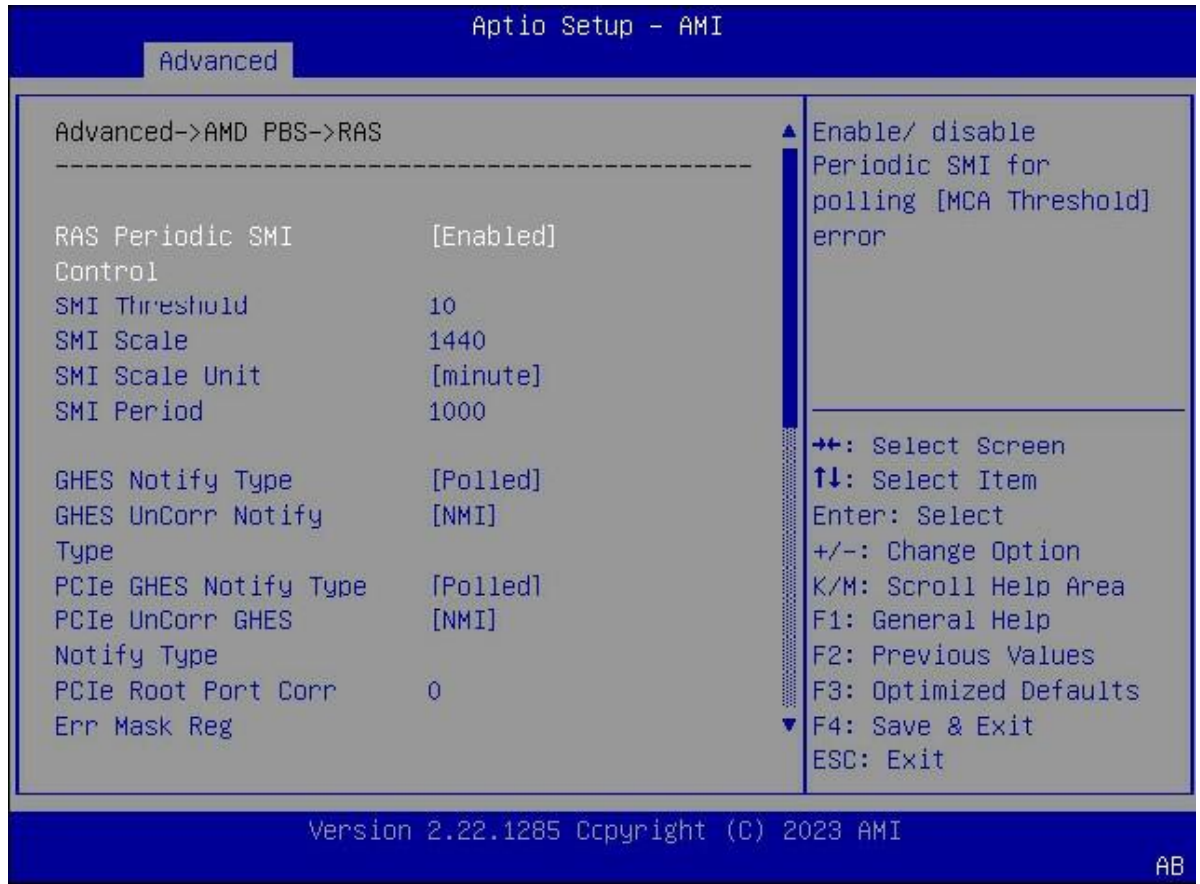
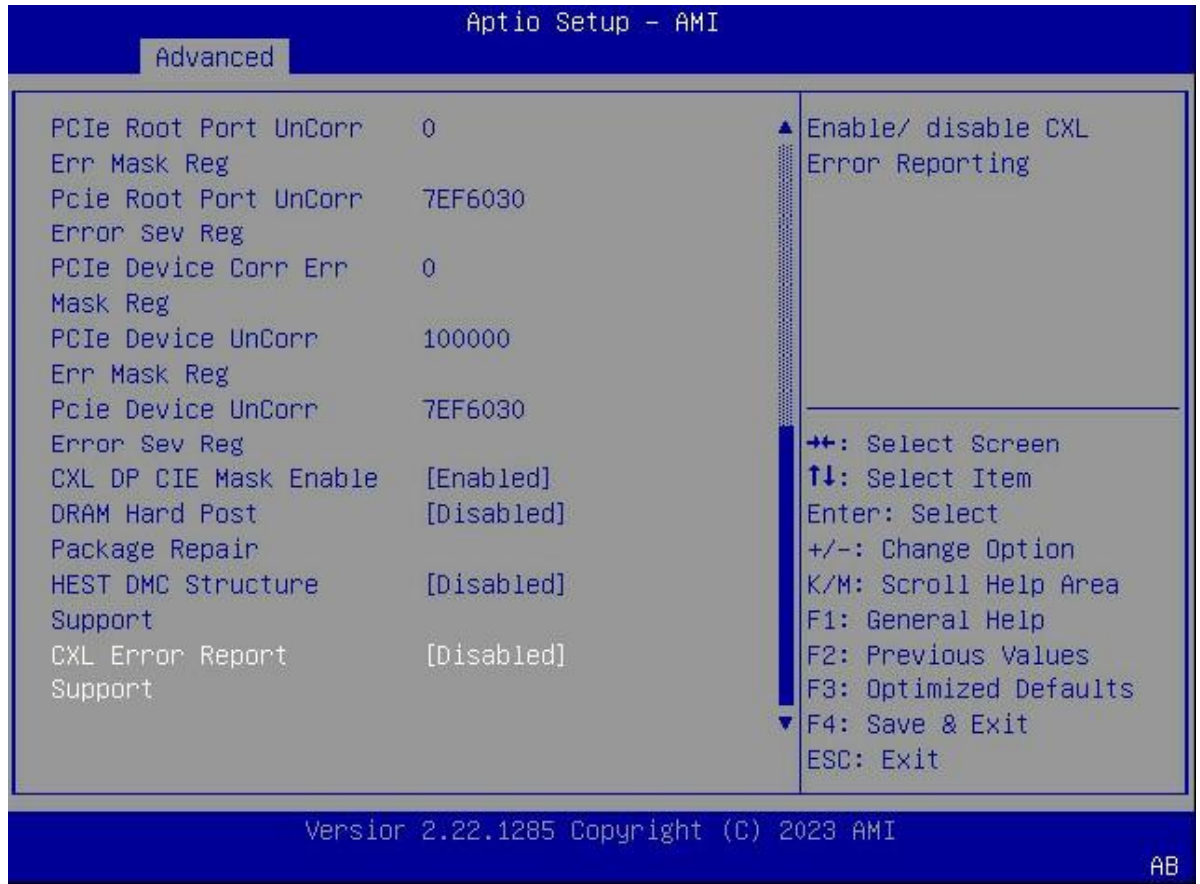


Figure 3-124 RAS Screen—2



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

Table 3-95 Parameter Descriptions for the RAS Screen

Parameter	Description	Default
RAS Periodic SMI Control	Enables or disables periodic SMI to respond to polling MCA errors. Options: - Enabled: enables periodic SMI to respond to polling MCA errors. - Disabled: disables periodic SMI to respond to polling MCA errors.	Enabled
SMI Threshold	Sets the SMI threshold. The SMI threshold limits the MCA threshold and the number of delay error SMI sources per unit of time.	10
SMI Scale	Sets the time scale for SMI.	1440

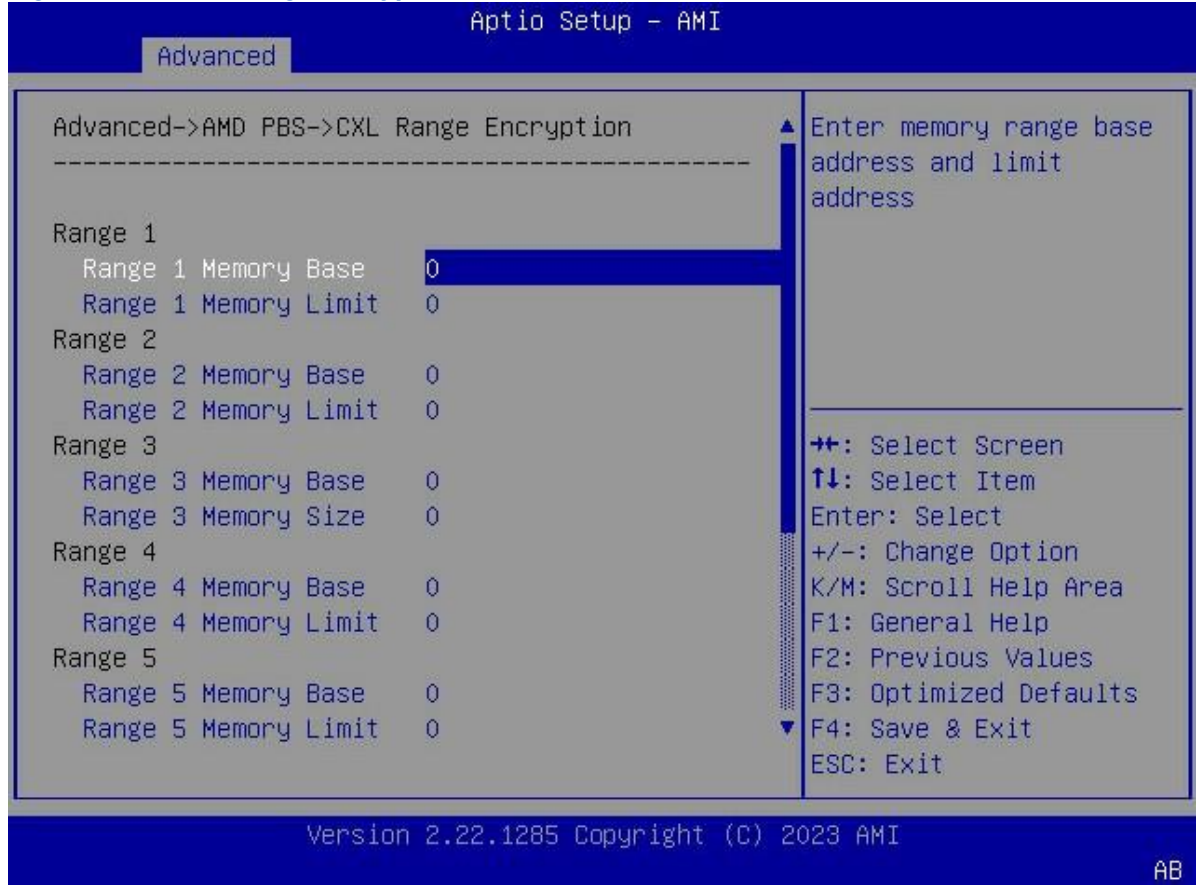
SMI Scale Unit	Select a unit for the SMI time scale. Options: ● millisecond	minute
----------------	--	--------

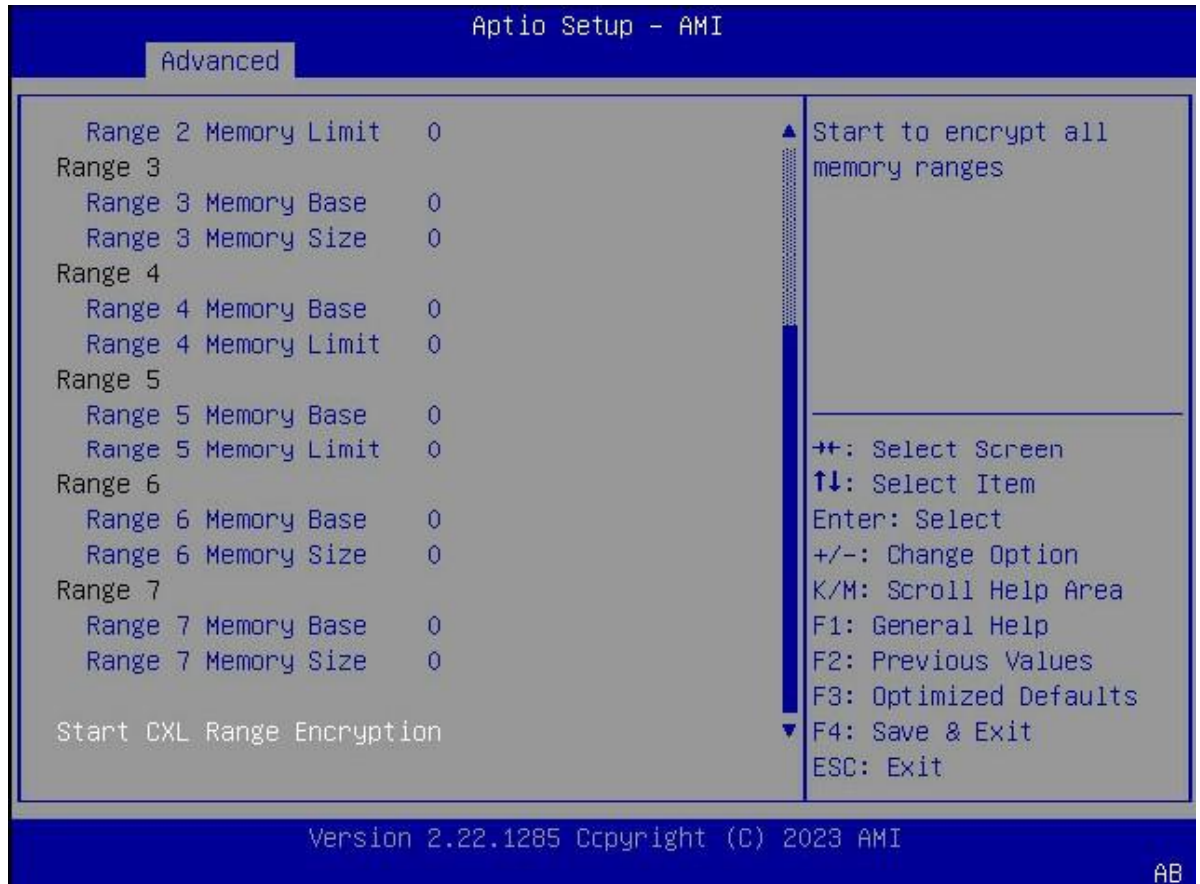
Parameter	Description	Default
	● Second ● minute	
SMI Period	Sets the polling interval, range: 0–32767, unit: milliseconds. Value 0 indicates that the polling interval is disabled.	1000
GHES Notify Type	Select the type of GHES notification. Options: ● Polled ● SCI	Polled
GHES UnCorr Notify Type	Select the type of GHES UnCorr notification. Options: ● Polled ● NMI	NMI
PCIE GHES Notify Type	Select the type of PCIE GHES notification. Options: ● Polled ● SCI	Polled
PCie UnCorr GHES Notify Type	Select the type of PCie UnCorr GHES notification. Options: ● Polled ● NMI	NMI
PCie Root Port UnCorr Err Mask Reg	Sets the Mask register for the AER uncorrectable errors of the PCie root port.	0
Pcie Root Port UnCorr Error Sev Reg	Sets the Severity register for the AER uncorrectable errors of the PCie root port.	7EF6030
PCie Device Corr Err Mask Reg	Sets the Mask register for the AER correctable errors of the PCie device.	0

PCIe Device UnCorr Err Mask Reg	Sets the Mask register for the AER uncorrectable errors of the PCIe device.	100000
Pcie Device UnCorr Error Sev Reg	Sets the Severity register for the AER uncorrectable errors of the PCIe device.	7EF6030
CXL DP CIE Mask Enable	Enables or disables the blocking of the CXL DP correctable errors (internal errors). Options: Enabled: enables the blocking of the CXL DP correctable errors (internal errors).	Enabled
Parameter	Description	Default
	Disabled: disables the blocking of the CXL DP correctable errors (internal errors).	
DRAM Hard Post Package Repair	Enables or disables the DRAM hard repair feature. Options: - Enabled: enables the DRAM hard repair feature. When this parameter is set to Enabled, the standby DRAM rows are allowed to replace the failed rows through a real-time remediation mechanism. - Disabled: disables the DRAM hard repair feature.	Disabled
HEST DMC Structure Support	Enables or disables HEST DMC structure support. Options: - Enabled: enables HEST DMC structure support. - Disabled: disables HEST DMC structure support.	Disabled
CXL Error Report Support	Enables or disables CXL error reporting support. Options: - Enabled: enables CXL error reporting support. - Disabled: disables CXL error reporting support.	Disabled

3.2.23.2 CXL Range Encryption

Figure 3-125 Through Figure 3-126 show the **CXL Range Encryption** screen.

Figure 3-125 CXL Range Encryption Screen—1**Figure 3-126 CXL Range Encryption Screen—2**



For a description of the parameters on the **CXL Range Encryption** screen, refer to [Table 3-96](#).
Table 3-96 Parameter Descriptions for the CXL Range Encryption Screen

Parameter	Description	Default
Range 1 Memory Base	Sets the start memory address of memory base range 1.	0
Range 1 Memory Limit	Sets the memory limit of memory base range 1.	0
Start CXL Range Encryption	Encrypts all memory ranges.	-

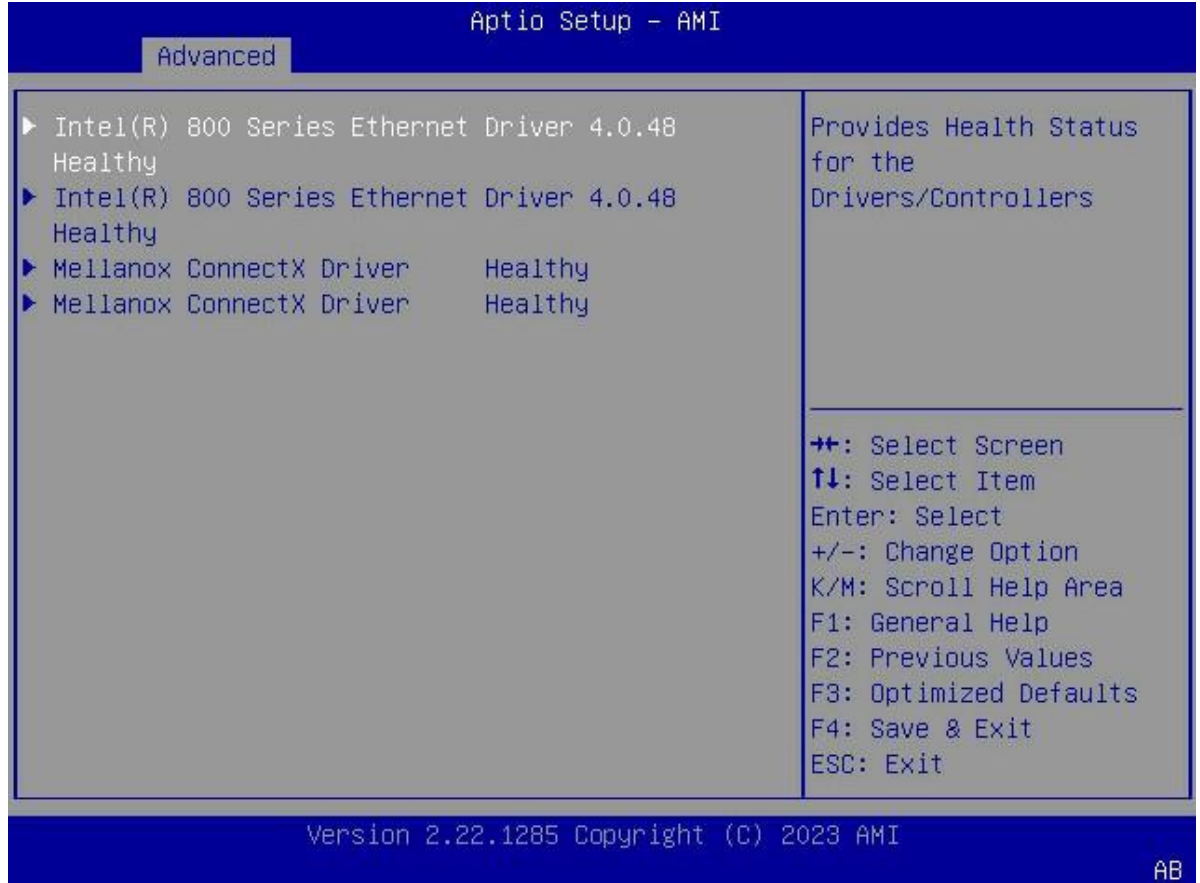
Note

The settings of **Range 2** and **Range 3** are the same as those of **Range 1**.

3.2.24 Driver Health

[Figure 3-127](#) shows the **Driver Health** screen.

Figure 3-127 Driver Health Screen



Select a driver on the screen and then press the **Enter** key. The health status of the driver is displayed.

3.2.25 Advanced Power Management Configuration

Figure 3-128 shows the **Advanced Power Management Configuration** screen.

Figure 3-128 Advanced Power Management Configuration Screen



For a description of the parameters on the **Advanced Power Management Configuration** screen, refer to [Table 3-97](#).

Table 3-97 Parameter Descriptions for the Advanced Power Management Configuration Screen

Parameter	Description	Default
Power Policy Select	Sets the power management policy. Options: ● Performance ● Efficient ● Custom ● Latency-Performance	Custom

3.3 Chipset

The **Chipset** screen provides the **South Bridge** and **North Bridge** configuration items as shown in [Figure 3-129](#). Information that can be set includes the northbridge memory information and the southbridge debugging information.

Figure 3-129 Chipset Screen



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

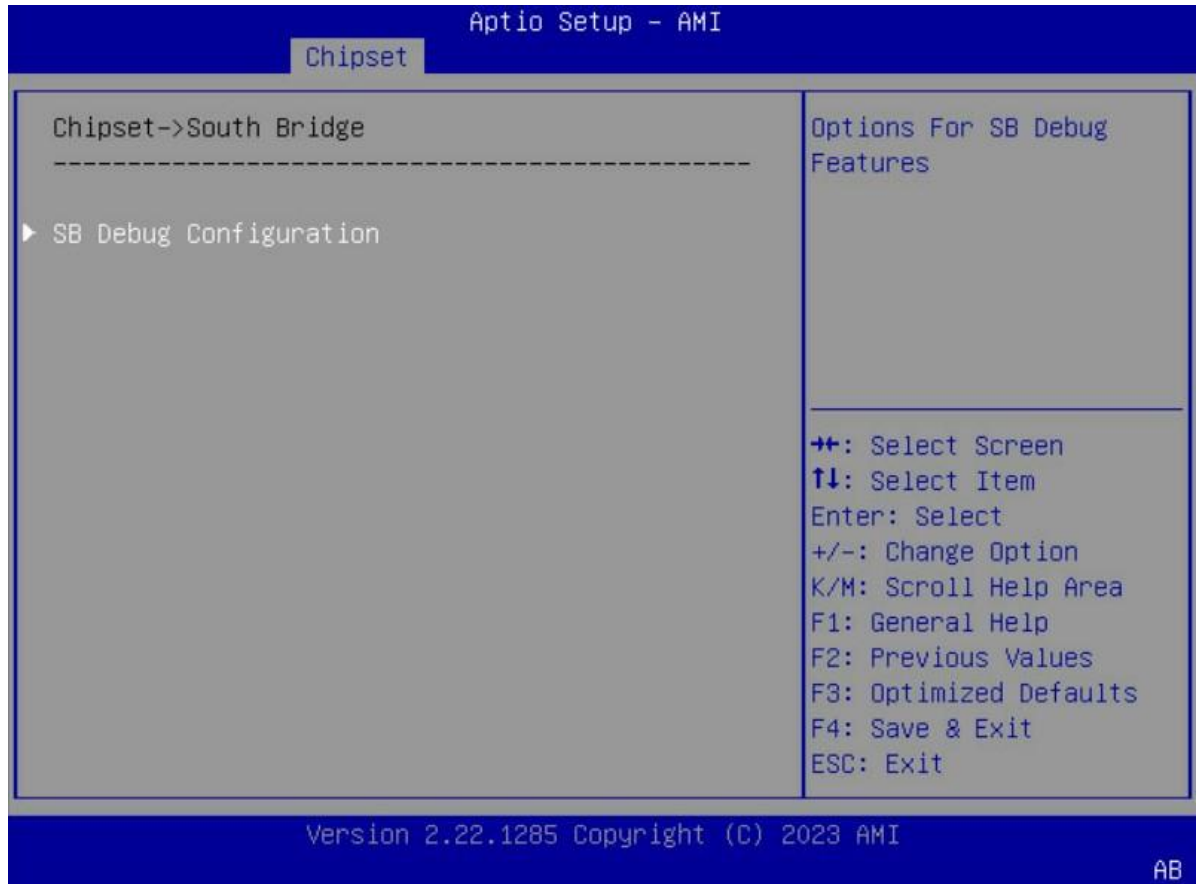
Table 3-98 Parameter Descriptions for the Chipset Screen

Parameter	Description	Default
PCIe Compliance Mode	Enables or disables the PCIe link compliance mode. Options: ● Off ● On	Off
South Bridge	Sets southbridge parameters. For details, refer to 3.3.1 South Bridge .	-
North Bridge	Sets northbridge parameters. For details, refer to 3.3.2 North Bridge .	-

3.3.1 South Bridge

[Figure 3-130](#) shows the **South Bridge** screen.

Figure 3-130 SB Debug Configuration Screen



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

Table 3-99 Parameter Descriptions for the South Bridge Screen

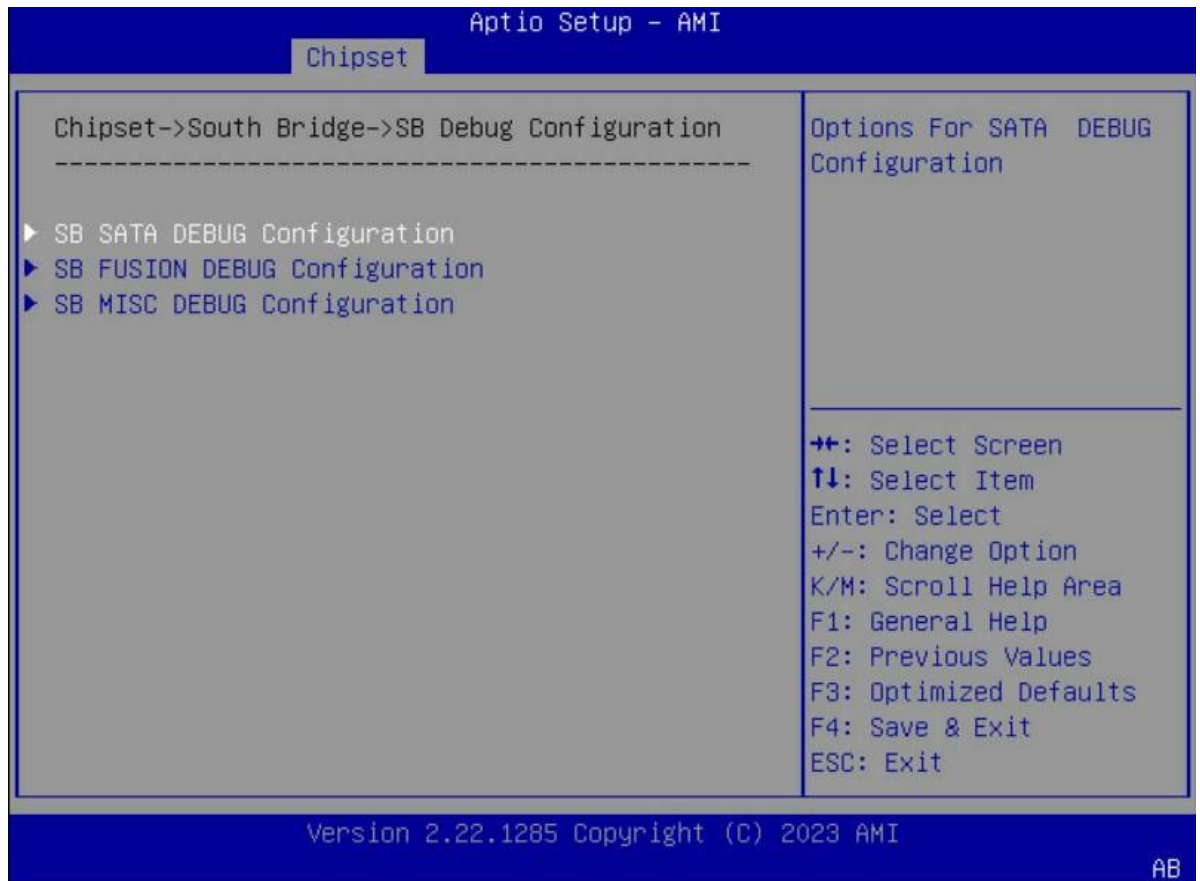
Parameter	Description
SB Debug Configuration	Sets southbridge debugging parameters. For details, refer to 3.3.1.1 SB Debug Configuration .

3.3.1.1 SB Debug Configuration

SB Debug Configuration

The **SB Debug Configuration** screen provides the **SB SATA Debug Configuration**, **SB Fusion Debug Configuration**, and **SB Misc Debug Configuration** items, as shown in [Figure 3-131](#).

Figure 3-131 SB Debug Configuration Screen



For a description of the parameters on the **SB Debug Configuration** screen, refer to [Table 3-100](#).

Table 3-100 Parameter Descriptions for the SB Debug Configuration Screen

Parameter	Description
SB SATA Debug Configuration	Sets SATA debugging parameters. For details, refer to SB SATA Debug Configuration .
SB Fusion Debug Configuration	Sets southbridge Fusion debugging parameters. For details, refer to SB Fusion Debug Configuration .
SB Misc Debug Configuration	Sets southbridge MISC debugging parameters. For details, refer to SB Misc Debug Configuration .

SB SATA Debug Configuration

[Figure 3-132](#) through [Figure 3-133](#) show the **SB SATA Debug Configuration** screen.

Figure 3-132 SB SATA Debug Configuration Screen—1

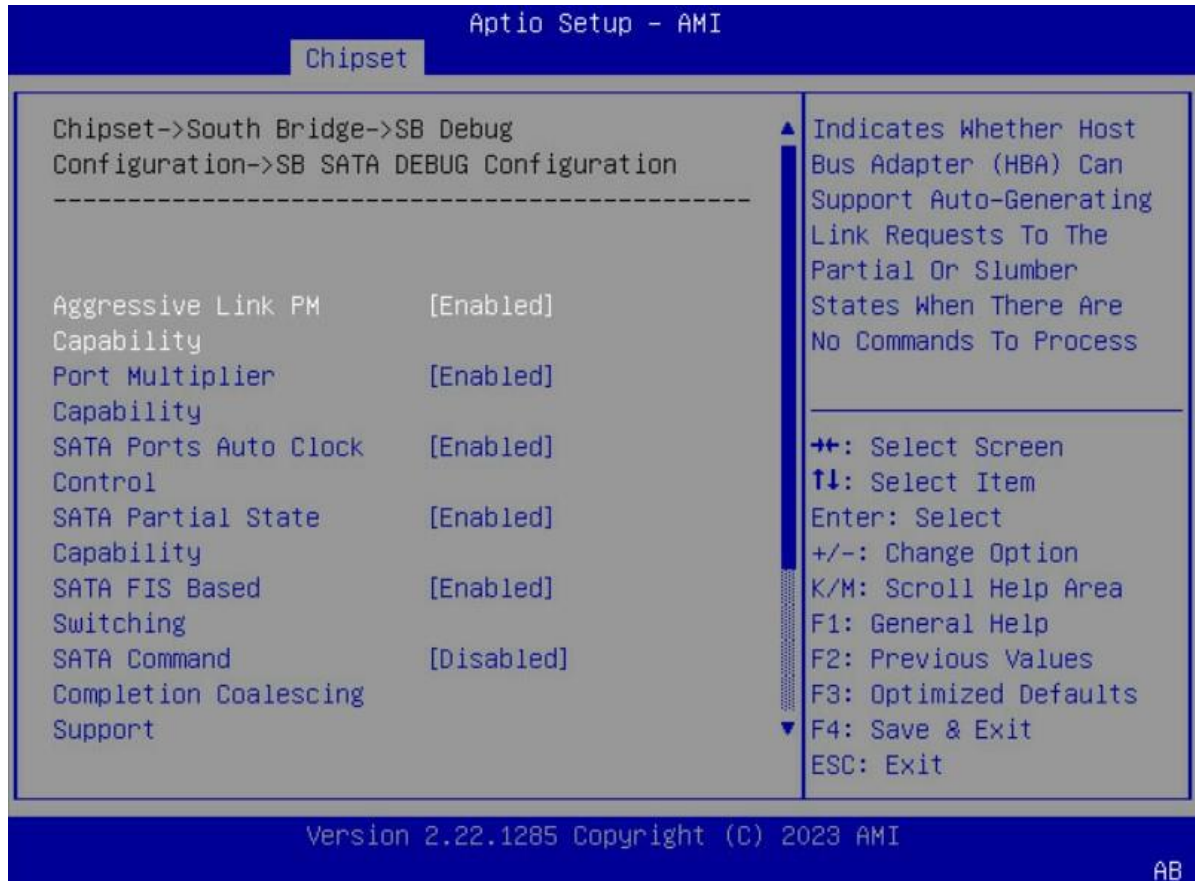
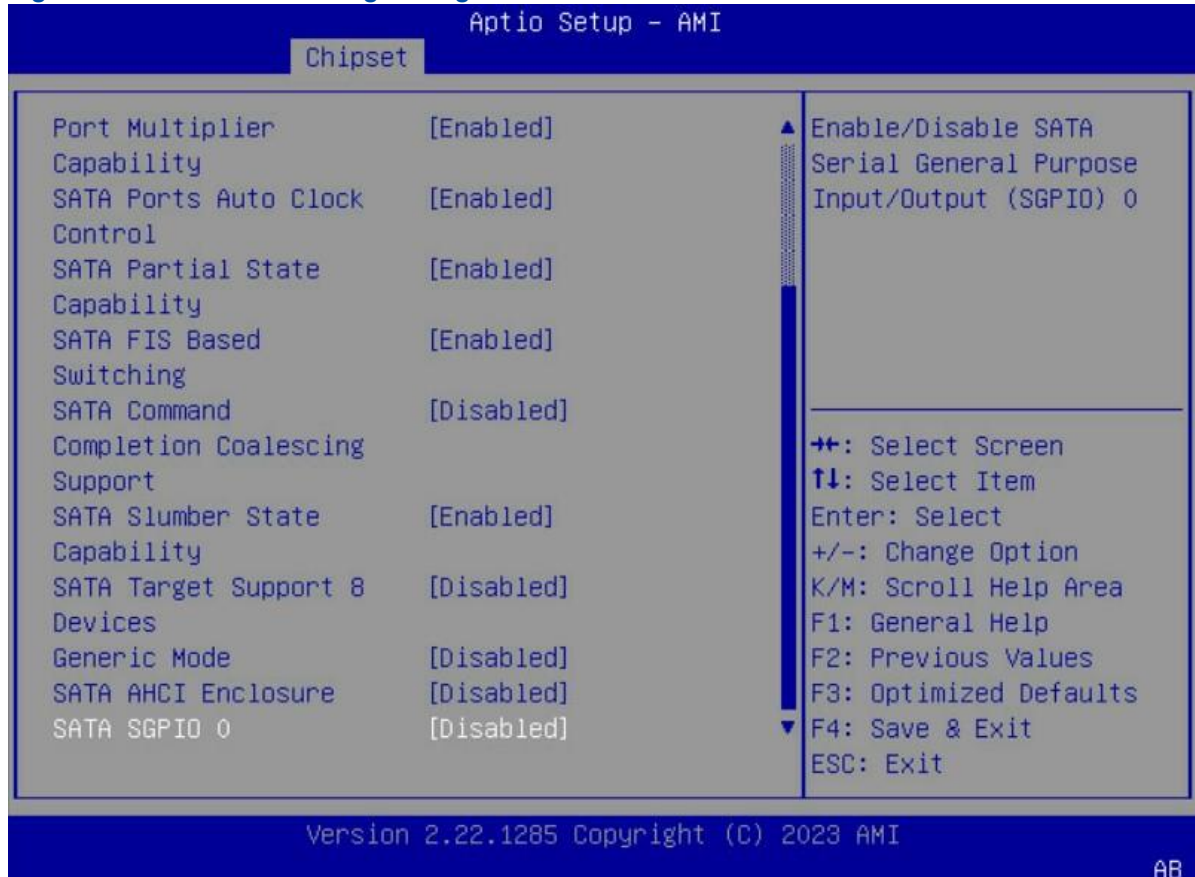


Figure 3-133 SB SATA Debug Configuration Screen—2



For a description of the parameters on the **SB SATA Debug Configuration** screen, refer to [Table 3-101](#).

Table 3-101 Parameter Descriptions for the SB SATA Debug Configuration Screen

Parameter	Description	Default
Aggressive Link PM Capability	Enables or disables Aggressive link performance. Options: - Enabled: enables Aggressive link performance. When this parameter is set to Enabled, the host bus adapter supports automatic generation of link requests pointing to partial or slumber state when there are no commands to process. - Disabled: disables Aggressive link performance.	Enabled
Port Multiplier Capability	Enables or disables the port support feature of the host bus adapter. Options: - Enabled: enables the port support feature of the host bus adapter. - Disabled: disables the port support feature of the host bus adapter.	Enabled

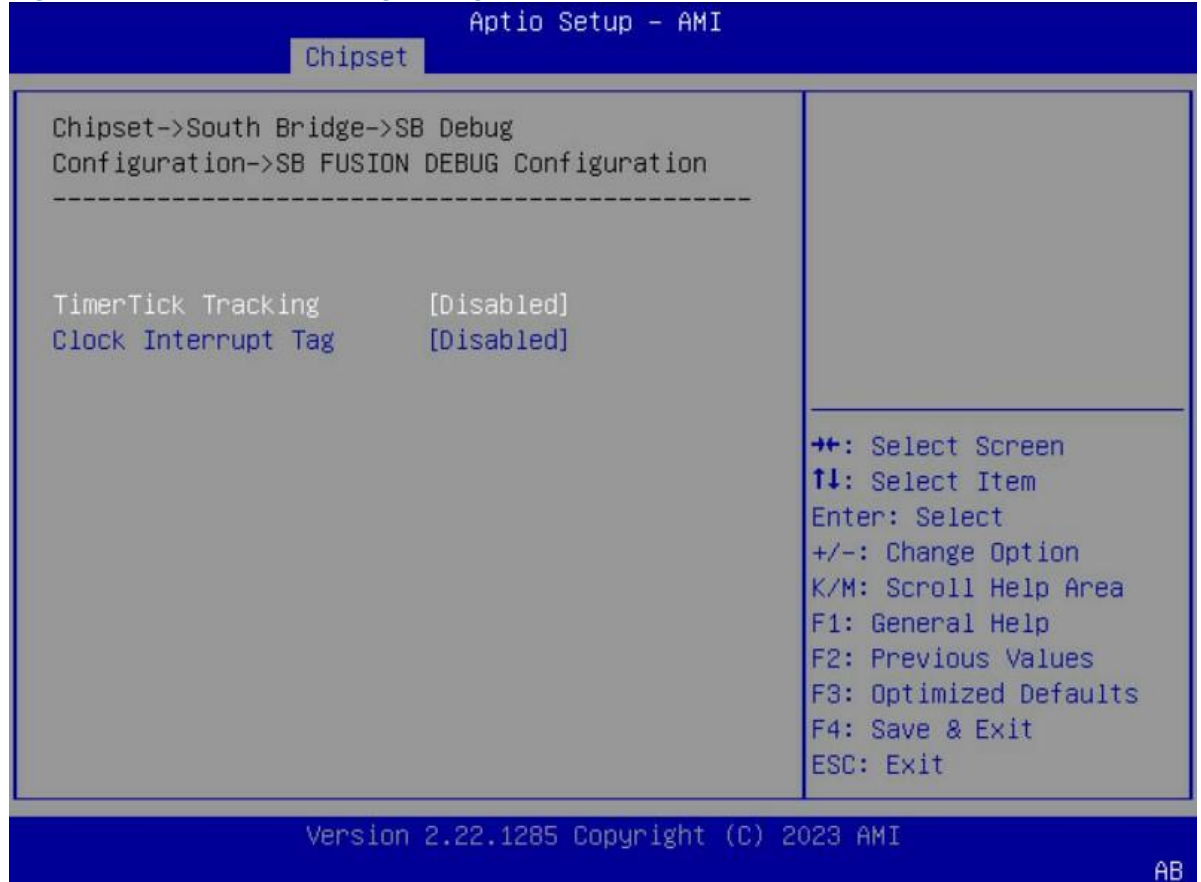
Parameter	Description	Default
SATA Ports Auto Clock Control	Enables or disables the automatic clock control feature of SATA ports. Options: - Enabled: enables the automatic clock control feature of SATA ports. - Disabled: disables the automatic clock control feature of SATA ports.	Enabled
SATA Partial State Capability	Enables or disables the SATA partial state feature. Options: - Enabled: enables the SATA partial state feature. - Disabled: disables the SATA partial state feature.	Enabled

SATA FIS Based Switching	Enables or disables the FIS-based switching mechanism. Options: ● Enabled: enables the FIS-based switching mechanism. ● Disabled: disables the FIS-based switching mechanism.	Enabled
SATA Command Completion Coalescing Support	Enables or disables the SATA command completion coalescing support feature. Options: ● Enabled: enables the SATA command completion coalescing support feature. ● Disabled: disables the SATA command completion coalescing support feature.	Disabled
SATA Slumber State Capability	Enables or disables the SATA slumber state capability. Options: ● Enabled: enables the SATA slumber state capability. ● Disabled: disables the SATA slumber state capability.	Enabled
SATA Target Support 8 Devices	Enables or disables the support for eight devices. Options: ● Enabled: enables the support for eight devices. ● Disabled: disables the support for eight devices.	Disabled
Generic Mode	Enables or disables generic mode. Options:	Disabled
Parameter	Description	Default
	● Enabled: enables generic mode. ● Disabled: disables generic mode.	
SATA AHCI Enclosure	Enables or disables the SATA AHCI enclosure. Options: ● Enabled: enables the SATA AHCI enclosure. ● Disabled: disables the SATA AHCI enclosure.	Disabled
SATA SGPIO 0	Enables or disables SATA SGPIO 0. Options: ● Enabled: enables SATA SGPIO 0. ● Disabled: disables SATA SGPIO 0.	Disabled

SB Fusion Debug Configuration

Figure 3-134 shows the **SB Fusion Debug Configuration** screen.

Figure 3-134 SB Fusion Debug Configuration Screen



For a description of the parameters on the **SB Fusion Debug Configuration** screen, refer to Table 3-102.

Table 3-102 Parameter Descriptions for the SB Fusion Debug Configuration Screen

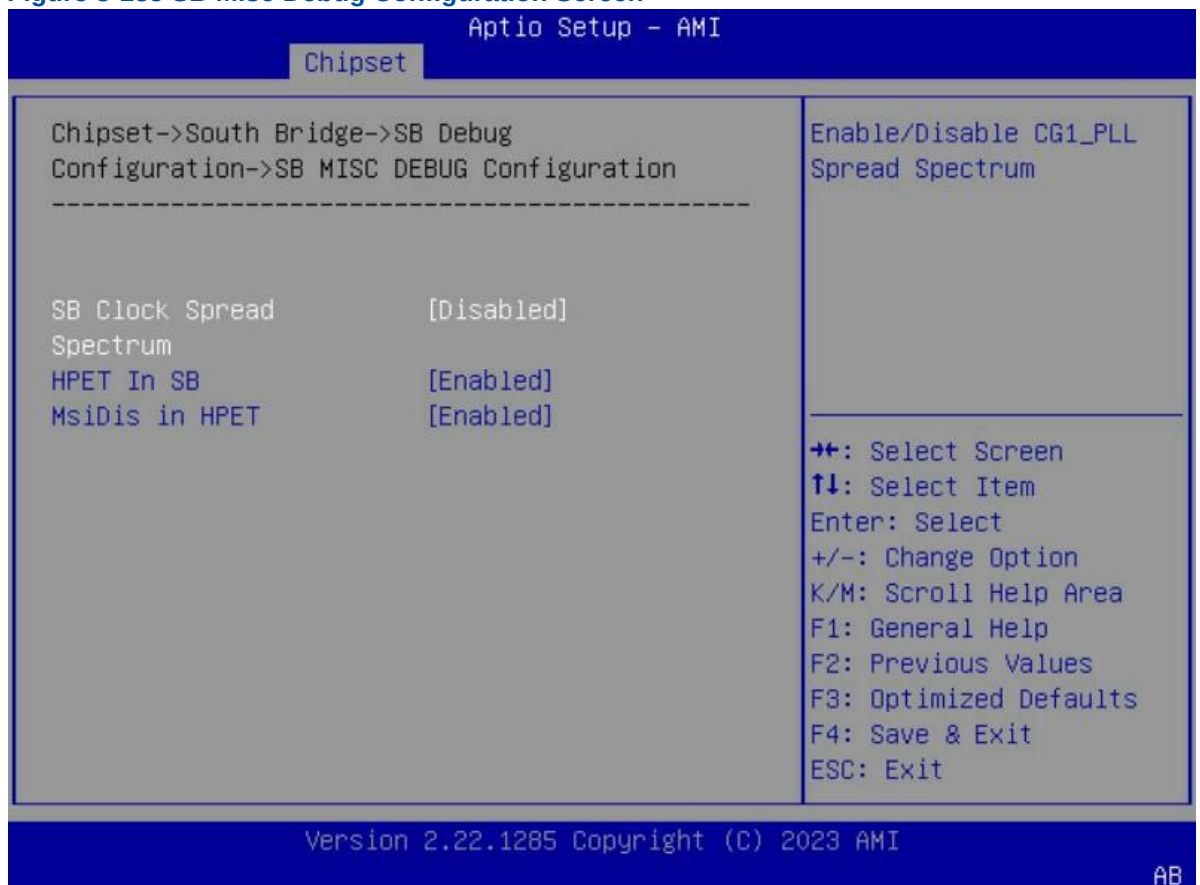
Parameter	Description	Default
TimerTick Tracking	Enables or disables the timer tick tracking feature. Options: - Enabled: enables the timer tick tracking feature. - Disabled: disables the timer tick tracking feature.	Disabled

Clock Interrupt Tag	Enables or disables the clock interrupt tag feature. Options: - Enabled: enables the clock interrupt tag feature. - Disabled: disables the clock interrupt tag feature.	Disabled
---------------------	--	----------

SB Misc Debug Configuration

Figure 3-135 shows the **SB Misc Debug Configuration** screen.

Figure 3-135 SB Misc Debug Configuration Screen



For a description of the parameters on the **SB Misc Debug Configuration** screen, refer to [Table 3-103](#).

Table 3-103 Parameter Descriptions for the SB Misc Debug Configuration Screen

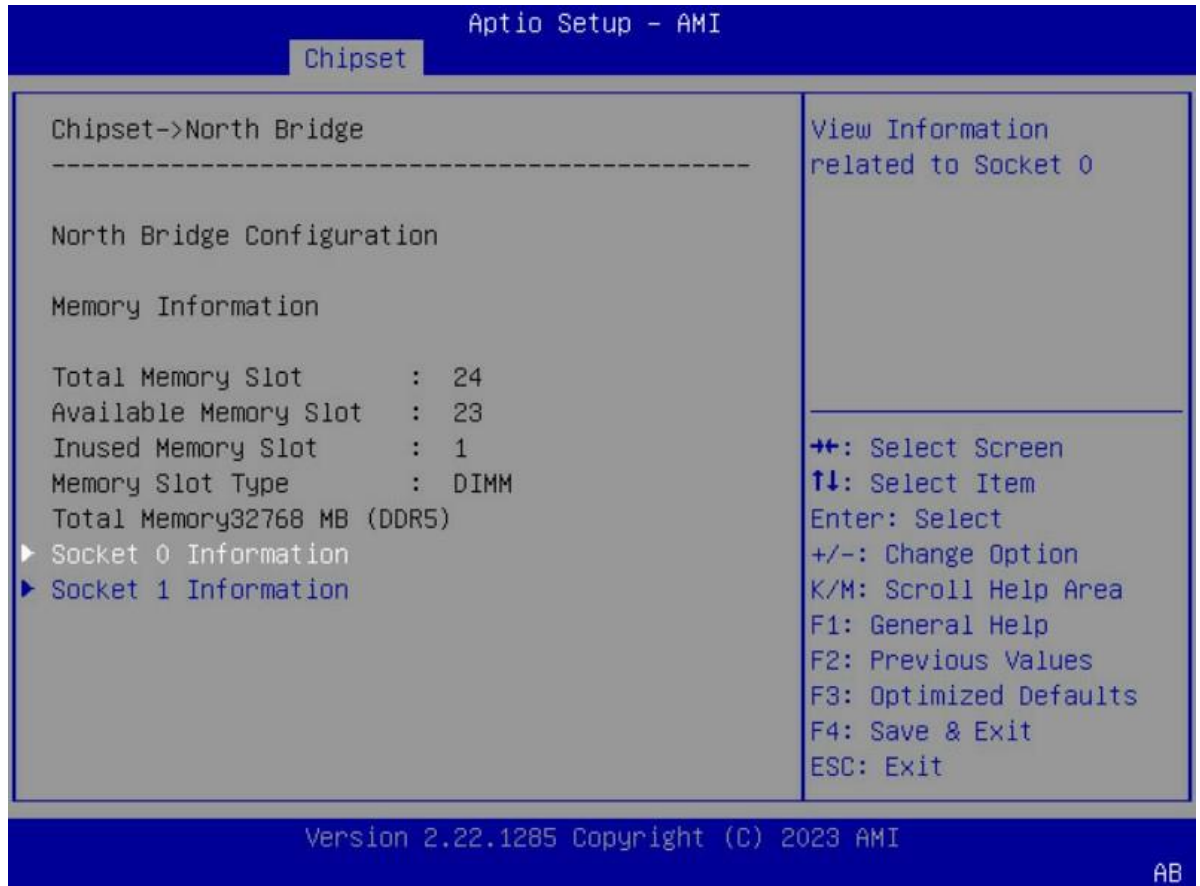
Parameter	Description	Default
-----------	-------------	---------

SB Clock Spread Spectrum	Enables or disables the southbridge clock spread spectrum. Options: • Enabled: enables the southbridge clock spread spectrum. • Disabled: disables the southbridge clock spread spectrum.	Disabled
HPET In SB	Enables or disables the HPET feature. Options: • Enabled: enables the HPET feature. • Disabled: disables the HPET feature.	Enabled
MsiDis in HPET	Enables or disables MSI capability disclosure to the HPET capability register. Options: • Enabled: enables MSI capability disclosure to the HPET capability register. • Disabled: disables MSI capability disclosure to the HPET capability register.	Enabled

3.3.2 North Bridge

Figure 3-136 shows the **North Bridge** screen.

Figure 3-136 North Bridge Screen



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

Table 3-104 Parameter Descriptions for the North Bridge Screen

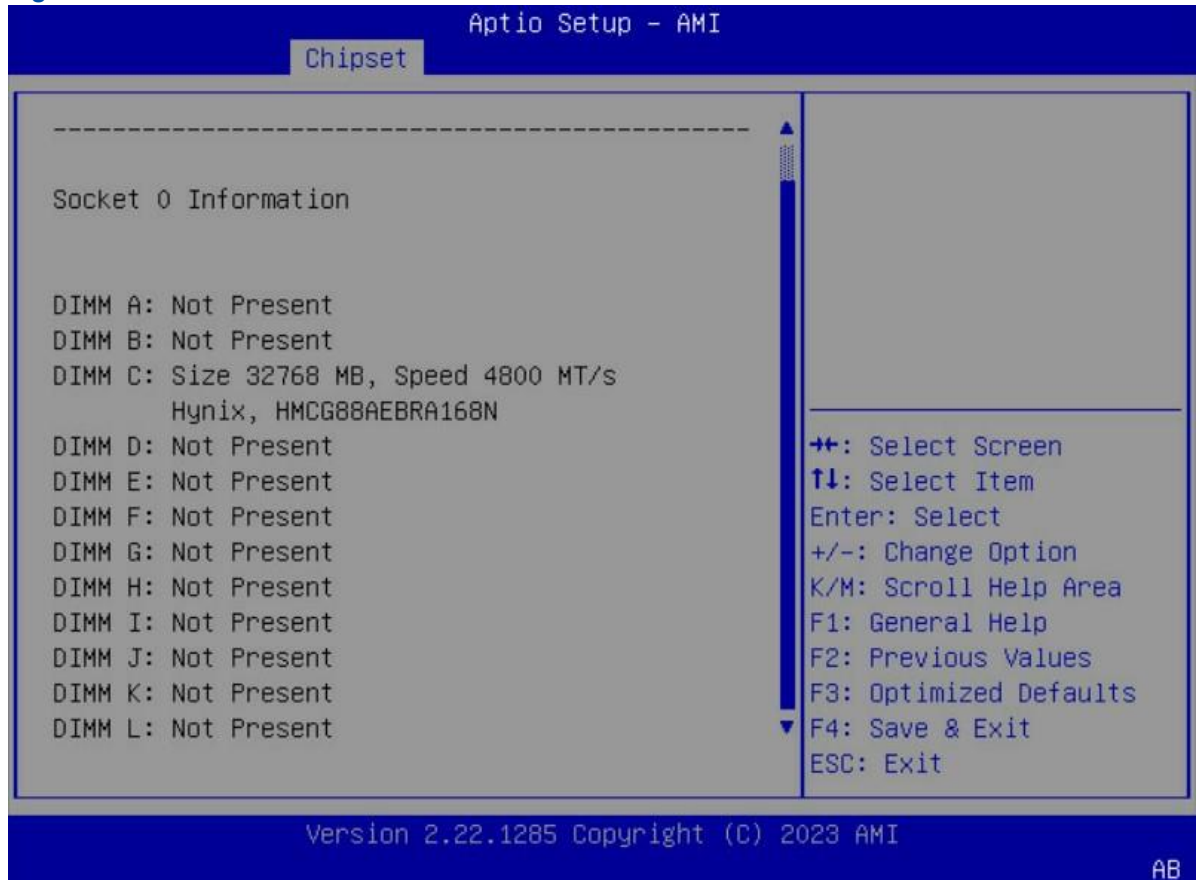
Parameter	Description	Setting Example
Total Memory Slot	Displays the total number of memory slots.	24
Available Memory Slot	Displays the number of unused memory slots.	23
Inused Memory Slot	Displays the number of memory slots in use.	1
Memory Slot Type	Displays the type of memory slot.	DIMM
Total Memory	Displays the total memory size.	32768 MB(DDR5)
Socket 0 Information	Sets the memory parameters for CPU 0 . For details, refer to 3.3.2.1 Socket 0 Information .	-

Socket 1 Information	Sets the memory parameters for CPU 1 .	-
Parameter	Description	Setting Example
	For details, refer to 3.3.2.1 Socket 0 Information .	

3.3.2.1 Socket 0 Information

[Figure 3-137](#) shows the **Socket 0 Information** screen.

Figure 3-137 Socket 0 Information Screen



For a description of the parameters on the **Socket 0 Information** screen, refer to [Table 3-105](#).

Table 3-105 Parameter Descriptions for the Socket 0 Information Screen

Parameter	Description
DIMM A	DIMM A presence information. If the device is not present, Not Present is displayed.

**Note**

The above description also applies to other DIMMs.

3.4 Security

Figure 3-138 through Figure 3-139 show the **Security** screen.

Figure 3-138 Security Screen—1



Figure 3-139 Security Screen—2



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

Table 3-106 Parameter Descriptions for the Security Screen

Parameter	Description	Default
Administrator Password	Sets the administrator password.	Administrator Password Not Installed
User Password	Sets the user password.	User Password Not Installed
HDD Security Configurations	Sets the HDD security parameters. The actual parameters displayed on the screen vary with hard disks, but the parameters that need to be configured are the same. P0:INTEL SSDSCKKB240GB is used as an example. For details, refer to 3.4.1 HDD Security Configuration .	-
Secure Boot	Sets secure boot parameters. For details, refer to 3.4.2 Secure Boot .	-

Secure Flash Update	Sets secure flash update parameters.	-
Parameter	Description	Default
	For details, refer to 3.4.3 Secure Flash Update .	
Security Freeze Lock	Enables or disables the security freezing lock. Options: - Enabled: enables the security freezing lock. - Disabled: disables the security freezing lock.	Enabled

3.4.1 HDD Security Configuration

Figure 3-140 shows the **HDD Security Configuration** screen.

Figure 3-140 HDD Security Configuration Screen—1

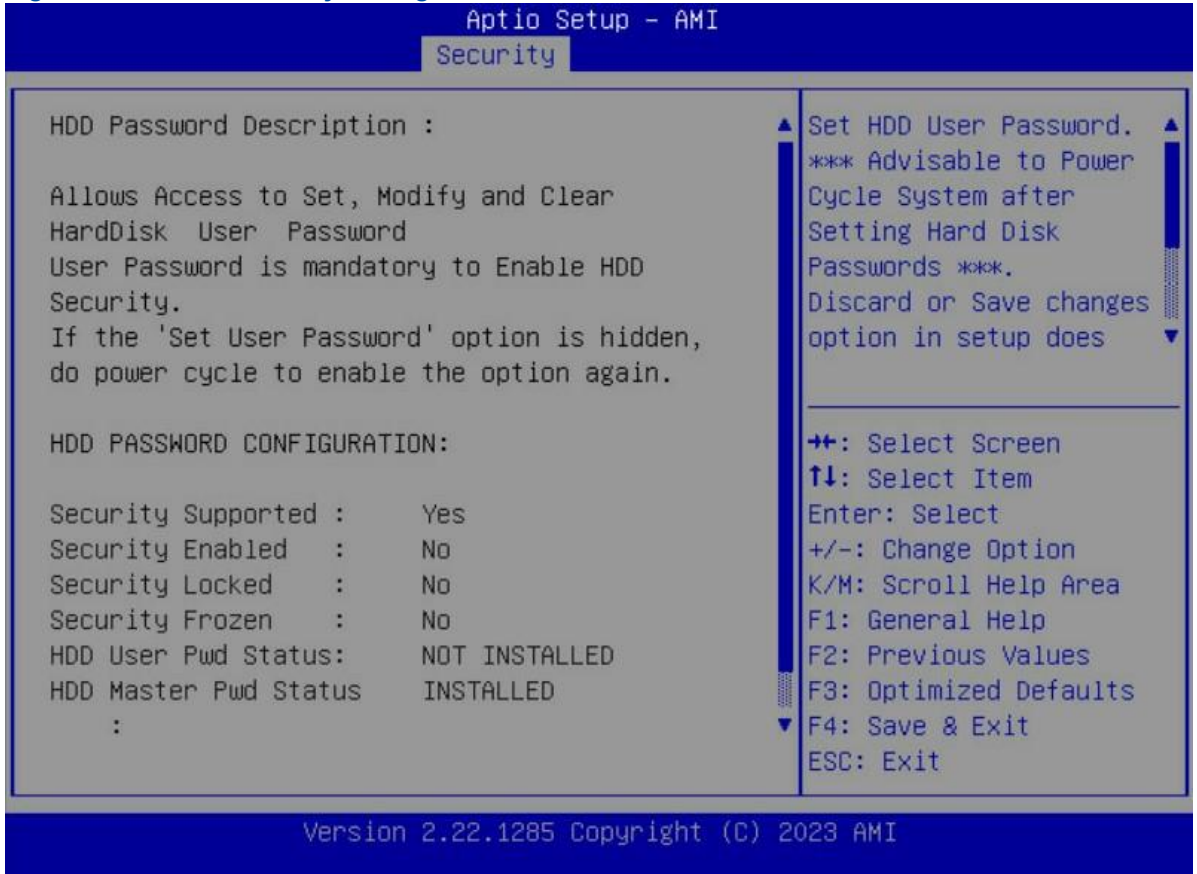
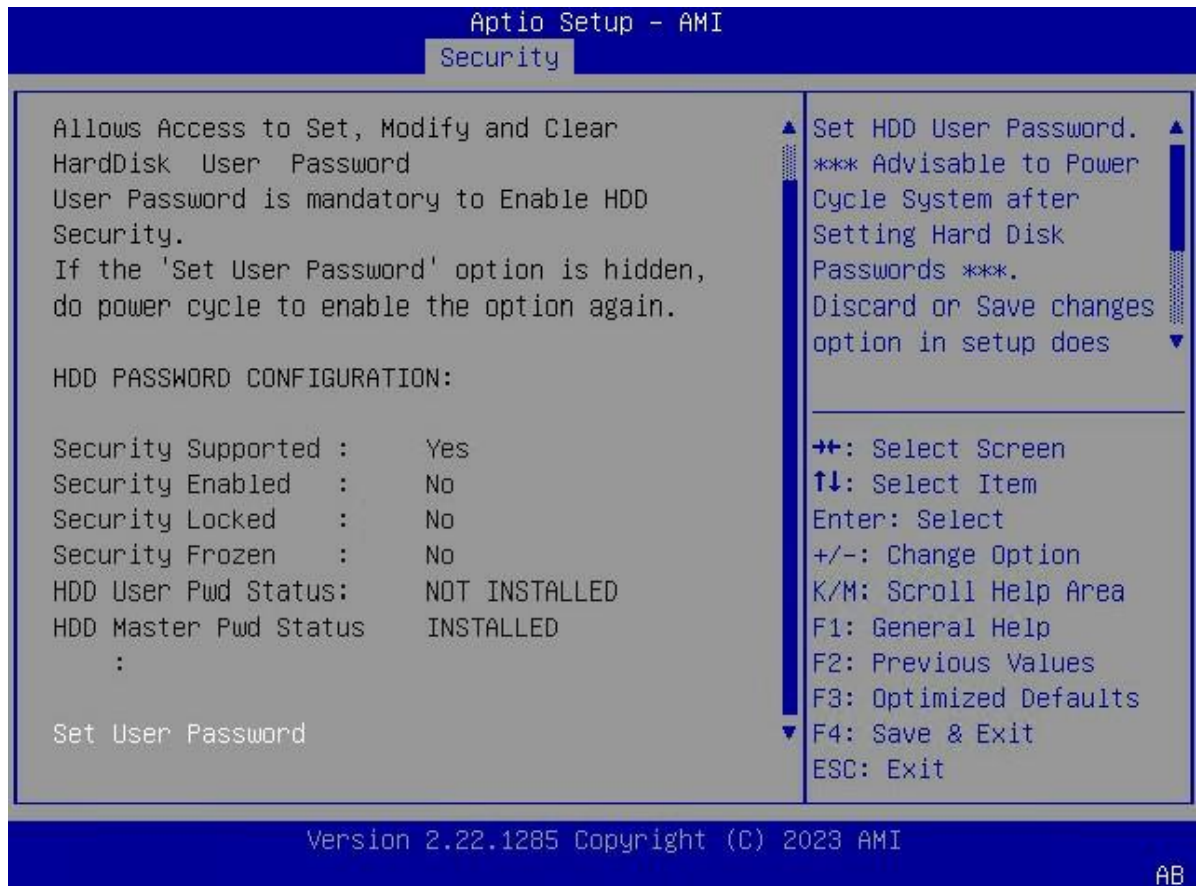


Figure 3-141 HDD Security Configuration Screen—2



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

Table 3-107 Parameter Descriptions for the HDD Security Configuration Screen

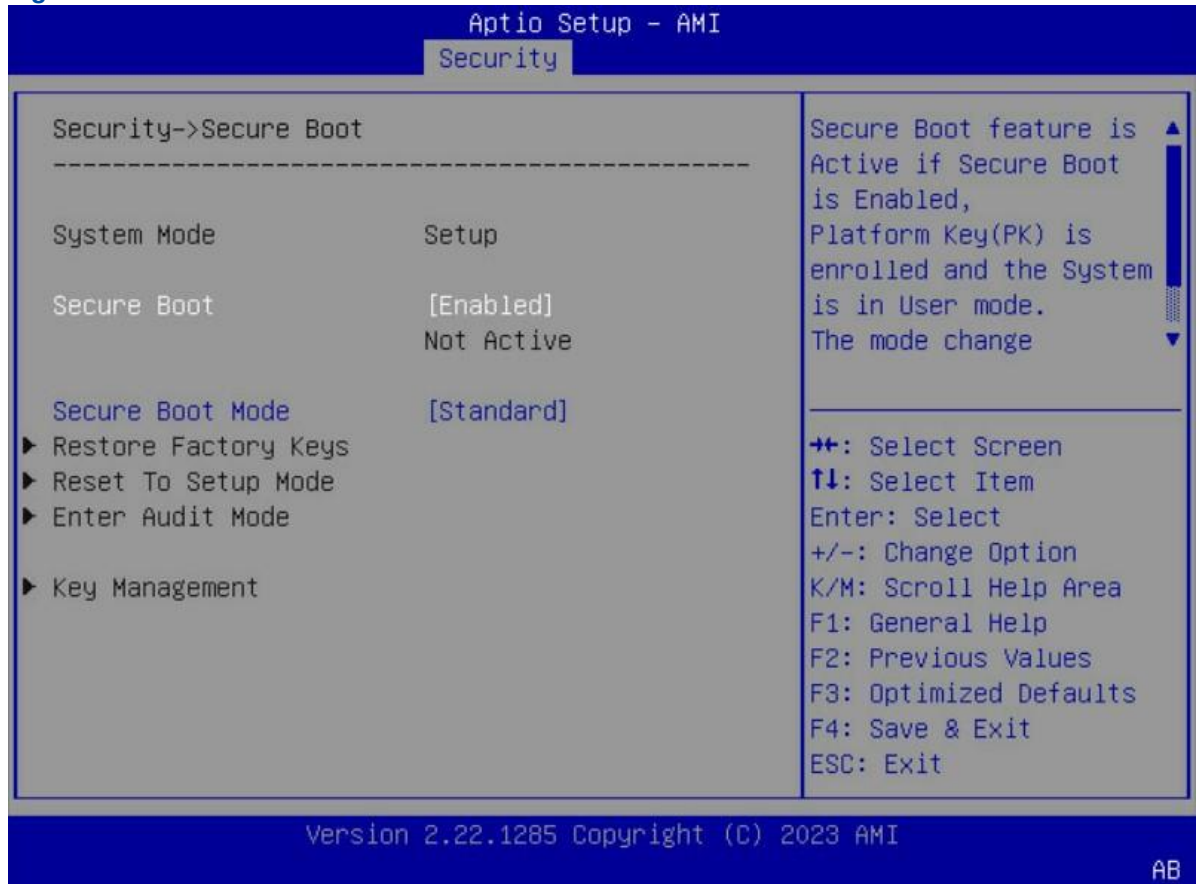
Parameter	Description	Setting Example
HDD Password Description	Displays the hard disk password configuration description.	-
Security Supported	Displays whether security is supported.	Yes
Security Enabled	Displays whether security is enabled.	No
Security Locked	Displays whether security is locked.	No
Security Frozen	Displays whether security is frozen.	No
HDD User Pwd Status	Displays HDD user password status.	NOT INSTALLED

Parameter	Description	Setting Example
HDD Master Pwd Status	Displays HDD master password status.	INSTALLED
Set User Password	Sets the HDD user password.	-

3.4.2 Secure Boot

Figure 3-142 shows the **Secure Boot** screen.

Figure 3-142 Secure Boot Screen



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

Table 3-108 Parameter Descriptions for the Secure Boot Screen

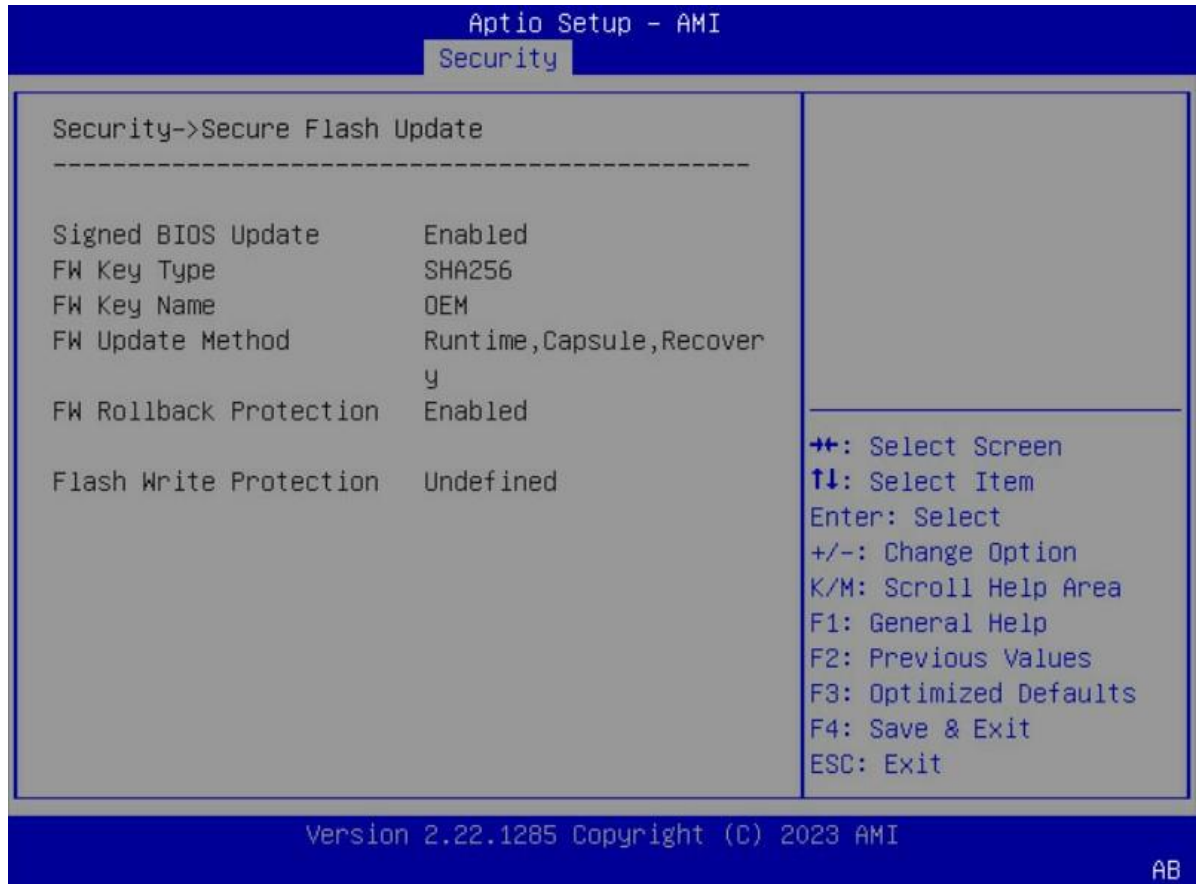
Parameter	Description	Default
System Mode	Sets the security system mode.	Setup

Secure Boot	Enables or disables the secure boot feature. Options: Enabled: enables the secure boot feature.	Enabled
Parameter	Description	Default
	Disabled: disables the secure boot feature.	
Secure Boot Mode	Sets the secure boot mode. Options: - Standard - Custom	Standard
Restore Factory keys	Restores the default factory key.	-
Reset To Setup Mode	Resets to setup mode.	-
Enter Audit Mode	Enters audit mode.	-
Key Management	Manages the key.	-

3.4.3 Secure Flash Update

Figure 3-143 shows the **Secure Flash Update** screen.

Figure 3-143 Secure Flash Update Screen



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

Table 3-109 Parameter Descriptions for the Secure Flash Update Screen

Parameter	Description	Default
Signed BIOS update	Enables or disables the signed BMC update feature.	Enabled
FW Key Type	Displays the firmware key type.	SHA256
FW Key Name	Displays the firmware key name.	OEM
FW Update Method	Displays the firmware update method.	Runtime, Capsule, Recovery
FW Rollback Protection	Enables or disables the firmware rollback protection feature.	Enabled
Flash Write Protection	Displays flash write protection.	Undefined

3.5 Boot

[Figure 3-144](#) through [Figure 3-145](#) show the **Boot** screen.

Figure 3-144 Boot Screen—1

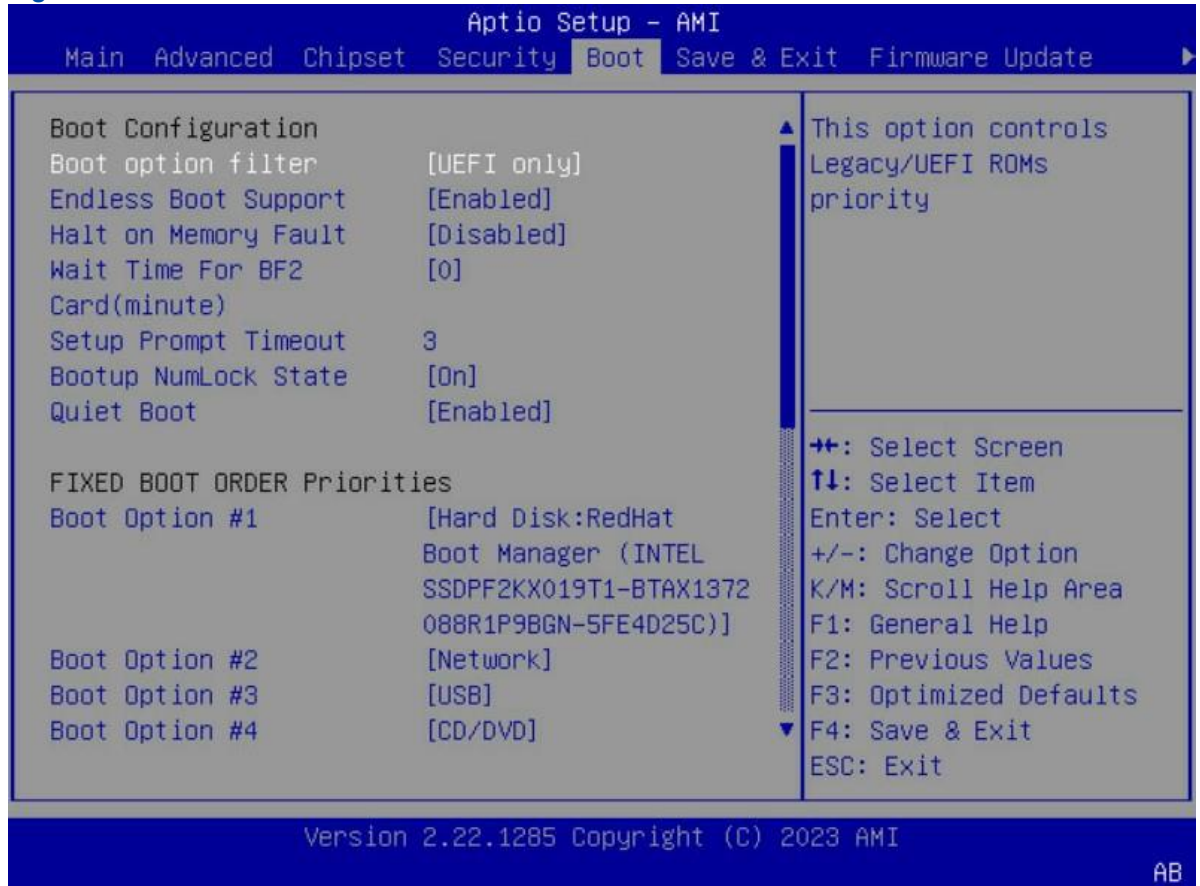
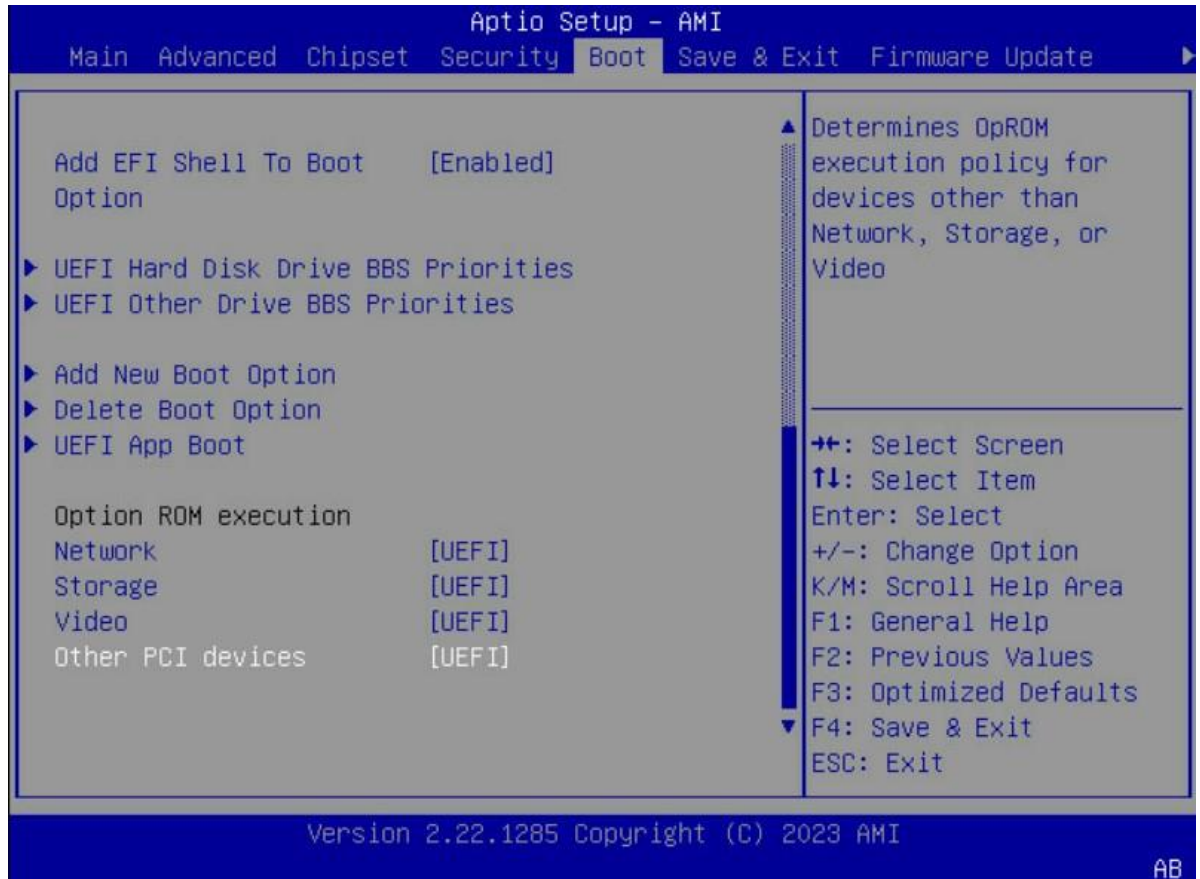


Figure 3-145 Boot Screen—2



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

Table 3-110 Parameter Descriptions for the Boot Screen

Parameter	Description	Default
Boot option filter	Select a boot mode. Options: • UEFI only • Legacy only	UEFI only
Endless Boot Support	Enables or disables the endless boot feature. Options: • Enabled: enables the endless boot feature. • Disabled: disables the endless boot feature.	Enabled
Halt on Memory Fault	Enables or disables halt on a memory fault. Options: • Enabled: enables halt on a memory fault. • Disabled: disables halt on a memory fault.	Enabled

Parameter	Description	Default
Wait Time For BF2 Card(minute)	Select the BF2 card waiting time (in minutes). Options: ● 0 ● 1 ● 2 ● 3 ● 4 ● 5	3
Setup Prompt Timeout	Sets the timeout period in seconds.	3
Bootup NumLock State	Enables or disables NumLock state of keypad. Options: ● On: enables NumLock state of keypad. ● Off: disables NumLock state of keypad.	On
Quiet Boot	Enables or disables the quiet boot feature. Options: ● Enabled: enables the quiet boot feature. ● Disabled: disables the quiet boot feature.	Enabled
Boot Option #1	Press the up/down key to select 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

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: OCP1 Port1: Intel(R) Ethernet Network Adapter E810-C-Q2 for OCP 3.0 (PXE IPv4)
----------------	---	---

Parameter	Description	Default
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
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
Add EFI Shell To Boot Option	This parameter is displayed when Boot option filter is set to UEFI only. Enables or disables the embedded shell. Options: ● Enabled: enables the embedded shell. When this parameter is set to Enabled, EFI Shell is added to the boot option. ● Disabled: disables the embedded shell.	Disabled

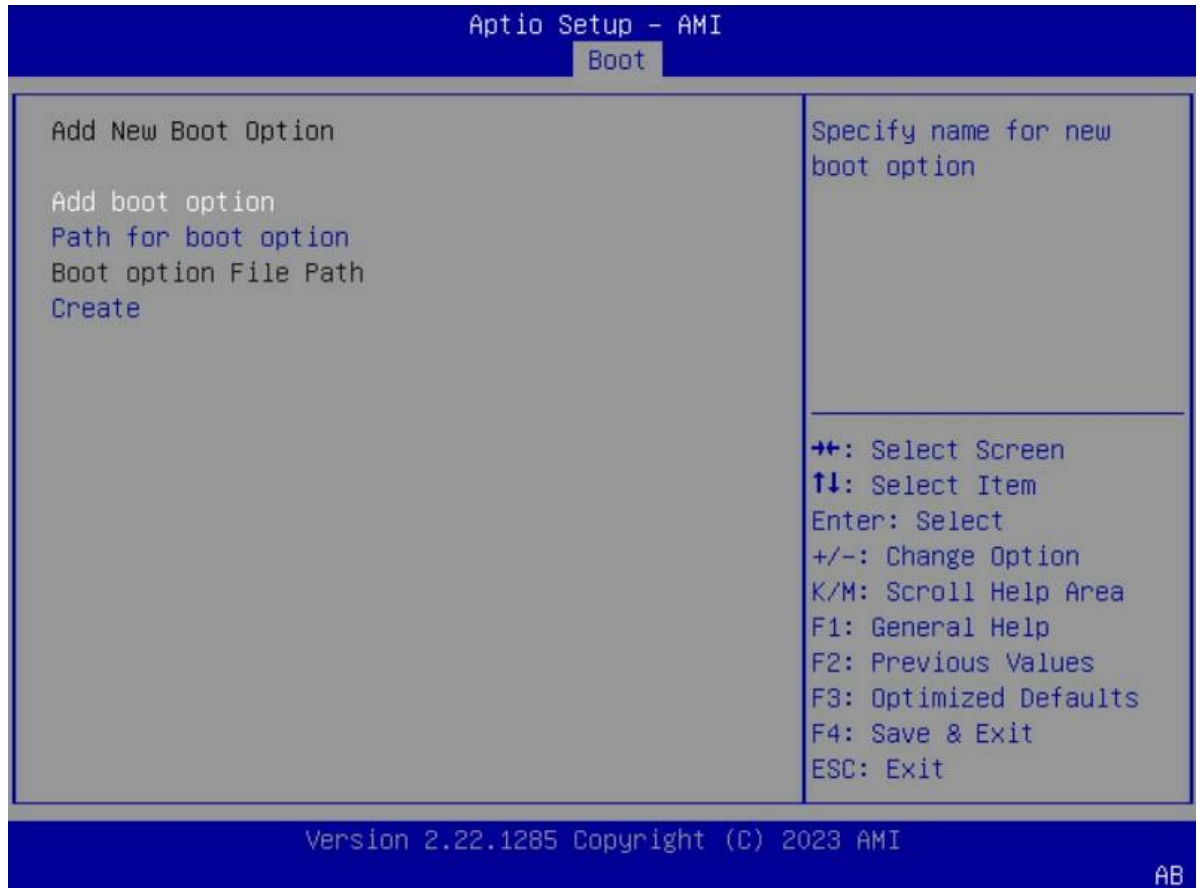
Parameter	Description	Default
UEFI NETWORK Drive BBS Priorities	Specifies the boot priorities of available UEFI drivers.	-
UEFI Other Drive BBS Priorities	Specifies the boot priorities of other available UEFI drivers.	-
Add New Boot Option	Adds a new EFI boot option to the boot order list. For details, refer to 3.5.1 Add New Boot Option.	-
Delete Boot Option	Removes an EFI boot option from the boot order list. For details, refer to 3.5.2 Delete Boot Option.	-
UEFI App Boot	Applies the launch item. For details, refer to 3.5.3 UEFI App Boot.	-

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

3.5.1 Add New Boot Option

[Figure 3-146](#) shows the **Add New Boot Option** screen.

Figure 3-146 Add New Boot Option Screen



For a description of the parameters on the **Add New Boot Option** screen, refer to [Table 3-111](#).

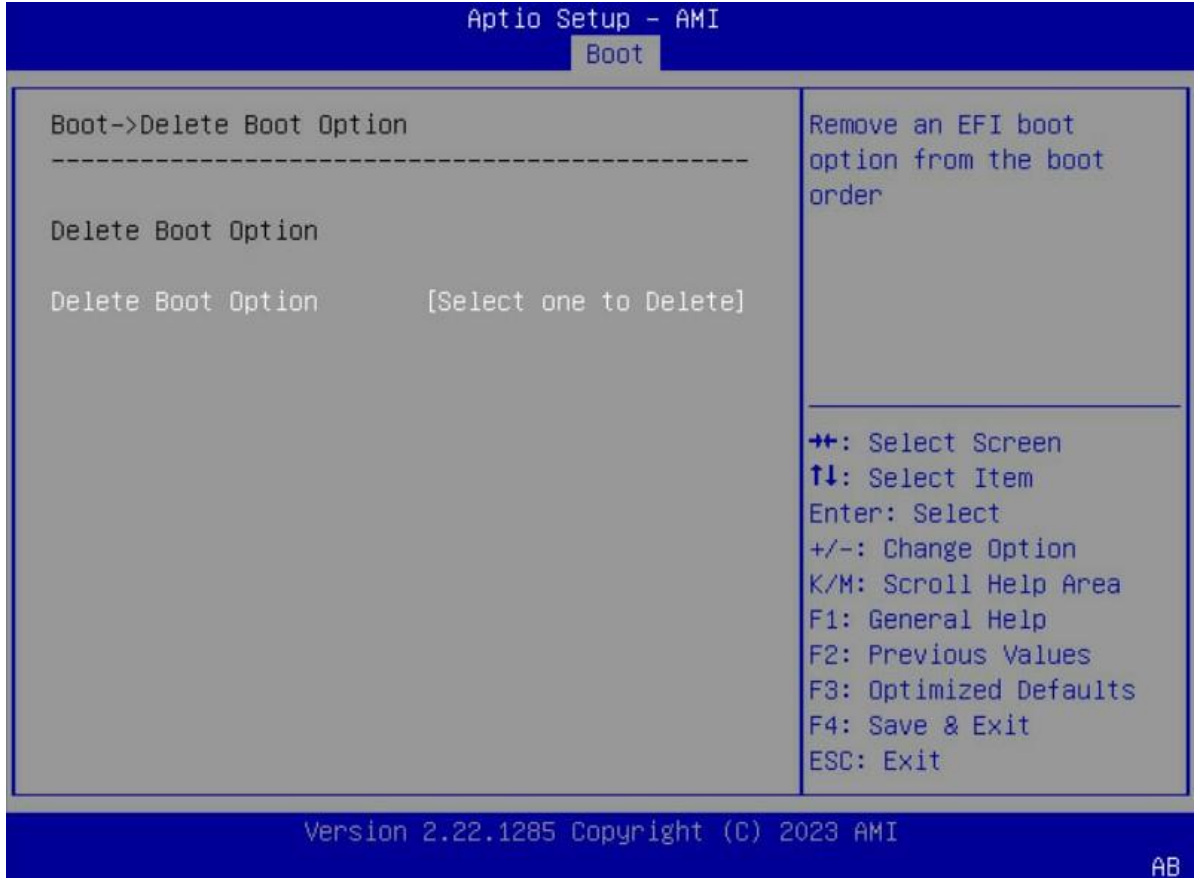
Table 3-111 Parameter Descriptions for the Add New Boot Option Screen

Parameter	Description
Add boot option	Enter a name for the new boot option.
Parameter	Description
Path for boot option	Enter the boot path for the new boot option.
Create	Creates a boot option.

3.5.2 Delete Boot Option

[Figure 3-147](#) shows the **Delete Boot Option** screen.

Figure 3-147 Delete Boot Option Screen



For a description of the parameters on the **Delete Boot Option** screen, refer to [Table 3-112](#).

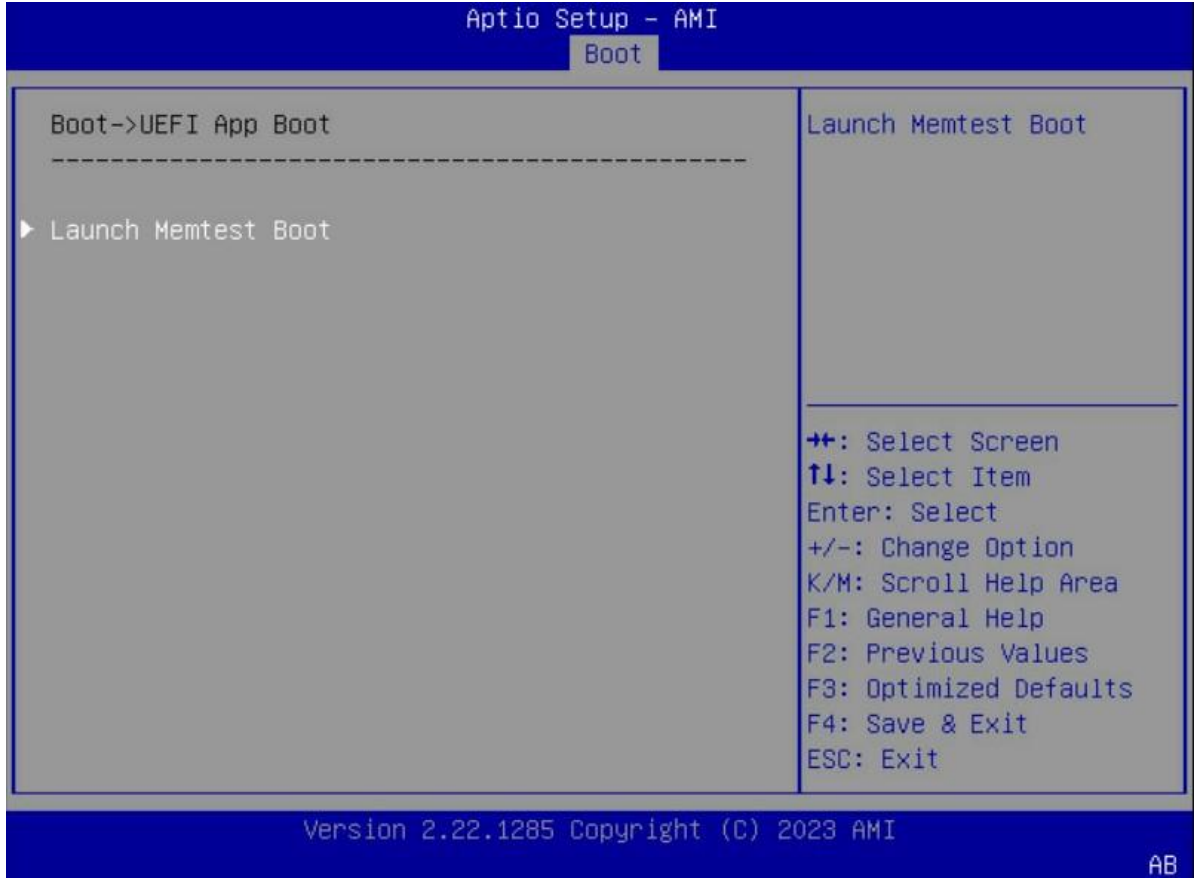
Table 3-112 Parameter Descriptions for the Delete Boot Option Screen

Parameter	Description
Delete Boot Option	Select the boot option that you want to delete.

3.5.3 UEFI App Boot

[Figure 3-148](#) shows the **UEFI App Boot** screen.

Figure 3-148 UEFI App Boot Screen



For a description of the parameters on the **UEFI App Boot** screen, refer to [Table 3-113](#).

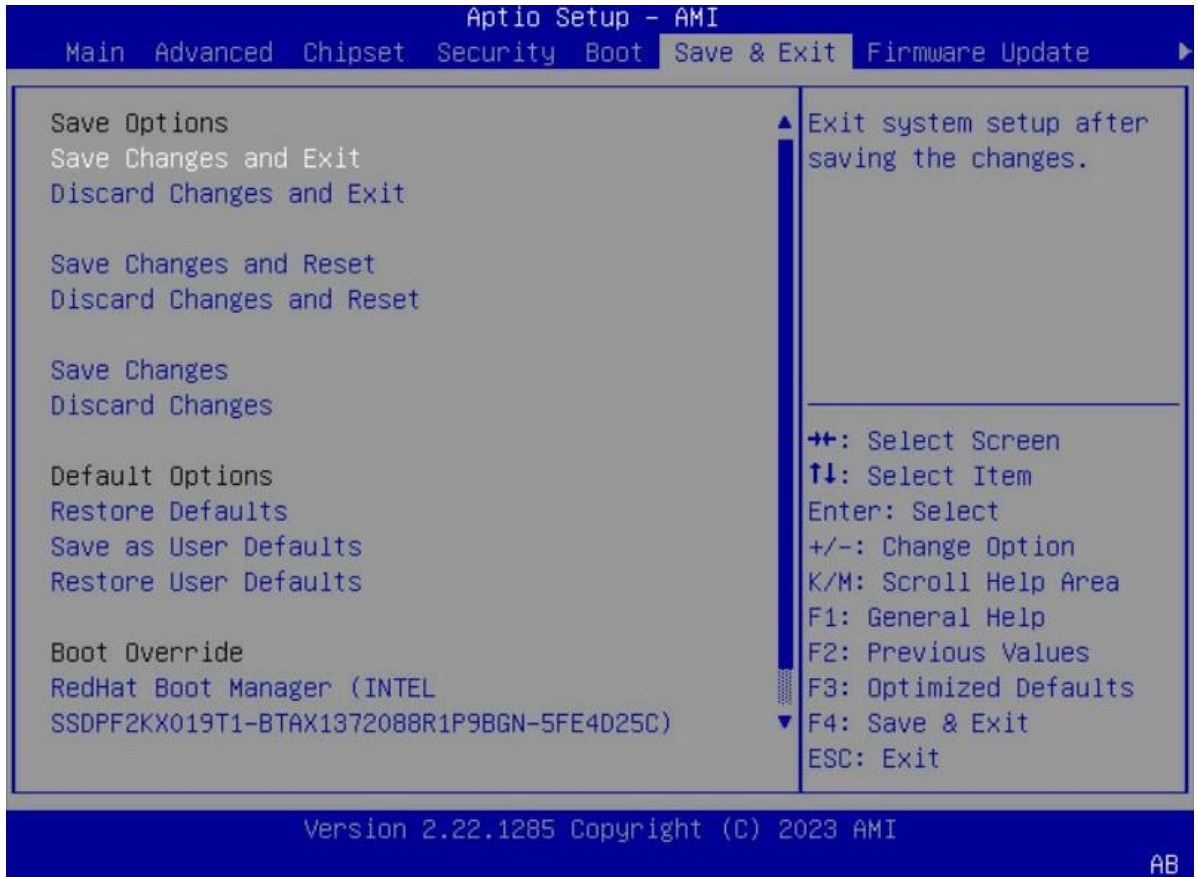
Table 3-113 Parameter Descriptions for the UEFI App Boot Screen

Parameter	Description
Launch Memtest Boot	Enables or disables the memory test boot feature.

3.6 Save & Exit

[Figure 3-149](#) shows the **Save & Exit** screen.

Figure 3-149 Save & Exit Screen



For a description of the parameters on the **Save & Exit** screen, refer to [Table 3-114](#).

Table 3-114 Parameter Descriptions for the Save & Exit Screen

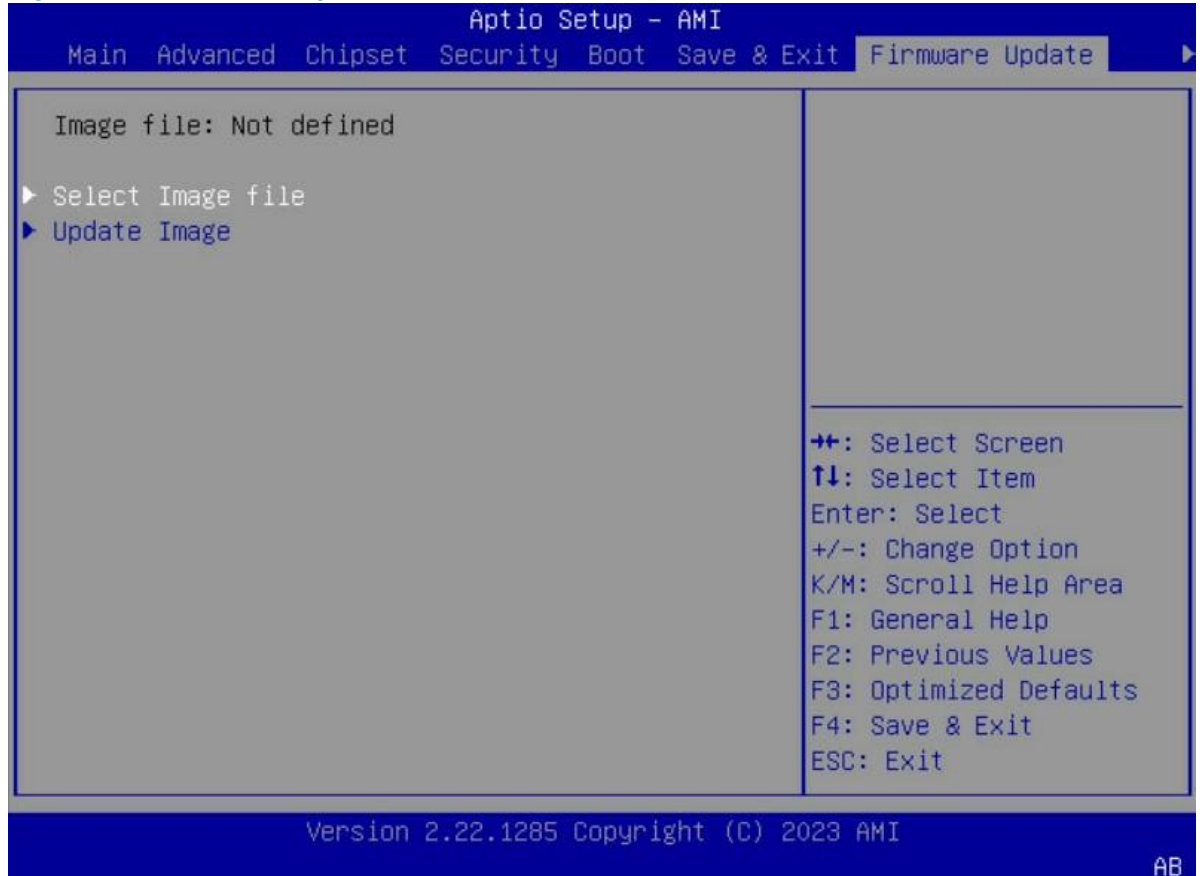
Parameter	Description
Save Changed and Exit	Saves the changes and exits from the BIOS.
Discard Changed and Exit	Exits the BIOS without saving any changes.
Save Changes and Reset	Saves the changes and then restarts the system.
Discard Changes and Reset	Restarts the system without saving any changes.
Save 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.

Boot Override	Overrides startup entries.
---------------	----------------------------

3.7 Firmware Update

Figure 3-150 shows the **Firmware Update** screen.

Figure 3-150 Firmware Update Screen



For a description of the parameters on the **Firmware Update** screen, refer to [Table 3-115](#).

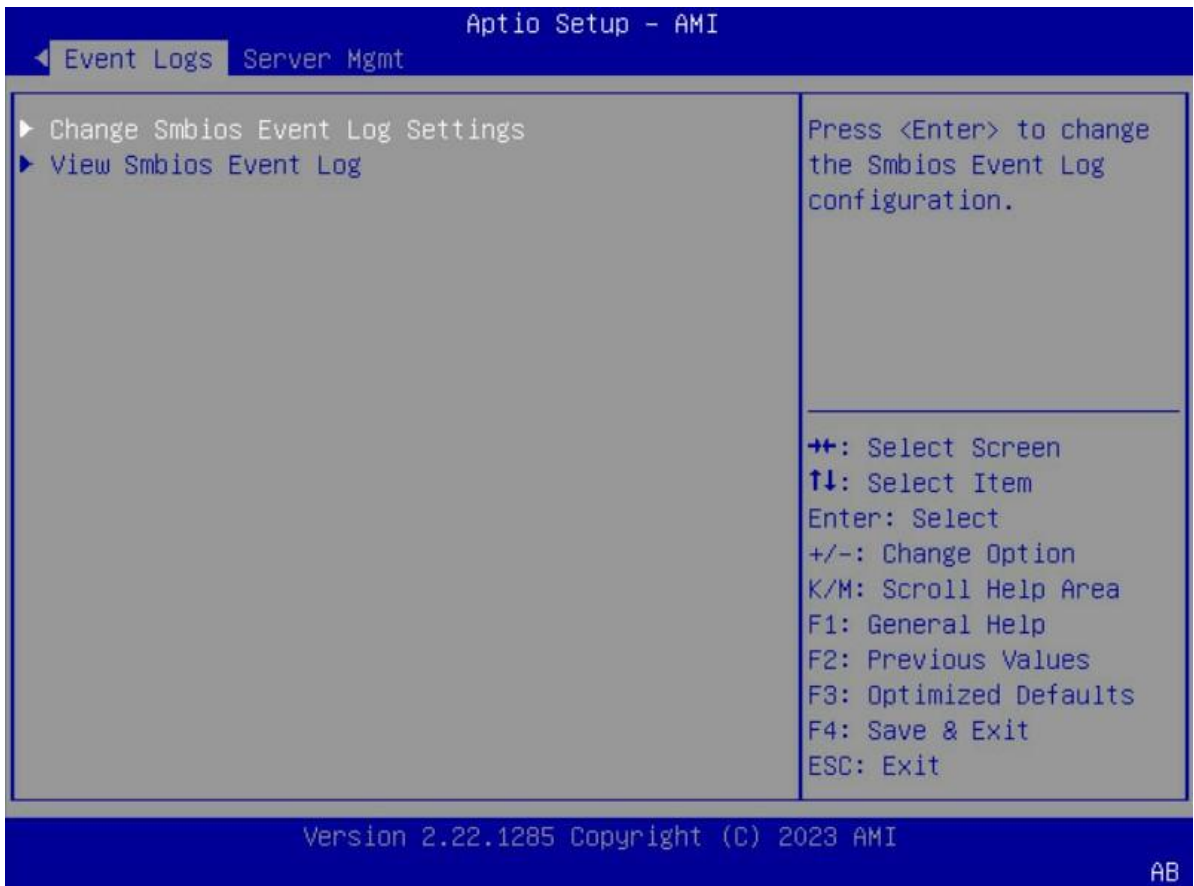
Table 3-115 Parameter Descriptions for the Firmware Update Screen

Parameter	Description	Setting Example
Image file	Image file.	Not defined
Select Image file	Select an image file.	-
Update Image	Updates the image file.	-

3.8 Event Logs

Figure 3-151 shows the **Event Logs** screen.

Figure 3-151 Event Logs Screen



For a description of the parameters on the **Event Logs** screen, refer to [Table 3-116](#).

Table 3-116 Parameter Descriptions for the Event Logs Screen

Parameter	Description
Change Smbios Event Log Settings	Modifies Smbios event log parameters. For details, refer to 3.8.1 Change Smbios Event Log Settings .
View Smbios Event Log	Displays Smbios event log parameters. For details, refer to 3.8.2 View Smbios Event Log .

3.8.1 Change Smbios Event Log Settings

[Figure 3-152](#) through [Figure 3-153](#) show the **Change Smbios Event Log Settings** screen.

Figure 3-152 Change Smbios Event Log Settings Screen—1

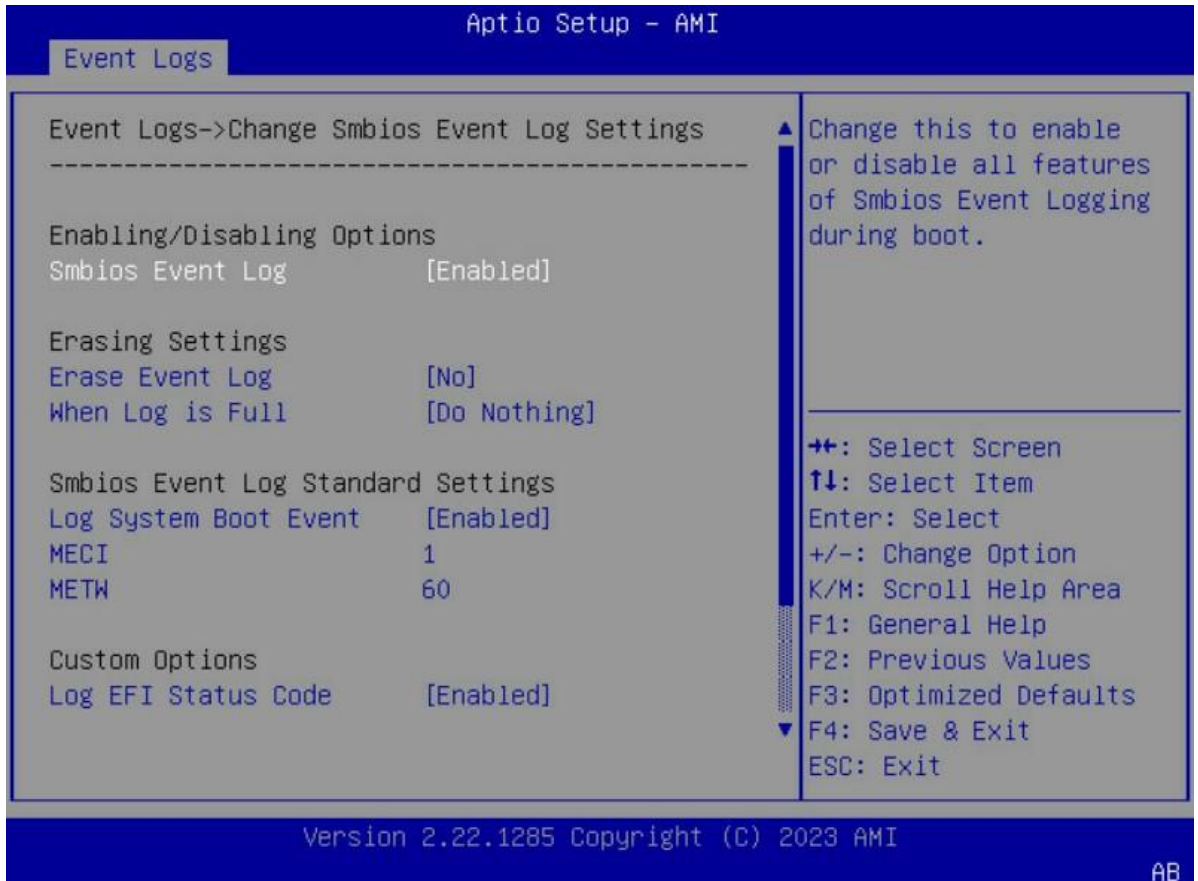
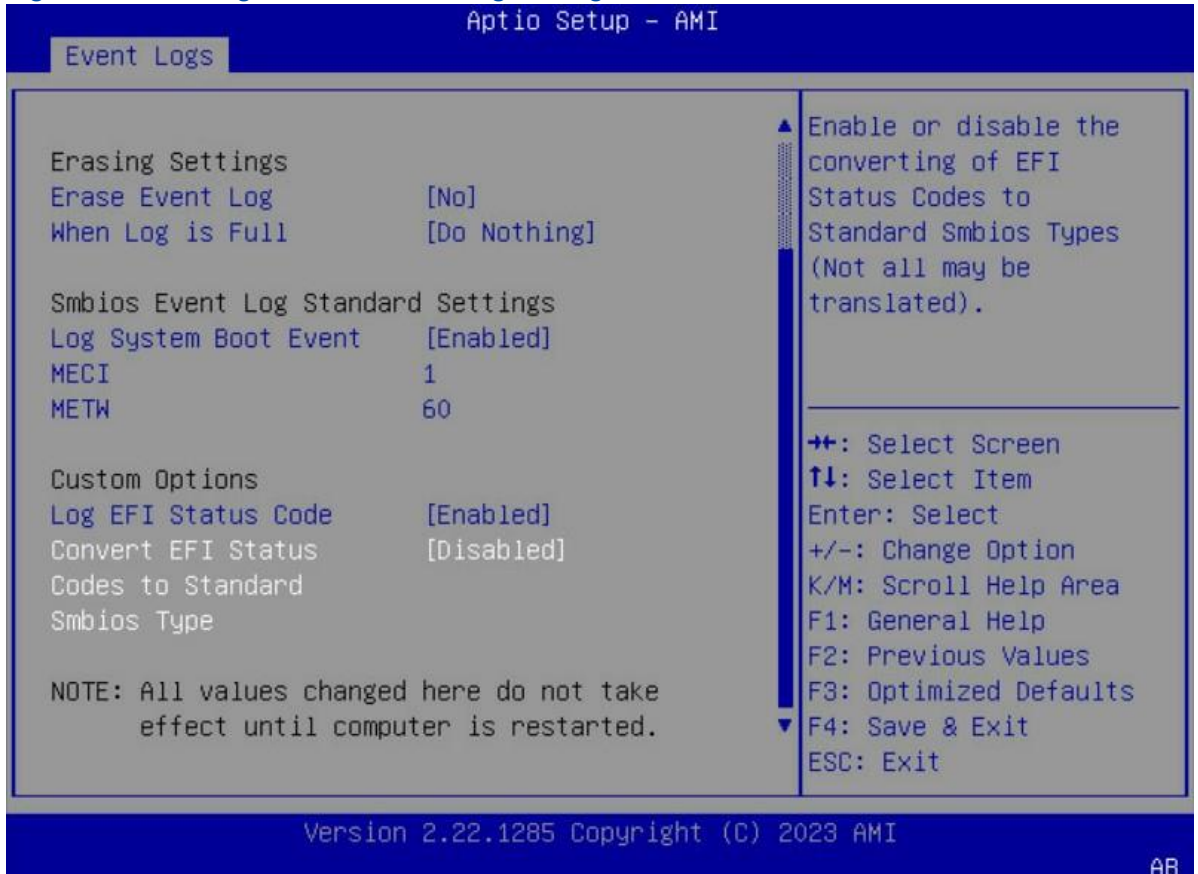


Figure 3-153 Change Smbios Event Log Settings Screen—2



For a description of the parameters on the **Change Smbios Event Log Settings** screen, refer to [Table 3-117](#).

Table 3-117 Parameter Descriptions for the Change Smbios Event Log Settings Screen

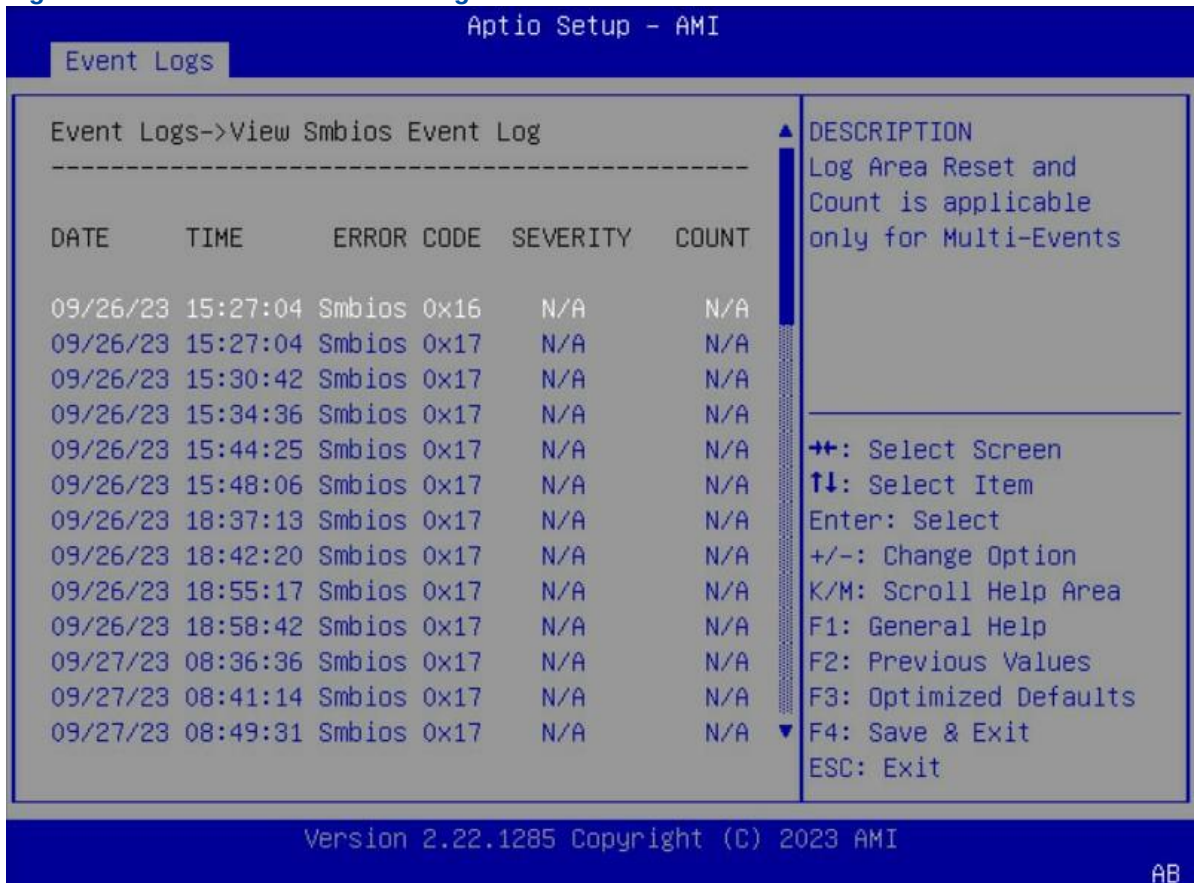
Parameter	Description	Default
Smbios Event Log	Enables or disables the Smbios event logging feature. Options: ● Enabled: enables the Smbios event logging feature. ● Disabled: disables the Smbios event logging feature.	Enabled
Erase Event Log	Select whether to clear event logs. Options: ● No ● Yes,Next reset ● Yes,Every reset	No
When Log if Full	Select the action to be taken when the Smbios log threshold is reached.	Do Nothing
Parameter	Description	Default
	Options: ● Do Nothing ● Erase Immediately	
Log System Boot Event	Enables or disables the system boot event logging feature. Options: ● Enabled: enables the system boot event logging feature. ● Disabled: disables the system boot event logging feature.	Enabled
MECI	Sets the MECI. Range: 1–255.	1
METW	Sets the METW. Range: 0–99. Unit: minutes.	60

Log EFI Status Code	Enables or disables the EFI status code logging feature. Options: - Enabled: enables the EFI status code logging feature. - Disabled: disables the EFI status code logging feature.	Enabled
Convert EFI Status Codes to Standard Smbios Type	Enables or disables the conversion from EFI status codes to standard Smbios-type codes. Options: - Enabled: enables the conversion. - Disabled: disables the conversion.	Disabled

3.8.2 View Smbios Event Log

Figure 3-154 shows the **View Smbios Event Log** screen.

Figure 3-154 View Smbios Event Log Screen



For a description of operations on the **View Smbios Event Log** screen, refer to [Table 3-118](#).

Table 3-118 Parameter Descriptions for the View Smbios Event Log Screen

Parameter	Description
-----------	-------------

DATE	Displays the date information.
TIME	Displays the time information.
ERROR CODE	Displays the error code information.
SEVERITY	Displays the severity level.
COUNT	Displays the count information.

3.9 Server Mgmt

Figure 3-155 through Figure 3-156 show the **Server Mgmt** screen.

Figure 3-155 Server Mgmt Screen—1

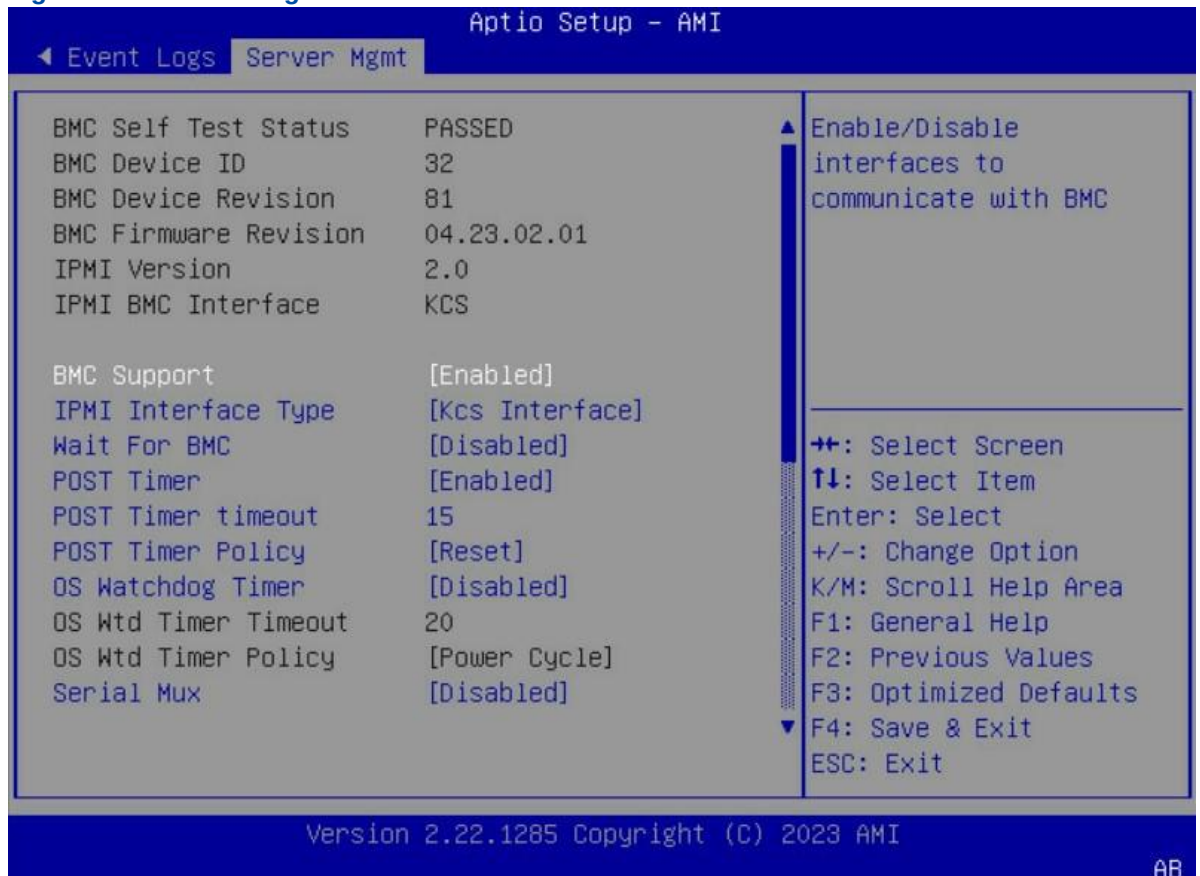
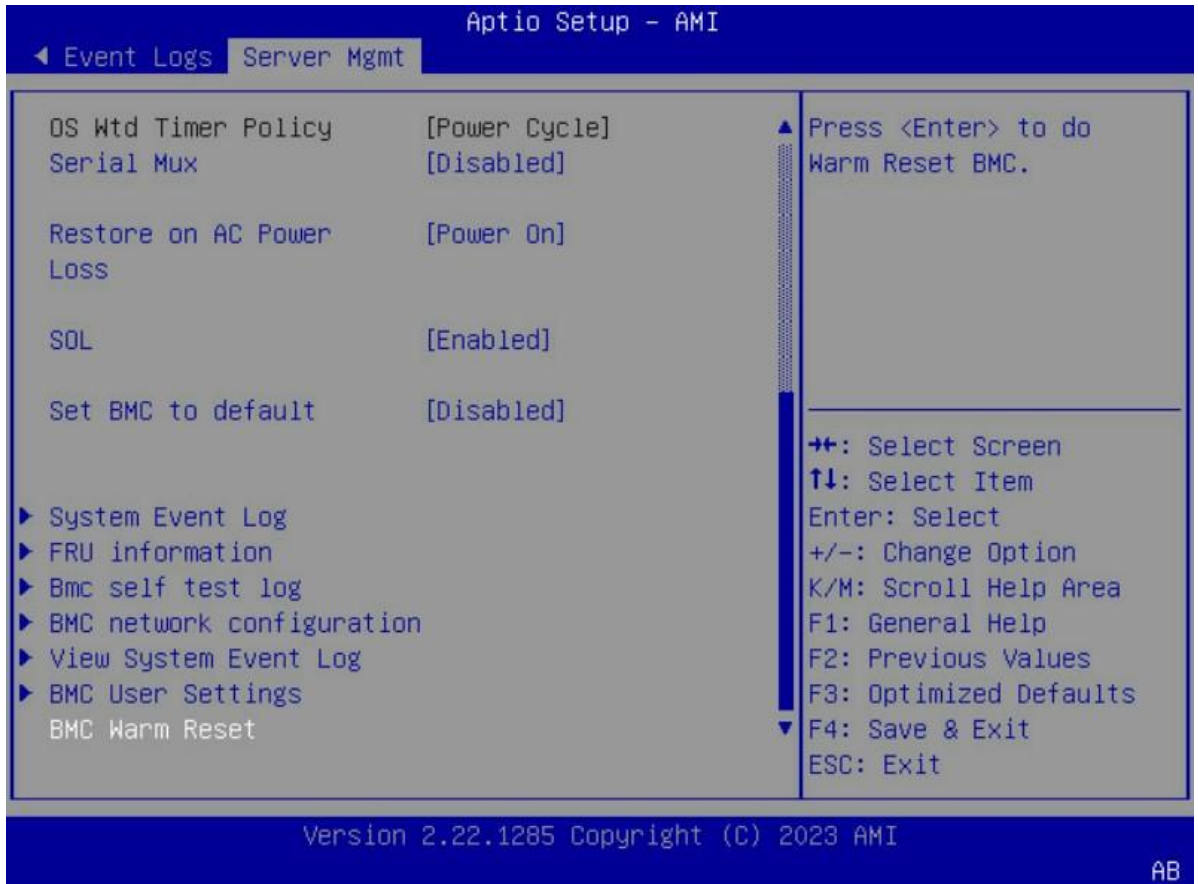


Figure 3-156 Server Mgmt Screen—2



For a description of the parameters on the **Server Mgmt** screen, refer to [Table 3-119](#).

Table 3-119 Parameter Descriptions for the Server Mgmt Screen

Parameter	Description	Default
BMC Self Test Status	Displays the BMC self-test status.	PASSED
BMC Device ID	Displays the ID of the BMC device.	32
BMC Device Revision	Displays the version of the BMC device.	81
BMC Firmware Revision	Displays the version of the BMC firmware.	04.23.01.01P2
IPMI Version	Displays the IPMI version.	2.0
IPMI BMC Interface	Displays the IPMI BMC interface type.	KCS
BMC Support	Enables or disables the BMC interface. Options: • Enabled: enables the BMC interface. • Disabled: disables the BMC interface.	Enabled

IPMI Interface Type	Sets the IPMI interface type. Options: ● Kcs Interface	Kcs Interface
---------------------	--	---------------

Parameter	Description	Default
	● Bt Interface ● Ipmb Interface	
Wait For BMC	Enables or disables timeout events for waiting for BMC. Options: ● Enabled: enables timeout events for waiting for BMC. ● Disabled: disables timeout events for waiting for BMC.	Disabled
POST Timer	Enables or disables the POST watchdog feature. Options: ● Enabled: enables the POST watchdog feature. ● Disabled: disables the POST watchdog feature.	Enabled
POST Timer timeout	Sets the timeout period of the OS watchdog timer. Range: 3–30, unit: minutes.	15
POST Timer Policy	Sets how the system responds when the OS watchdog timer expires. Options: ● Do Nothing ● Reset ● Power Down ● Power Cycle	Power Cycle

OS Watchdog Timer	Enables or disables the operating system's watchdog timer. Options: ● Enabled: enables the operating system watchdog timer. ● Disabled: disables the operating system watchdog timer. If this parameter is set to Disabled, the POST Timer timeout and POST Timer Policy parameters cannot be configured.	Disabled
OS Wtd Timer Timeout	Enter the timeout period of the operating system watchdog timer. Range: 3–30, unit: minutes.	20
OS Wtd Timer Policy	Sets how the system responds when the operating system watchdog timer expires.	Power Cycle

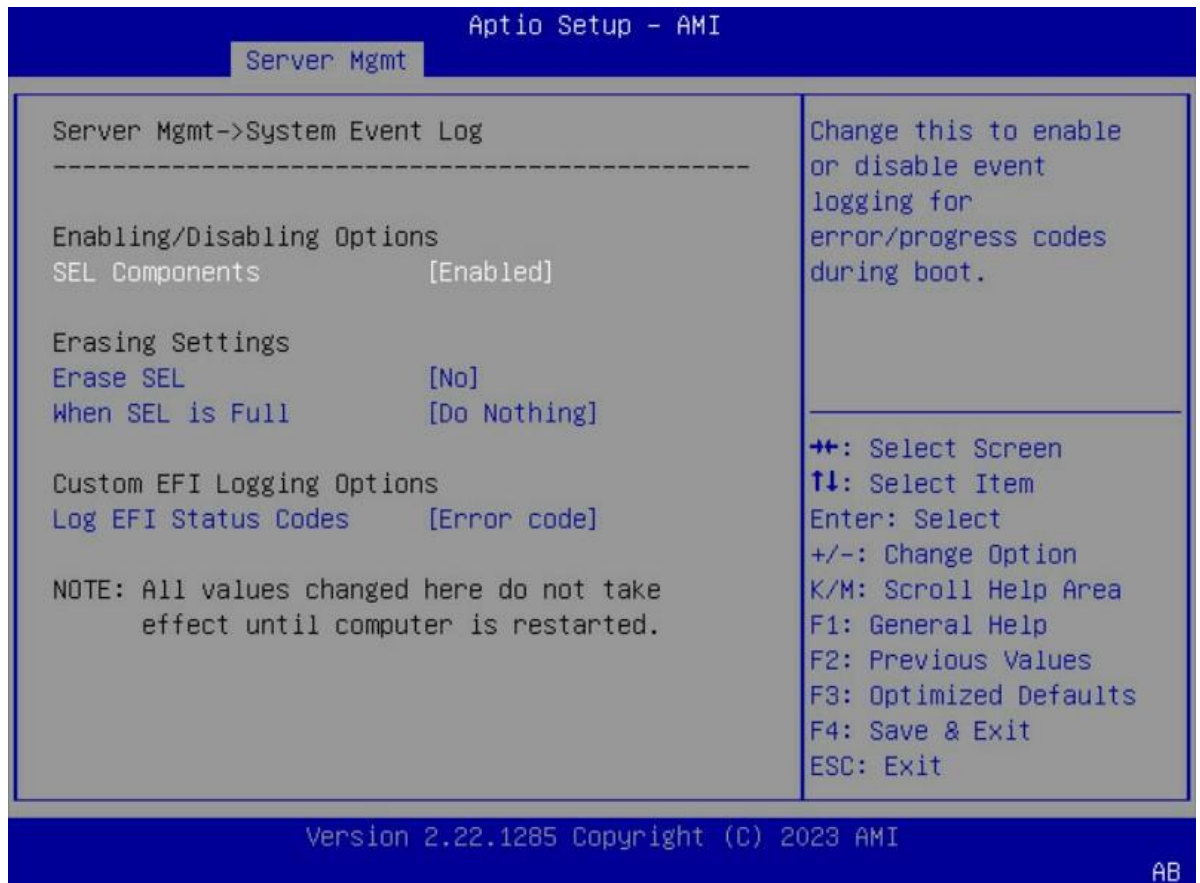
Parameter	Description	Default
	Options: ● Do Nothing ● Reset ● Power Down ● Power Cycle	
Serial Mux	Enables or disables the serial multi-line multiplexing feature. Options: ● Enabled: enables the serial multi-line multiplexing feature. ● Disabled: disables the serial multi-line multiplexing feature.	Enabled
Restore on AC power Loss	Select the startup mode after AC power-off. Options: ● Power Off ● Last State ● Power On	Power Off

SOL	Enables or disables the BMC SOL control feature. - Enabled: enables the BMC SOL control feature. - Disabled: disables the BMC SOL control feature.	Enabled
Set BMC to default	Enables or disables BMC default settings. Options: - Enabled: enables BMC default settings. - Disabled: disables BMC default settings.	Disabled
System Event Log	Sets the system event log parameters. For details, refer to 3.9.1 System Event Log .	-
View FRU information	Views FRU information. For details, refer to 3.9.2 FRU Information .	-
BMC self test log	Sets the BMC self-test log parameters. For details, refer to 3.9.3 BMB Self Test Log .	-
BMC network configuration	Sets BMC network parameters. For details, refer to 3.9.4 BMC network configuration .	-
View System Event Log	Displays system event logs.	-
BMC User Settings	Sets BMC user parameters.	-
Parameter	Description	Default
	For details, refer to 3.9.5 BMC User Settings .	
BMC Warm Reset	Performs a warm reset on the BMC.	-

3.9.1 System Event Log

[Figure 3-157](#) shows the **System Event Log** screen.

Figure 3-157 System Event Log Screen



For a description of operations on the **System Event Log** screen, refer to [Table 3-120](#).

Table 3-120 Parameter Descriptions for the System Event Log Screen

Parameter	Description	Default
SEL Components	Enables or disables error/progress code event logging during startup. Options: - Enabled: enables error/progress code event logging during startup. - Disabled: disables error/progress code event logging during startup.	Enabled
Erase SEL	Select whether to clear SEL.	No
Parameter	Description	Default
	Options: - No - Yes, On next reset - Yes, On every reset	

When SEL is Full	Select the action when SEL reaches maximum capacity. Options: • Do Nothing • Erase Immediately • Delete Oldest Record	Do Nothing
Log EFI Status Codes	Select the status code logging method. Options: • Disabled • Both • Error code • Progress code	Error code

3.9.2 FRU Information

[Figure 3-158](#) through [Figure 3-159](#) show the **FRU Information** screen.

Figure 3-158 FRU Information Screen—1

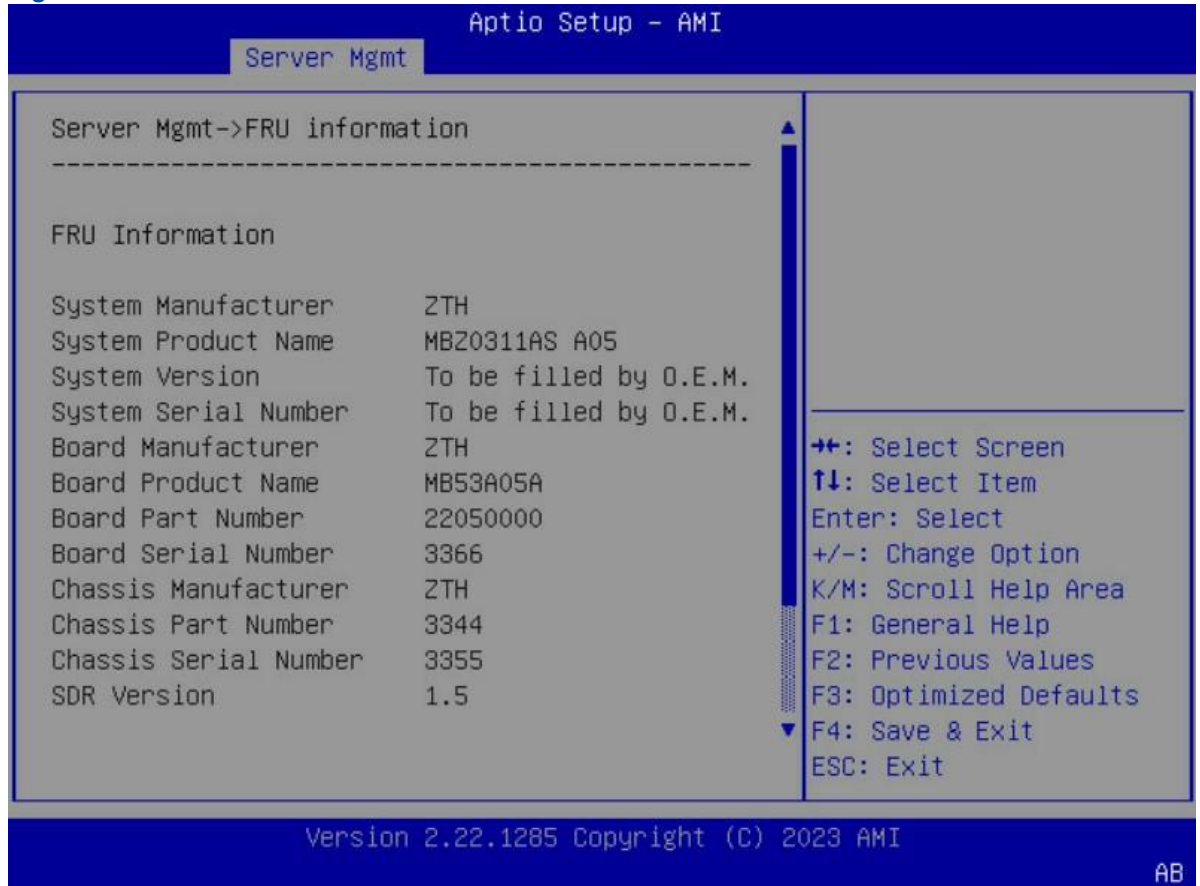
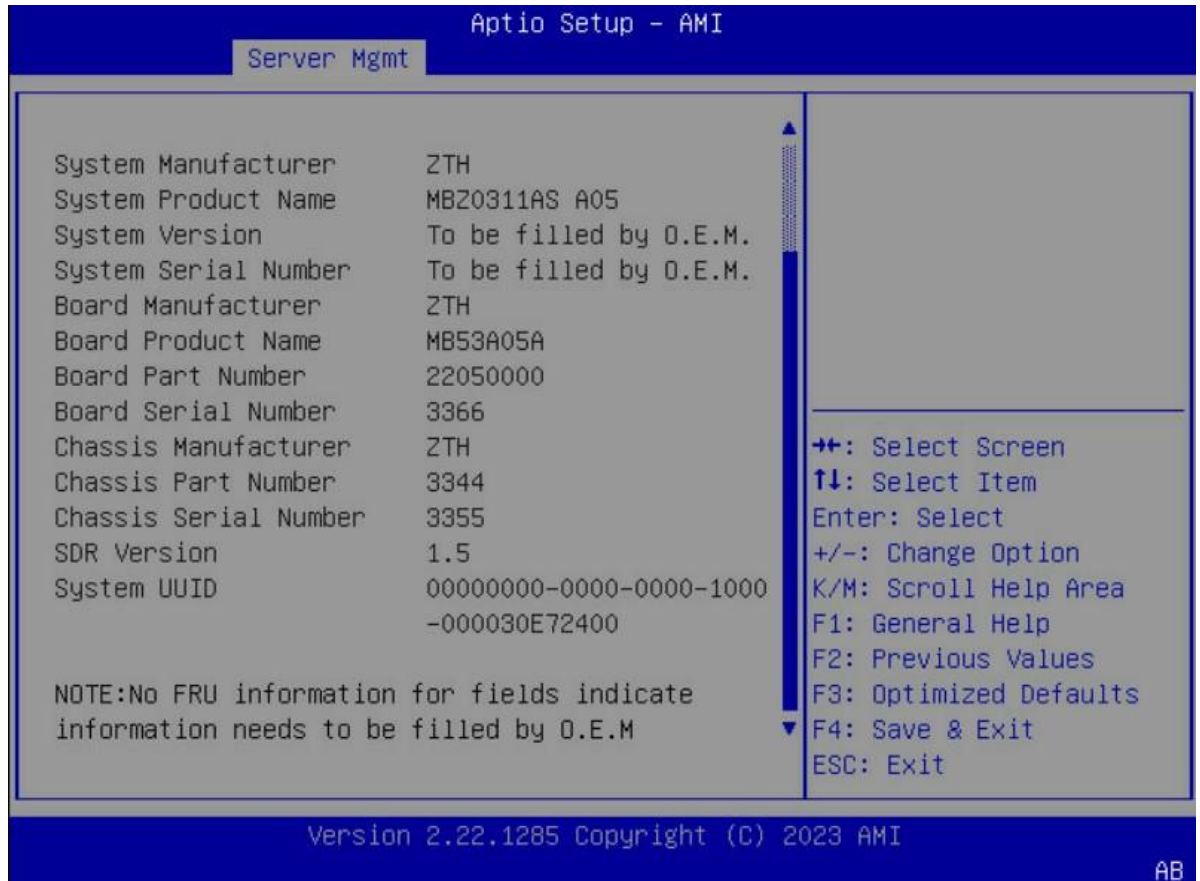


Figure 3-159 FRU Information Screen—2



For a description of the parameters on the **FRU Information** screen, refer to [Table 3-121](#).

Table 3-121 Parameter Descriptions for the FRU Information Screen

Parameter	Description	Setting Example
System Manufacturer	Displays the system manufacturer.	To be filled by O.E.M
System Product Name	Displays the system product name.	To be filled by O.E.M
System Version	Displays the system version.	To be filled by O.E.M
System Serial Number	Displays the serial number of the system.	To be filled by O.E.M
Board Manufacturer	Displays the motherboard manufacturer.	To be filled by O.E.M
Board Product Name	Displays the motherboard product name.	To be filled by O.E.M
Board Part Number	Displays the part number of the motherboard.	To be filled by O.E.M

Board Serial Number	Displays the serial number of the mainboard.	To be filled by O.E.M
Parameter	Description	Setting Example
Chassis Manufacturer	Displays the chassis manufacturer.	To be filled by O.E.M
Chassis Part Number	Displays the part number of the chassis.	To be filled by O.E.M
Chassis Serial Number	Displays the serial number of the chassis.	To be filled by O.E.M
SDR Version	Displays the SDR version.	1.5
System UUID	Displays the system UUID .	00000000 - 0000 - 0000 - 1000 - 000030E72400

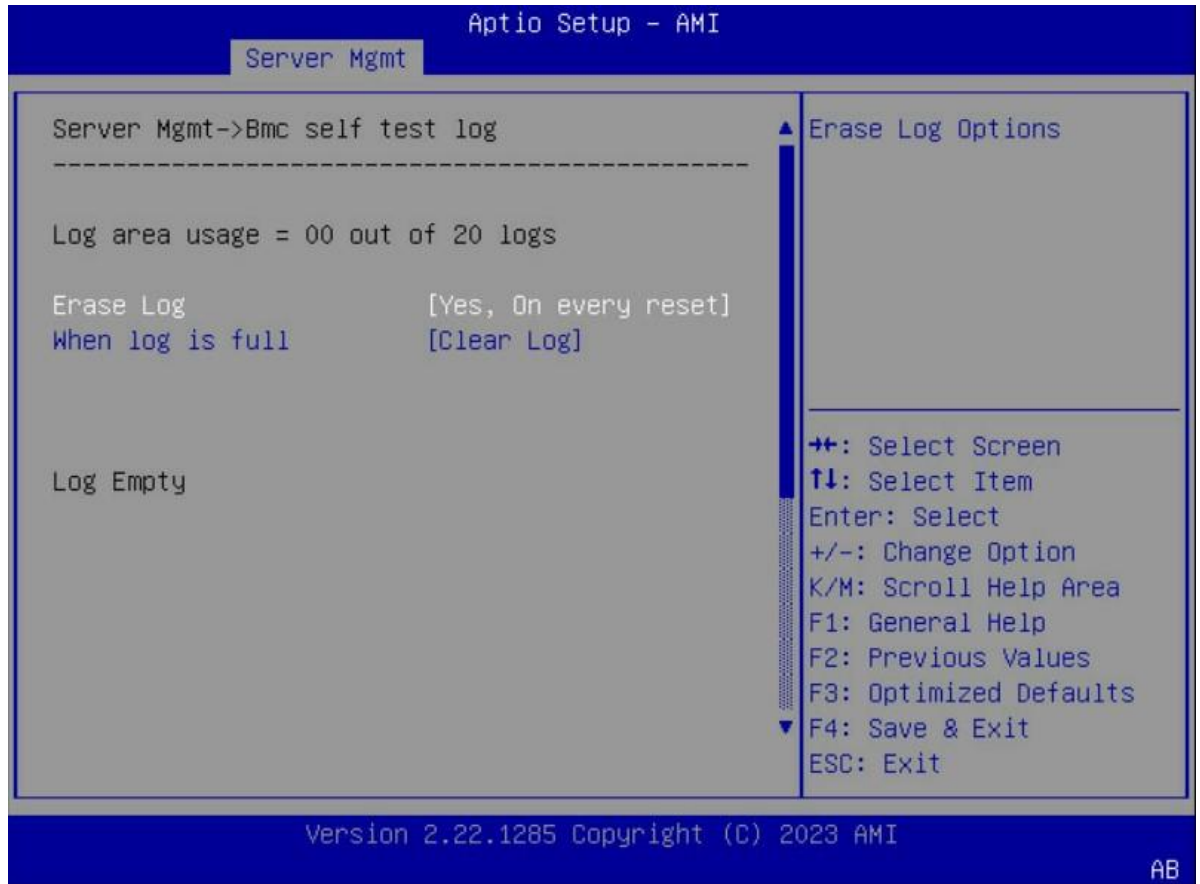
**Note**

If **To be filled by O.E.M** is displayed in the field, it indicates that there is no FRU information, which needs to be specified by the **OEM**.

3.9.3 BMB Self Test Log

Figure 3-160 shows the **Bmc self test log** screen.

Figure 3-160 BMB Self Test Log Screen



For a description of the parameters on the **Bmc self test log** screen, refer to [Table 3-122](#).

Table 3-122 Parameter Descriptions for the Bmc Self Test Log Screen

Parameter	Description	Default
Log area usage	Displays the log area usage.	00 out of 20 logs
Erase Log	Select a log clearance mode. Options: • Yes, On every reset • No	Yes, On every reset
When log if full	Select the operation performed after the maximum log capacity is reached. Options: • Clear Log • Do not log any more	Clear Log

3.9.4 BMC network configuration

[Figure 3-161](#) through [Figure 3-164](#) show the **BMC network configuration** screen.

Figure 3-161 BMC Network Configuration Screen—1

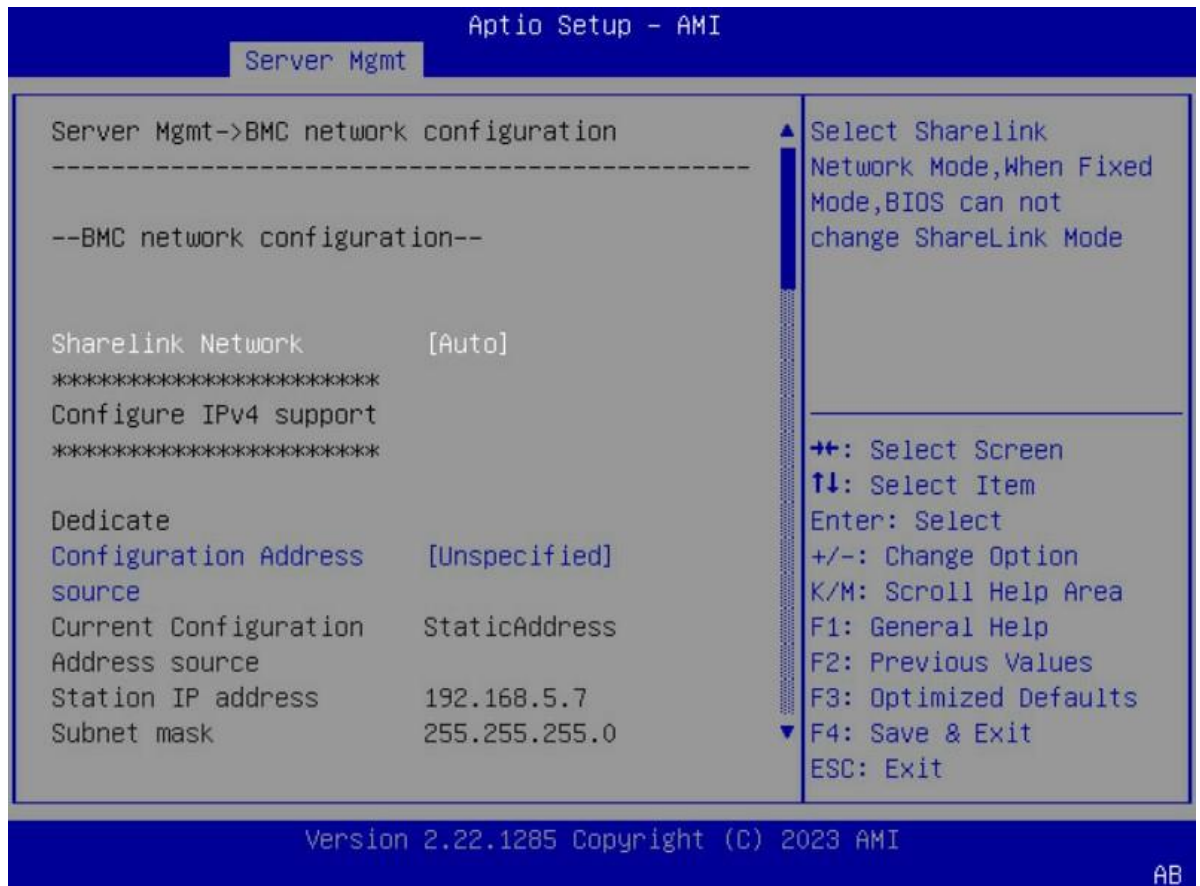


Figure 3-162 BMC Network Configuration Screen—2

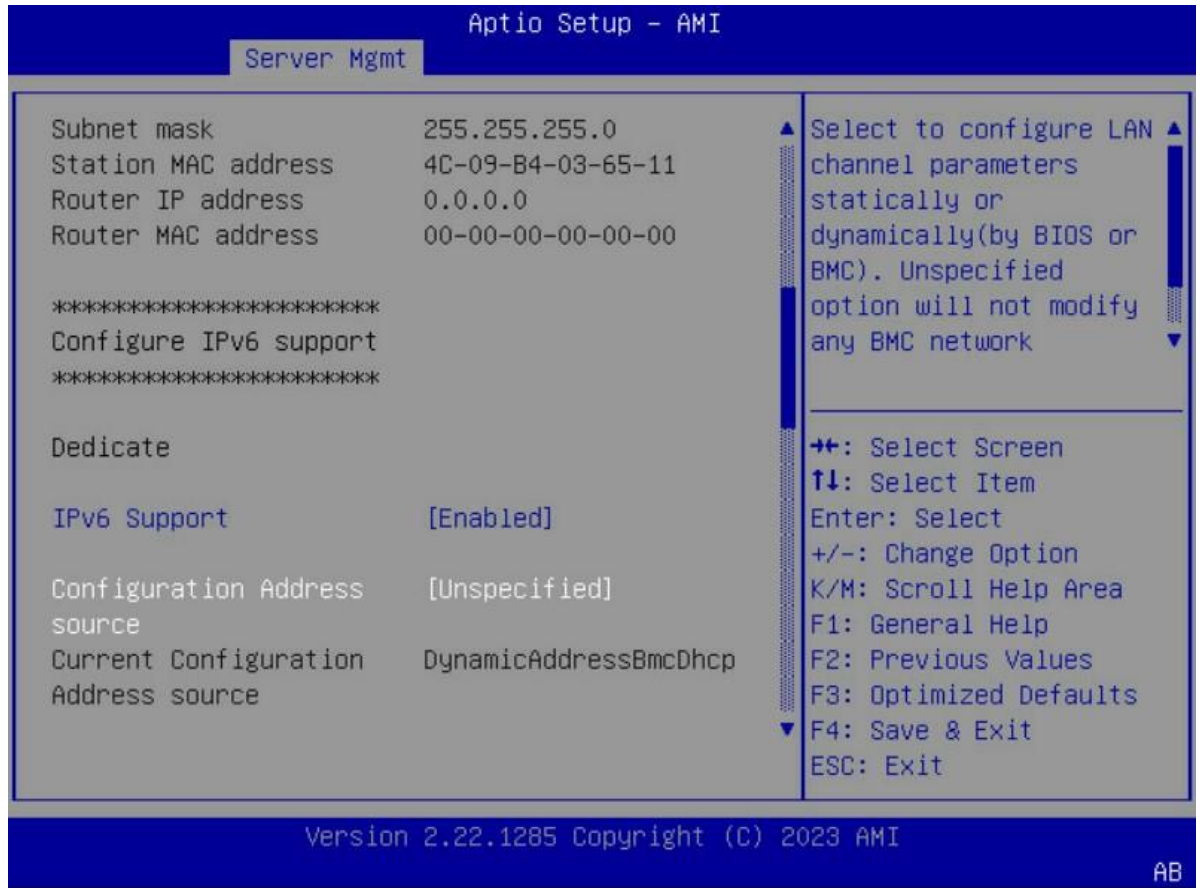


Figure 3-163 BMC Network Configuration Screen—3

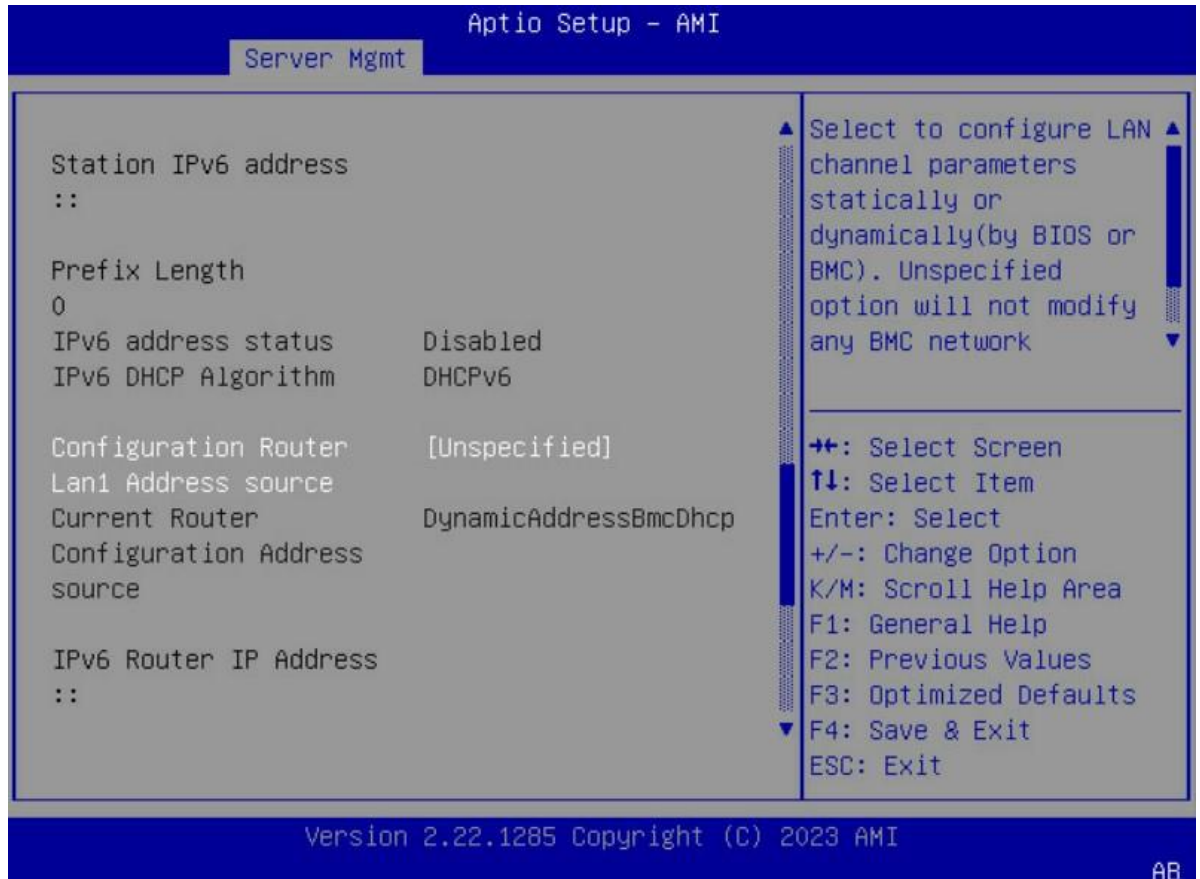
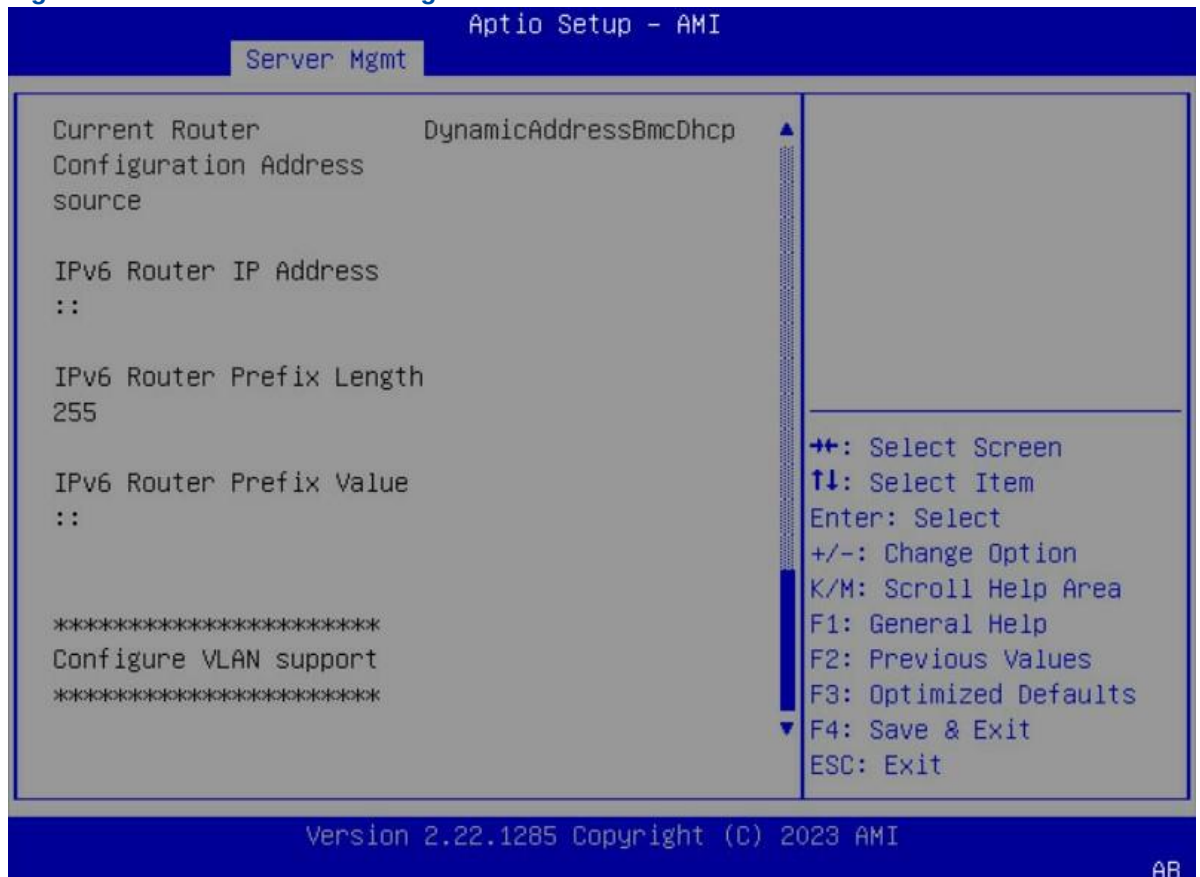


Figure 3-164 BMC Network Configuration Screen—4



For a description of the parameters on the **BMC network configuration** screen, refer to [Table 3-123](#).

Table 3-123 Parameter Descriptions for the BMC Network Screen

Parameter	Description	Default
Sharelink Network	Enables or disables the shared network port feature. Options: • Auto. • Enable: enables the shared network port feature. • Disabled: disables the shared network port feature.	Disabled
Configuration Address source	Sets the address type of the dedicated network interface of the IPv4 network. Options: • Unspecified • Static • DynamicBmcDhcp • DynamicBmcNonDhcp	Unspecified

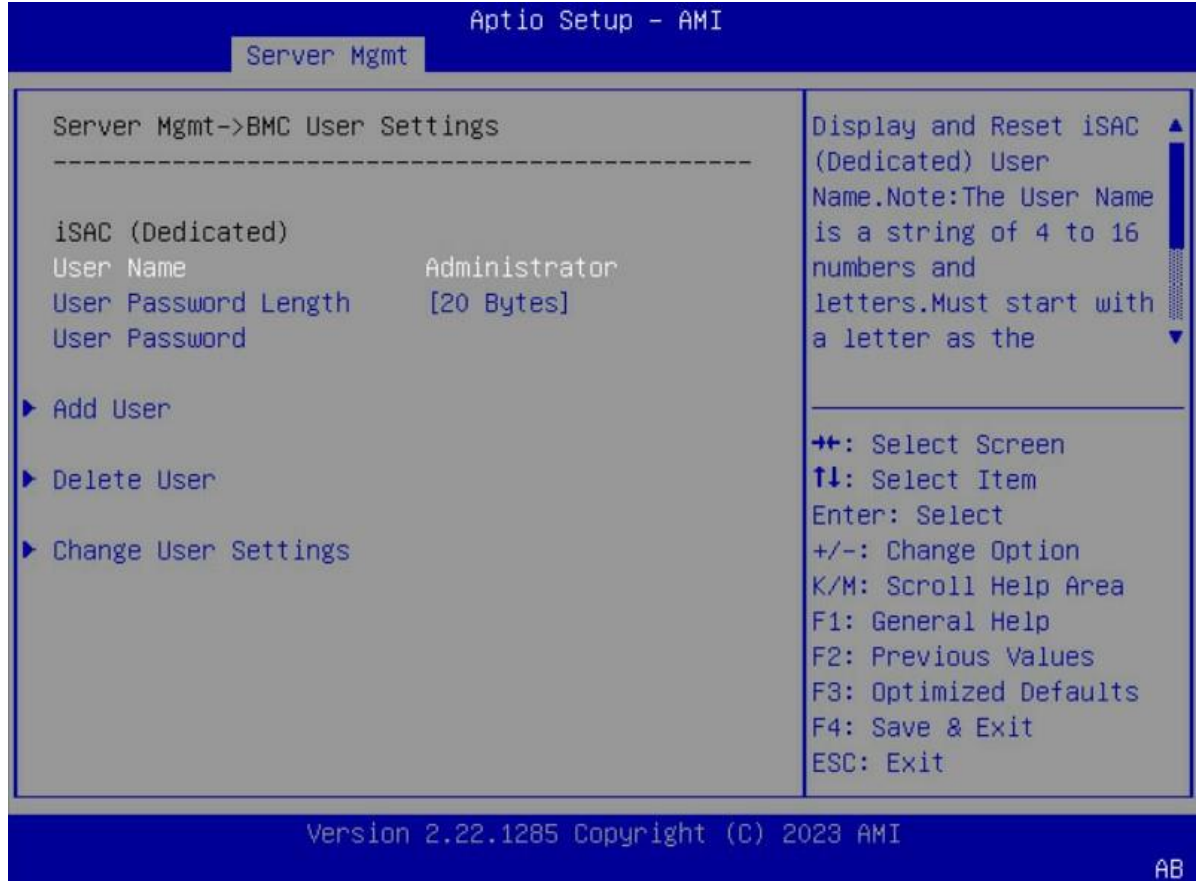
Parameter	Description	Default
Current Configuration Address source	Displays the current address type of the dedicated network port of the IPv4 network.	StaticAddress
Station IP address	Displays the IP address of the dedicated network port of the IPv4 network.	192.168.5.143
Subnet mask	Displays the subnet mask of the dedicated network port of the IPv4 network.	255.255.255.0
Station MAC address	Enter the MAC address of the dedicated network port of the IPv4 network.	74-4A-B1-C7-11-34
Router IP address	IP address of the gateway of the dedicated network port of the IPv4 network.	0.0.0.0
Router MAC address	MAC address of the gateway of the dedicated network port of the IPv4 network.	00-00-00-00-00-00

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.	Enable
Configuration Address source	Sets the type of address of the dedicated network interface of the the IPv6 network. Options: - Unspecified - Static - DynamicBmcDhcp - DynamicBmcNonDhcp	Unspecified
Current Configuration Address source	Displays the type of address of the dedicated network interface of the the IPv6 network.	DynamicAddressBmcDhcp
Station IPv6 address	Displays the IPv6 address of the interface.	-
Prefix Length	Displays the prefix length of the dedicated network interface of the the IPv6 network.	0
IPv6 address status	Displays the IPv6 address status.	Disabled
IPv6 DHCP Algorithm	Displays IPv6 DHCP algorithm information.	DHCPv6
Configuration Router Lan1 Address source	Sets the gateway LAN1 address type. Options: - Unspecified - Static	Unspecified
Parameter	Description	Default
	- DynamicBmcDhcp - DynamicBmcNonDhcp	
Current Router Configuration Address source	Displays the gateway LAN1 address type.	DynamicAddressBmcDhcp
IPv6 Router IP Address	Displays the IPv6 gateway IP address.	-
IPv6 Router Prefix Length	Displays the prefix length of the IPv6 gateway IP address.	255
IPv6 Router Prefix Value	Displays the IPv6 gateway prefix value.	-

3.9.5 BMC User Settings

Figure 3-165 shows the **BMC User Settings** screen.

Figure 3-165 BMC User Settings Screen



For a description of the parameters on the **BMC User Settings** screen, refer to [Table 3-124](#).

Table 3-124 Parameter Descriptions for the BMC User Settings Screen

Parameter	Description	Default
User Name	Sets the username.	Administrator
Parameter	Description	Default
	The username is a case-sensitive character string of 4 to 16 characters including digits and letters. It must start with a letter.	
User Password Length	Sets the length of the user password.	20 Bytes
User Password	Creates a new password for the username.	-

Add User	Adds a user. For details, refer to 3.9.5.1 Add User .	-
Delete User	Deletes a user. For details, refer to 3.9.5.2 Delete User .	-
Change User Settings	Modifies user settings. For details, refer to 3.9.5.3 Change User Settings .	-

3.9.5.1 Add User

[Figure 3-166](#) shows the **Add User** screen.

Figure 3-166 Add User Screen

Aptio Setup - AMI

Server Mgmt

Server Mgmt->BMC User Settings->Add User

BMC Add User Details

User Name

User Password

User Access [Disable]

Channel No 0

User Privilege Limit [No Access]

Enter BMC User Name

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

Version 2.22.1285 Copyright (C) 2023 AMI

AB

For a description of the parameters on the **Add User** screen, refer to [Table 3-125](#).

Table 3-125 Parameter Descriptions for the Add User Screen

Parameter	Description	Default
User Name	Enter the BMC username.	-
User Password	Enter the password for the BMC username. The following parameters can be set only after you enter the correct 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

3.9.5.2 Delete User

Figure 3-167 shows the **Delete User** screen.

Figure 3-167 Delete User Screen

The screenshot shows the 'Aptio Setup - AMI' interface with the 'Server Mgmt' tab selected. The main menu on the left lists 'Server Mgmt->BMC User Settings->Delete User'. The right pane is titled 'Enter BMC User Name' and contains a list of navigation keys: '←→: Select Screen', '↑↓: Select Item', 'Enter: Select', '+/-: Change Option', 'K/M: Scroll Help Area', 'F1: General Help', 'F2: Previous Values', 'F3: Optimized Defaults', 'F4: Save & Exit', and 'ESC: Exit'. At the bottom, it says 'Version 2.22.1285 Copyright (C) 2023 AMI' and 'AB' in the bottom right corner.

For a description of the parameters on the **Delete User** screen, refer to [Table 3-126](#).

Table 3-126 Parameter Descriptions for the Delete User Screen

Parameter	Description
User Name	Enter the BMC username that you want to delete.
User Password	Enter the password for the BMC username that you want to delete.

3.9.5.3 Change User Settings

Figure 3-168 shows the **Change User Settings** screen.

Figure 3-168 Change User Settings Screen

Aptio Setup - AMI

Server Mgmt

Server Mgmt->BMC User Settings->Change User Settings

BMC Change User Settings

User Name

User Password

Change User Password

User Access [Disable]

Channel No 0

User Privilege Limit [No Access]

Enter BMC User Name

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

Version 2.22.1285 Copyright (C) 2023 AMI

AB

For a description of the parameters on the **Change User Settings** screen, refer to [Table 3-127](#).

Table 3-127 Parameter Descriptions for the Change User Settings Screen

Parameter	Description	Default
User Name	Enter the BMC username that you want to modify.	-
User Password	Enter the password for the BMC username that you want to modify.	-
Change User Password	Enter the new password for the BMC username.	-
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 user privilege restrictions.	No Access

Chapter 4

Reference: Control Keys for BIOS Setup

For a description of the available control keys in the BIOS of the Genoa platform, refer to Table 4-1.

Table 4-1 Descriptions of Control Keys

Shortcut 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.
F1	Displays the help information about the shortcut keys on the BIOS Setup screen
F2	Loads the last settings.
F3	Loads the default settings.
F4	Saves the settings and exits the BIOS.
ESC	Exits the current screen.

Glossary

ABL

- AGESA Boot Loader

ACPI

- Advanced Configuration and Power Interface

ACS

- Access Control Service

AER

- Advanced Error Reporting

ANSI

- American National Standards Institute

APIC

- Advanced Programmable Interrupt Controller

ARI

- Assist Request Instruction

ASCII

- American Standard Code for Information Interchange

ASID

- Address Space Identifier

ASPM

- Active State Power Management

BIOS

- Basic Input/Output System

BIST

- Built-In Self-Test

BMC

- Baseboard Management Controller

CA

- Certificate Authentication

CCD

- Charge Coupled Device

CD

- Compact Disk

CE

- Correctable Error

COM

- Component Object Model

CPPC

- Collaborative Processor Performance Control

CPU

- Central Processing Unit

CV

- Connectivity Verification

CXL

- Compute Express Link

DAC

- Digital Analog Converter

DDR

- Double Data Rate

DF

- Data Fabric

DHCP

- Dynamic Host Configuration Protocol

DID

- Dialogue Identification

DMA

- Direct Memory Access

DRAM

- Dynamic Random Access Memory

DVD

- Digital Versatile Disc

ECC

- Error Check and Correction

EFI

- Extensible Firmware Interface

EMS

- Emergency Management Service

FAR

- Forwarding Action Rule

FCH

- Frame Control Header

FRU

- Field Replaceable Unit

FW

- Firewall

GMI

- Global Memory Interconnect

HBA

- Host Bus Adapter

HDD

- Hard Disk Drive

HPET

- High Performance Event Timer

HSMP

- Host System Management Port

I/O

- Input/Output

ID

- Identification

IO

- Input & Output

IOMMU

- Input/Output Memory Management Unit

IP

- Internet Protocol

IPMI

- Intelligent Platform Management Interface

IPv4

- Internet Protocol Version 4

IPv6

- Internet Protocol Version 6

KVM

- Keyboard, Video and Mouse

MAC

- Media Access Control

MBIST

- Memory Built-In Self Test

MCA

- Machine Check Architecture

MMIO

- Memory-mapped I/O

MPIO

- Multiple-Path IO

NBIO

- North Bridge IO

NIC

- Network Interface Card

NMI

- Non-Maskable Interrupt

NUMA

- Non-Uniform Memory Access Architecture

NVME

- Non-Volatile Memory Express

NVMe

- Non-Volatile Memory Express

OC

- Overload Control

OCP

- Open Computer Project

OEM

- Original Equipment Manufacturer

OS

- Operating System

PBS

- Peak Burst Size

PC

- Personal Computer

PCI

- Peripheral Component Interconnect

PCIe

- Peripheral Component Interconnect Express

PHY

- Physical layer

PM

- Power Module

PMU

- Power Module Unit

POST

- Power-On Self-Test

PPIN

- Protected Processor Identification Number

PSP

- Programmable Signal Processor

PXE

- Preboot eXecution Environment

RAM

- Random Access Memory

RAM

- Random Access Memory

RAS

- Reliability, Availability and Serviceability

RCD

- Route Control Digit

RIB

- Routing Information Base

ROM

- Read-Only Memory

OS

- Operating System

RTP

- Real-time Transport Protocol

SATA

- Serial ATA

SB

- South Bridge

SCI

- Serial Communications Interface

SEL

- System Event Log

SEV-ES

- Secure Encrypted Virtualization-Encrypted State**SEV**
- Secure Encrypted Virtualization

SLIT

- System Locality Information Table

SMI

- System Management Interruption

SMT

- Simultaneous Multi-Threading

SMU

- Service Manager Unit

SOL

- Serial Over LAN

SPD

- Serial Presence Detect

SPI

- Serial Peripheral Interface

SR-IOV

- Single-Root I/O Virtualization

TDP

- Thermal Design Power

UEFI

- Unified Extensible Firmware Interface

UMC

- Unified Memory Controller

USB

- Universal Serial Bus

UUID

- Universal Unique Identifier

VGA

- Video Graphic Adapter

VID

- VLAN Identifier

VLAN

- Virtual Local Area Network