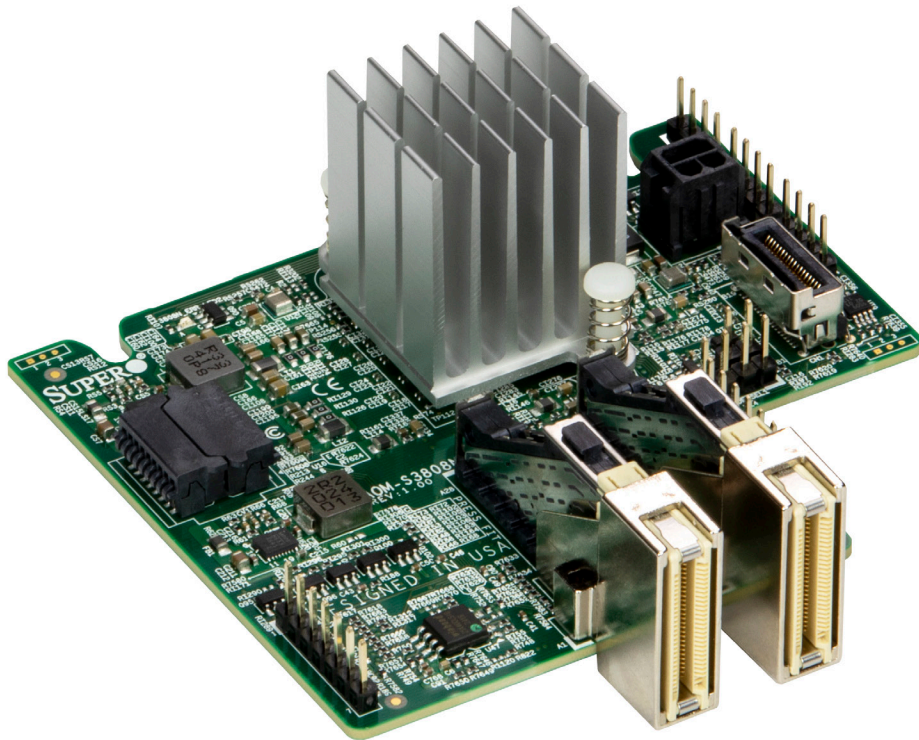




AOM-S3808NI-4NM



USER'S MANUAL

Revision 1.0

The information in this user's manual has been carefully reviewed and is believed to be accurate. The manufacturer assumes no responsibility for any inaccuracies that may be contained in this document, and makes no commitment to update or to keep current the information in this manual, or to notify any person or organization of the updates. **Please Note: For the most up-to-date version of this manual, please see our website at www.supermicro.com.**

Super Micro Computer, Inc. ("Supermicro") reserves the right to make changes to the product described in this manual at any time and without notice. This product, including software and documentation, is the property of Supermicro and/or its licensors, and is supplied only under a license. Any use or reproduction of this product is not allowed, except as expressly permitted by the terms of said license.

IN NO EVENT WILL Super Micro Computer, Inc. BE LIABLE FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, SPECULATIVE OR CONSEQUENTIAL DAMAGES ARISING FROM THE USE OR INABILITY TO USE THIS PRODUCT OR DOCUMENTATION, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN PARTICULAR, SUPER MICRO COMPUTER, INC. SHALL NOT HAVE LIABILITY FOR ANY HARDWARE, SOFTWARE, OR DATA STORED OR USED WITH THE PRODUCT, INCLUDING THE COSTS OF REPAIRING, REPLACING, INTEGRATING, INSTALLING OR RECOVERING SUCH HARDWARE, SOFTWARE, OR DATA.

Any disputes arising between manufacturer and customer shall be governed by the laws of Santa Clara County in the State of California, USA. The State of California, County of Santa Clara shall be the exclusive venue for the resolution of any such disputes. Supermicro's total liability for all claims will not exceed the price paid for the hardware product.

FCC Statement: This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in industrial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the manufacturer's instruction manual, may cause harmful interference with radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case you will be required to correct the interference at your own expense.

California Best Management Practices Regulations for Perchlorate Materials: This Perchlorate warning applies only to products containing CR (Manganese Dioxide) Lithium coin cells. "Perchlorate Material-special handling may apply. See www.dtsc.ca.gov/hazardouswaste/perchlorate".



WARNING: This product can expose you to chemicals including lead, known to the State of California to cause cancer and birth defects or other reproductive harm. For more information, go to www.P65Warnings.ca.gov.

The products sold by Supermicro are not intended for and will not be used in life support systems, medical equipment, nuclear facilities or systems, aircraft, aircraft devices, aircraft/emergency communication devices or other critical systems whose failure to perform be reasonably expected to result in significant injury or loss of life or catastrophic property damage. Accordingly, Supermicro disclaims any and all liability, and should buyer use or sell such products for use in such ultra-hazardous applications, it does so entirely at its own risk. Furthermore, buyer agrees to fully indemnify, defend and hold Supermicro harmless for and against any and all claims, demands, actions, litigation, and proceedings of any kind arising out of or related to such ultra-hazardous use or sale.

Manual Revision 1.0

Release Date: April 23, 2025

Unless you request and receive written permission from Super Micro Computer, Inc., you may not copy any part of this document. Information in this document is subject to change without notice. Other products and companies referred to herein are trademarks or registered trademarks of their respective companies or mark holders.

Copyright © 2025 by Super Micro Computer, Inc.
All rights reserved.

Printed in the United States of America

Preface

About This Manual

This user's guide is written for system integrators, IT technicians, and knowledgeable end users. It provides information for the installation and use of the AOM-S3808NI-4NM add-on module.

About This Add-On Card

The AOM-S3808NI-4NM is an OS Boot PCIe Gen 4.0 x4 M.2 SSD carrier card that enables the user to add up to two NVMe drives with RAID 0 and RAID 1. Leveraging the cutting-edge power of PCI Express 4.0 technology, the M.2 solid state technology is an optimized, high-performance, scalable storage solution.

An Important Note to the User

All graphic images and layout drawings shown in this user's guide are based upon the latest PCB revision available at the time of publishing this user's guide. The add-on card you have received may or may not look exactly the same as the graphics shown in this user's guide.

Returning Merchandise for Service

A receipt or copy of your invoice marked with the date of purchase is required before any warranty service will be rendered. You can obtain service by calling your vendor for a Returned Merchandise Authorization (RMA) number. When returning to the manufacturer, the RMA number should be prominently displayed on the outside of the shipping carton and mailed prepaid or hand-carried. Shipping and handling charges will be applied for all orders that must be mailed when service is complete. For faster service, RMA authorizations may be requested online (<http://www.supermicro.com/support/rma/>).

This warranty only covers normal consumer use and does not cover damages incurred in shipping or from failure due to the alteration, misuse, abuse, or improper maintenance of products.

During the warranty period, contact your distributor first for any product problems.

Conventions Used in the Manual

Special attention should be given to the following symbols for proper installation and to prevent damage done to the components or injury.



Warning! Indicates important information given to prevent equipment/property damage or personal injury.



Warning! Indicates high voltage may be encountered while performing a procedure.



Important: Important information given to ensure proper system installation or to relay safety precautions.



Note: Additional information given to differentiate various models or to provide information for proper system setup.

Important Links

For your system to work properly, follow the links below to download all necessary drivers/utilities and the user's manual for your server.

- Supermicro product manuals: <http://www.supermicro.com/support/manuals/>
- Product drivers and utilities: <https://www.supermicro.com/wdl/driver>
- Product safety info: http://www.supermicro.com/about/policies/safety_information.cfm
- A secure data deletion tool designed to fully erase all data from storage devices can be found at our website: https://www.supermicro.com/about/policies/disclaimer.cfm?url=/wdl/utility/Lot9_Secure_Data_Deletion_Utility/
- If you have any questions, contact our support team at: support@supermicro.com
- Frequently Asked Questions: <https://www.supermicro.com/FAQ/index.php>
- If you have any feedback on Supermicro product manuals, contact our writing team at: Techwriterteam@supermicro.com

This manual may be periodically updated without notice. Check the Supermicro website for possible updates to the manual revision level.

Naming Convention

AOM-	S	3808N	I	-	4	N	M
Prefix	1st	2nd	3rd		4th	5th	6th

Character	Representation	Options
Prefix	Product Family	<ul style="list-style-type: none"> AOM = Add on Module Cards
1st	Form Factor	<ul style="list-style-type: none"> S = Standard PCI-E M = M.2 O = AIOM/OCP P = Special Form Factor
2nd	Chipset (Optional)	<ul style="list-style-type: none"> SAS chip: 3616,3816,3908,3916... etc. 3616 = SAS3616 3808N = SAS3808N 3816 = SAS3816 3908 = SAS3908
3rd	Controller Type	<ul style="list-style-type: none"> T = IT Mode I = iMR Mode= iR mode M = MR Mode N = No active controller
4th	Generation	<ul style="list-style-type: none"> 3 = PCIe Gen3 4 = PCIe Gen4 5 = PCIe Gen5 6 = PCIe Gen6
5th	Protocol Type	<ul style="list-style-type: none"> N = NVMe S = SAS T = SATA H = Hybrid/ Tri-mode
6th	Device Type (Optional)	<ul style="list-style-type: none"> M = M.2 MB = M.2 Stack (back to back) MS = M.2 Flat (side by side) U = U.2 E = E1.S/E3.S S = Switch T = Retimer D = Redriver
7th	MB Platform (Optional)	<ul style="list-style-type: none"> Reserved
8th	Customer Code (Optional)	<ul style="list-style-type: none"> OEM customer abbreviation

Contacting Supermicro

Headquarters

Address: Super Micro Computer, Inc.
980 Rock Ave.
San Jose, CA 95131 U.S.A.

Tel: +1 (408) 503-8000

Fax: +1 (408) 503-8008

Email: marketing@supermicro.com (General Information)
Sales-USA@supermicro.com (Sales Inquiries)
Government_Sales-USA@supermicro.com (Gov. Sales Inquiries)
support@supermicro.com (Technical Support)
RMA@supermicro.com (RMA Support)
Webmaster@supermicro.com (Webmaster)

Website: www.supermicro.com

Europe

Address: Super Micro Computer B.V.
Het Sterrenbeeld 28, 5215 ML
's-Hertogenbosch, The Netherlands

Tel: +31 (0) 73-6400390

Fax: +31 (0) 73-6416525

Email: Sales_Europe@supermicro.com (Sales Inquiries)
Support_Europe@supermicro.com (Technical Support)
RMA_Europe@supermicro.com (RMA Support)

Website: www.supermicro.nl

Asia-Pacific

Address: Super Micro Computer, Inc.
3F, No. 150, Jian 1st Rd.
Zhonghe Dist., New Taipei City 235
Taiwan (R.O.C)

Tel: +886-(2) 8226-3990

Fax: +886-(2) 8226-3992

Email: Sales-Asia@supermicro.com.tw (Sales Inquiries)
Support@supermicro.com.tw (Technical Support)
RMA@supermicro.com.tw (RMA Support)

Website: www.supermicro.com.tw

Table of Contents

Chapter 1 Introduction

1.1 Overview.....	8
1.2 Key Features.....	8
1.3 Specifications.....	9

Chapter 2 Hardware Components

2.1 Add-On Card Image and Layout.....	10
2.2 Major Components.....	13
2.3 LED Indicators.....	14

Chapter 3 Installation

3.1 Overview.....	16
3.2 Static-Sensitive Devices.....	16
3.3 Before Installation.....	17
3.4 Installation.....	18
3.5 Installing the Drivers in Windows.....	20
3.6 Uninstalling the Drivers.....	20

Chapter 4 Firmware Update

4.1 Update Firmware in BIOS.....	21
4.2 Update Firmware in UEFI.....	29
4.3 Update Firmware in BMC.....	31

Chapter 5 Drive Management

5.1 RAID Minimum Drive Requirements.....	35
5.2 Managing Physical Drive.....	36
5.3 Creating RAID.....	39
5.4 Deleting RAID in BIOS.....	52
5.5 Managing JBOD State.....	58
5.6 Managing Unconfigured Good State.....	69

Chapter 6 Secure Boot Settings

6.1 Boot Mode Select Feature.....	74
6.2 Secure Boot/Secure Boot Mode/CSM Support Features.....	75
6.3 Secure Boot Settings.....	81

Chapter 1

Introduction

1.1 Overview

Congratulations on purchasing your add-on card from an acknowledged leader in the industry. Supermicro products are designed with the utmost attention to detail to provide you with the highest standards of quality and performance. For product support and updates, refer to our website at <https://www.supermicro.com/en/products/storage/cards>.

1.2 Key Features

The key features of this add-on card include the following:

- OS Boot Storage Adapter
- Broadcom® SAS3808N RAID Controller: RAID 0/1 or JBOD
- PCIe Gen 4.0 x4 Host interface
- MCIO x4
- Micro-Hi 2x2 power connectors
- Supports 22X110, 22X80 mm M.2 form factor with adapter MCP-220-12108-0N (optional)
- Supports two hot swappable M.2 modules
- Supports MCTP over PCIe
- Supports BMC-enabled management
- Supports Secure Erase
- Supports Hardware Secure Boot
- Supports on-board LEDs for SAS3808N Activity and Status
- FW Update through BMC
- UEFI Configuration Utility
- StorCLI

- LSA
- Thermal operating range: System dependent (55°C or higher with enough airflow)

1.3 Specifications

OS Support

- Windows, Linux, and VMware

Physical Dimensions

- Card PCB dimensions: 3.43" x 3.35" (87.122 mm x 85.09 mm) (L x W)



Note: This product is only sold as part of an integrated solution with Supermicro server systems.

Chapter 2

Hardware Components

2.1 Add-On Card Image and Layout

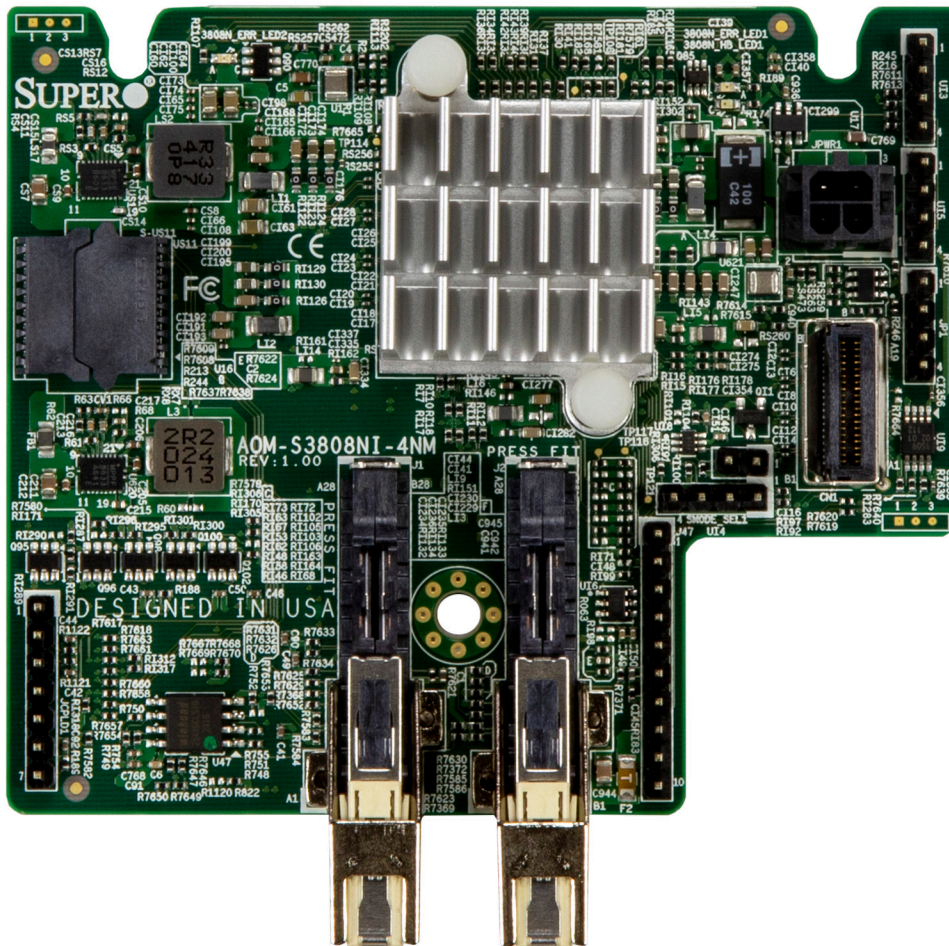


Figure 2-1: AOM-S3808NI-4NM Top View

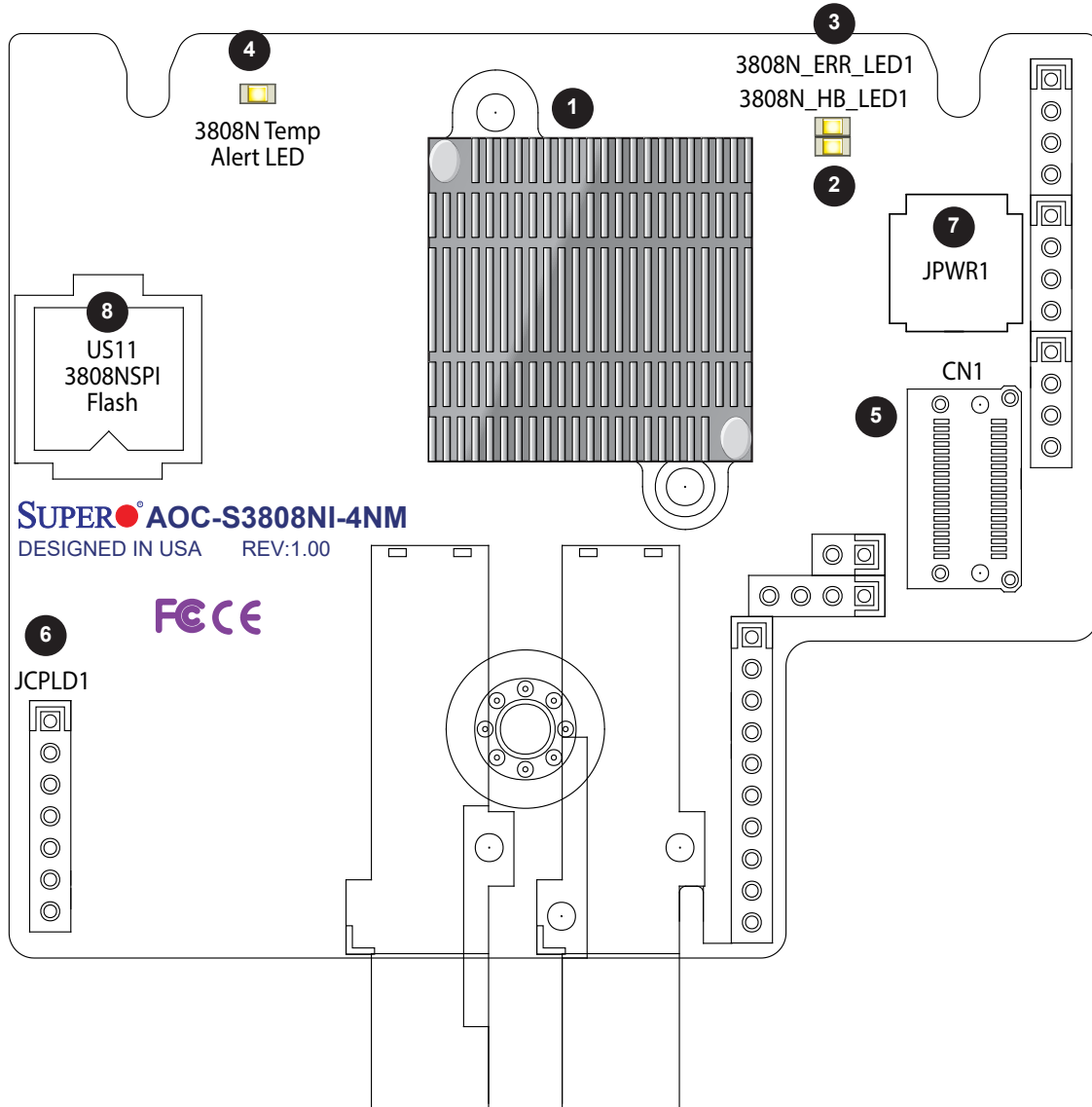


Figure 2-3: AOM-S3808NI-4NM Layout

2.2 Major Components

The following major components are installed on the AOM-S3808NI-4NM:

AOM-S3808NI-4NM Major Components		
No.	Component Name	Definition
1	Broadcom SAS3808N Controller	Broadcom SAS3808N RAID Controller
2	3808N_ERR_LED1	System Fault LED
3	3808N_HB_LED1	Heartbeat LED
4	3808N Temp Alert LED	Thermal Alert LED
5	CN1	MCIO x4 PCIe Port 1
6	JCPLD1	CPLD JTAG Programming Header
7	JPWR1	Micro-Hi 2x2 Power Connector
8	US11	3808NSPI Flash

2.3 LED Indicators

System Fault LED

The System Fault LED is located at 3808N_ERR_LED1 on the add-on card. When a fault has occurred with the controller chip, LED1 will illuminate red. Refer to [page 12](#) for its location.

System Fault LED Status	
Color/State	Definition
Red Solid	Controller: Fault
Off	Controller: Normal

Thermal Alert LED

A thermal alert LED is located at 3808N Temp Alert LED. When the system has reached an abnormally high temperature, the LED will light up red to signal the potential overheating issue. Refer to [page 12](#) for its location.

Thermal Alert LED Status	
Color/State	Definition
Red	Thermal Alert
Off	No issue

System Heartbeat LED

The System Heartbeat LED is located at 3 on the add-on card. When the LED is blinking green at 1 Hz, the controller is operational and functioning normally. Refer to [page 12](#) for its location.

System Heartbeat LED Status	
Color/State	Definition
Green Blinking	Controller: Normal
Off	Power failure on controller

Chapter 3

Installation

3.1 Overview

As a part of an integrated solution, your system came with the adapter pre-installed. We do not recommend removing and reinstalling any part of your system components. If you need to remove or reinstall a system component, including this add-on card, follow the instructions in this chapter to ensure proper system setup.

3.2 Static-Sensitive Devices

Electrostatic Discharge (ESD) can damage electronic components. To avoid damaging your add-on card, it is important to handle it very carefully. The following measures are generally sufficient to protect your equipment from ESD.

Precautions

- Use a grounded wrist strap designed to prevent static discharge.
- Touch a grounded metal object before removing the add-on card from the antistatic bag.
- Handle the add-on card by its edges only; do not touch its components or peripheral chips.
- Put the add-on card back into the antistatic bags when not in use.
- Be sure to remove the power cord first before adding, removing, or changing any hardware components to avoid damaging the system or components.
- For grounding purposes, make sure that your system chassis provides excellent conductivity between the power supply, the cage, the mounting fasteners, and the add-on card.

Unpacking

The add-on card is shipped in antistatic packaging to avoid static damage. When unpacking your component or system, make sure you are static protected.



Note: To avoid damaging your components and to ensure proper installation, always connect the power cord last, and always unplug it before adding, removing, or changing any hardware components.

3.3 Before Installation

To install the add-on card properly, be sure to follow the instructions below.

1. Power down the system.
2. Remove the power cord from the wall socket.
3. Use industry-standard antistatic equipment (such as gloves or a wrist strap) and follow the instructions listed on [page 16](#) to avoid damage caused by ESD.
4. Familiarize yourself with the server, motherboard, and/or chassis documentation.
5. Confirm that your operating system includes the latest updates and hot fixes.

3.4 Installation

The AOM-S3808NI-4NM module supports two M.2 SSDs of 80 mm or 110 mm in length. Visit the Supermicro website for a current list of supported M.2 SSDs.

Installing Cables

To connect the power and MCIO cables to then install the PCIe and BPN cards, refer to the following steps:

1. Connect the power cable CBL-PWEX-1136YB-25 on JPWR3 (MB) to JPWR1 (AOM).

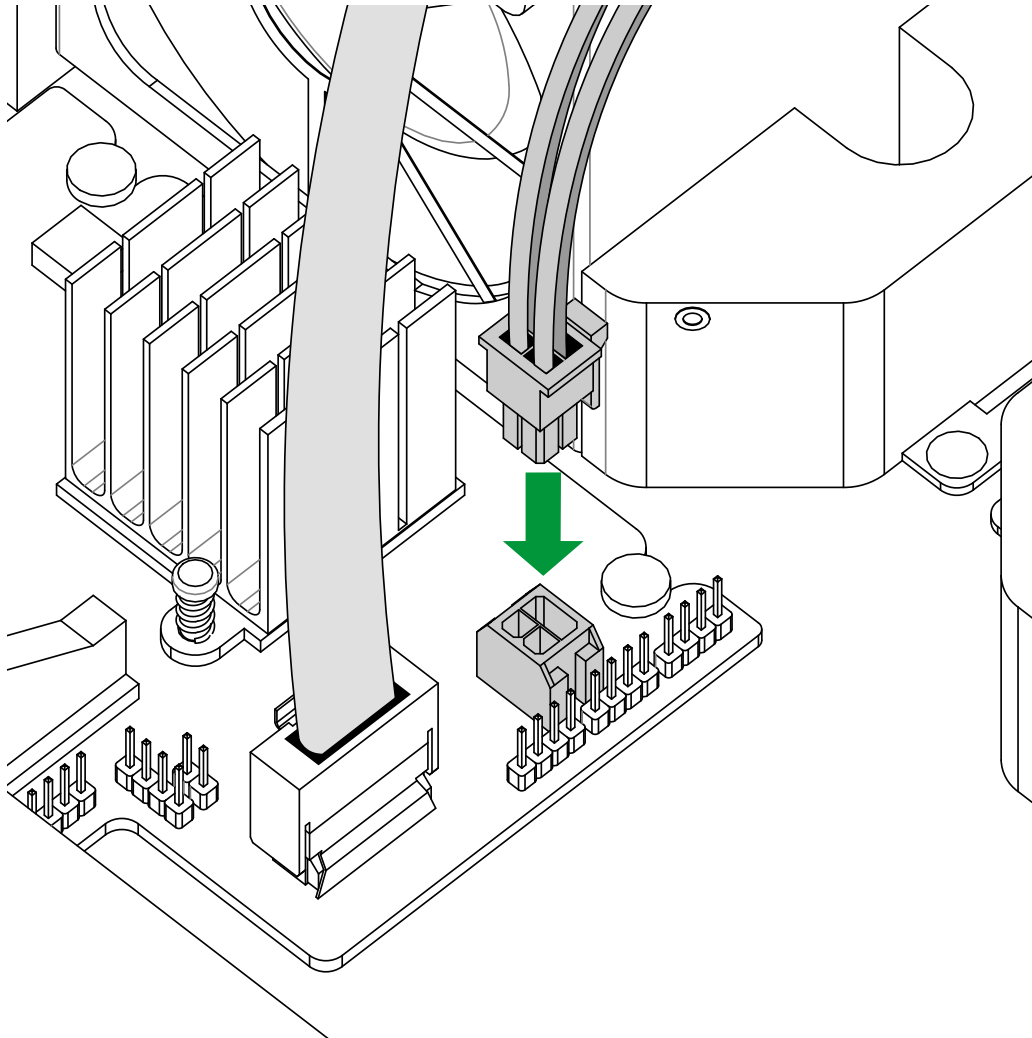


Figure 3-4: Connect Power Cable

2. Connect the MCIO cable CBL-MCIO-1465QQM5 on EJRAID1 (MB) to CN1 (AOM).

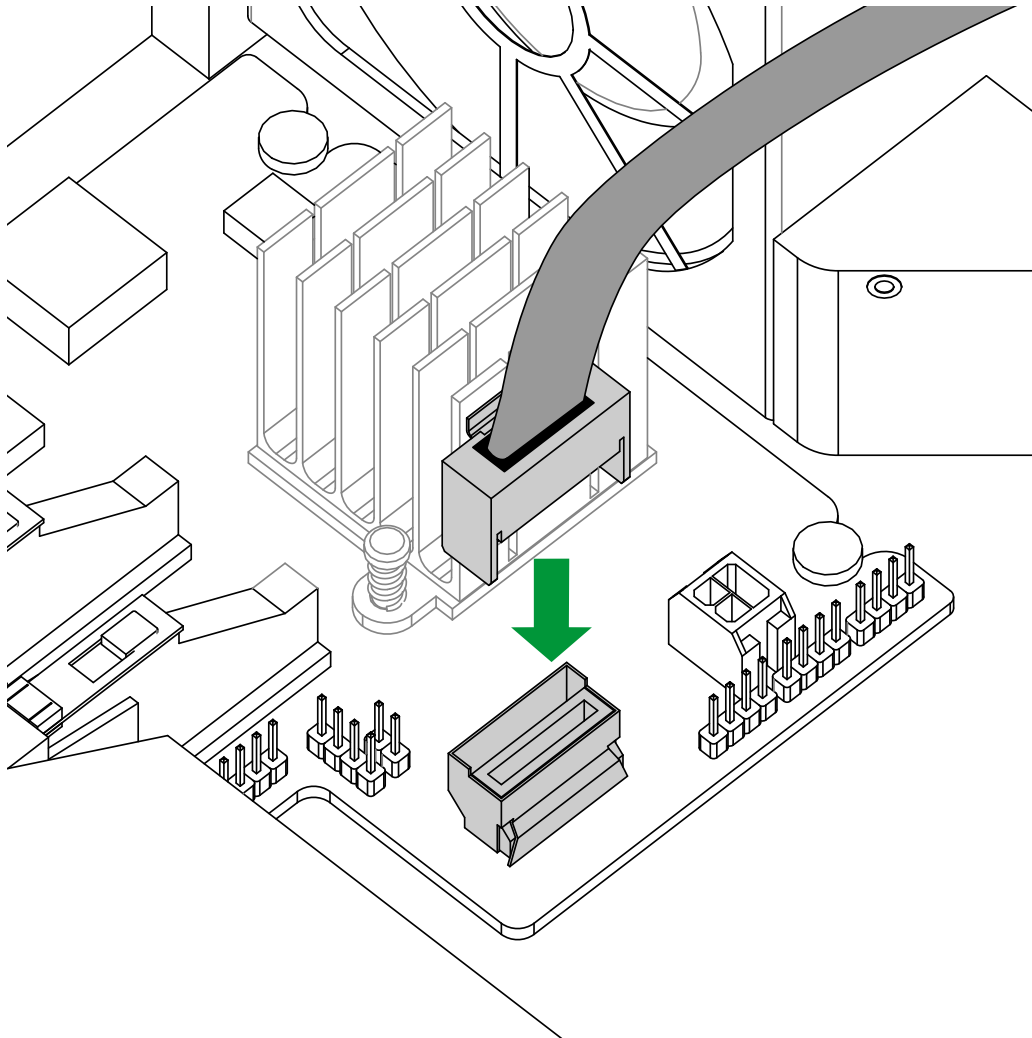


Figure 3-5: Connect MCIO Cable

3. Install 2x PCIe Gen4 x4 M.2 on MCP-220-12108-0N-01_R1.00.
4. Install 2x MCP-220-12108-0N-01_R1.00 on J1/J2 on AOM-S3808NI-4NM.

3.5 Installing the Drivers in Windows

Refer to the instructions that came with your M.2 SSD and follow the manufacturer's recommended steps for installing the NVMe driver. Download the latest drivers from the Supermicro project board at <https://www.supermicro.com/wdl/driver>.

3.6 Uninstalling the Drivers

To Uninstall the Drivers in Windows

Follow the instructions provided by your M.2 SSD manufacturer.

To Uninstall the Drivers in Linux

Run the following command to uninstall the NVMe drivers.

```
./RemoveService.sh
```

Chapter 4

Firmware Update

4.1 Update Firmware in BIOS

This chapter provides instructions on how to update the firmware in BIOS. Use the arrow keys to highlight your chosen option, and click <Enter> to select. Click <Esc> to exit an option menu or return to the previous page.

1. Navigate to the **Advanced** tab, where you can manage RAID Controller configurations.
2. Navigate to and select **BROADCOM <SAS 3808N> Configuration Utility**.

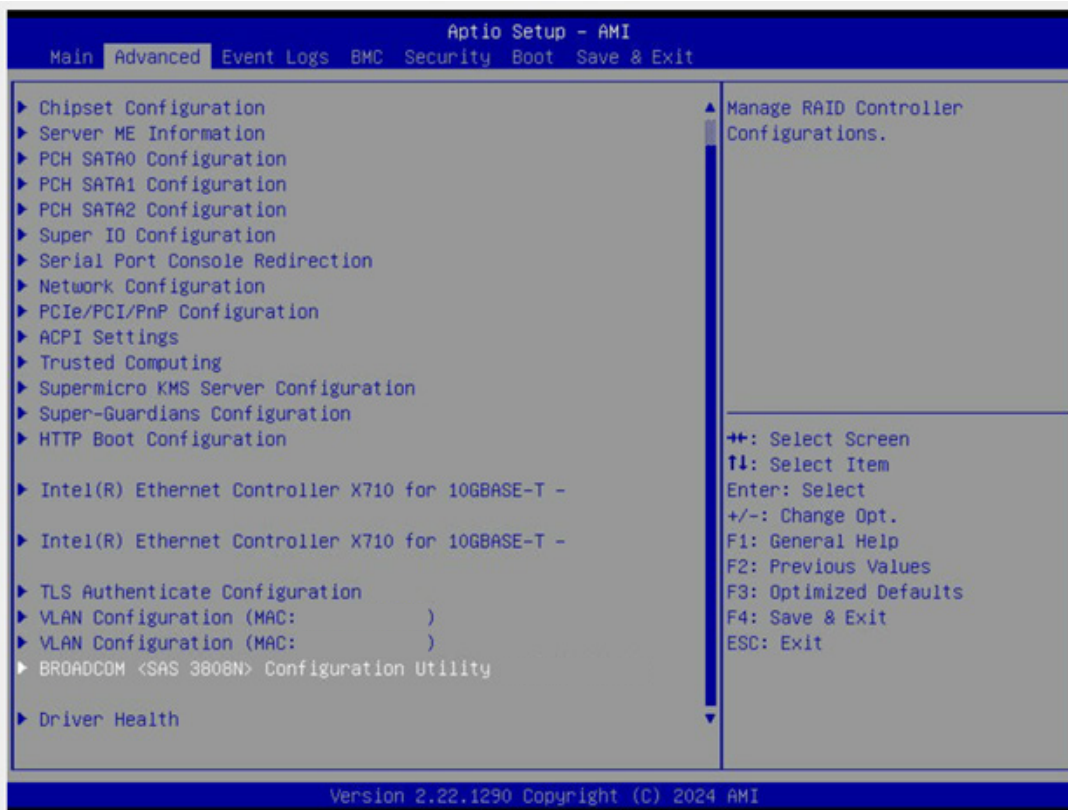


Figure 4-1: BROADCOM <SAS 3808N> Configuration Utility Selected

3. Select **Update Firmware**, which will allow you to update the controller firmware to the necessary newer version.

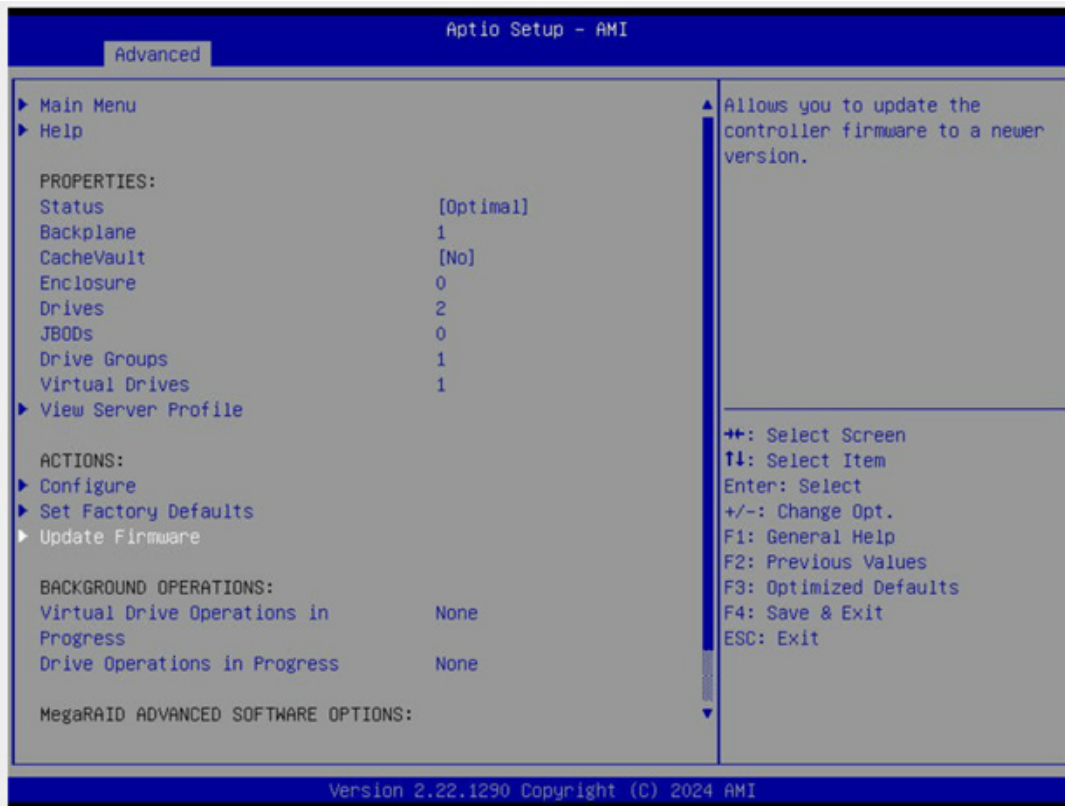


Figure 4-2: Update Firmware Selected

4. Ensure that **Select Directory** is set to the **bin** option.

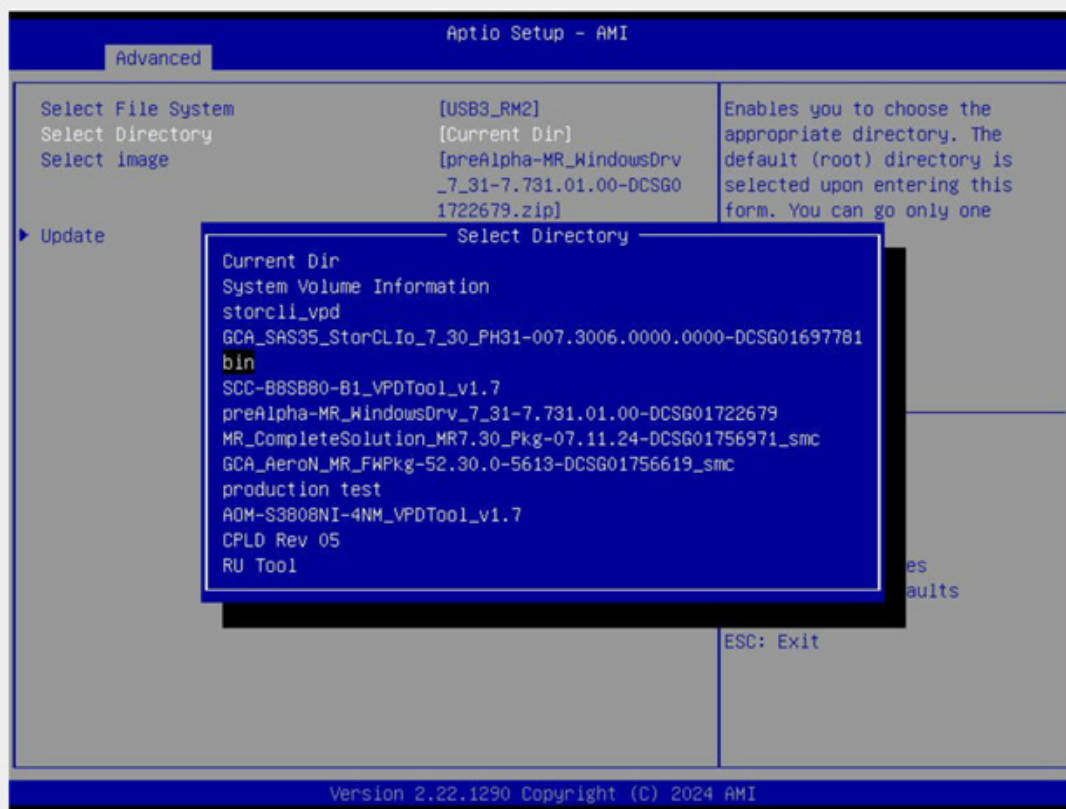


Figure 4-3: bin Option Selected

5. Navigate to **Select Image**.



Figure 4-4: Select Image Selected

6. Select the appropriate firmware image. Be aware that the applicable image size restriction depends on the controller type.

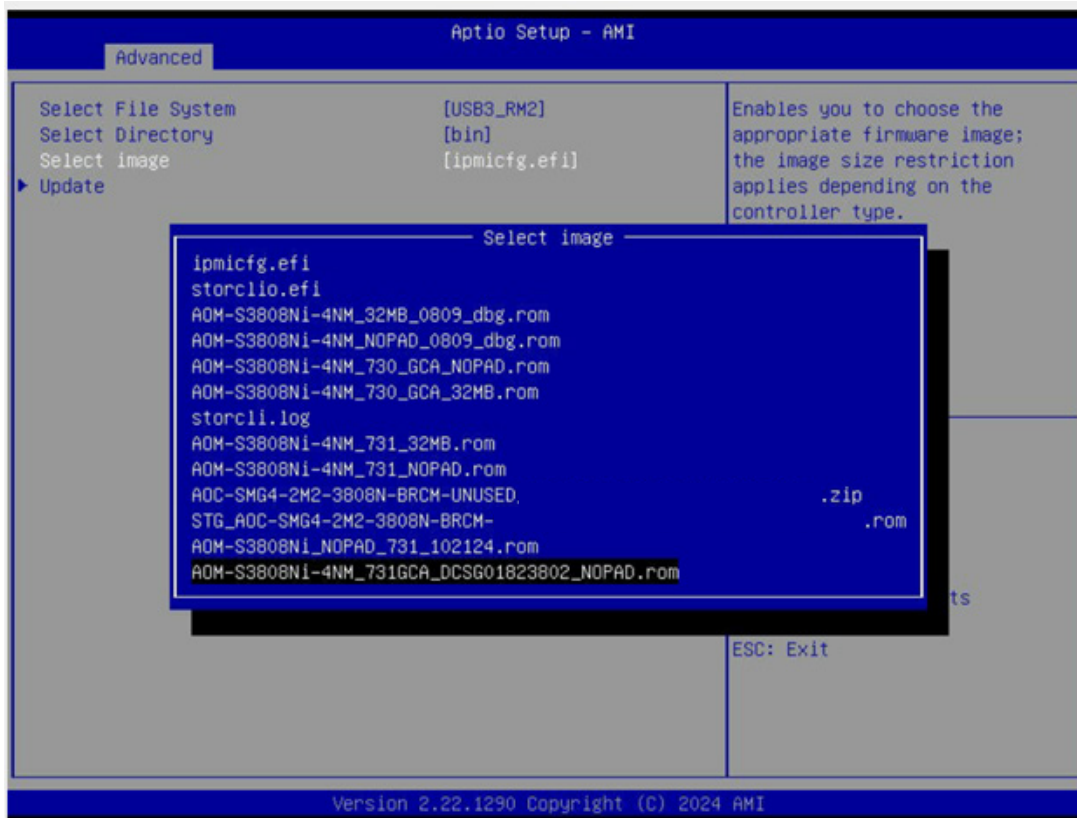


Figure 4-5: Appropriate Firmware Selected

7. Once all chosen options are in place, select **Update**.

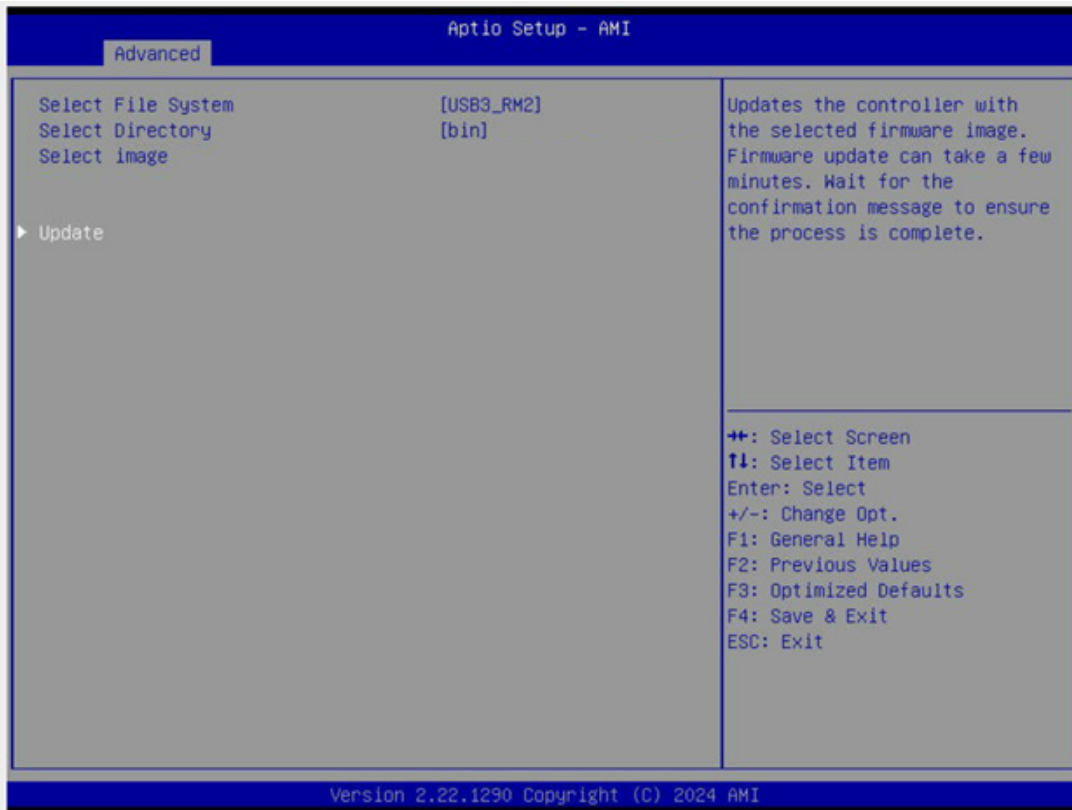


Figure 4-6: Update Selected

8. You will be presented with a confirmation window where you can review the current and selected firmware versions. To proceed and make the **Yes** option available, select **Confirm** and ensure that it is set to **Enabled**.
9. Once the **Confirm** option is enabled, select **Yes** to proceed with the update.

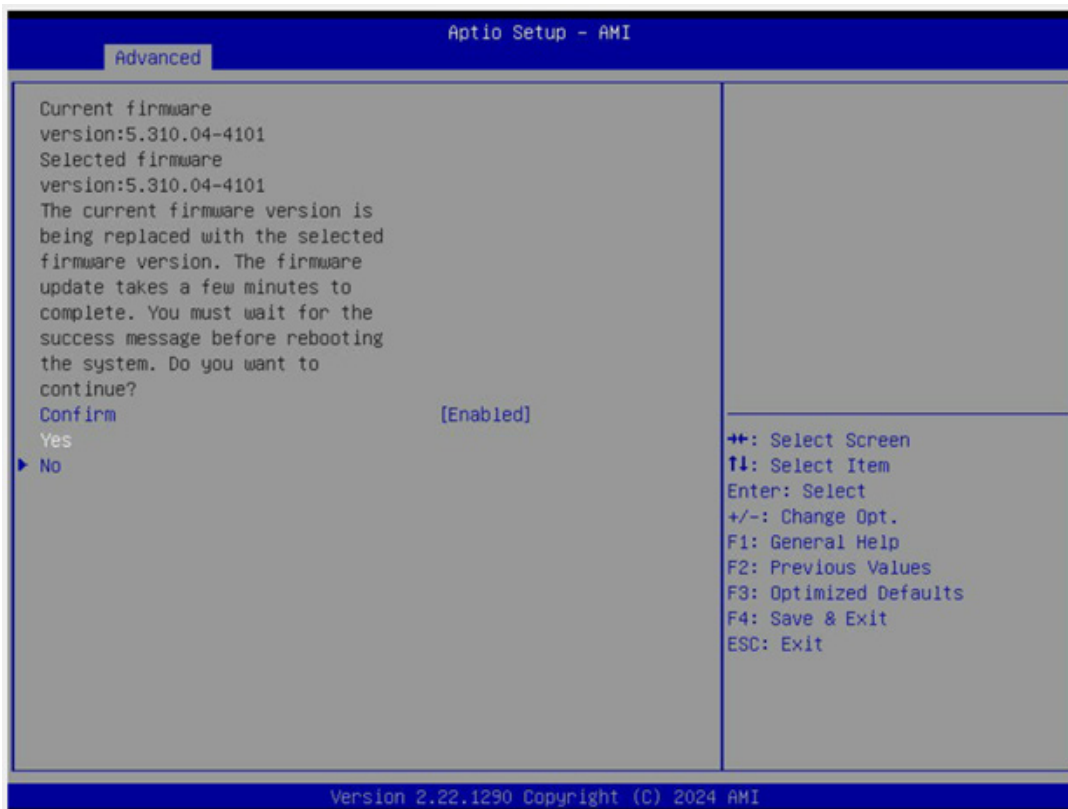



Figure 4-7: Confirm Enabled and Yes Option Selected

- You will be presented with a window confirming that the operation has been performed successfully. Select **OK** to proceed and return to the main menu.

 **Note:** Updates may take a few minutes to complete. Be sure you see the confirmation window *first* before rebooting the system.

- To save this update, navigate to the **Save & Exit** tab.
- Navigate to and select the updated component.
- Select **Yes** to save the updated configuration of setup values. If you do not wish to save the configuration as it currently is, select No to cancel and exit the confirmation menu.

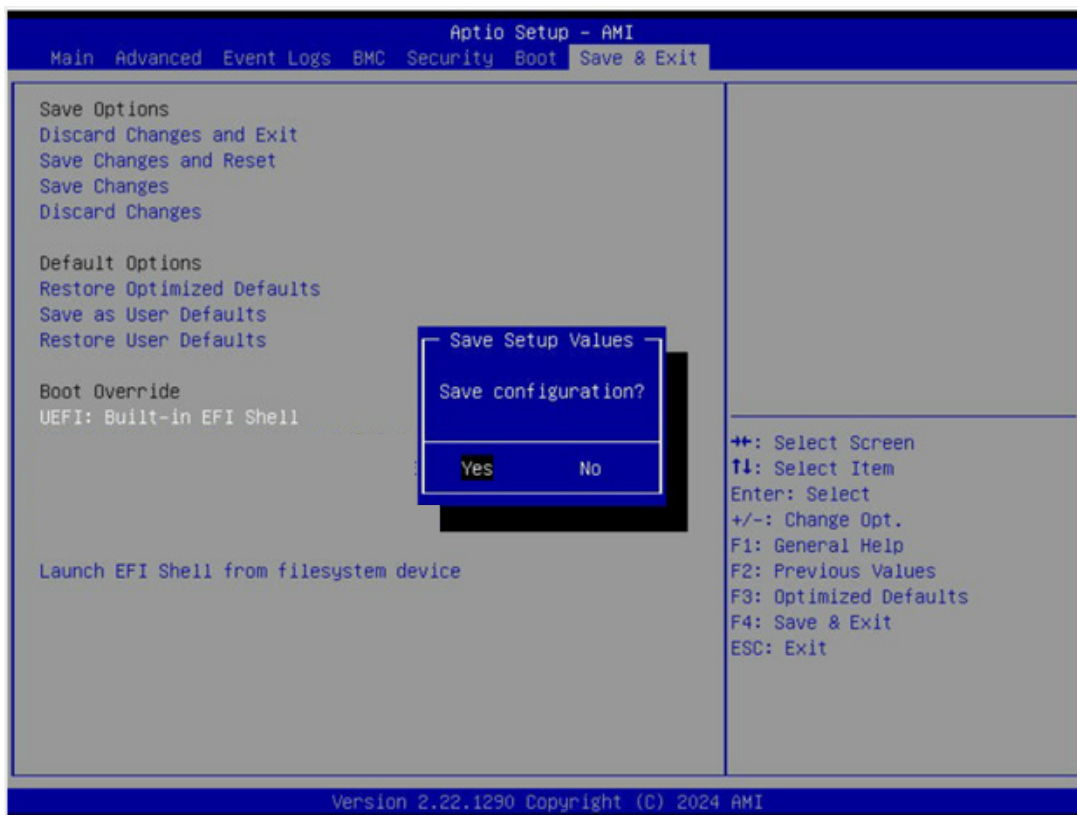


Figure 4-8: Yes Option to Save Configuration Selected

4.2 Update Firmware in UEFI

The section provides instructions on how to update the firmware in UEFI.

1. Utilize the following commands to access the directory:

```
Shell> fs0:
```

```
FS0:\> ls
```

1. Utilize the following command:

```
FS0:\> cd bin
```

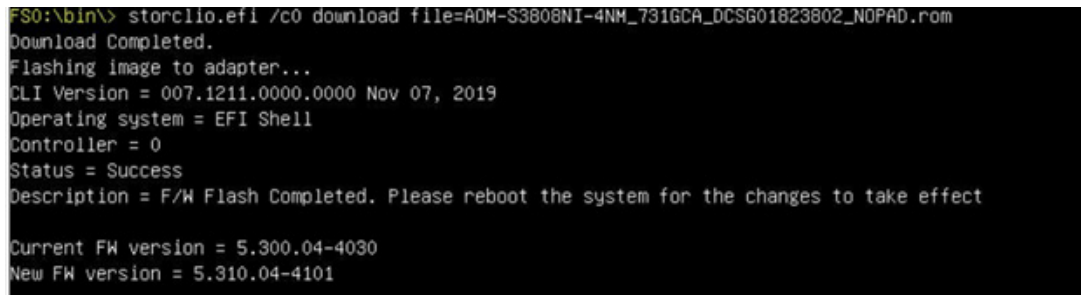
```
Mapping table
FS0: Alias(s):HD0y0b;;BLK1:
  PciRoot(0x0)/Pci(0x14,0x0)/USB(0x18,0x0)/HD(1,MBR,0xC3072E18,0x1E0,0x3ABFE20)
BLK0: Alias(s):
  PciRoot(0x0)/Pci(0x14,0x0)/USB(0x18,0x0)
BLK2: Alias(s):
  PciRoot(0x30)/Pci(0x1,0x0)/Pci(0x0,0x0)/Ctrl(0x0)/Scsi(0x1,0x0)
Press ESC in 1 seconds to skip startup.nsh or any other key to continue.
Shell> fs0:
FS0:\> ls
Directory of: FS0:\
01/13/2025  22:45 <DIR> r      16,384  ADM-S3806NI-4NM_VPDTool_v1.7
02/25/2025  23:39 <DIR>      16,384  bin
10/23/2024  14:18 <DIR>      16,384  CFLD Rev 05
08/16/2024  14:36 <DIR>      16,384  GCA_AeroN_MR_FWPKg-52.30.0-5613-DCSG01756619_smc
08/16/2024  14:31      13,424,474  GCA_AeroN_MR_FWPKg-52.30.0-5613-DCSG01756619_smc.zip
07/17/2024  15:31 <DIR>      16,384  GCA_SAS35_StorCLIo_7_30_PH31-007.3006.0000.0000-DCSG01697781
08/16/2024  14:36 <DIR>      16,384  MR_CompleteSolution_MR7.30_Pkg-07.11.24-DCSG01756971_smc
08/16/2024  14:33      484,254,142  MR_CompleteSolution_MR7.30_Pkg-07.11.24-DCSG01756971_smc.zip

08/16/2024  11:25 <DIR>      16,384  preAlpha-MR_WindowsDrv_7_31-7.731.01.00-DCSG01722679
08/16/2024  11:19      2,345,657  preAlpha-MR_WindowsDrv_7_31-7.731.01.00-DCSG01722679.zip
11/14/2024  10:27 <DIR>      16,384  production test
11/13/2024  15:25 <DIR>      16,384  RU Tool
11/13/2024  15:17      520,129  RU Tool.zip
10/18/2024  23:44 <DIR>      16,384  SCC-888880-B1_VPDTool_v1.7
10/18/2024  23:42 <DIR>      16,384  storcli_vpd
      4 File(s)  500,544,402 bytes
      11 Dir(s)
FS0:\> cd bin
```

Figure 4-9: Flash Firmware in UEFI

1. Depending on the firmware package file location, run the following command to update the firmware. Be sure to input the correct file location in your command.

```
Fs0:\bin\> storcli.efi /c0 download file=AOM-S3808NI-4NM_731GCA_
DCSG01823802_NOPAD.rom
```



```
Fs0:\bin\> storcli.efi /c0 download file=AOM-S3808NI-4NM_731GCA_DCSG01823802_NOPAD.rom
Download Completed.
Flashing image to adapter...
CLI Version = 007.1211.0000.0000 Nov 07, 2019
Operating system = EFI Shell
Controller = 0
Status = Success
Description = F/W Flash Completed. Please reboot the system for the changes to take effect

Current FW version = 5.300.04-4030
New FW version = 5.310.04-4101
```

Figure 4-10: Flash Firmware in UEFI

4.3 Update Firmware in BMC

The section provides instructions on how to update the firmware in the BMC.

1. Select the **Dashboard** tab on the left navigation menu after entering the BMC.
2. On the Dashboard page, select the blue **Firmware Update** option at the top of the page.

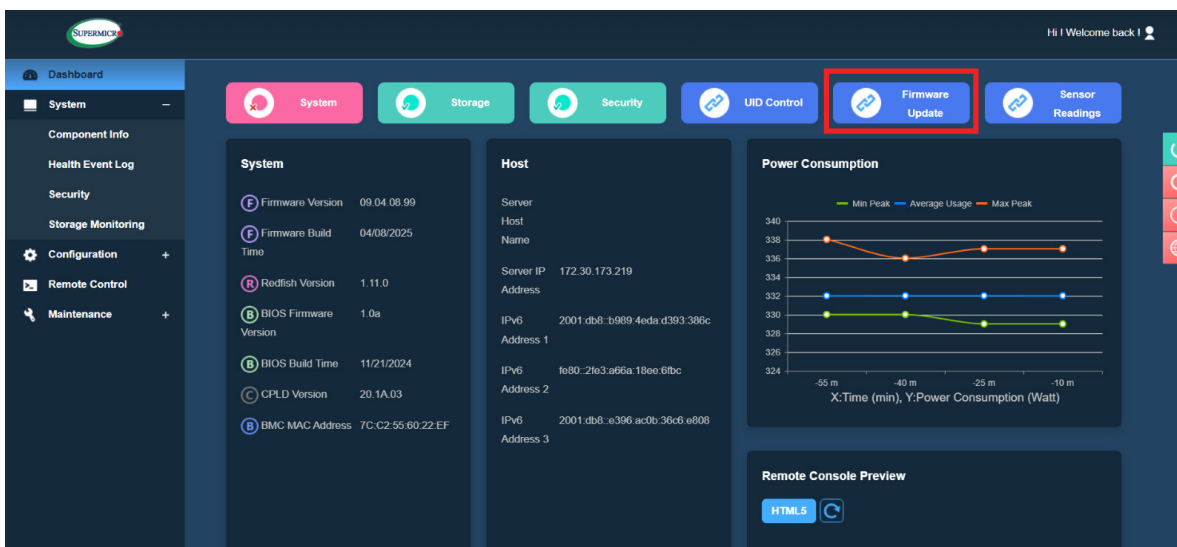


Figure 4-12: Dashboard Page Firmware Update Selected

3. Among the file format types, select **SAS3808N**.
4. Once the option is selected, click **Next**.

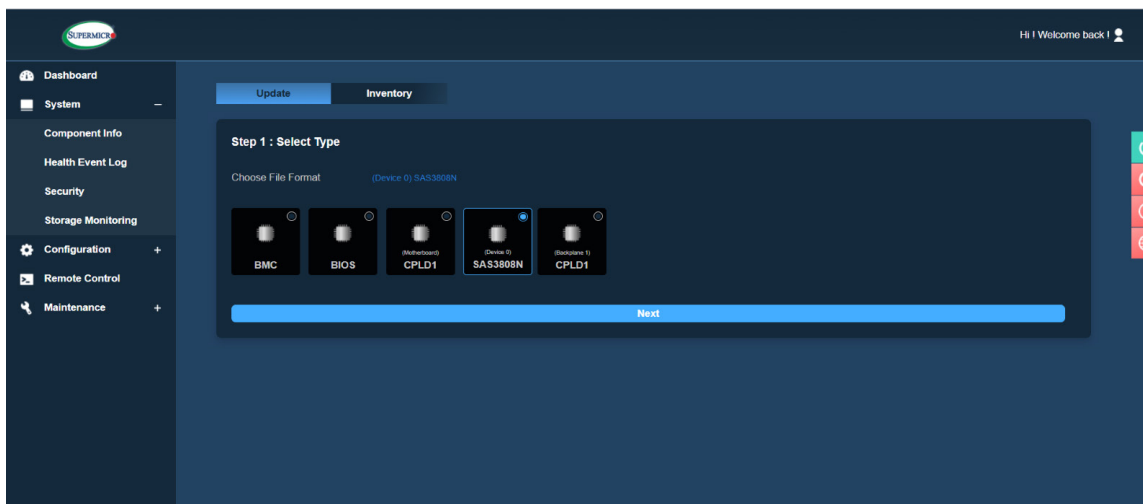


Figure 4-13: Firmware Update Step 1

5. This will make Step 2 available. **Select File** to upload the chosen firmware file.
6. Once the file is selected and appears listed, click **Upload**. Loading the firmware might take a few minutes.

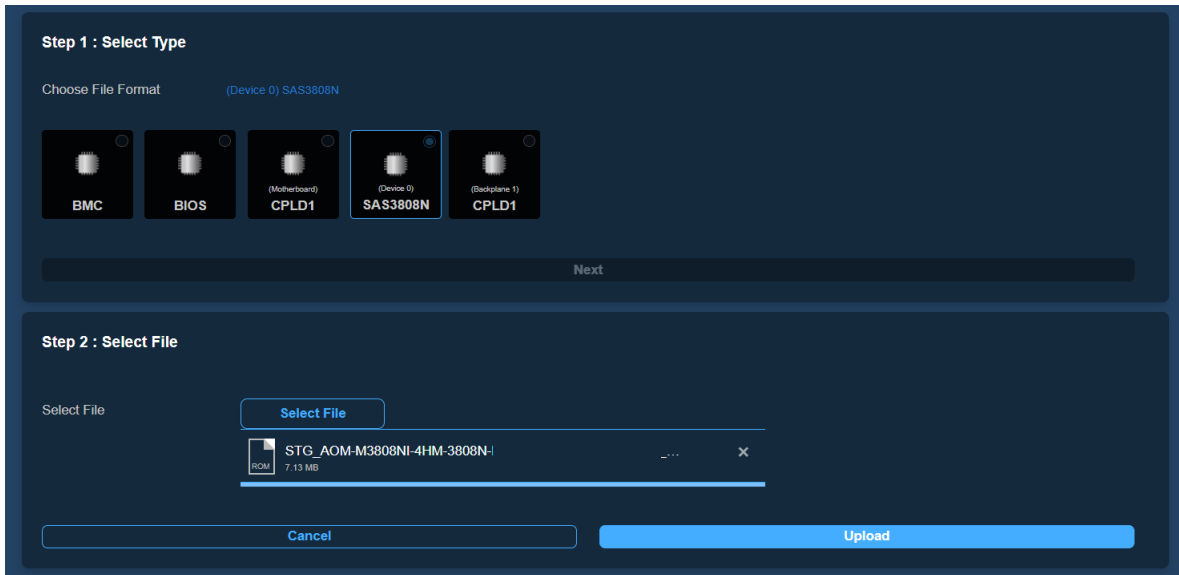


Figure 4-14: Firmware Update Step 2

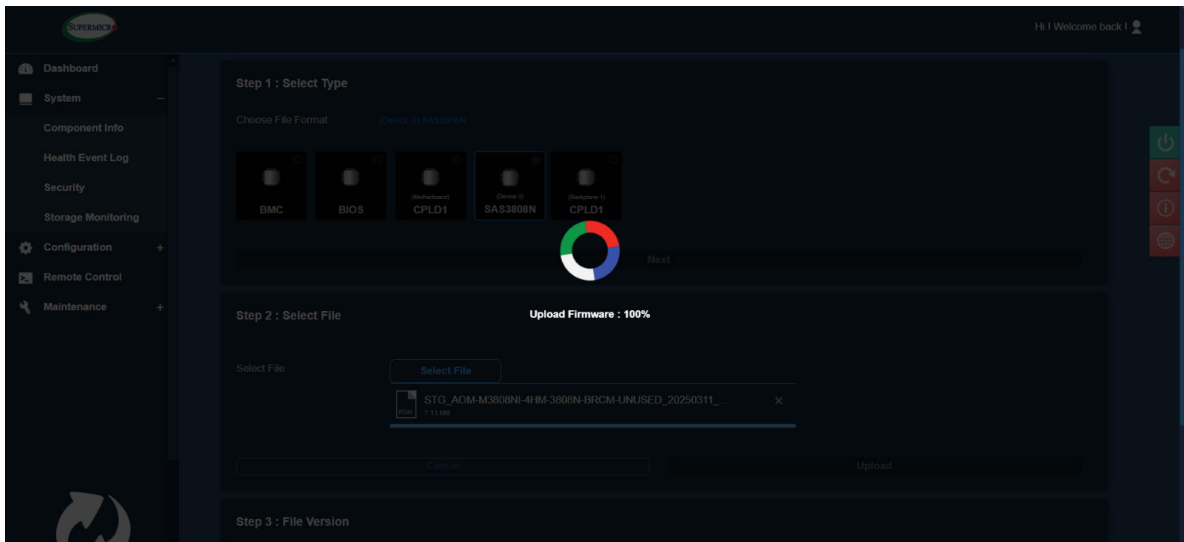


Figure 4-15: Upload Loading

7. This will make Step 3 available with the uploaded firmware file info listed. Review to ensure that it is the correct file version.
8. Click **Update** to proceed with updating the firmware. The update process might take a few minutes.

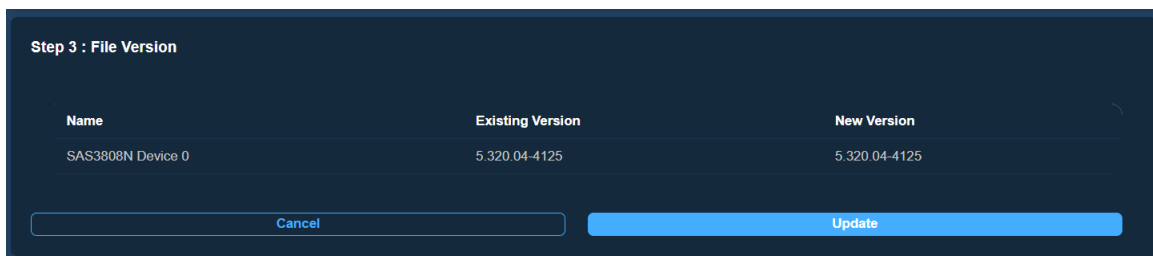


Figure 4-16: Firmware Update Step 3

To review if the firmware update is successful, take the following steps:

1. Select the **System** tab on the left navigation menu.
2. Select the **Storage Monitoring** tab from the System tab's drop-down submenu.

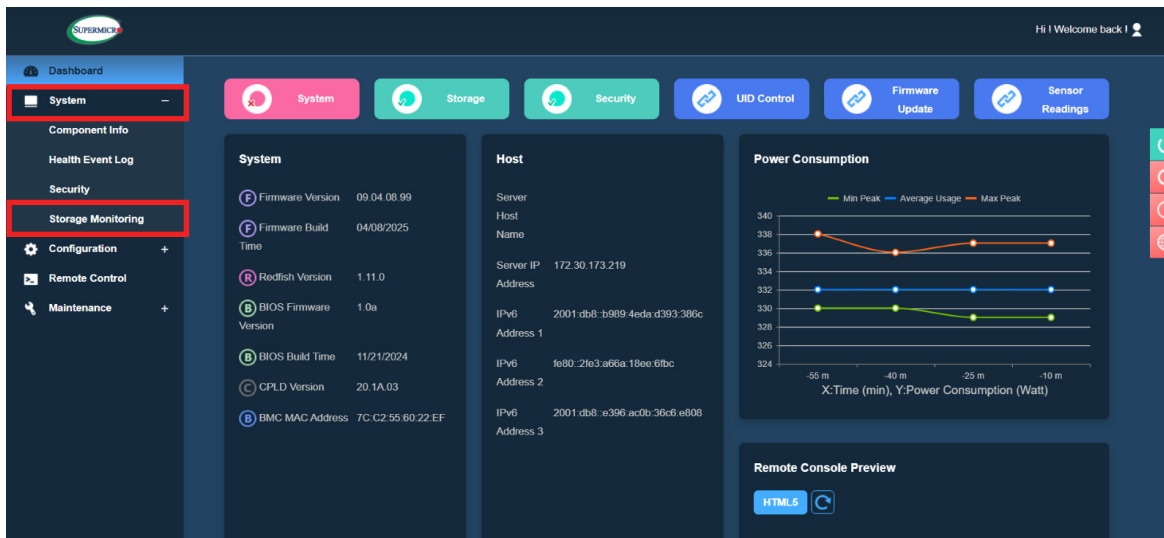


Figure 4-17: Dashboard Page System and Storage Monitoring Selected

3. Select the **Controller View** tab at the top of the page.
4. Be sure that you are on the correct device. It will be listed in the scroll-down menu below **Broadcom**. This will allow you to view device information.
5. Scroll to find the **View-Broadcom** item. It should display the new firmware file's version number.

Chapter 5

Drive Management

This chapter provides instructions on how to configure RAID using the BROADCOM <SAS 3808N> Configuration Utility and reference the FAQ regarding managing the AOM with BMC IPMI WebGUI or Broadcom 3rd Party Utility. If you do not wish to configure the RAID settings, you may skip this section and go directly to OS installation.

5.1 RAID Minimum Drive Requirements

The AOM-S3808NI-4NM add-on card supports up to two M.2 SSDs with RAID 0 and RAID 1. Use the table to determine the minimum number of hard drives needed to set up a RAID environment.

RAID	Minimum Hard Drives
RAID 0	2
RAID 1	2

5.2 Managing Physical Drive

Follow the steps below to manage the available physical drives through BIOS. Use the arrow keys to highlight your chosen option, and click <Enter> to select. Click <Esc> to exit an option menu or return to the previous page.

1. Navigate to Controller to enter the **Main Menu**.

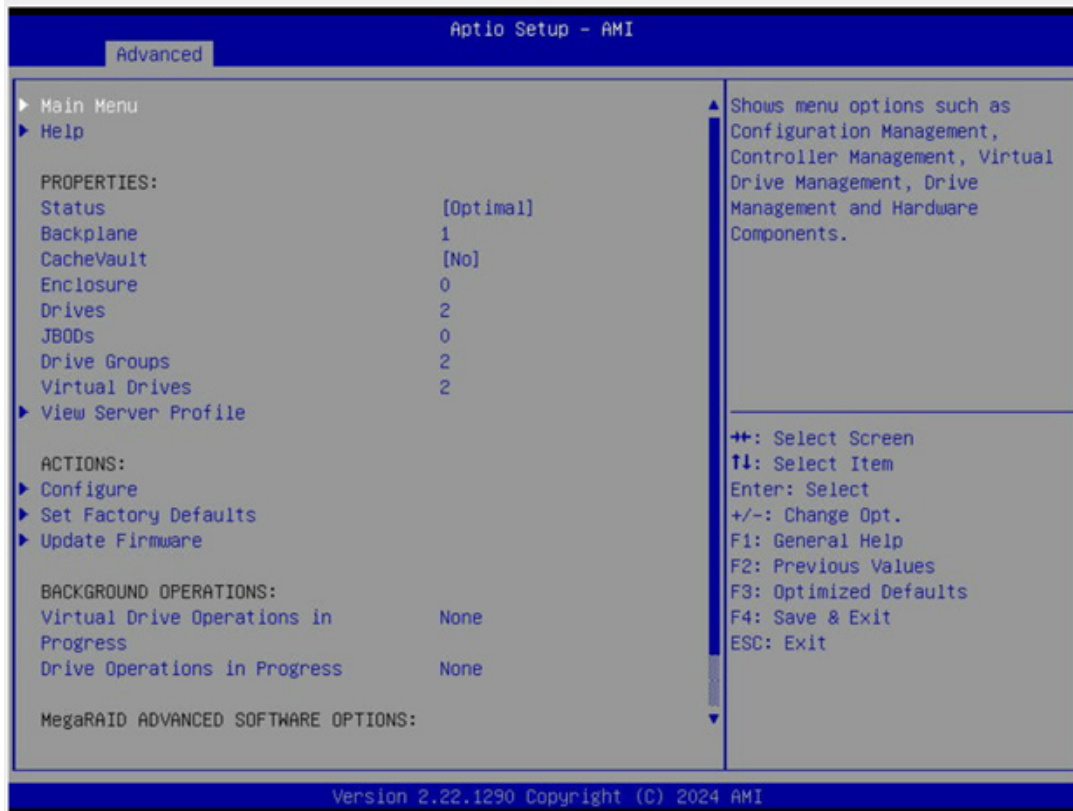


Figure 5-1: Main Menu Selected

2. Select **Drive Management**.



Figure 5-2: Drive Management Selected

3. Select a physical drive from the list. You will be able to use this menu to perform several operations (including **Rebuild** and **Initialize drive**), view basic properties of the drive, and navigate to view additional advanced properties.



Figure 5-3: Physical Drive Selected

5.3 Creating RAID

Follow the steps to create a virtual drive through BIOS. Use the arrow keys to highlight your chosen option, and click <Enter> to select. Click <Esc> to exit an option menu or return to the previous page.

1. Reset the system.
2. Press to enter the BIOS Setup Utility.
3. Select <Advanced> and **BROADCOM <SAS 3808N> Configuration Utility**.

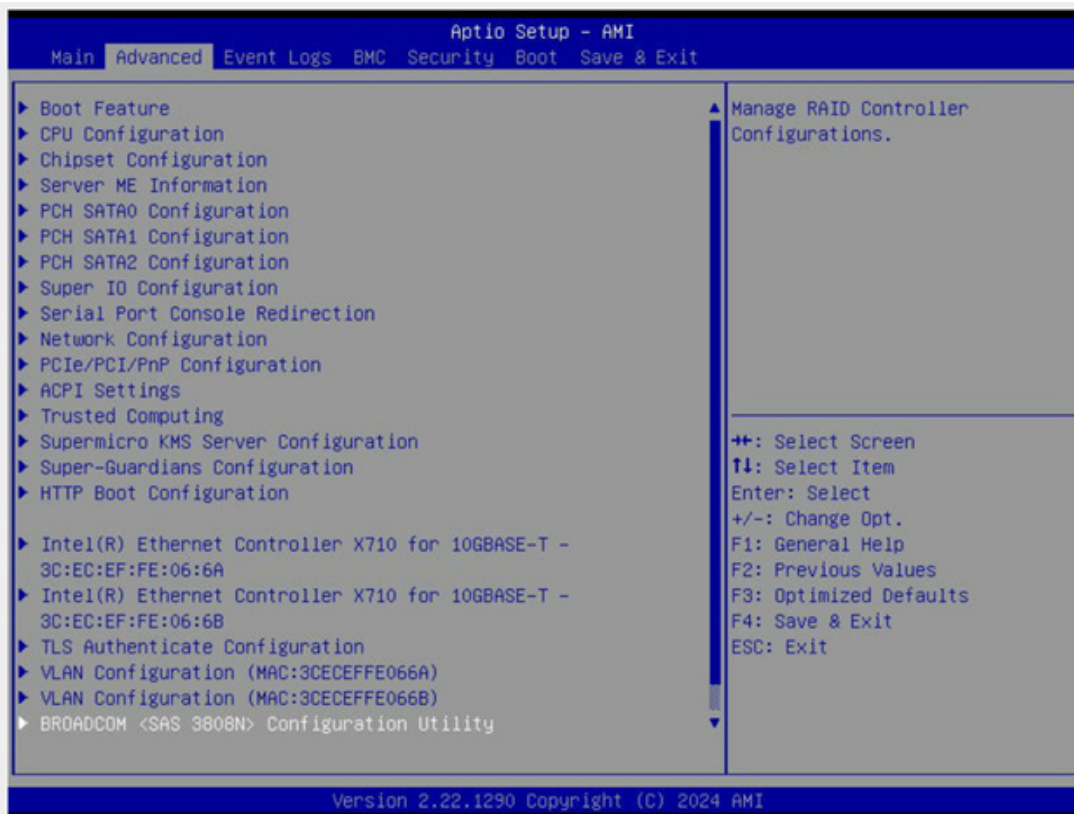


Figure 5-4: BROADCOM <SAS 3808N> Configuration Utility Selected

4. Enter the **Main Menu** page.

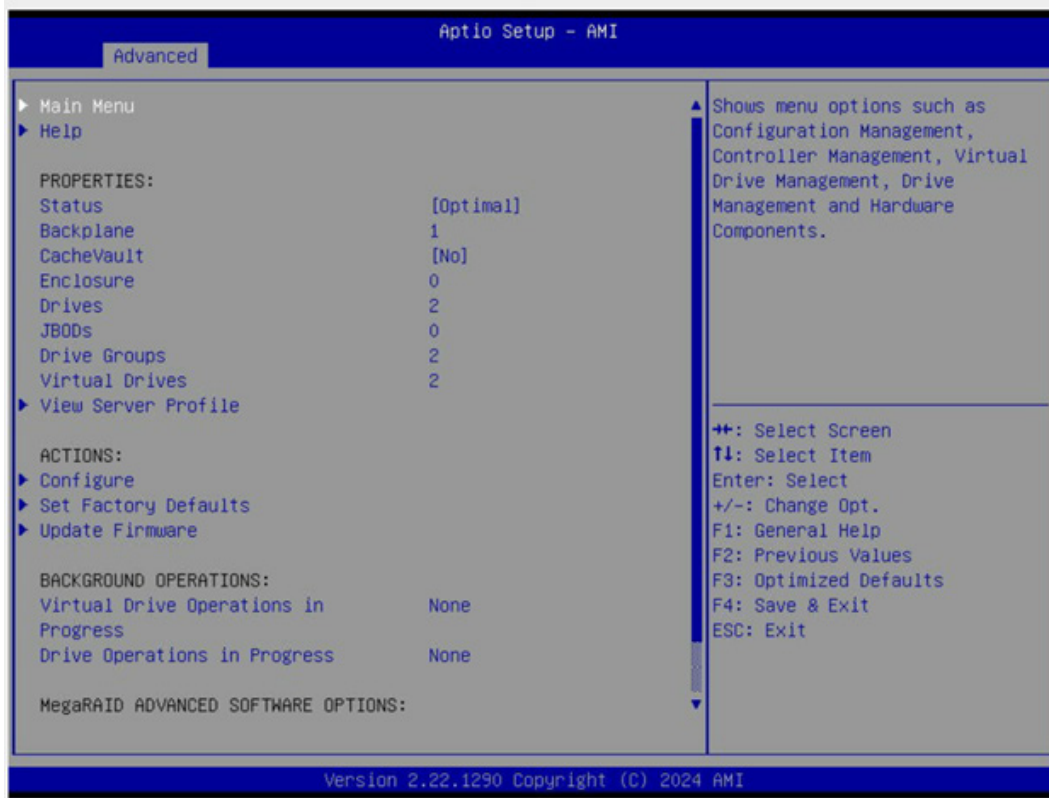


Figure 5-5: Main Menu Selected

5. Select **Configuration Management** from the Main Menu's submenu.

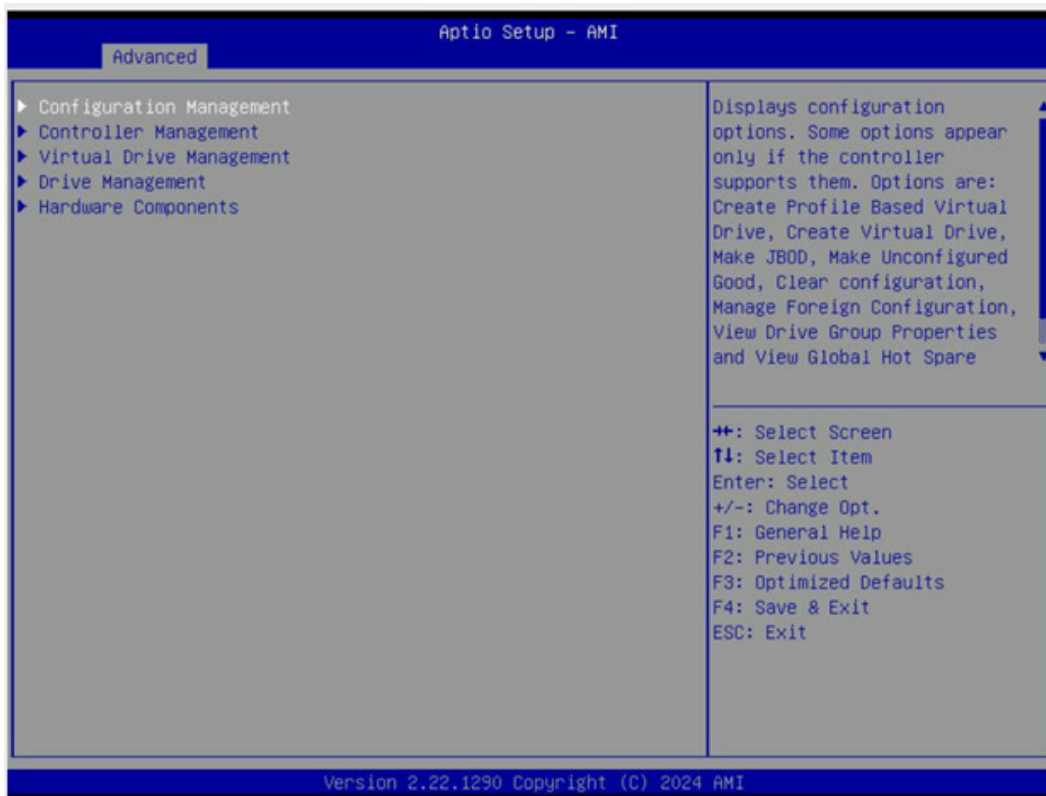


Figure 5-6: Configuration Management Selected

6. Select **Create Virtual Drive**.

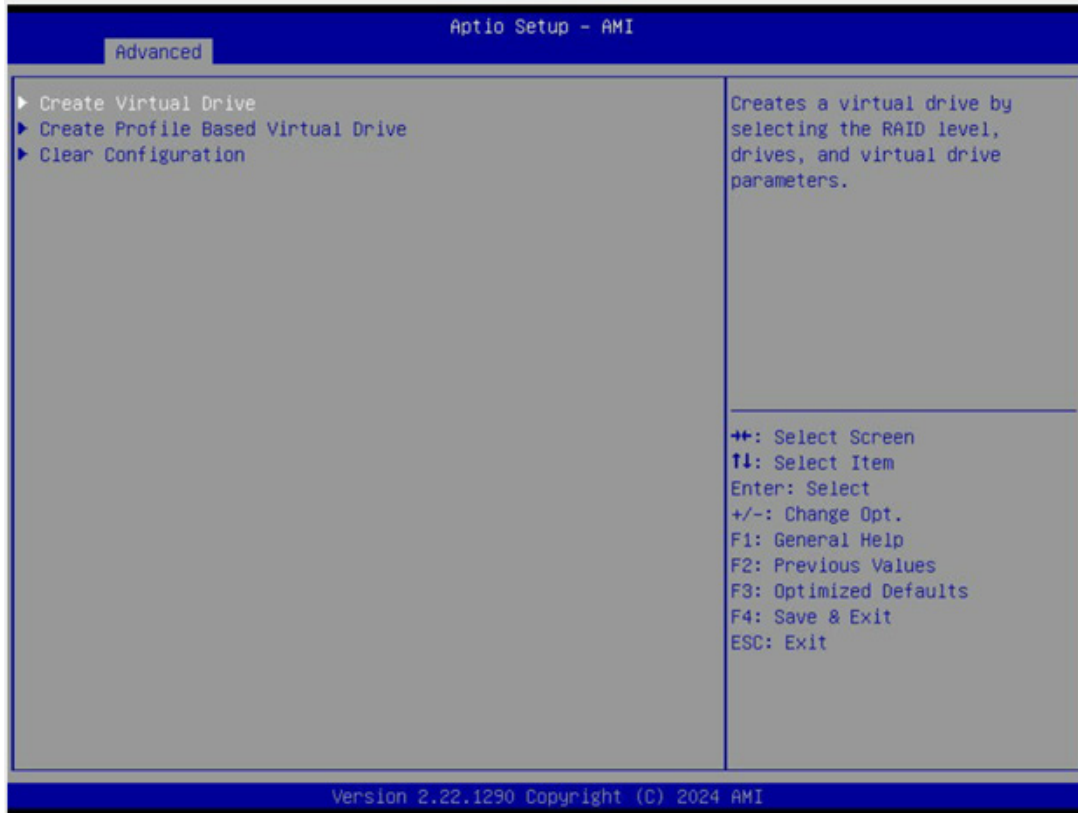


Figure 5-7: Create Virtual Drive Selected

7. On the **Create Virtual Drive** menu, navigate to **Select RAID Level**.
8. Select a RAID level.

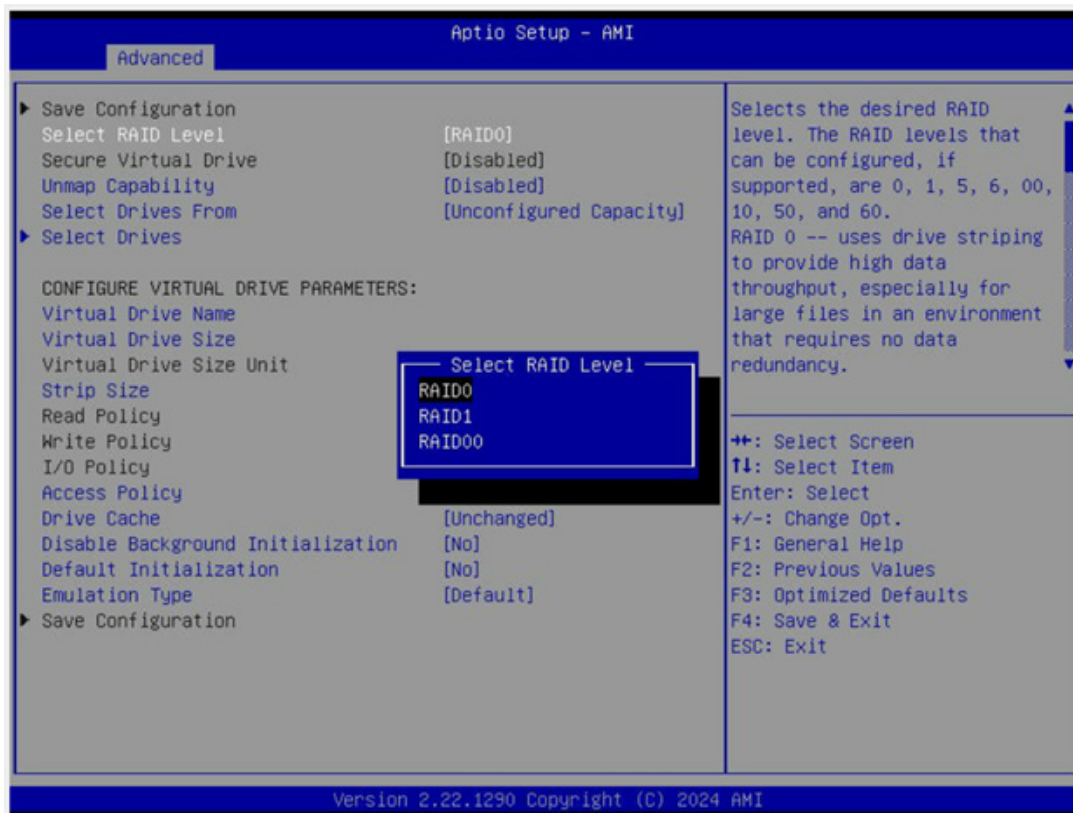


Figure 5-8: RAID Level Selected

9. Navigate to **Select Drives**.

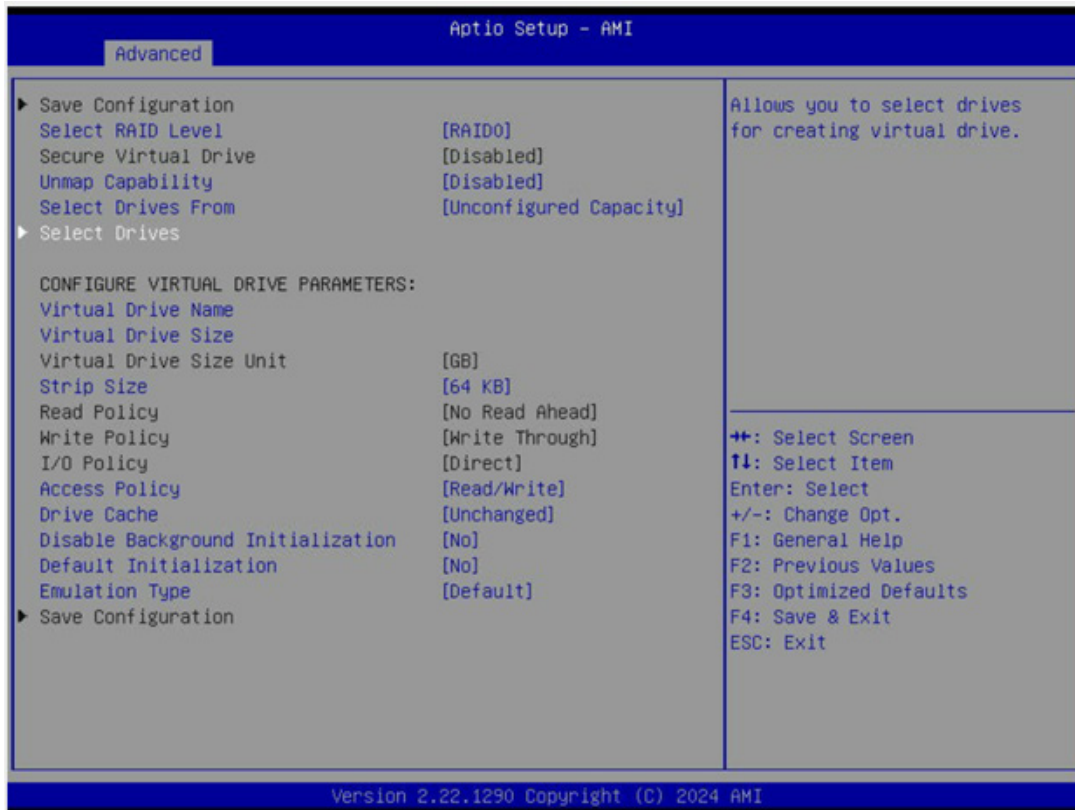


Figure 5-9: Select Drives Selected

10. On the **Select Drives** menu, select an unconfigured drive.
11. Choose **Enabled**.

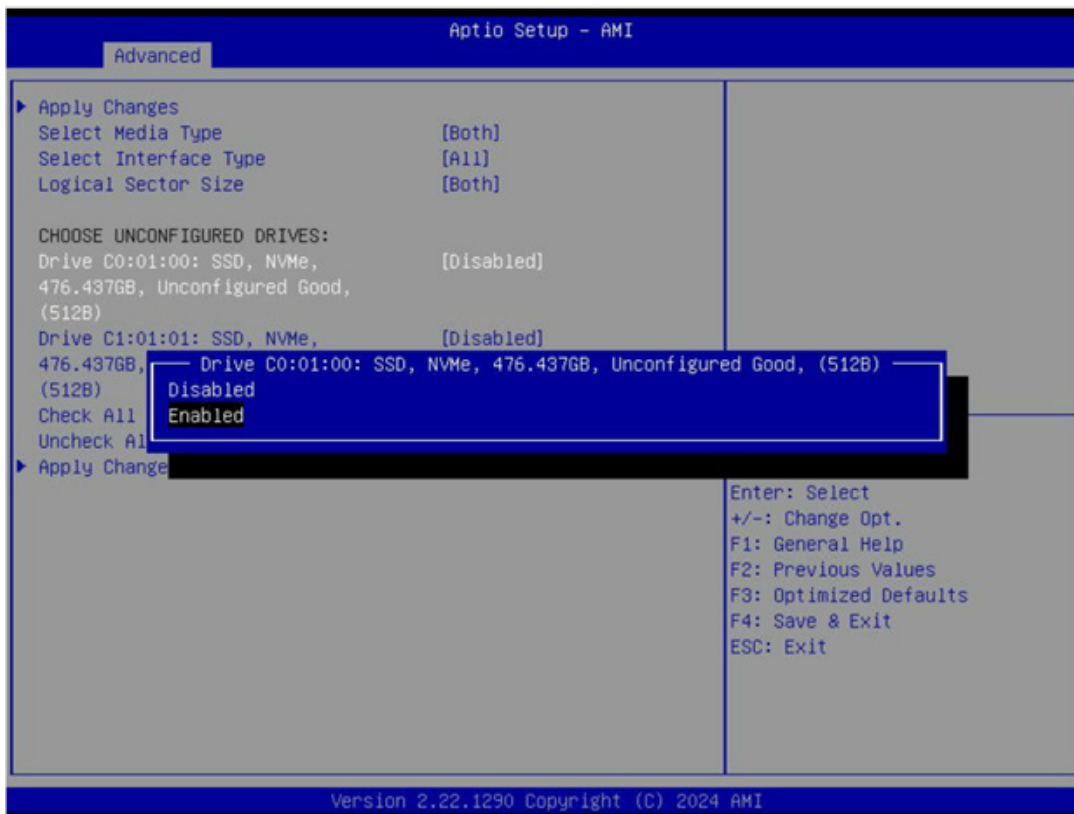


Figure 5-10: Enabled Selected

12. Select **Apply Changes**.

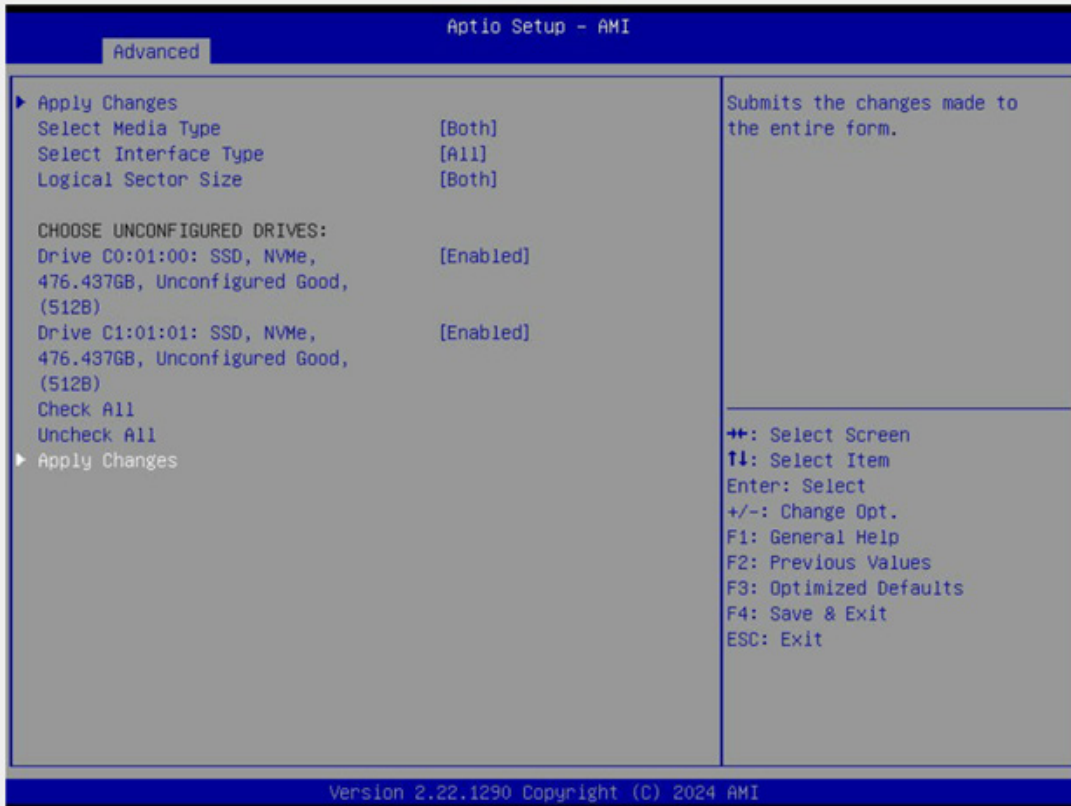


Figure 5-11: Apply Changes Selected

The virtual drives were saved successfully. You will get a prompt message confirming that the operation was performed successfully.



Figure 5-12: OK Option Selected

You will then need to save the system configuration. To do so, take the following steps:

1. On the **Create Virtual Drive** menu, navigate to **Save Configuration**.

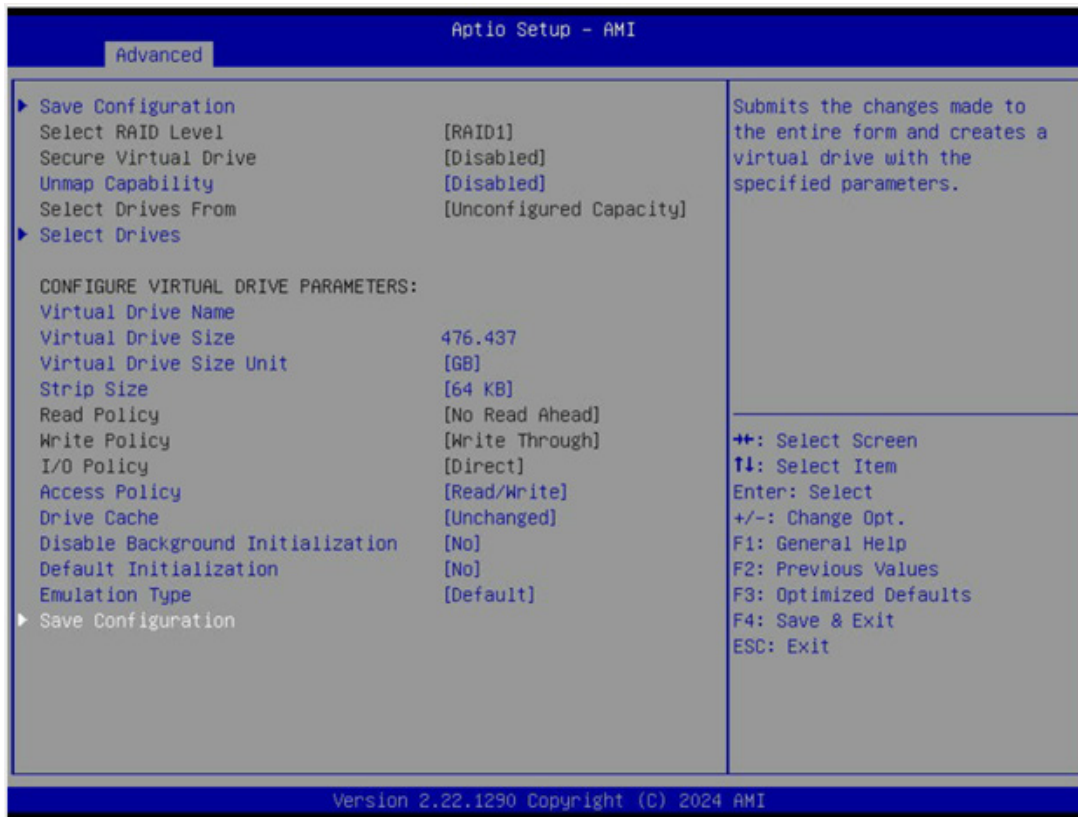


Figure 5-13: Save Configuration Selected

2. To proceed and make the **Yes** option available to you, first select **Confirm**.
3. Select **Enabled** to enable the **Yes** option.
4. Select **Yes**. If you do not want to proceed with changes, select **No**.



Figure 5-14: Confirm State Menu

5. Select **OK** to proceed.

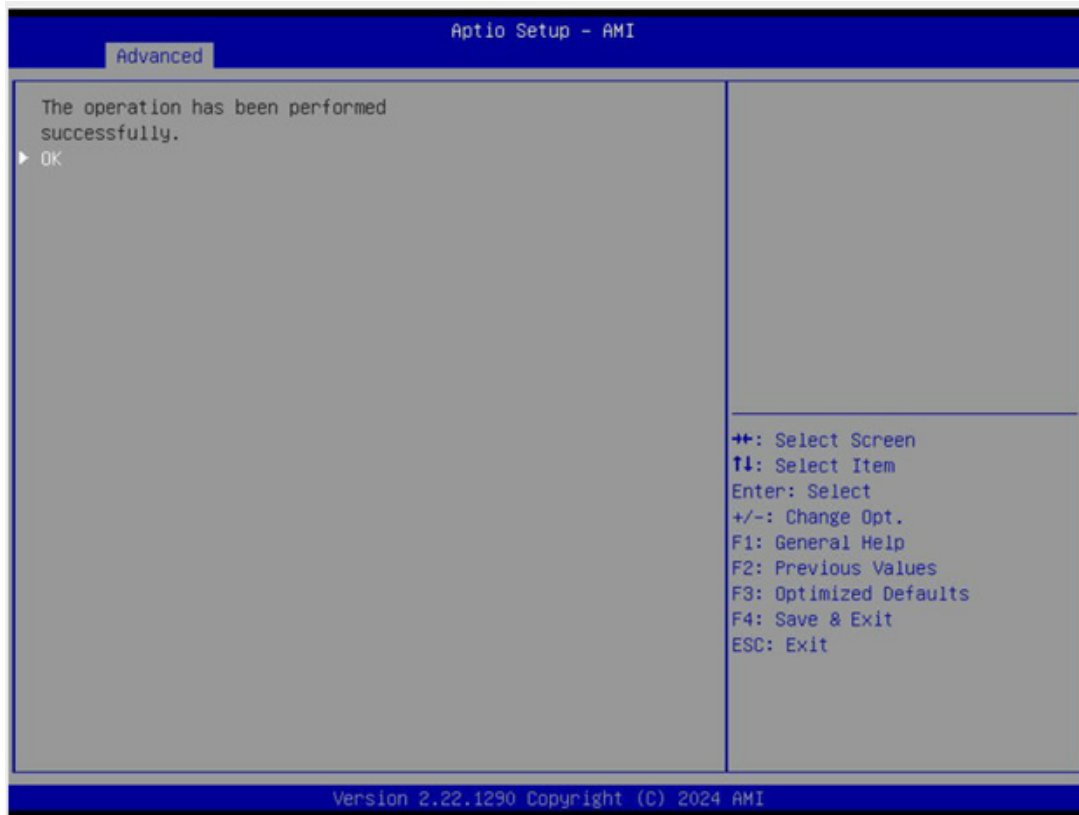


Figure 5-15: OK Selected

A prompt message will appear once the virtual drive creation is successful



Figure 5-16: Prompt Message

5.4 Deleting RAID in BIOS

Follow the steps to delete RAID through BIOS. Use the arrow keys to highlight your chosen option, and click <Enter> to select. Click <Esc> to exit an option menu or return to the previous page.

1. Navigate to the **Advanced** tab, where you can manage RAID Controller configurations.
2. Navigate to and select **BROADCOM <SAS 3808N> Configuration Utility**.

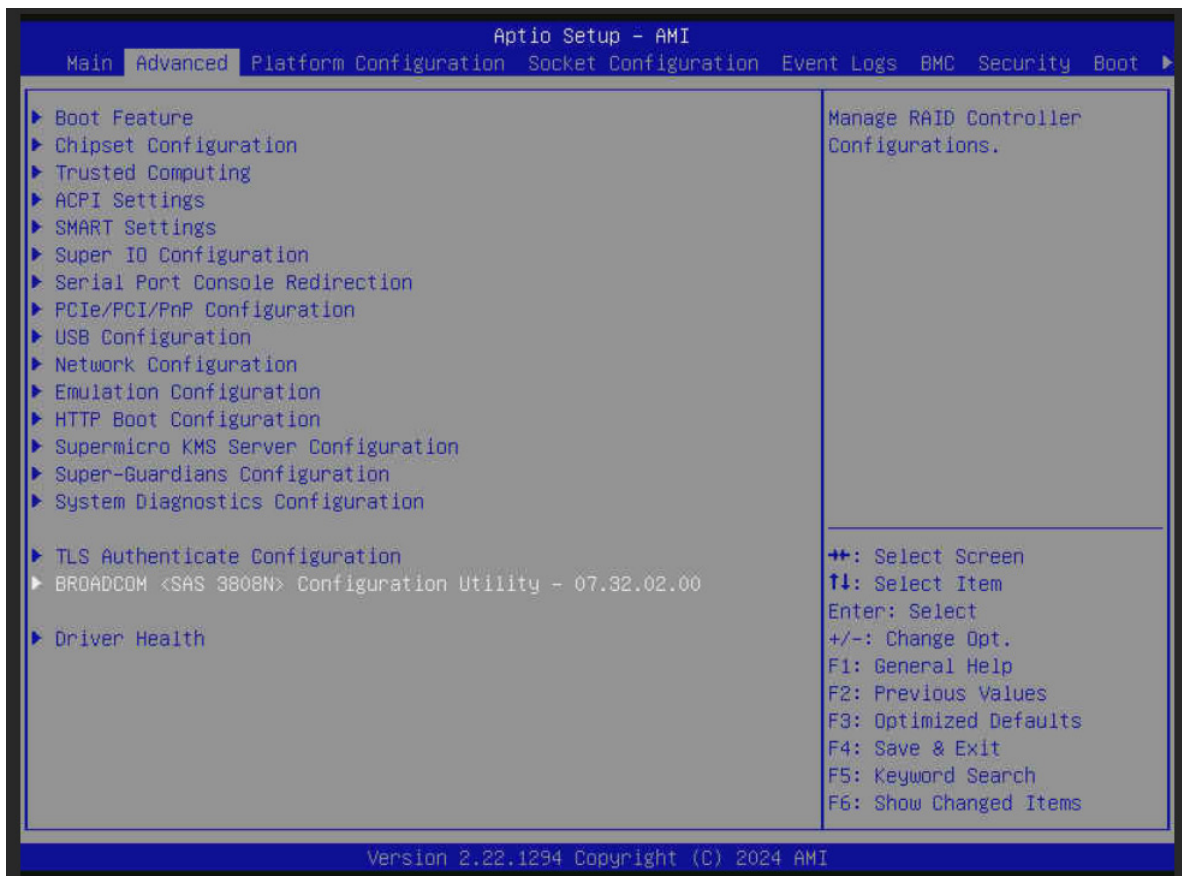


Figure 5-17: BROADCOM <SAS 3808N> Configuration Utility Selected

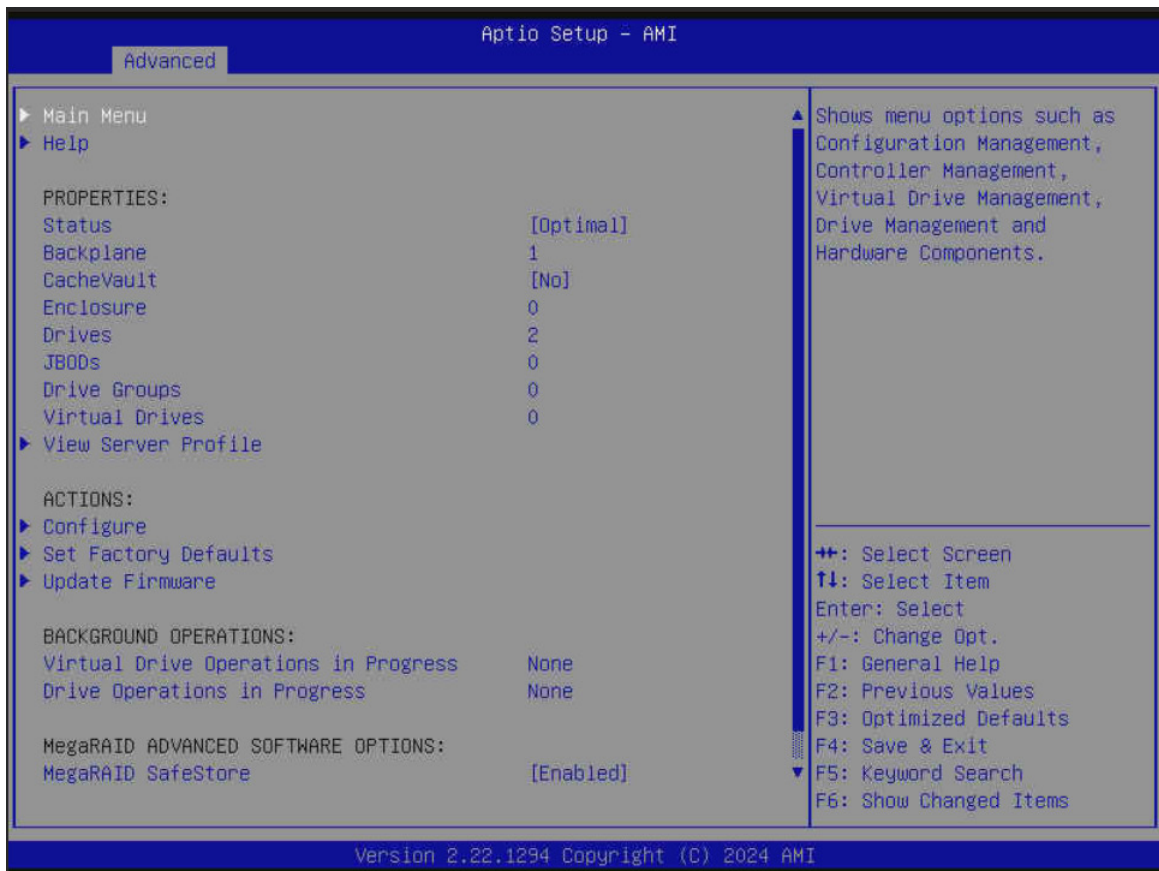
3. Select **Main Menu**.

Figure 5-18: Main Menu Selected

4. Select **Configuration Management**.

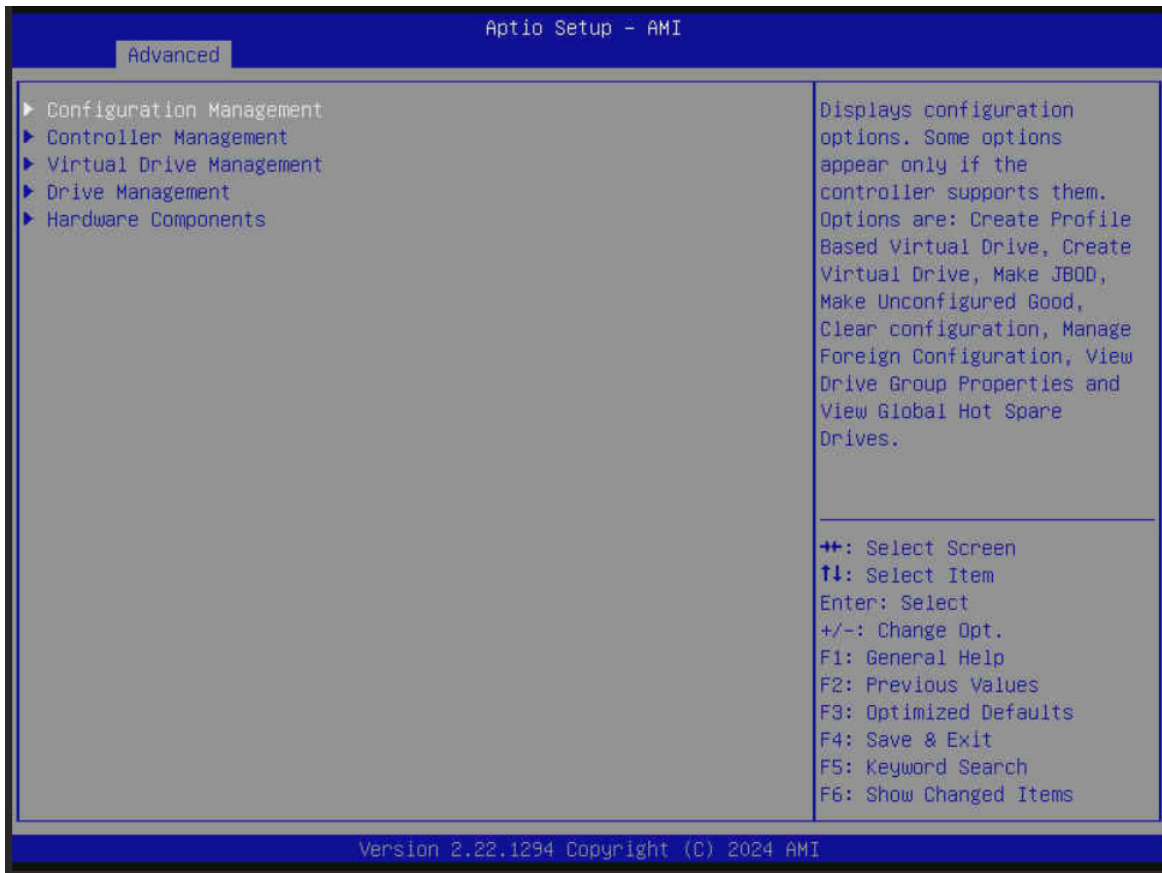
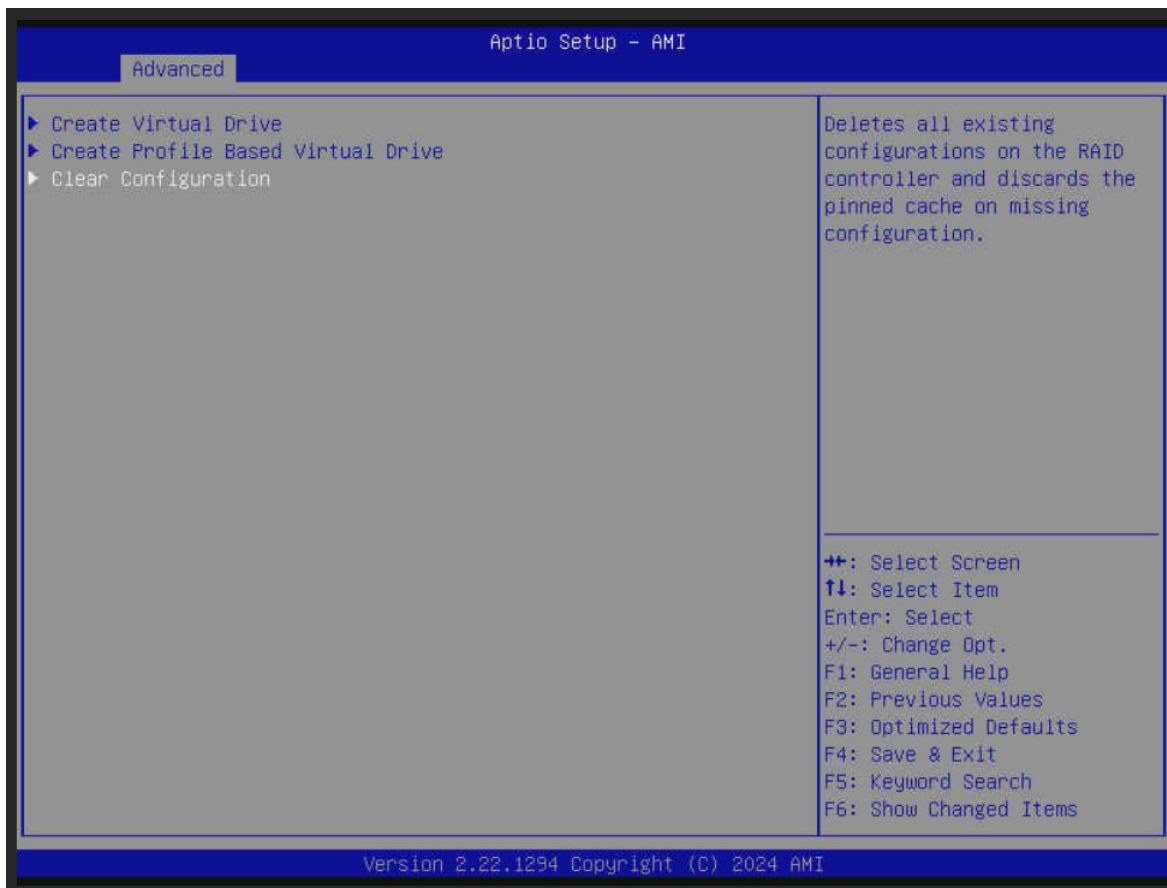


Figure 5-19: Configuration Management Selected

5. Select **Clear Configuration**.**Figure 5-20: Clear Configuration Selected**

- You will be presented with a confirmation window to delete all virtual drives, hot spare drives, pinned caches, and applicable JBODs attached to this controller. To proceed and make the **Yes** option available, select **Confirm** and ensure that it is set to **Enabled**.
- Once the **Confirm** option is enabled, select **Yes** to confirm the update. If you do not want to proceed with deleting all virtual drives, hot spare drives, pinned caches, and applicable JBODs attached to this controller at this time, select **No**.




Figure 5-21: Yes Option Selected

- You will be presented with a window confirming that the operation has been performed successfully. Select **OK** to proceed and return to the main menu.



Figure 5-22: OK Option Selected

 **Note:** Updates may take a few minutes to complete. Be sure you see the confirmation window *first* before rebooting the system.

The RAID has been deleted.

5.5 Managing JBOD State

This add-on card is based on a SAS 3808N iMR controller, and therefore supports a JBOD mode. Under certain conditions, such as when the add-on card is in JBOD mode, the drive state will then also change to JBOD. Use the arrow keys to highlight your chosen option, and press <Enter> to select. Click <Esc> to exit an option menu or return to the previous page. Take the following steps to enable/disable JBOD mode:

1. Navigate to **Controller** to enter the **Main Menu**.



Figure 5-23: Main Menu Selected

2. Select **Controller Management**.

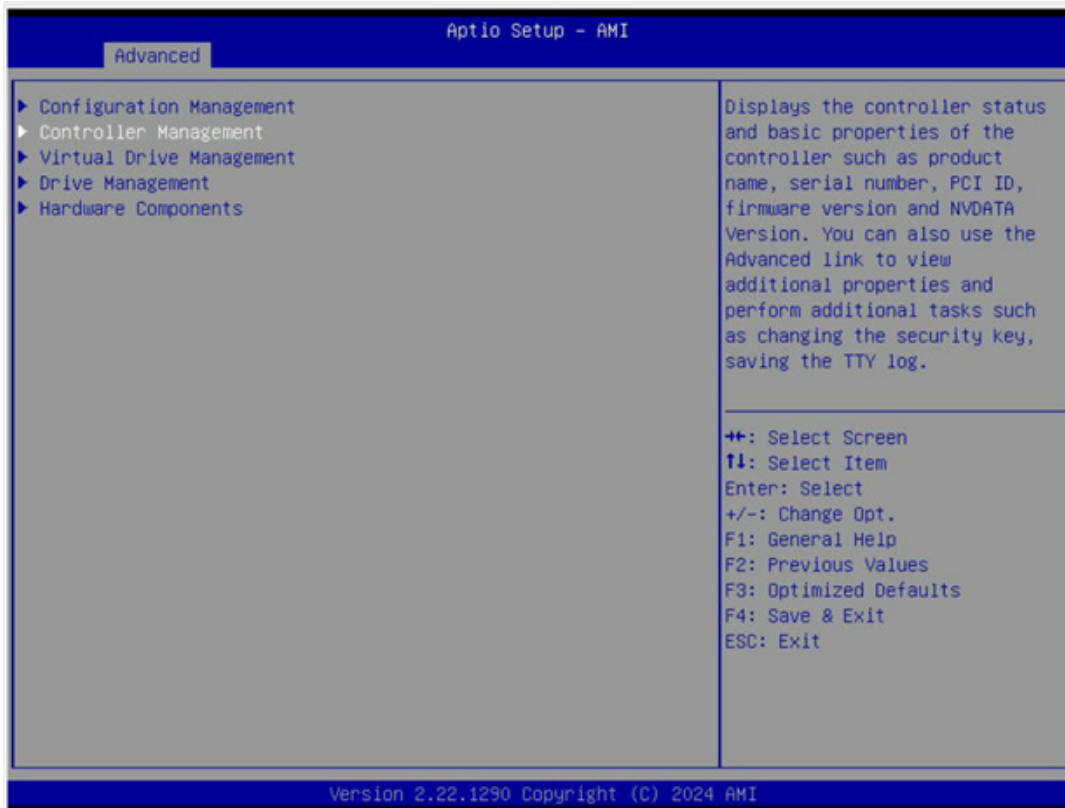


Figure 5-24: Controller Management Selected

3. Select **Advanced Controller Properties** to view and modify advanced controller properties.

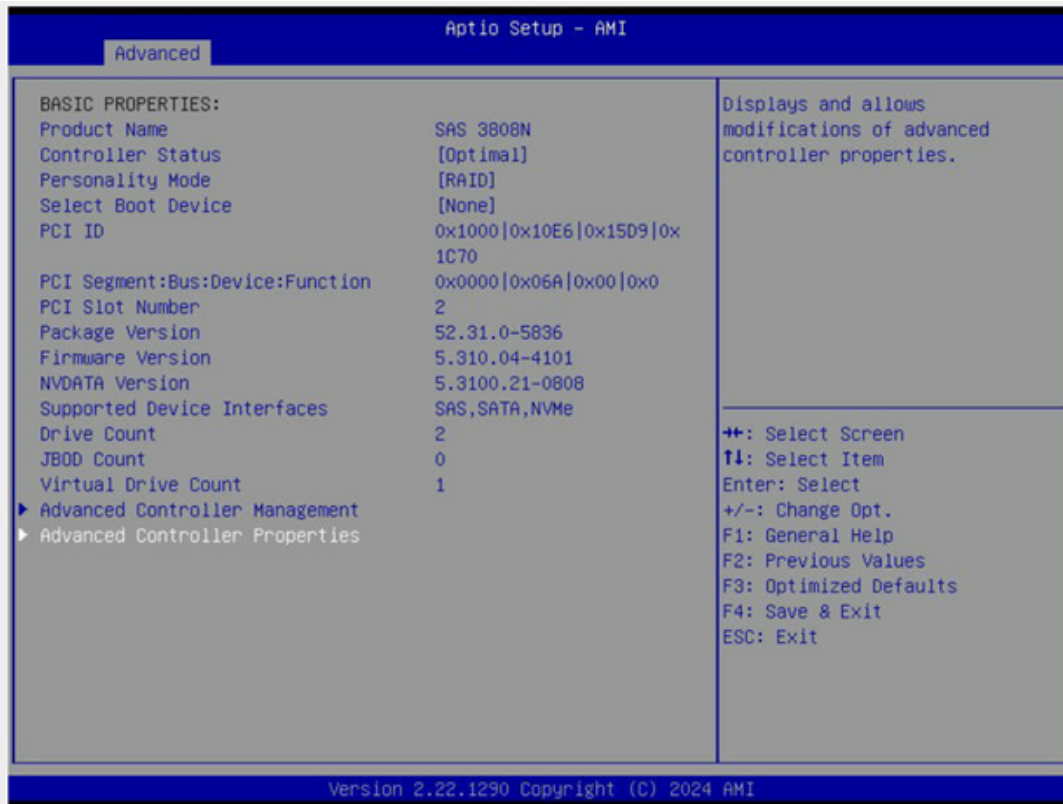


Figure 5-25: Advanced Controller Properties Selected

4. Select **JBOD Mode**.
5. Change the settings to **Disabled** or **Enabled**.

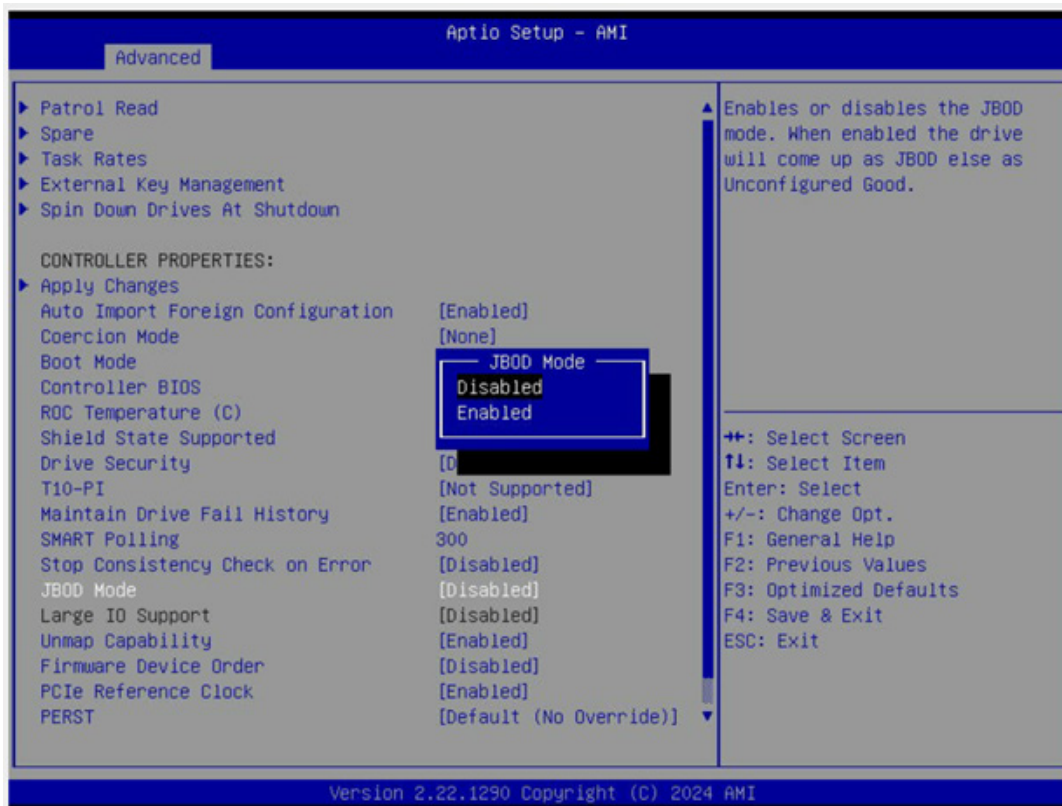



Figure 5-26: JBOD Mode State Menu

6. Confirm by selecting **Apply Changes**. If you do not want to proceed with changes, select **Cancel**.



Figure 5-27: Apply Changes Selected

 **Note:** You can also enable or disable JBOD Mode by entering the following StorCLI commands.

```
storcli /cx set JBOD=on
```

```
storcli /cx set JBOD=off
```

7. Once the JBOD mode is enabled for the add-on card, you can configure the JBOD by selecting **Configure** (under the **Advanced** tab).

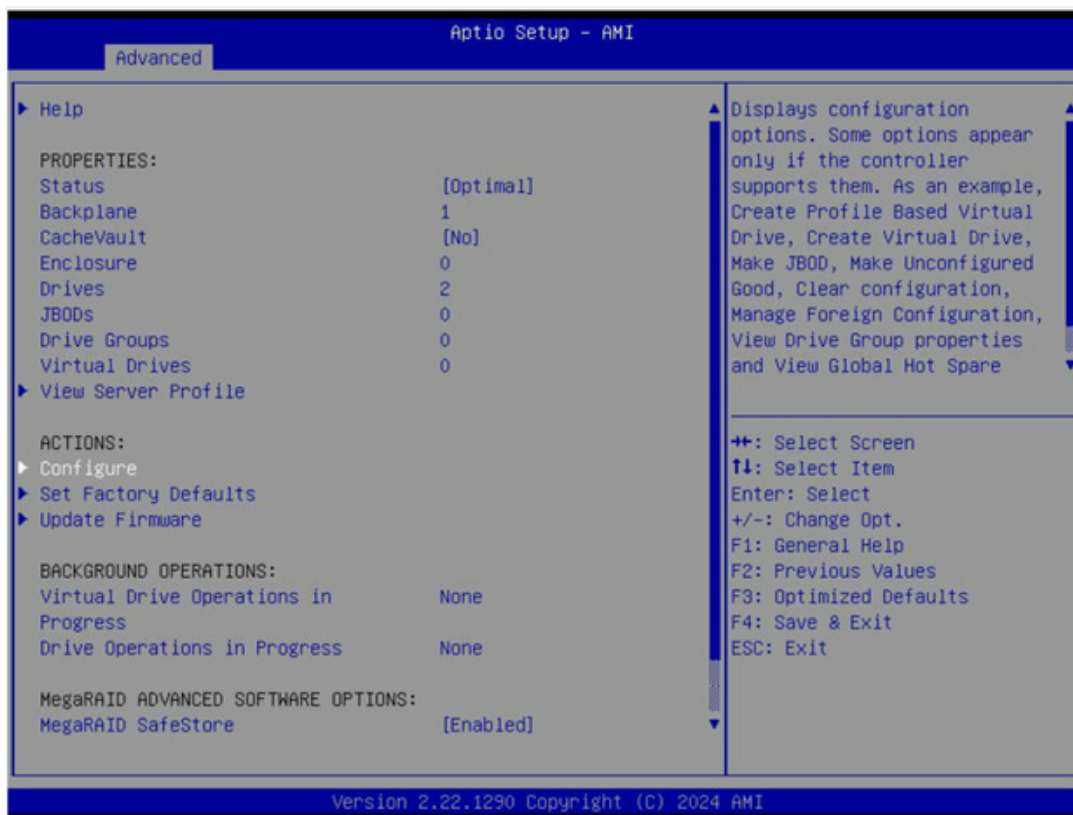


Figure 5-28: Configure Selected

8. Select **Make JBOD**.

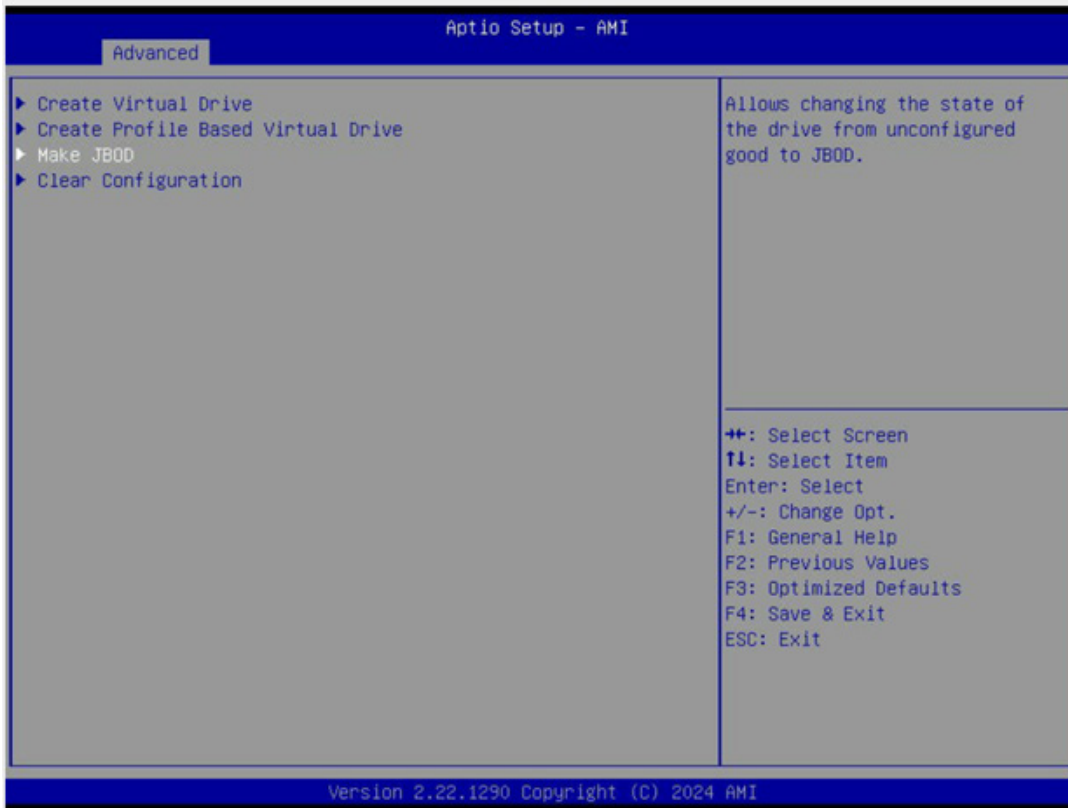


Figure 5-29: Make JBOD Selected

9. Select drive.

10. Choose **Enabled**.

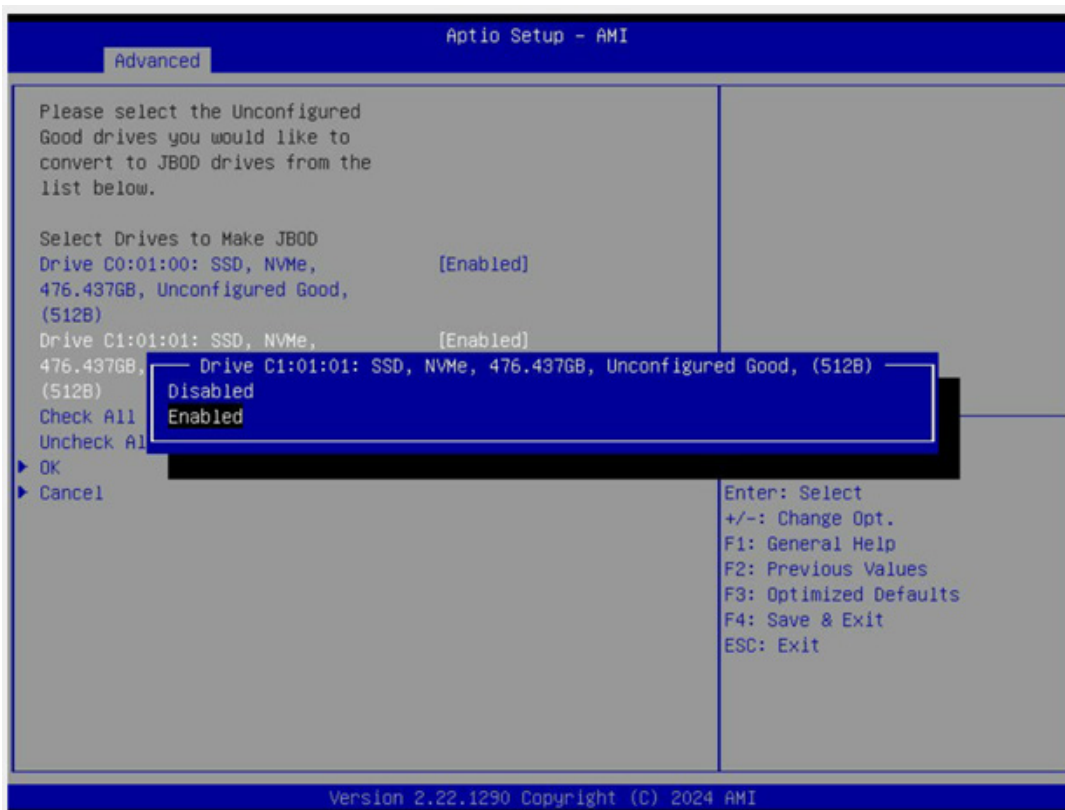


Figure 5-30: Enabled Selected

11. Select **OK** to commit to the changes.

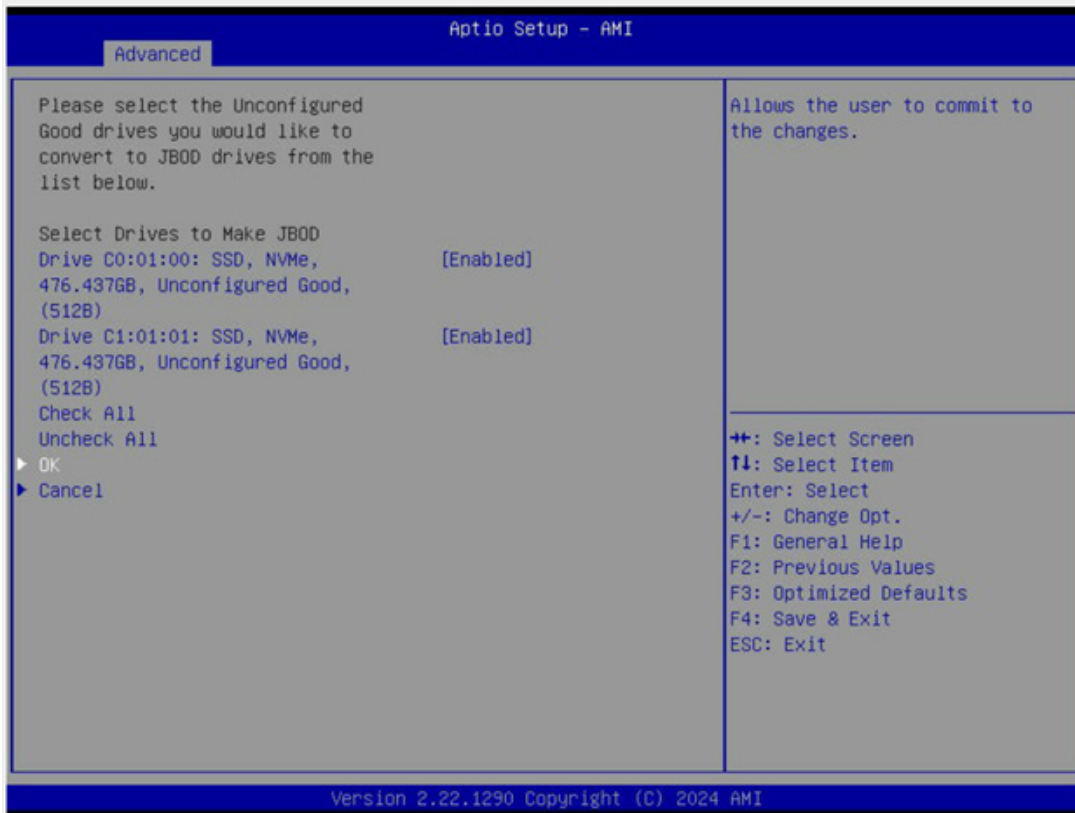


Figure 5-31: OK Option Selected

12. Select **OK** to proceed.



Figure 5-32: OK Option Selected

The drives will display the JBOD state in the listings.



Figure 5-33: Drive Selected

5.6 Managing Unconfigured Good State

Under certain conditions, such as when the add-on card has been in JBOD mode, the drive state will change to JBOD. To build a Virtual Drive (VD) or RAID, the drive state must be reset to **Unconfigured Good**. To do so, JBOD Mode must first be disabled. Follow these steps to change the drive state to **Unconfigured Good**. Use the arrow keys to highlight your chosen option, and press <Enter> to select. Click <Esc> to exit an option menu or return to the previous page.

1. Navigate to **Controller** to enter the **Main Menu**.
2. Select to enter **Drive Management**, which will list all drives. When **JBOD Mode** is enabled, the drive state will be **JBOD**.



Figure 5-34: Drive Management Selected



Figure 5-35:

3. Once the drive is chosen, select **Operation**. The options will include **Select operation**, **Start Locate**, **Stop Locate**, **Make Unconfigured Good**, and **Make Bootable Drive**.
4. Select **Make Unconfigured Good**.

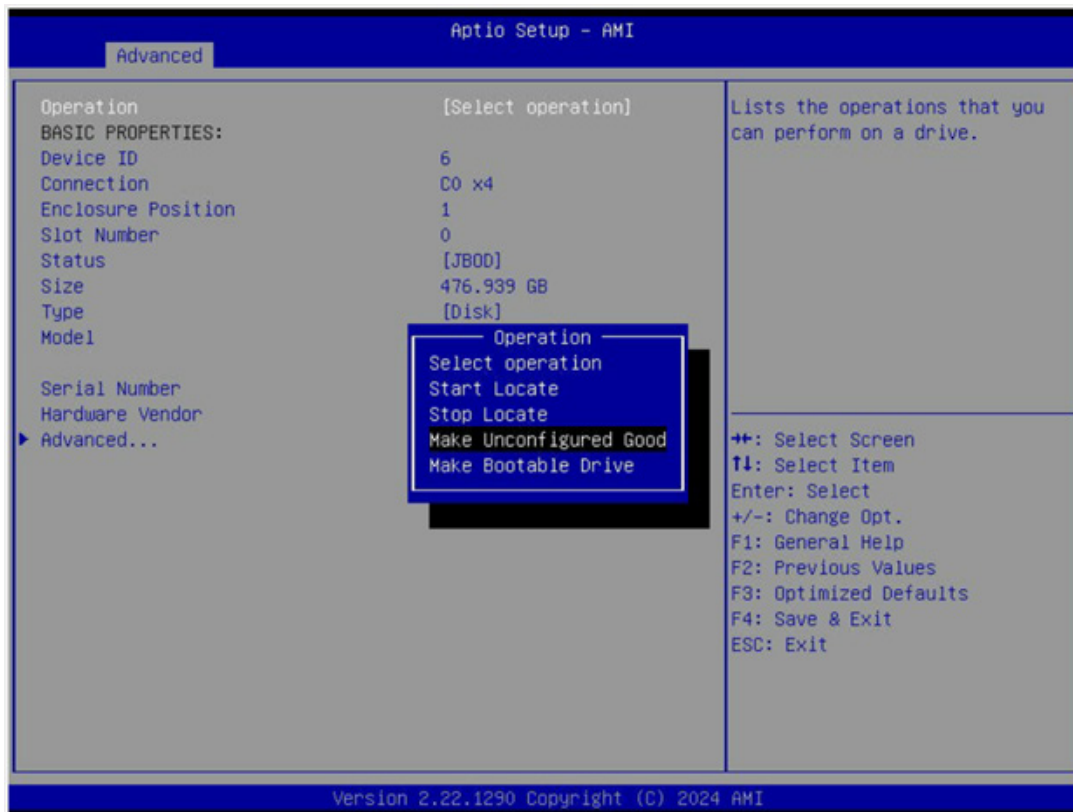


Figure 5-36: Make Unconfigured Good Selected

5. Select **Go**.



Figure 5-37: Go Option Selected

- You will be presented with a warning that any existing data in the JBOD drive will be lost if you proceed. To proceed and make the **Yes** option available to you, first select **Confirm**.
- Select **Enabled** to enable the **Yes** option.
- Select **Yes**. If you do not want to proceed with changes, select **No**.



Figure 5-38: Yes Option Selected



Note: You can also set the drive state as Unconfigured Goods by entering the following StorCLI command.

```
storcli /cx/ex/sx set good force
```

- Select a drive.

Chapter 6

Secure Boot Settings

Secure boot is a Unified Extensible Firmware Interface (UEFI) feature that ensures boot loaders are digitally signed and validated. This chapter provides instructions on how to enable the secure boot features. Use the arrow keys to highlight your chosen option, and press <Enter> to select. Click <Esc> to exit an option menu or return to the previous page.

6.1 Boot Mode Select Feature

1. Press during system boot to enter the **BIOS Setup Utility**.
2. Navigate to the **Boot** tab.
3. Select **Boot Mode Select**. The options are **LEGACY**, **UEFI**, and **DUAL**.
4. Set **Boot Mode Select** to **UEFI**.
5. For the changes to take effect, press <F4> to save the settings.
6. Exit the BIOS Setup Utility.

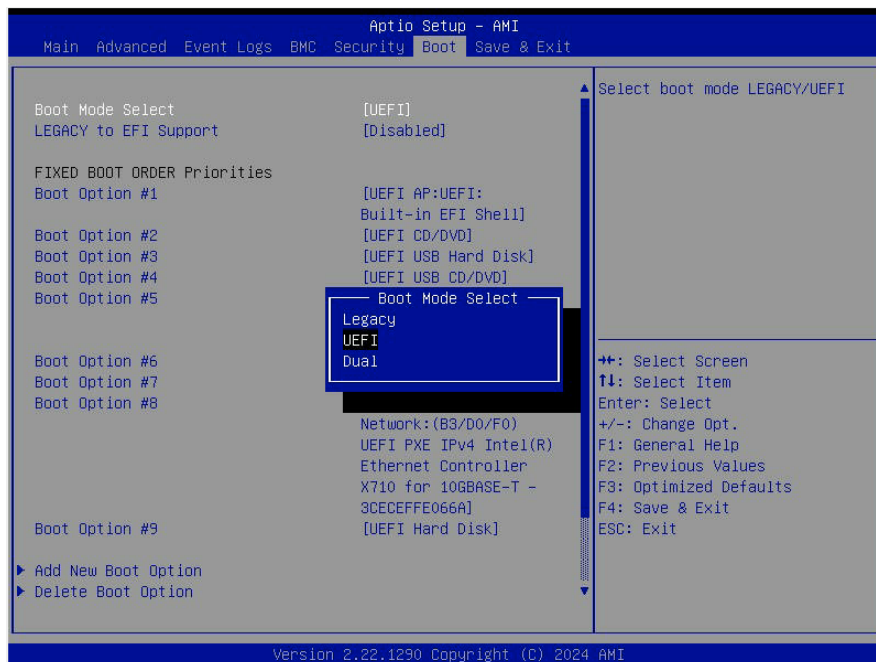


Figure 6-1: Boot Mode Select Menu

6.2 Secure Boot/Secure Boot Mode/CSM Support Features

1. Press during system boot to enter the **BIOS Setup Utility**.
2. Navigate to the **Security** tab.

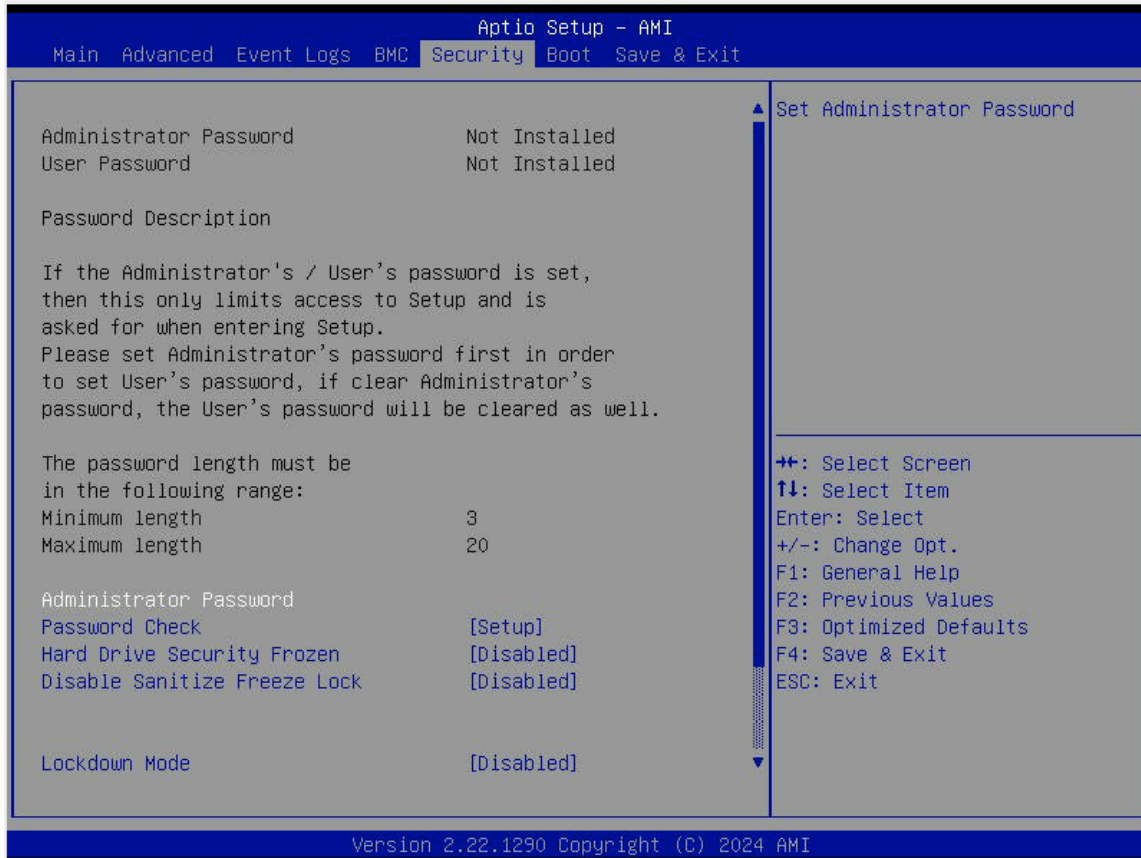


Figure 6-2: Security Tab

3. Select **Secure Boot** to access the menu items.

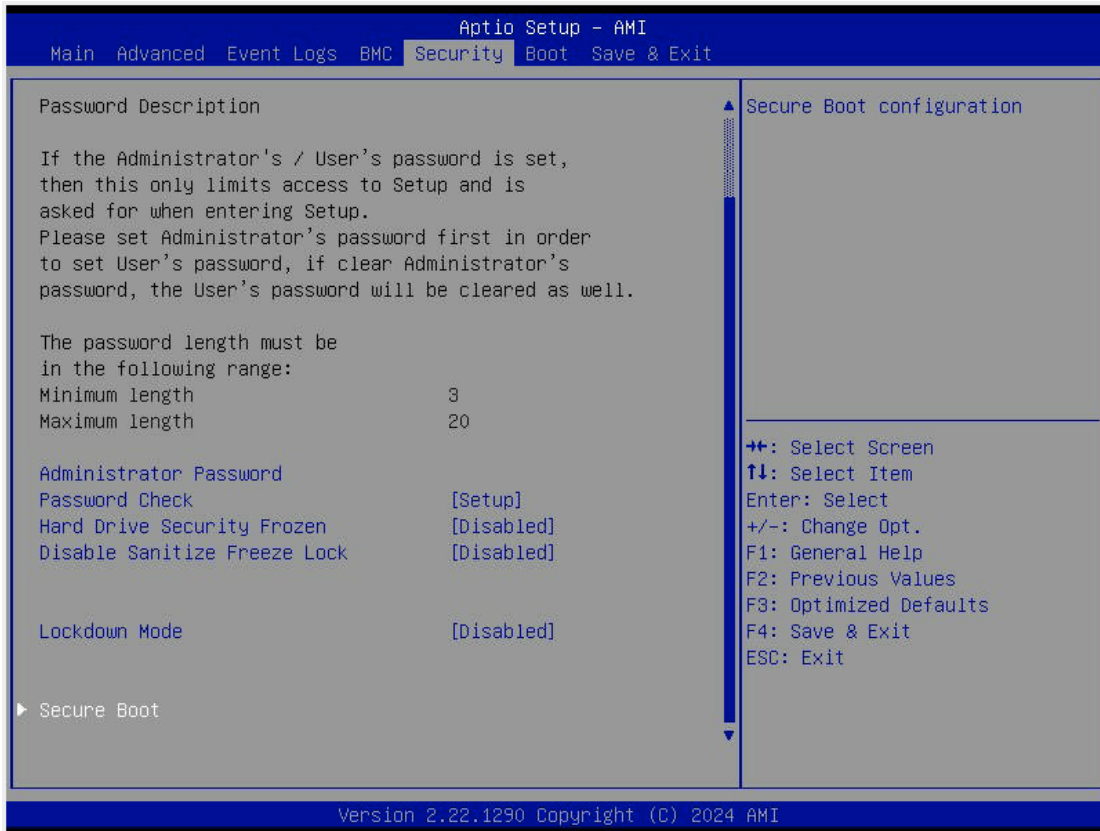


Figure 6-3: Secure Boot Selected

Secure Boot

This feature is available when the Platform Key (PK) is pre-registered, where the platform operates in the User mode and Compatibility Support Module (CSM) support is disabled in the BIOS Setup Utility. Select Enabled for secure boot flow control. The options are **Disabled** and Enabled.



Figure 6-4: Secure Boot Disabled Selected

Secure Boot Mode

Use this feature to set the secure boot mode. The options are Standard and **Custom**. Select Standard to load the manufacturer's default secure variables. Select Custom to change the image execution policy and to manage secure boot keys.

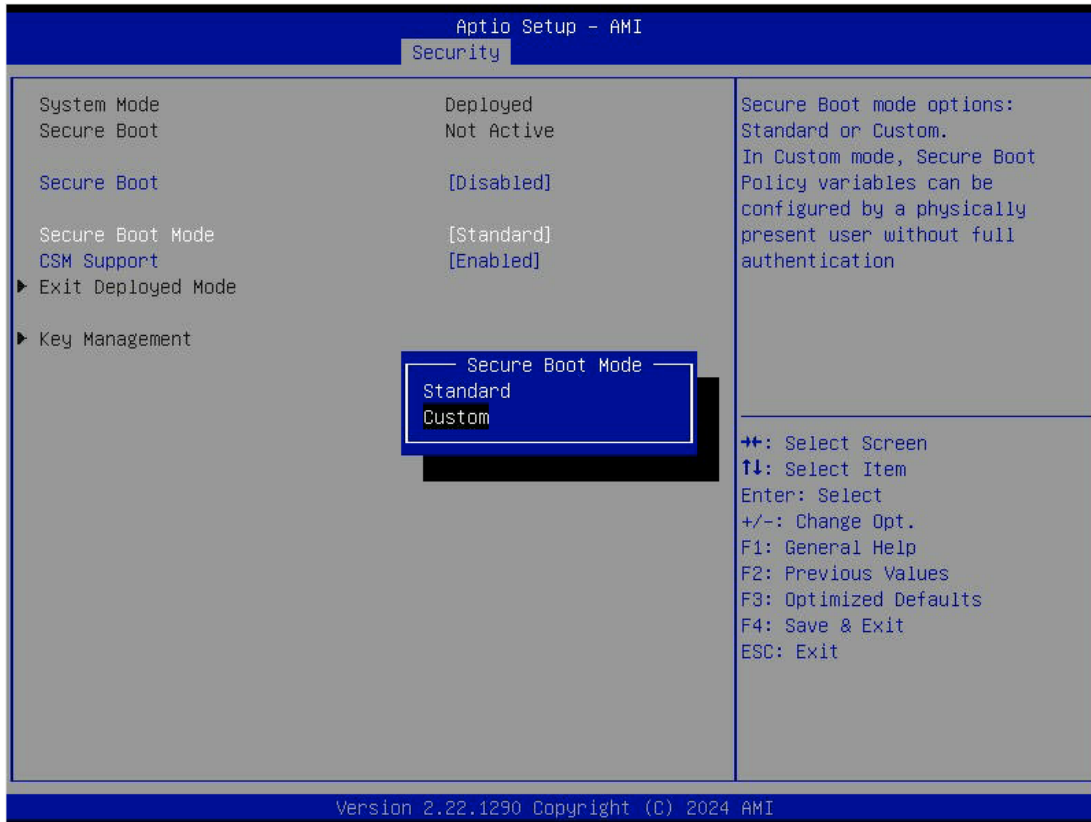


Figure 6-5: Secure Boot Custom Selected

CSM Support

Select Enabled for legacy Compatibility Support Module (CSM) support, which will provide compatibility support for traditional legacy BIOS used for system boot.

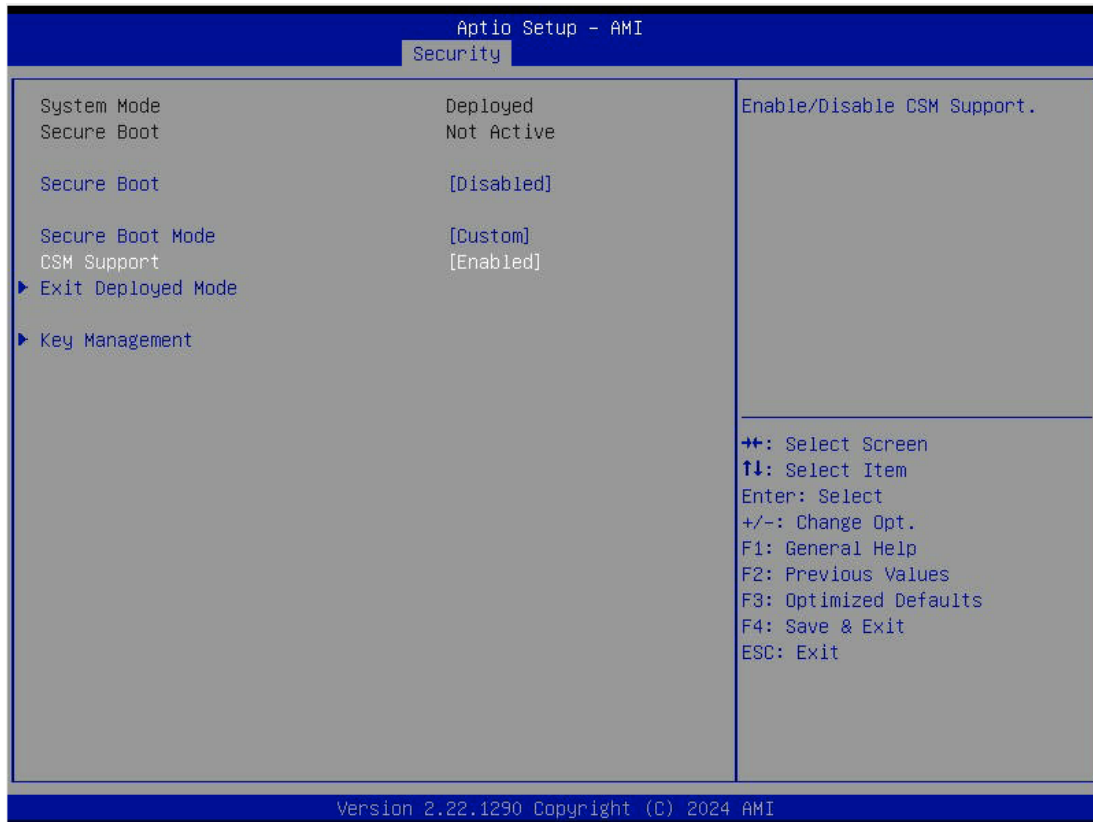


Figure 6-6: CSM Support Selected

The options are Disabled and **Enabled**.

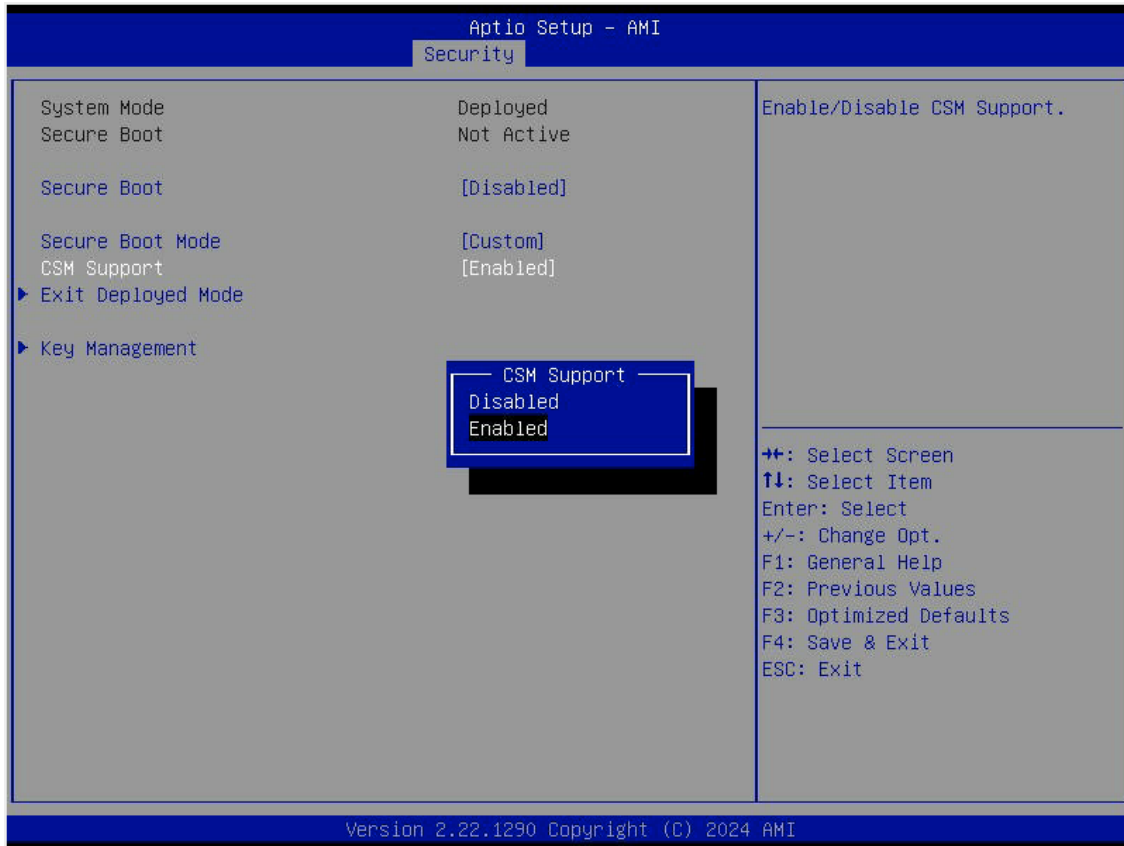


Figure 6-7: CSM Support Enabled Selected

6.3 Secure Boot Settings

To have secure boot support, follow the steps below:

1. Set **Secure Boot Mode** to **Standard**.

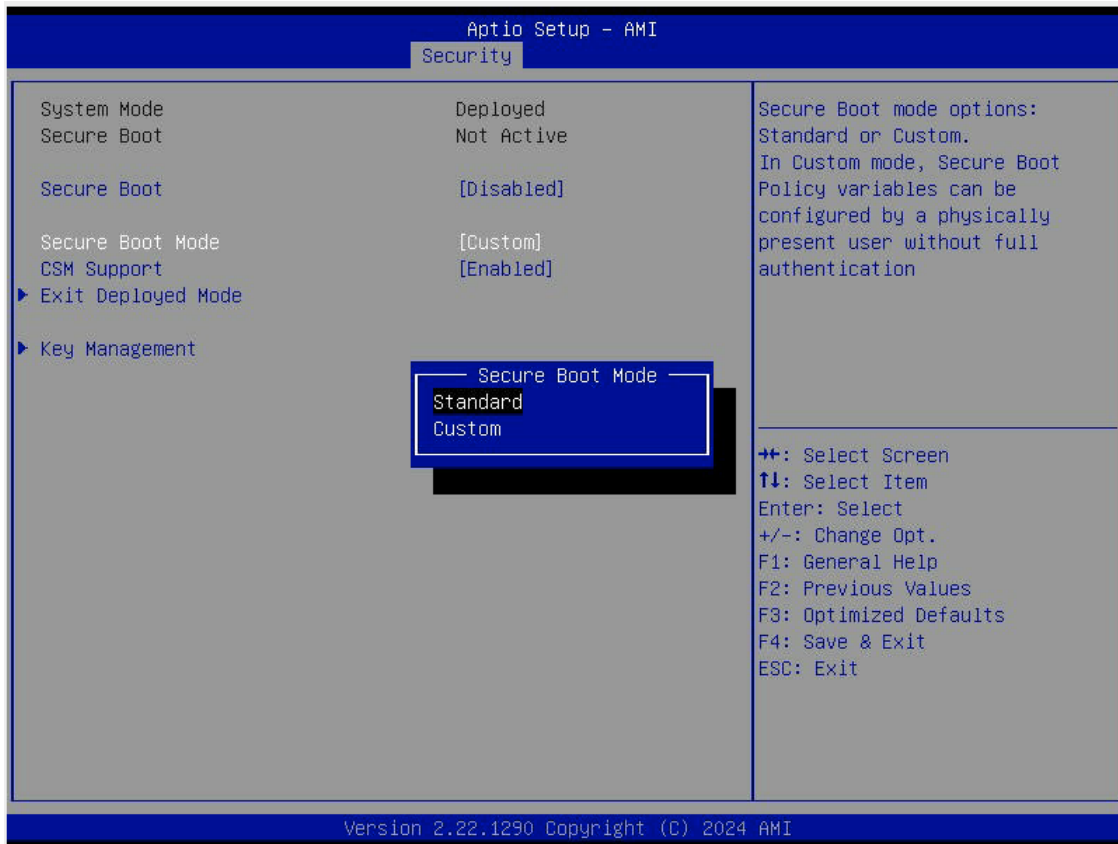


Figure 6-8: Secure Boot Mode Standard Option Selected

Press **Yes** to install factory default keys as needed.

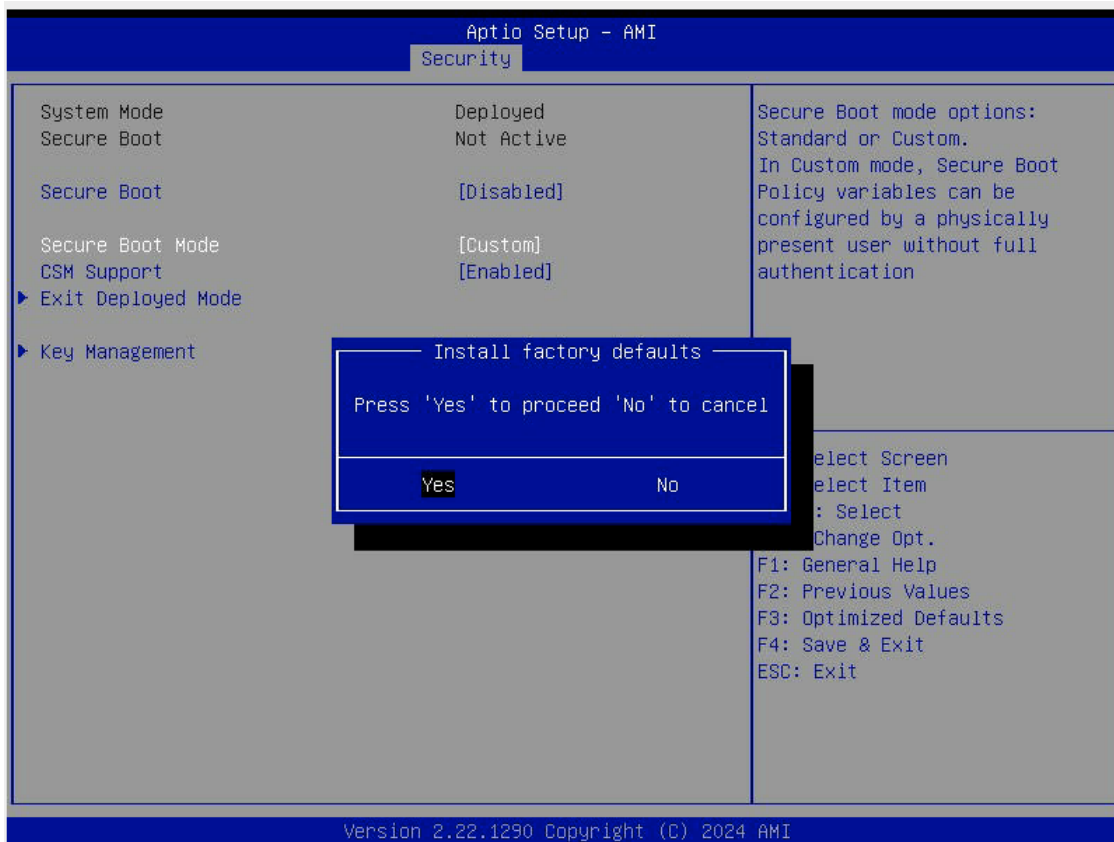



Figure 6-9: Confirming to Install Factory Defaults

 **Note:** The Key Management menu will become unavailable when Secure Boot Mode is set to Standard.

2. For the changes to take effect, press **<F4>** to save the settings.
3. Exit the **BIOS Setup Utility**.
4. Press **** during system boot to enter the **BIOS Setup Utility**.

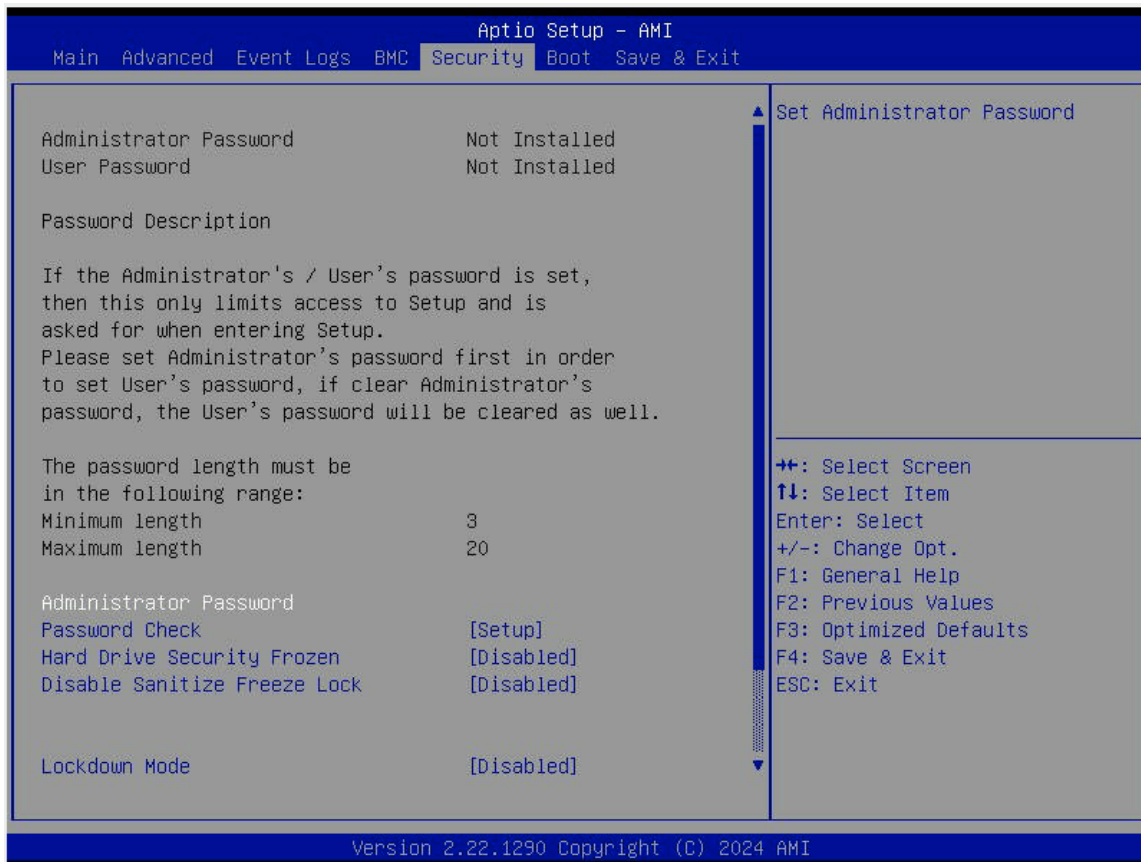
5. Navigate to the **Security** tab.

Figure 6-10: Security Tab Main Menu

6. Enter the **Secure Boot** menu.

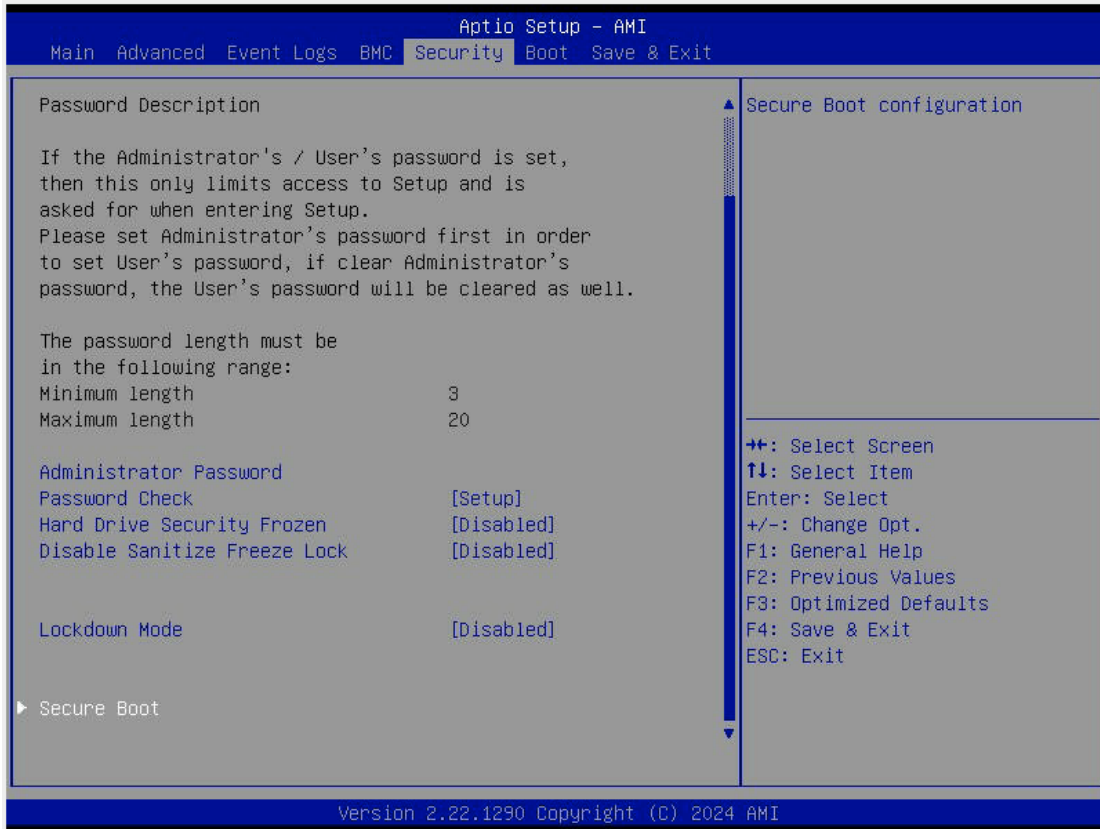


Figure 6-11: Secure Boot Selected

7. Navigate to the **CSM Support** option.

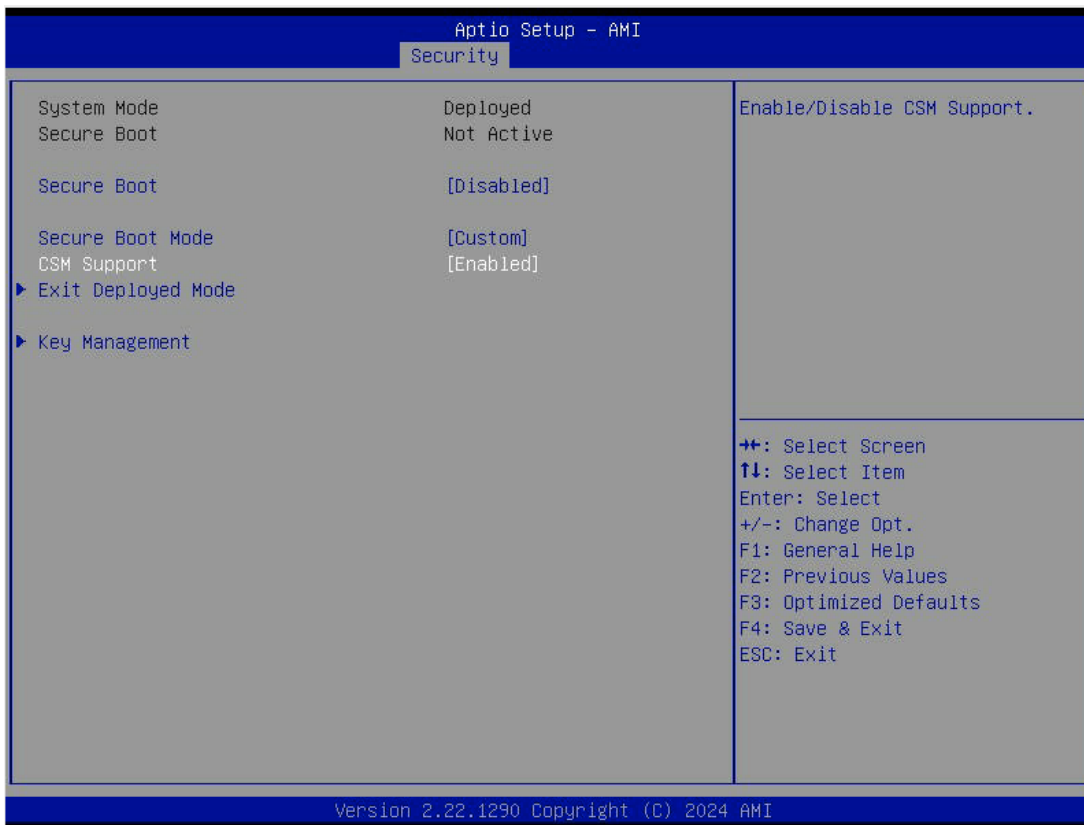
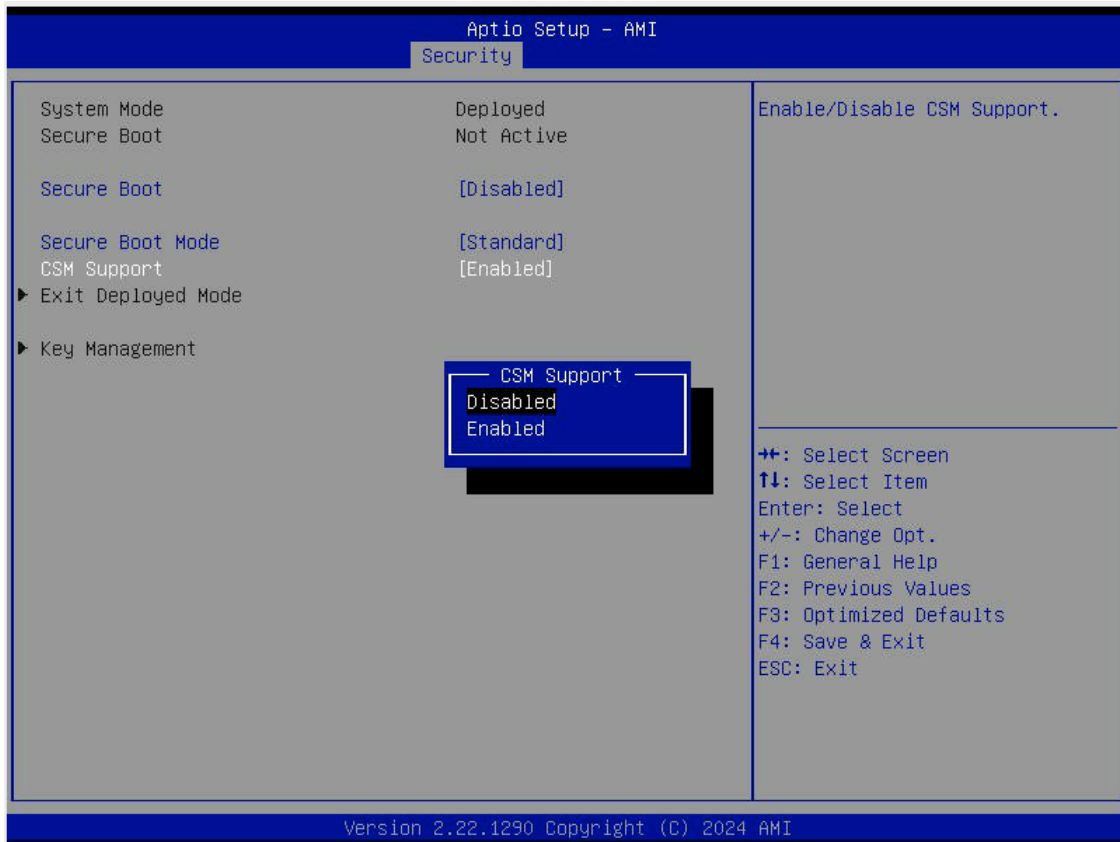


Figure 6-12: CSM Support Selected

8. Set it to **Disabled**.**Figure 6-13: CSM Support Disabled**

9. For the changes to take effect, press **<F4>** to save the settings.
10. Exit the BIOS Setup Utility.
11. Press **** during system boot to enter the BIOS Setup Utility.

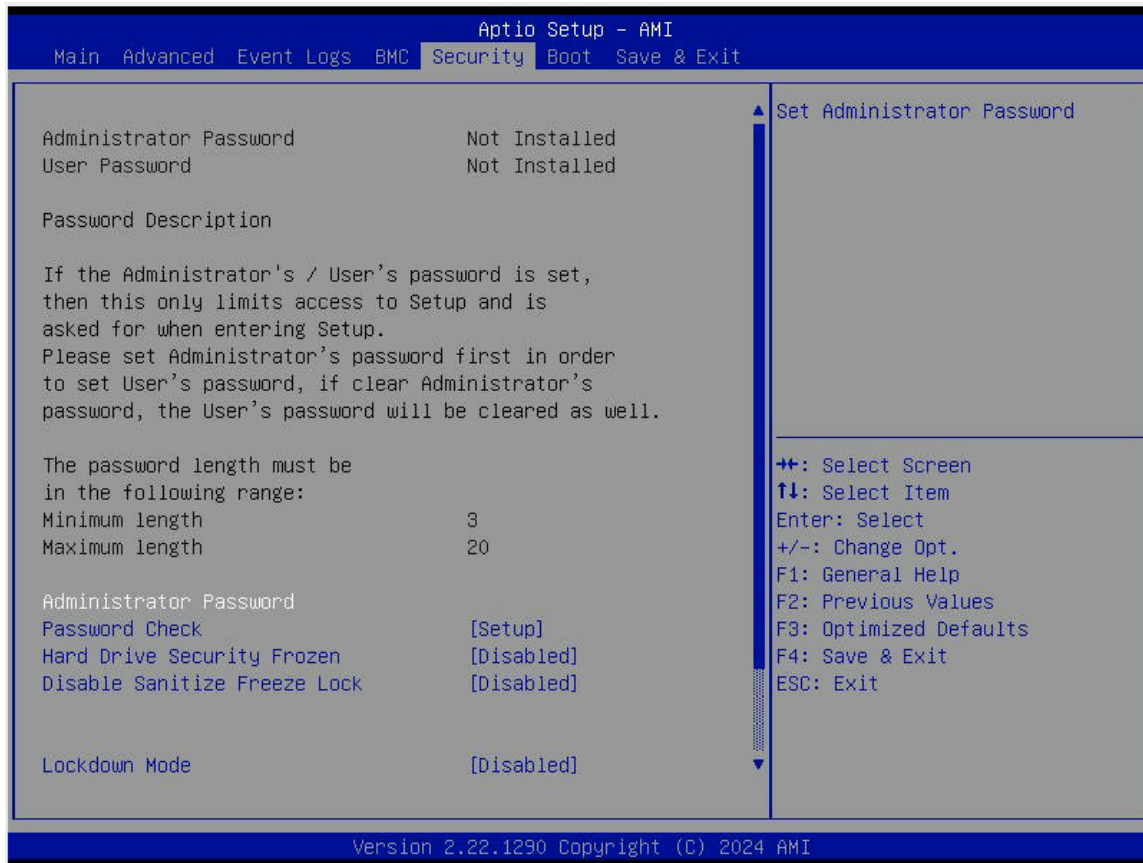
12. Navigate to the **Security** tab.

Figure 6-14: Security Tab Main Menu

13. Enter the **Secure Boot** menu.

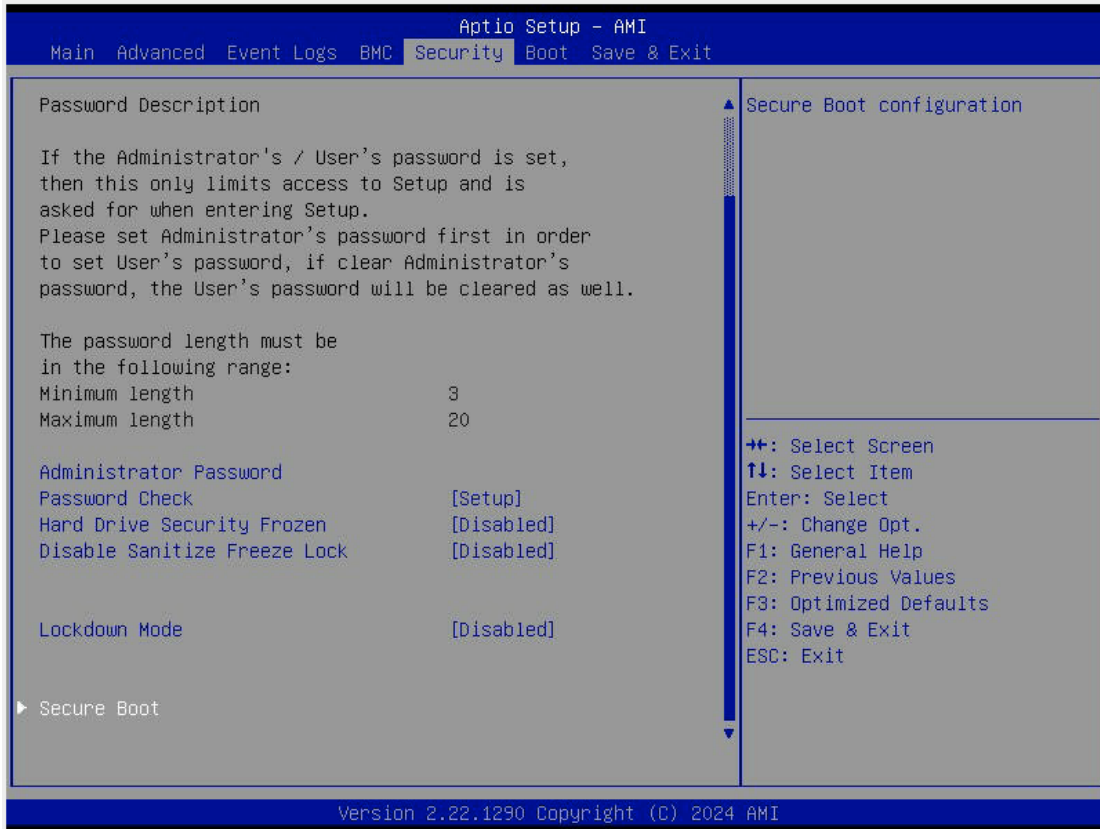
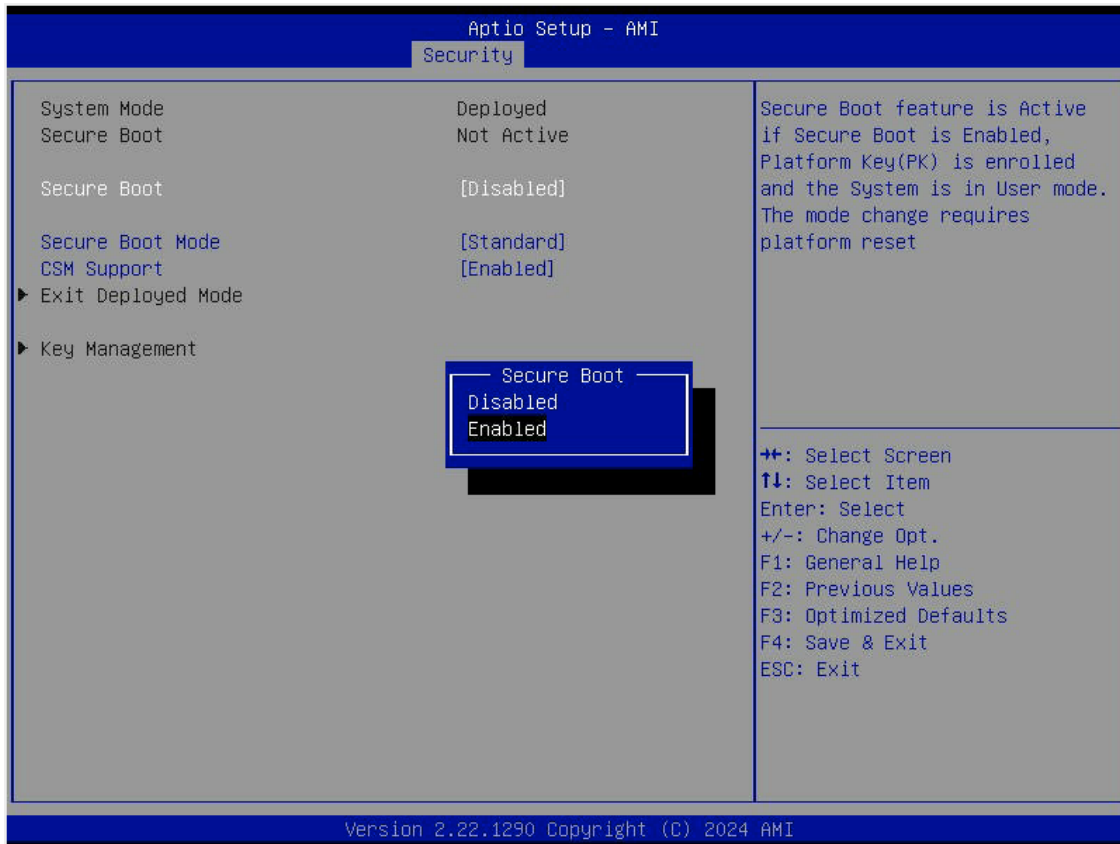


Figure 6-15: Secure Boot Selected

14. Set **Secure Boot** to **Enabled**.**Figure 6-16: Secure Boot Enabled Selected**

15. For the changes to take effect, press **<F4>** to save the settings.
16. Exit the **BIOS Setup Utility**.
17. Press **** during system boot to enter the **BIOS Setup Utility**.

18. Navigate to the **Security** tab.

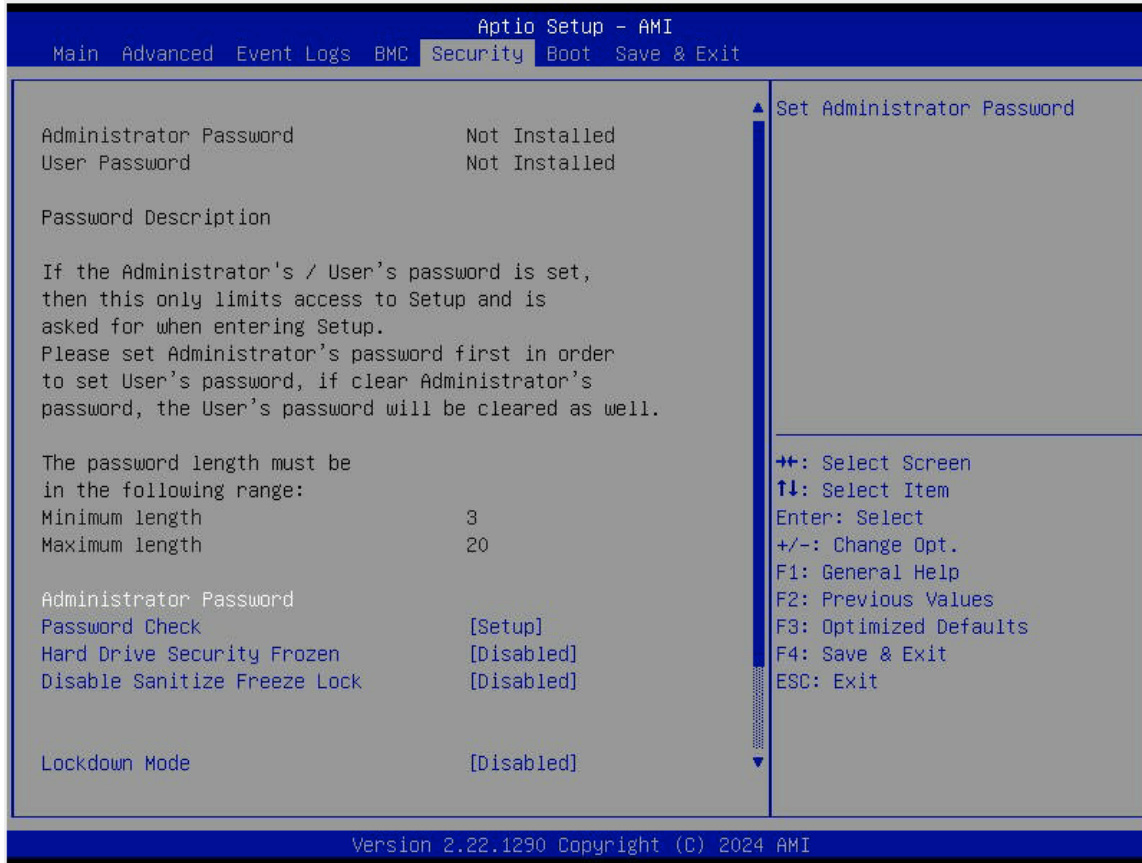


Figure 6-17: Security Tab Main Menu

19. Enter the **Secure Boot** menu.

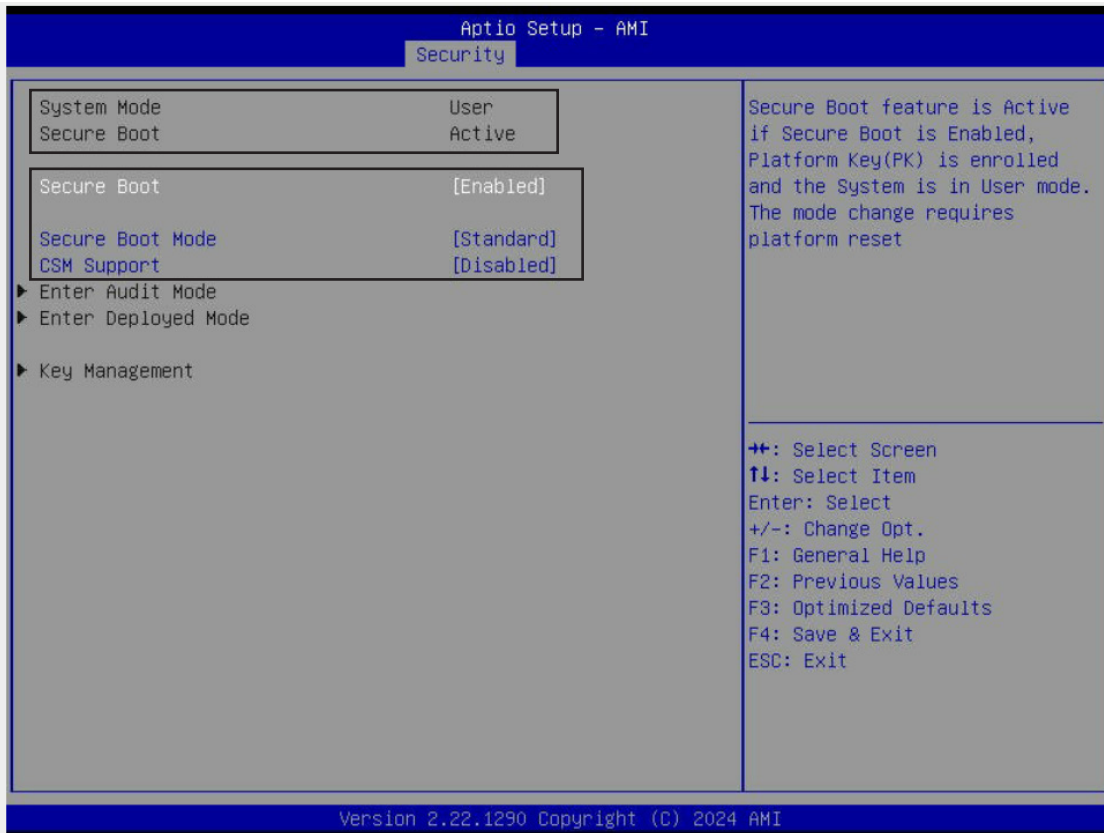



Figure 6-18: Security Boot Selected

 **Note:** Once Secure Boot is enabled, CSM Support will become disabled, and the legacy environment is no longer valid. The authorized UEFI support includes UEFI OS, AOC UEFI FW, and UEFI PXE server.

20. Now that **Secure Boot** is enabled, navigate to the **Advanced** tab.

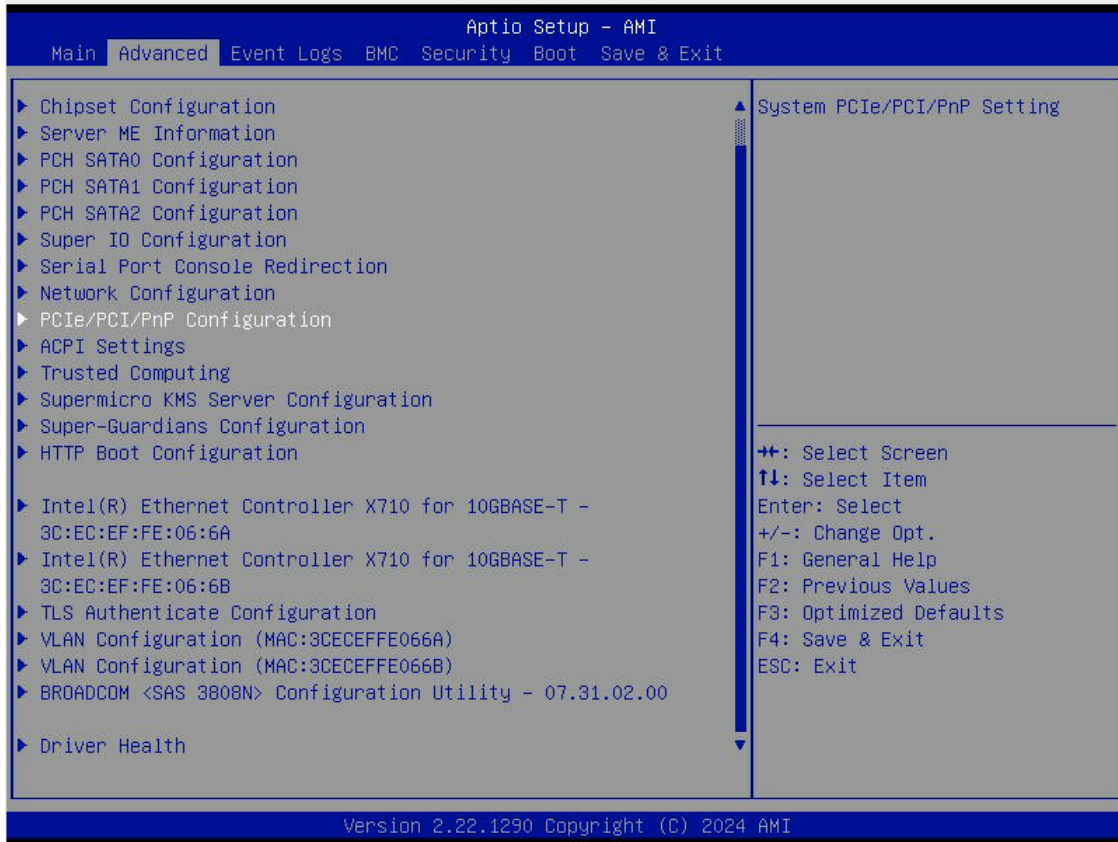


Figure 6-19: Advanced Menu

21. Select **BROADCOM <SAS 3808N> Configuration Utility**. The BROADCOM <SAS 3808N> Configuration Utility Advanced Menu will appear.

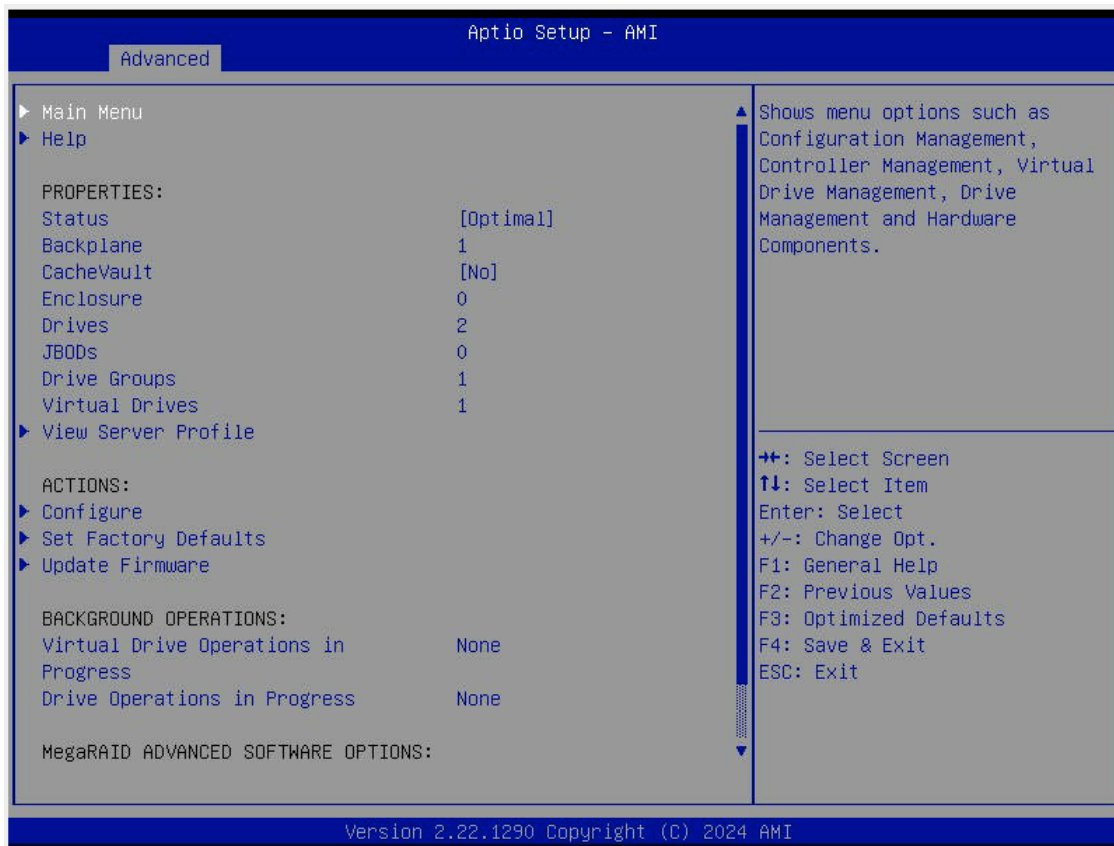


Figure 6-20: BROADCOM <SAS 3808N> Configuration Advanced Menu

(Disclaimer Continued)

The products sold by Supermicro are not intended for and will not be used in life support systems, medical equipment, nuclear facilities or systems, aircraft, aircraft devices, aircraft/emergency communication devices or other critical systems whose failure to perform be reasonably expected to result in significant injury or loss of life or catastrophic property damage. Accordingly, Supermicro disclaims any and all liability, and should buyer use or sell such products for use in such ultra-hazardous applications, it does so entirely at its own risk. Furthermore, buyer agrees to fully indemnify, defend and hold Supermicro harmless for and against any and all claims, demands, actions, litigation, and proceedings of any kind arising out of or related to such ultra-hazardous use or sale.