Intel® RAID Software User Guide for full featured and entry level RAID controllers

Guidance for configuring different families of Intel® RAID Controllers.

Rev 1.0

July 2017

Intel® Server Products and Solutions

<Blank page>

Document Revision History

Date	Revision	Changes
July 2017	1.0	Initial release.

Disclaimers

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software, or service activation. Learn more at Intel.com, or from the OEM or retailer.

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

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

The products described may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

This document is classified as preliminary and contains information on products in the design phase of development. Do not finalize a design with this information. Revised product information will be published as available. Verify with your local sales office that you have the latest document revision before finalizing a design.

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

Table of Contents

1 Overview **11**
1.1 Supported Hardware 11
1.2 Software 12
1.2.1 Drivers 12
1.2.2 Configuration Utilities 12
1.3 RAID Terminology 12
1.3.1 Fault Tolerance 13
1.3.2 Enclosure Management 14
1.3.3 Performance 14
2 RAID Levels, Concepts, and Features **16**
2.1 Summary of RAID Levels 16
2.2 Selecting a RAID Level 16
2.2.1 RAID 0 - Data Striping 17
2.2.2 RAID 1 - Disk Mirroring/Disk Duplexing 17
2.2.3 RAID 5 - Data Striping with Striped Parity 18
2.2.4 RAID 6 - Distributed Parity and Disk Striping 19
2.2.5 RAID IME (RAID 1E) 19
2.2.6 RAID 10 - Combination of RAID 1 and RAID 0 20
2.2.7 RAID 50 - Combination of RAID 5 and RAID 0 21
2.2.8 RAID 60 - Combination of RAID 6 and RAID 0 22
2.3 RAID Configuration Strategies 23
2.3.1 Maximizing Fault Tolerance 23
2.3.2 Maximizing Performance 24
2.3.3 Maximizing Storage Capacity 25
2.3.4 Array Purpose 26
2.3.5 Configuration Planning 26
2.4 RAID Fatures 26
2.4.1 RAID Availability Concept 26
2.4.2 Spare Drives 27
2.4.3 Rebuild 27
2.4.4 Drive in Foreign State 27
2.4.5 Copyback 27
2.4.6 UEFI 2.0 Support 28
2.4.7 MegaRAID Fast Path 28
2.4.8 4K Sector Drive Support 29
2.4.9 Larger than 2 TB Drive Support 30
2.4.10 Error Handling 30
2.4.11 Shield State 30
2.4.12 Dimmer Switch or Power Save feature 31
2.4.13 Online capacity expansion 31

2.4.14 Fault Tolerant Features 31
2.4.15 Cache Options and Settings 32
2.4.16 Background Tasks 32
2.4.17 Audible Alarm 33
3 Intel® RAID Firmware 34
4 Intel® RAID Drivers 35
4.1 RAID Driver Installation for Microsoft Windows* 35
4.1.1 Installation in a New Microsoft Windows* Operating System 35
4.1.2 Installation in an Existing Microsoft Windows* Operating System 35
4.2 RAID Driver Installation for Red Hat* Enterprise Linux* 36
4.3 RAID Driver Installation for SuSE* Linux* 36
5 Intel® RAID Configuration Utilities 37
5.1 Intel® RAID BIOS Console 2 for 6 Gb/s Intel® RAID Controllers 37
5.1.1 Start Intel® RAID BIOS Console 2 37
5.1.2 Intel® RAID BIOS Console 2 Screens and Options 37
5.1.3 Virtual Drives Screen 41
5.1.4 Physical Drives Screen 42
5.1.5 Configuration Mismatch Screen 42
5.1.6 Setting Up a RAID Array Using the Configuration Wizard 42
5.1.7 Creating RAID 0, 1, 5, or 6 using Intel® RAID BIOS Console 2 44
5.1.8 Creating RAID 10, 50, or 60 using Intel® RAID BIOS Console 2 46
5.1.9 Setting Drive Parameters 49
5.1.10 Creating a Hot Spare 50
5.1.11 Viewing Event Details 52
5.2 Integrated RAID M BIOS Configuration Utility for 12 Gb/s Intel® RAID Controllers 55
5.2.1 Starting the RCU 55
5.2.2 Exiting the RCU 55
5.2.3 RCU Keystrokes 55
5.2.4 RCU Menus 56
5.2.5 VD Mgmt Menu 56
5.2.6 PD Mgmt Menu 57
5.2.7 Ctrl Mgmt Menu 57
5.2.8 Properties Menu 58
5.2.9 Foreign View Menu 59
5.2.10 Controller Advanced Software Options 59
5.2.11 RAID Premium Feature Keys 60
5.2.12 Creating a Storage Configuration 61
5.2.13 Clearing the Configuration 63
5.2.14 Setting Advanced Virtual Drive Properties 63
5.2.15 Managing CacheCade Virtual Drives 64
5.2.16 Using LSI* MegaRAID* SafeStore* Encryption Software 68
5.2.17 Enabling Drive Security 68

5.2.18 Changing Security Settings 69
5.2.19 Disabling Drive Security 70
5.2.20 Importing or Clearing a Foreign Configuration 71
5.2.21 Discarding Preserved Cache 73
5.2.22 Converting JBOD Drives to Unconfigured Good Drives 73
5.2.23 Converting Unconfigured Good Drives to JBOD Drives 74
5.2.24 Viewing and Changing Device Properties 75
5.2.25 Viewing Controller Properties 75
5.2.26 Modifying Controller Properties 75
5.2.27 Viewing and Changing Virtual Drive Properties 77
5.2.28 Deleting a Virtual Drive 78
5.2.29 Deleting a Virtual Drive Group 78
5.2.30 Expanding a Virtual Drive 78
5.2.31 RAID migration 79
5.2.32 Erasing a Virtual Drive 79
5.2.33 Managing Link Speed 80
5.2.34 Managing Power Save Settings for the Controller 81
5.2.35 Managing Power Save Settings for the Drive Group 82
5.2.36 Managing BBU Information 82
5.2.37 Managing Dedicated Hot Spares 83
5.2.38 Securing a Drive Group 84
5.2.39 Locating Physical Drives 84
5.2.40 Performing a Break Mirror Operation 84
5.2.41 Performing a Join Mirror Operation 85
5.2.42 Managing Storage Configurations 86
5.2.43 Creating Global Hot Spares 88
5.2.44 Removing a Hot Spare Drive 88
5.2.45 Making a Drive Offline 88
5.2.46 Making a Drive Online 89
5.2.47 Instant Secure Erase 89
5.2.48 Erasing a Physical Drive 89
5.3 Human Interface Infrastructure (HII) Configuration Utility 90
5.3.1 Dashboard view 90
5.3.2 Main Menu 91
5.3.3 Controller Management 95
6 Configuring the Tri-Mode RAID controllers 101
6.1 Operating modes 101
Appendix A. Glossary 102

List of Figures

Figure 1. RAID 0 – data striping ... 17
Figure 2. RAID 1 – disk mirroring/disk duplexing ... 17
Figure 3. RAID 5 – data striping with striped parity ... 18
Figure 4. Example of distributed parity across two blocks in a stripe (RAID 6) ... 19
Figure 5. RAID IME with three disks ... 20
Figure 6. RAID 10 – combination of RAID 1 and RAID 0 ... 20
Figure 7. RAID 50 – combination of RAID 5 and RAID 0 ... 21
Figure 8. RAID 60 – combination of RAID 6 and RAID 0 ... 22
Figure 10. Intel® RAID BIOS Console 2 – controller selection ... 38
Figure 9. Intel® RAID BIOS Console 2 main screen ... 39
Figure 11. Intel® RAID BIOS Console 2 – controller properties ... 39
Figure 12. Intel® RAID BIOS Console 2 – additional controller properties ... 40
Figure 13. Intel® RAID BIOS Console 2 Configuration Wizard – configuration type ... 42
Figure 14. Intel® RAID BIOS Console 2 Configuration Wizard – select configuration ... 43
Figure 15. Intel® RAID BIOS Console 2 Configuration Wizard – configuration method ... 43
Figure 16. Intel® RAID BIOS Console 2 Configuration Wizard – drive group definition ... 44
Figure 17. Intel® RAID BIOS Console 2 Configuration Wizard – virtual drive definition example for RAID 5 ... 45
Figure 18. Intel® RAID BIOS Console 2 Configuration Wizard – configuration preview ... 45
Figure 19. Intel® RAID BIOS Console 2 – initialization settings ... 46
Figure 20. Intel® RAID BIOS Console 2 Configuration Wizard – definition of multiple drive groups ... 47
Figure 21. Intel® RAID BIOS Console 2 Configuration Wizard – virtual drive definition example for RAID 10 .. 47
Figure 22. Intel® RAID BIOS Console 2 Configuration Wizard – view virtual drive preview ... 48
Figure 23. Intel® RAID BIOS Console 2 – initialization settings ... 48
Figure 24. Intel® RAID BIOS Console 2 – RAID 60 example of main screen logical view ... 49
Figure 25. Intel® RAID BIOS Console 2 – RAID 60 example of virtual drive properties screen ... 49
Figure 26. Intel® RAID BIOS Console 2 – choosing a hot spare drive ... 51
Figure 27. Intel® RAID BIOS Console 2 – creating a hot spare drive ... 51
Figure 34. Intel® RAID BIOS Console 2 – viewing a hot spare drive ... 52
Figure 29. Intel® RAID BIOS Console 2 – hot spare drive listed in main screen ... 52
Figure 30. Intel® RAID BIOS Console 2 – event information screen ... 53
Figure 31. Intel® RAID BIOS Console 2 – selecting events to view ... 53
Figure 32. Intel® RAID BIOS Console 2 – viewing an event ... 54
Figure 33. RCU – VD Mgmt menu screen ... 57
Figure 34. RCU – PD Mgmt menu screen ... 57
Figure 35. SCU – Ctrl Mgmt menu first screen ... 58
Figure 36. RCU – Ctrl Mgmt menu second screen ... 58
Figure 37. RCU – Properties menu screen ... 59
Figure 38. RCU – Foreign View menu screen ... 59
Figure 39. RCU – advanced software options ... 60
Figure 40. RCU – advanced software options with key AXXRPFKSSD2 installed ... 60

Figure 41. RCU – create a new virtual drive ... 62
Figure 42. RCU– clear configuration dialog ... 63
Figure 43. RCU – create virtual drive advanced properties ... 63
Figure 44. RCU – create CacheCade* virtual drive ... 65
Figure 45. RCU – modify CacheCade* virtual drive ... 65
Figure 46. RCU – Manage SSD Caching ... 66
Figure 47. RCU – disabling SSD caching dialog ... 67
Figure 48. Ctrl-R Utility – deleting a virtual drive dialog ... 67
Figure 49. RCU – Create security key screen ... 69
Figure 50. RCU – change security key screen ... 70
Figure 51. RCU – foreign configuration options ... 71
Figure 52. RCU – import foreign configuration ... 72
Figure 53. RCU – clear foreign configuration ... 72
Figure 54. RCU – manage preserved cache ... 73
Figure 55. RCU – convert JBOD drives to unconfigured good drives ... 74
Figure 56. RCU – convert unconfigured good drives to JBOD drives ... 75
Figure 57. RCU – virtual drive properties ... 77
Figure 58. RCU – advanced virtual drive properties ... 78
Figure 59. RCU – expand virtual drive ... 79
Figure 60. RCU – erase virtual drive ... 80
Figure 61. RCU – manage link speed ... 80
Figure 62. RCU – manage power save ... 81
Figure 63. RCU – manage drive group power save settings ... 82
Figure 64. RCU – battery properties window ... 82
Figure 65. RCU – dedicated hot spare window ... 83
Figure 66. RCU – break mirror message dialog ... 84
Figure 67. RCU – choose join mirror option ... 85
Figure 68. RCU – join mirror arm with existing virtual drive confirmation dialog ... 85
Figure 69. RCU – join mirror arm as new virtual drive confirmation dialog ... 85
Figure 70. RCU – choose join mirror copy option ... 86
Figure 71. RCU – initialize a virtual drive ... 86
Figure 72. Consistency check ... 87
Figure 73. RCU – Copyback operation ... 88
Figure 74. HII CU - Select RAID Controller ... 90
Figure 74. HII CU – Dashboard View ... 91
Figure 76. HII CU – Main Menu ... 91
Figure 6. HII CU – Create Virtual Drive Screen ... 93
Figure 78. HII CU - Controller Management Screen ... 95
Figure 79. HII CU – Virtual drive Management ... 98
Figure 80. HII CU – Drive Management ... 99
Figure 81. HII CU – Hardware Components ... 100
Figure 82. HII CU – Profile Management ... 101

List of Tables

Table 1. Supported Intel® RAID products 11
Table 2. RAID 0 overview 17
Table 3. RAID 1 overview 18
Table 4. RAID 5 overview 18
Table 5. RAID 6 overview 19
Table 6. RAID IME overview 20
Table 7. RAID 10 overview 21
Table 8. RAID 50 overview 22
Table 9. RAID 60 overview 23
Table 10. RAID levels and fault tolerance 24
Table 11. RAID levels and performance 24
Table 12. RAID levels and capacity 25
Table 14. Suggestions based on requirements for array configuration 26
Table 14. Advanced format support on Intel® RAID Modules and Controllers 29
Table 19. Intel® RAID BIOS Console 2 toolbar icon descriptions 38
Table 15. RCU keystrokes 55
Table 17. Intel® RAID premium feature keys 61
Table 18. SSD cache Drive Sector Size 68
Table 19. RCU controller settings 76
Table 1. Virtual Drive Management Property Settings 93
Table 21. Basic Controller Properties 95
Table 22. Advanced Controller Properties 96

1 Overview

This document describes the configuration utilities for the different families of Intel® RAID Controllers. It also describes RAID options and enhanced and premium features. The software described in this document is designed for use with Intel® RAID Controllers generations 2.5. 3 and Tri-Mode, or product codes starting with RS25, RMS25, RMT3, RS3, RMS3, RMS3, RSP3 and RMS3P, all these controllers use either the MegaRAID® (MR) or the MegaRAID® Entry (iMR) software stack.

1.1 Supported Hardware

This manual covers the following Intel® RAID families.

Table 1. Supported Intel® RAID products

Intel® RAID controller family	Generation	Intel Product Code (iPC)
Intel® RAID Adapters	Gen 2.5, 6 Gb/s	RS25NB008, RS25DB080, RS25AB080 and RS25SB008
	Gen 3, 12 Gb/s	RS3SC008, RS3MC044, RS3DC040, RS3DC080 and RS3WC080
	Tri-Mode	RSP3TD160F, RSP3MD088F, RSP3DD080F and RSP3WD080E
Intel® RAID Modules	Gen 2.5, 6 Gb/s	RMS25PB080, RMS25PB040, RMT3PB080, RMS25CB080, RMS25CB040 and RMT3CB080
	Gen 3, 12 Gb/s	RMS3CC040, RMS3CC080, RMS3HC080 and RMS3AC160
	Tri-Mode	RMSP3AD160F, RMSP3CD080F and RMSP3HD080E
On-Board SAS controller	Gen 3, 12 Gb/s	RS3YC
Bridge Boards	Gen 3, 12 Gb/s	AHWKPTP12GBGB (RS3LC) and AHWKPTP12GBGBR5 (RS3LC5)

The Intel® RAID Controllers RS25NB008, RS25DB080, RS25AB080, RS25SB008, RS3SC008, RS3MC044, RS3DC040, RS3DC080, RMS25PB080, RMS25PB040, RMT3PB080, RMS25CB080, RMS25CB040, RMT3CB080, RMS3CC040, RMS3CC080, RMS3AC160, RSP3TD160F, RSP3MD088F, RSP3DD080F, RMSP3AD160F and RMSP3CD080F use the MR stack; these controllers are considered full-featured.

The Intel® RAID Controllers RS3WC080, RMS3HC080, RSP3WD080E and RMSP3HD080E use the iMR sotware stack. The iMR sotware stack is a subset of the MR stack with less capabilities but more cost effective.

This guide uses the following convention to name the RAID cards:
RAID module: a RAID card with mezzanine connector. These cards are only compatible with the Intel® systems.
RAID adapter: a RAID Add in card with low-Profile MD2 form factor.
RAID controller: either a RAID module or a RAID adapter.

Caution: Some levels of RAID are designed to increase the availability of data and some to provide data redundancy. However, installing a RAID controller is not a substitute for a reliable backup strategy. It is highly recommended to back up data regularly through a tape drive or other backup strategy to guard against data loss. It is especially important to back up all data before working on any system components and before installing or changing the RAID controller or configuration.

1.2 Software

1.2.1 Drivers

Intel provides software drivers for the different operating systems like Windows, Linux, VMware, etc. For a complete list of supported Oss visit the download page for at https://downloadcenter.intel.com/

For more information on Intel RAID drivers, see chapter 3.

Note: Only the combinations of controller, driver, and Intel® Server Board or System listed in the Tested Hardware and Operating System List (THOL) were tested. Check the supported operating system list for both the RAID controller and server board to verify operating system support and compatibility using the THOL Builder here: http://serverconfigurator.intel.com

1.2.2 Configuration Utilities

The firmware installed on the RAID controller provides pre-operating system configuration.

- **Intel® RAID BIOS Console 2 (pre-boot)** – For the 6 Gb/s Intel® RAID Controllers, press **<Ctrl+G>** during the server boot to enter the Intel® RAID BIOS Console 2 utility. For detailed information on the 6 Gb/s Intel RAID Controller configuration utility, see section 5.1.
- **Integrated RAID M BIOS Configuration Utility (pre-boot)** – For the 12 Gb/s Intel® RAID Controllers, press **<Ctrl+R>** during the server boot to enter the 12Gb/s Intel® RAID Controller configuration utility. For detailed information on the 12 Gb/s Intel RAID Controller configuration utility, see section 5.2 .
- **Human Interface Infrastructure (HII) (pre-boot)** – When the system is configured for optimized UEFI boot mode, the RAID modules and controllers can be configured using the HII utility. For detailed information on the HII configuration utility, see section 5.3.
  Note: The Intel® Tri-Mode controllers are designed to work in the optimized UEFI boot mode, therefore the HII is the only way to get them configured in a pre-boot environment.

Post-boot Configuration and monitoring utilities are also available that are not covered on this guide.

- **CLI based monitoring and Configuring Utilities (post-boot)** –CmdTool2 and the StorCli are RAID utilities used to configure, monitor and diagnose controllers and RAID configurations. They use commands and they run from the EFI shell, Windows and Linux OS. More details on these utilities can be found in the Intel RAID Utilities Guide.
- **GUI based monitoring and Configuring Utilities (post-boot)**- RAID Web Console 2 (RWC2) and RAID Web Console 3 (RWC3) are RAID graphic utilities used to configure, monitor and diagnose controllers and RAID configurations. They run on the Windows and Linux OS. More details on these utilities can be found in the Intel RAID Utilities Guide.

1.3 RAID Terminology

Redundant array of independent disks (RAID) is a group of physical disks put together to provide increased input/output (I/O) performance by allowing multiple, simultaneous disk access; fault tolerance; and reliability by reconstructing failed drives from remaining data. The physical drive group is called an **array**, and the partitioned sets are called **virtual disks**. A virtual disk can consist of a part of one or more physical arrays and one or more entire arrays.

Using two or more configured RAID arrays in a larger virtual disk is called **spanning**. It is represented by a double digit in the RAID mode/type (10, 50, or 60).

Running more than one array on a given physical drive or set of drives is called a **sliced configuration**.

The only drive that the operating system works with is the virtual disk, also called a virtual drive. The virtual drive is used by the operating system as a single drive (lettered storage device in Microsoft Windows*).

The RAID controller is the mastermind that must configure the physical array and the virtual disks and initialize them for use, check them for data consistency, allocate the data between the physical drives, and rebuild a failed array to maintain data redundancy. The features available per controller are highlighted later in this document and in the hardware guide for the RAID controller.

The common terms used when describing RAID functions and features can be grouped into two areas: fault tolerance (data protection and redundancy) and performance.

1.3.1 Fault Tolerance

Fault tolerance describes a state in which, even with a drive failure, the data on the virtual drive is still complete and the system is available after the failure and during repair of the array. Most RAID modes are able to endure a physical disk failure without compromising data integrity or processing capability of the virtual drive.

RAID mode 0 is not fault tolerant. With RAID 0, if a drive fails, then the data is no longer complete and no longer available. Backplane fault tolerance can be achieved by a spanned array where the arrays are on different backplanes.

True fault tolerance includes the automatic ability to restore the RAID array to redundancy so that another drive failure does not destroy its usability.

1.3.1.1 Hot Spare

True fault tolerance requires the availability of a spare disk that the controller can add to the array and use to rebuild the array with the data from the failed drive. This spare disk is called a hot spare. It must be a part of the array before a disk failure occurs. A hot spare is a physical drive that is maintained by the RAID controller but not used for data storage in the array unless another drive fails. Upon failure of one of the array's physical drives, the hot-spare drive is used to hold the recreated data and restore data redundancy.

Hot-spare drives can be global (available to any array on a controller) or dedicated (only usable by one array). There can be more than one hot spare per array in which case the drive of the closest capacity is used. If both dedicated and global hot-spare drives are available, the dedicated drive is used first. If the hot swap rebuild fails, that hot spare is also marked failed. Since RAID 0 is not redundant, there is no hot spare value.

If a hot-spare drive is not an option, it is possible to perform a hot or cold swap of the failed drive to provide the new drive for rebuild after the drive failure. A swap is the manual substitution of a replacement drive in a disk subsystem. If a swap is performed while the system is running, it is a hot swap. A hot swap can only be performed if the backplane and enclosure support it. If the system does not support hot-swap drives, then the system must be powered down before the drive swap occurs. This is a cold swap.

In all cases (hot spare, hot swap, or cold swap), the replacement drive must be at least as large as the drive it replaces. In all three cases, the failed drive is removed from the array. If using a hot spare, then the failed drive can remain in the system. When a hot spare is available and an automatic rebuild starts, the failed drive may be automatically removed from the array before the utilities detect the failure. Only the event logs show that the failure happened.

If the system is shut down during the rebuild, all rebuilds should automatically restart on reboot.

Note: If running a sliced configuration (RAID 0, RAID 5, and RAID 6 on the same set of physical drives), then the rebuild of the spare does not occur until the RAID 0 array is deleted.

On Intel® RAID Controllers RS2WC080 and RS2WC040, if the virtual drive is in degrade mode due to a failed physical drive, auto rebuild is not supported for a hot-plugged drive until a manual selection is made by users. As part of just a bunch of drives (JBOD) implementation for Intel® RAID Controllers RS2WC080 and RS2WC040, all new drives that are hot-plugged automatically become JBOD. Users need to manually move the JBOD drive to Unconfigured Good before auto rebuild starts. For more details, refer to the Hardware User Guide (HWUG) for the above controllers.

1.3.1.2 Data Redundancy

Data redundancy is provided by mirroring or by disk striping with parity stripes.

Disk mirroring is found only in RAID 1 and 10. With mirroring, the same data simultaneously writes to two disks. If one disk fails, the contents of the other disk can be used to run the system and reconstruct the failed array. This provides 100% data redundancy but uses the most drive capacity, since 50% of the total capacity is available. Until a failure occurs, both mirrored disks contain the same data at all times. Either drive can act as the operational drive.

Parity is the ability to recreate data by using a mathematical calculation derived from multiple data sets. Parity is basically a checksum of all the data known as the “ABCsum”. When drive A fails, the controller uses the ABCsum to calculate what remains on drives B+C. The remainder must be recreated onto new drive A.

Parity can be dedicated (all parity stripes placed on the same drive) or distributed (parity stripes spread across multiple drives). Calculating and writing parity slows the write process but provides redundancy in a much smaller space than mirroring. Parity checking is also used to detect errors in the data during consistency checks and patrol reads.

RAID 5 uses distributed parity and RAID 6 uses dual distributed parity meaning two different sets of parity are calculated and written to different drives each time. RAID modes 1 and 5 can survive a single disk failure, although performance may be degraded, especially during the rebuild. RAID modes 10 and 50 can survive multiple disk failures across the spans, but only one failure per array. RAID mode 6 can survive up to two disk failures. RAID mode 60 can sustain up to two failures per array.

Data protection is also provided by running calculations on the drives to make sure data is consistent and that drives are good. The controller uses consistency checks, background initialization, and patrol reads. You should include these in regular maintenance schedules.

- The **consistency check** operation verifies that data in the array matches the redundancy data (parity or checksum). This is not provided in RAID 0 in which there is no fault tolerance.
- **Background initialization** is a consistency check that is forced five minutes after the creation of a virtual disk. Background initialization also checks for media errors on physical drives and ensures that striped data segments are the same on all physical drives in an array.
- **Patrol read** check for physical disk errors that could lead to drive failure. These checks usually include an attempt at corrective action. Patrol read can be enabled or disabled with automatic or manual activation. This process starts only when the RAID controller is idle for a defined period of time and no other background tasks are active, although a patrol read check can continue to run during heavy I/O processes.

1.3.2 Enclosure Management

Enclosure management is the intelligent monitoring of the disk subsystem by software or hardware usually within a disk enclosure. It increases the ability for the user to respond to a drive or power supply failure by monitoring those sub systems.

1.3.3 Performance

Performance improvements come from multiple areas including disk striping and disk spanning, accessing multiple disks simultaneously, and setting the percentage of processing capability to use for a task.

1.3.3.1 Disk Striping

Disk striping writes data across all of the physical disks in the array into fixed size partitions or stripes. In most cases, the stripe size is user-defined. Stripes do not provide redundancy but improve performance since striping allows multiple physical drives to be accessed at the same time. These stripes are interleaved in a repeated sequential manner and the controller knows where data is stored. The same stripe size should be kept across RAID arrays.

Terms used with strip sizing are listed below:

- **Strip size** – One disk section.
- **Stripe size** – Total of one set of strips across all data disks, not including parity stripes.
- **Stripe width** – The number of disks involved.

1.3.3.2 Disk Spanning

Disk spanning allows more than one array to be combined into a single virtual drive. The spanned arrays must have the same stripe size and must be contiguous. Spanning alone does not provide redundancy but RAID modes 10, 50, and 60 all have redundancy provided in their pre-spanned arrays through RAID 1, 5, or 6.

Note: Spanning two contiguous RAID 0 drives does not produce a new RAID level or add fault tolerance. It does increase the size of the virtual volume and improves performance by doubling the number of spindles. Spanning for RAID 10, RAID 50, and RAID 60 requires two to eight arrays of RAID 1, 5, or 6 with the same stripe size and that always uses the entire drive.

1.3.3.3 CPU Usage

Resource allocation provides the user with the option to set the amount of compute cycles to devote to various tasks, including the rate of rebuilds, initialization, consistency checks, and patrol read. Setting resource allocation to 100% gives total priority to the rebuild. Setting it at 0% means the rebuild only occurs if the system is not doing anything else. The default rebuild rate is 30%.

2 RAID Levels, Concepts, and Features

The RAID controller supports RAID levels 0, 1E, 5, 6, 10, 50, and 60. The supported RAID levels are summarized below. In addition, the controller supports independent drives (configured as RAID 0). This chapter describes the RAID levels in detail.

2.1 Summary of RAID Levels

- **RAID 0** – Uses striping to provide high data throughput, especially for large files in an environment that does not require fault tolerance. In Intel® IT/IR RAID, RAID 0 is also called Integrated Striping (IS), which supports striped arrays with two to ten disks.
- **RAID 1** – Uses mirroring so that data written to one disk drive simultaneously writes to another disk drive. This is good for small databases or other applications that require small capacity but complete data redundancy. In Intel® IT/IR RAID, RAID 1 is also called Integrated Mirroring (IM) which supports two-disk mirrored arrays and hot-spare disks.
- **RAID 5** – Uses disk striping and parity data across all drives (distributed parity) to provide high data throughput, especially for small random access.
- **RAID 6** – Uses distributed parity, with two independent parity blocks per stripe, and disk striping. A RAID 6 virtual disk can survive the loss of two disks without losing data.
- **RAID IME** – Integrated Mirroring Enhanced (IME) which supports mirrored arrays with three to ten disks, plus hot-spare disks. This is implemented in Intel® IT/IR RAID.
- **RAID 10** – A combination of RAID 0 and RAID 1; consists of striped data across mirrored spans. It provides high data throughput and complete data redundancy but uses a larger number of spans.
- **RAID 50** – A combination of RAID 0 and RAID 5; uses distributed parity and disk striping and works best with data that requires high reliability, high request rates, high data transfers, and medium-to-large capacity.

Note: It is not recommended to have a RAID 0, RAID 5, and RAID 6 virtual disk in the same physical array. If a drive in the physical array has to be rebuilt, the RAID 0 virtual disk causes a failure during the rebuild.

- **RAID 60** – A combination of RAID 0 and RAID 6; uses distributed parity, with two independent parity blocks per stripe in each RAID set, and disk striping. A RAID 60 virtual disk can survive the loss of two disks in each of the RAID 6 sets without losing data. It works best with data that requires high reliability, high request rates, high data transfers, and medium-to-large capacity.

2.2 Selecting a RAID Level

To ensure the best performance, select the optimal RAID level when the system drive is created. The optimal RAID level for a disk array depends on a number of factors:

- The number of physical drives in the disk array;
- The capacity of the physical drives in the array;
- The need for data redundancy; and
- The disk performance requirements.

2.2.1 RAID 0 - Data Striping

RAID 0 provides disk striping across all drives in the RAID array. RAID 0 does not provide any data redundancy, but does offer the best performance of any RAID level. RAID 0 breaks up data into smaller segments and then stripes the data segments across each drive in the array. The size of each data segment is determined by the stripe size. RAID 0 offers high bandwidth.

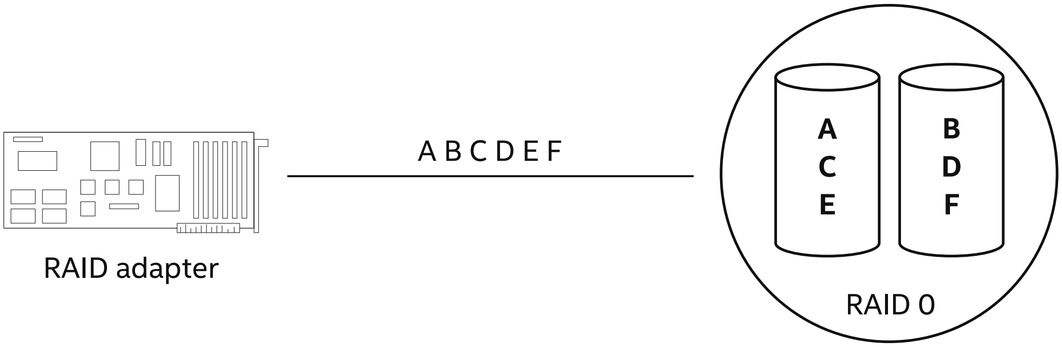


Figure 1. RAID 0 – data striping

Note: RAID level 0 is not fault tolerant. If a drive in a RAID 0 array fails, the whole virtual disk (all physical drives associated with the virtual disk) fails.

By breaking up a large file into smaller segments, the RAID controller can use both SAS drive and SATA drives to read or write the file faster. RAID 0 involves no parity calculations to complicate the write operation. This makes RAID 0 ideal for applications that require high bandwidth but do not require fault tolerance.

Table 2. RAID 0 overview

Uses	Use for applications that require high bandwidth but do not require fault tolerance.
Strong points	• Provides increased data throughput for large files. • No capacity loss penalty for parity.
Weak points	• Does not provide fault tolerance or high bandwidth. • If any drive fails, all data is lost.
No. of drives	1 to 32
Capacity	N*C, where N is number of disks and C is disk capacity.

2.2.2 RAID 1 - Disk Mirroring/Disk Duplexing

In RAID 1, the RAID controller duplicates all data from one drive to a second drive. RAID 1 provides complete data redundancy, but at the cost of doubling the required data storage capacity. Table 3 provides an overview of RAID 1.

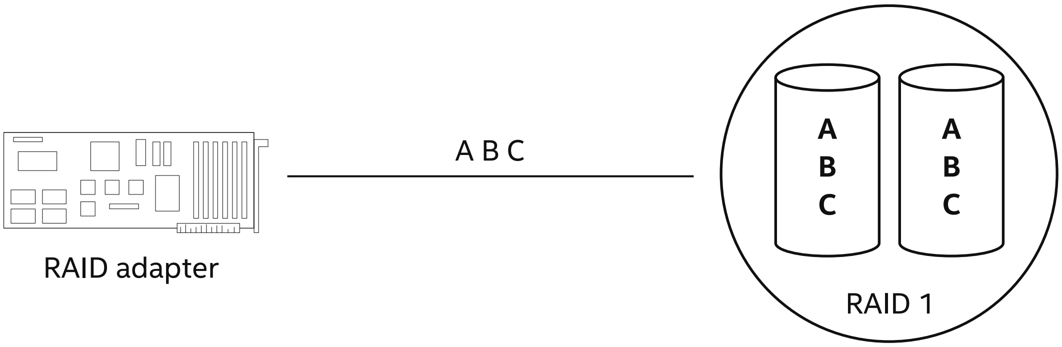


Figure 2. RAID 1 – disk mirroring/disk duplexing

Table 3. RAID 1 overview

Uses	Use for small databases or any other environment that requires fault tolerance but small capacity.
Strong points	• Provides complete data redundancy. • Ideal for any application that requires fault tolerance and minimal capacity.
Weak points	• Requires twice as many disk drives. • Performance is impaired during drive rebuilds.
Drives	2 to 32 (must be an even number of drives)
Capacity	(N*C)/2, where N is number of disks and C is disk capacity.

2.2.3 RAID 5 - Data Striping with Striped Parity

RAID 5 includes disk striping at the block level and parity. Parity is the data's property of being odd or even, and parity checking detects errors in the data. In RAID 5, the parity information is written to all drives. RAID 5 is best suited for networks that perform a lot of small I/O transactions simultaneously.

RAID 5 addresses the bottleneck issue for random I/O operations. Because each drive contains both data and parity, numerous writes can take place concurrently.

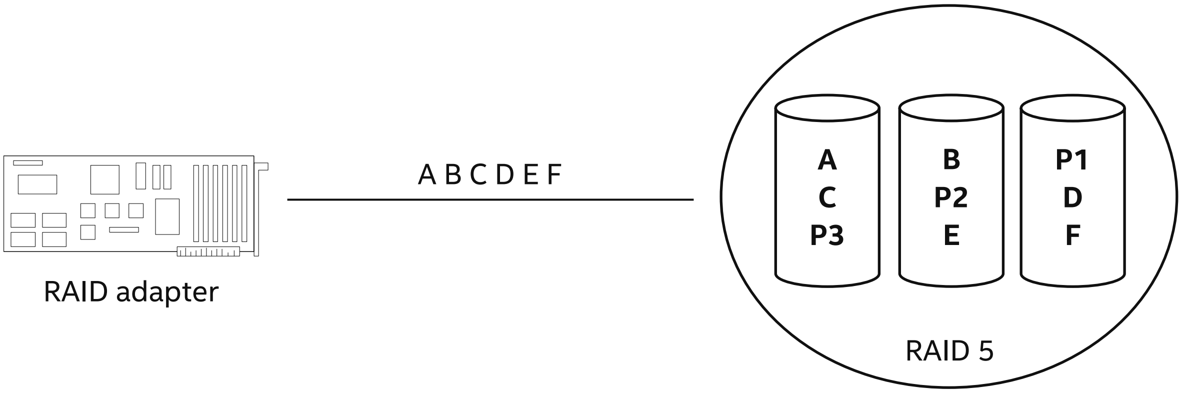


Figure 3. RAID 5 – data striping with striped parity

Table 4 provides an overview of RAID 5.

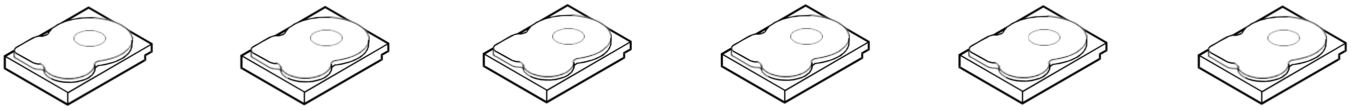
Table 4. RAID 5 overview

Uses	Provides high data throughput, especially for large files. Use RAID 5 for transaction processing applications because each drive can read and write independently. If a drive fails, the RAID controller uses the parity drive to recreate all missing information. Use also for office automation and online customer service that requires fault tolerance. Use for any application that has high read request rates but low write request rates.
Strong points	• Provides data redundancy, high read rates, and good performance in most environments. • Provides redundancy with lowest loss of capacity.
Weak points	• Not well suited to tasks requiring lot of writes. • Suffers more impact if no cache is used (clustering). • If a drive is being rebuilt, disk drive performance is reduced. • Environments with few processes do not perform as well because the RAID overhead is not offset by the performance gains in handling simultaneous processes.
No. of drives	3 to 32
Capacity	(N*C)(N-1)/N, where N is number of disks and C is disk capacity.

2.2.4 RAID 6 - Distributed Parity and Disk Striping

RAID 6 is similar to RAID 5 (disk striping and parity), but instead of one parity block per stripe, there are two. With two independent parity blocks, RAID 6 can survive the loss of two disks in a virtual disk without losing data.

The following figure shows a RAID 6 data layout. The second set of parity drives is denoted by Q. The P drives follow the RAID 5 parity scheme.



Segment 1	Segment 2	Segment 3	Segment 4	Parity (P1-P4)	Parity (Q1-Q4)
Segment 6	Segment 7	Segment 8	Parity (P5-P8)	Parity (Q5-Q8)	Segment 5
Segment 11	Segment 12	Parity (P9-P12)	Parity (Q9-Q12)	Segment 9	Segment 10
Segment 16	Parity (P13-P16)	Parity (Q13-Q16)	Segment 13	Segment 14	Segment 15
Parity (P17-P20)	Parity (Q17-Q20)	Segment 17	Segment 18	Segment 19	Segment 20

Figure 4. Example of distributed parity across two blocks in a stripe (RAID 6)

Parity is distributed across all drives in the array. When only three hard drives are available for RAID 6, the situation requires that P equals Q equals original data, which means that the original data has three copies across the three hard drives.

Table 5 provides an overview of RAID 6.

Table 5. RAID 6 overview

Uses	Provides a high level of data protection through the use of a second parity block in each stripe. Use RAID 6 for data that requires a high level of protection from loss. In the case of a failure of one drive or two drives in a virtual disk, the RAID controller uses the parity blocks to recreate the missing information. If two drives in a RAID 6 virtual disk fail, two drive rebuilds are required, one for each drive. These rebuilds do not occur at the same time. The controller rebuilds one failed drive at a time. Use for office automation and online customer service that requires fault tolerance. Use for any application that has high read request rates but low write request rates.
Strong points	• Provides data redundancy, high read rates, and good performance in most environments. • Can survive the loss of two drives or the loss of a drive while another drive is being rebuilt. • Provides the highest level of protection against drive failures of all of the RAID levels. • Read performance is similar to that of RAID 5.
Weak points	• Not well suited to tasks requiring lot of writes. A RAID 6 virtual disk has to generate two sets of parity data for each write operation, which results in a significant decrease in performance during writes. • Disk drive performance is reduced during a drive rebuild. • Environments with few processes do not perform as well because the RAID overhead is not offset by the performance gains in handling simultaneous processes. • RAID 6 costs more because of the extra capacity required by using two parity blocks per stripe.
Drives	3 to 32

2.2.5 RAID IME (RAID 1E)

An Integrated Mirroring Enhanced (IME) volume can be configured with up to ten mirrored disks (one or two global hot spares can also be added). Figure 5 shows the logical view and physical view of an IME volume with three mirrored disks. Each mirrored stripe is written to a disk and mirrored to an adjacent disk. This type of configuration is also called RAID 1E.

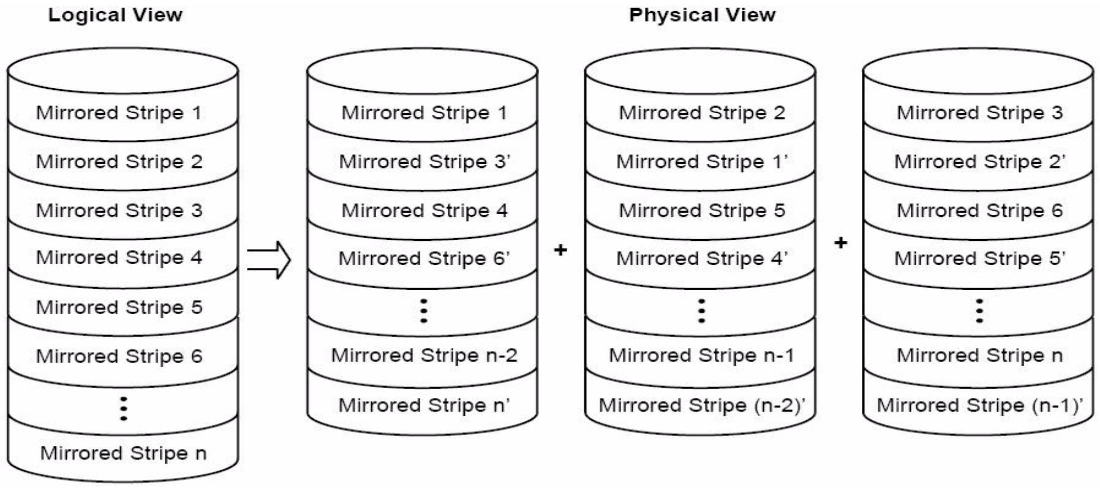


Figure 5. RAID IME with three disks

Table 6. RAID IME overview

Uses	Use RAID IME for small databases or any other environment that requires fault tolerance but small capacity.
Strong points	• Provides complete data redundancy. • Ideal for any application that requires fault tolerance and minimal capacity.
Weak points	• Requires twice as many disk drives. • Performance is impaired during drive rebuilds.
Drives	3 to 10

2.2.6 RAID 10 - Combination of RAID 1 and RAID 0

RAID 10 is a combination of RAID 0 and RAID 1. RAID 10 consists of stripes across mirrored drives. RAID 10 breaks up data into smaller blocks and then mirrors the blocks of data to each RAID 1 set. Each RAID 1 set then duplicates its data to its other drive. The size of each block is determined by the stripe size parameter, which is set during the creation of the RAID set. RAID 10 supports up to eight spans.

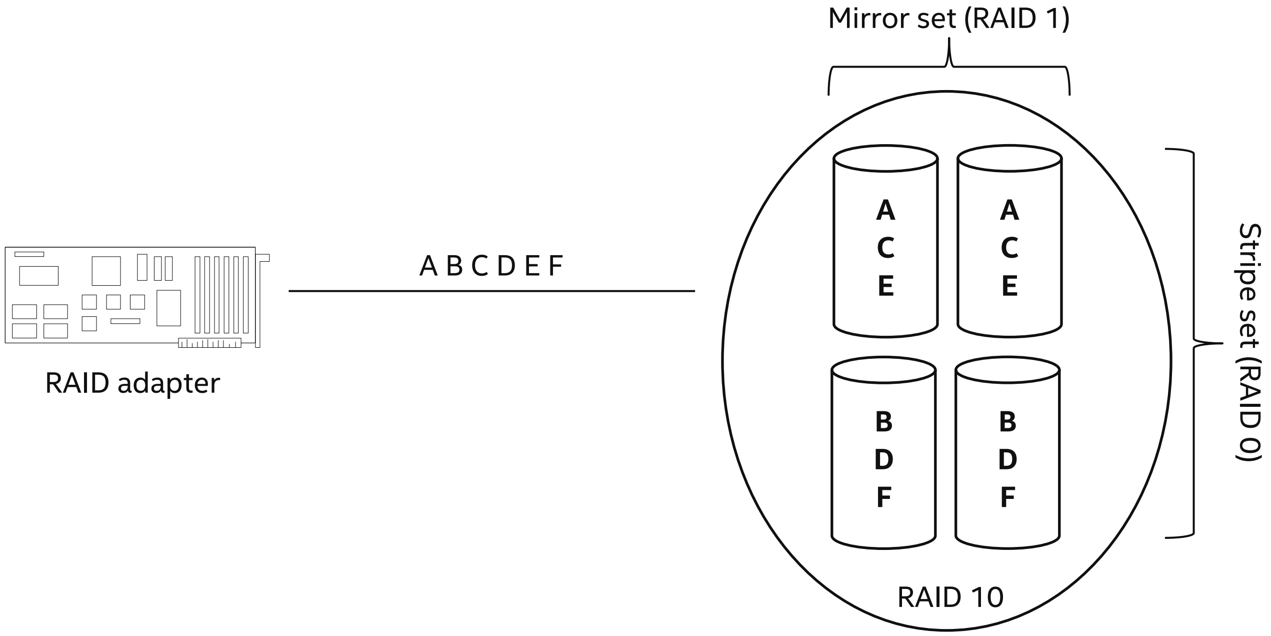


Figure 6. RAID 10 – combination of RAID 1 and RAID 0

Table 7 provides an overview of RAID 10.

Table 7. RAID 10 overview

Uses	Appropriate when used with data storage that requires 100 percent redundancy of mirrored arrays and that needs the enhanced I/O performance of RAID 0 (striped arrays). RAID 10 works well for medium-sized databases or any environment that requires a higher degree of fault tolerance and moderate to medium capacity.
Strong points	• Provides both high data transfer rates and complete data redundancy.
Weak points	• Requires twice as many drives as all other RAID levels except RAID 1.
No. of drives	4 to 240
Capacity	(N*C)/2, where N is number of disks and C is disk capacity.

2.2.7 RAID 50 - Combination of RAID 5 and RAID 0

RAID 50 provides the features of both RAID 0 and RAID 5. RAID 50 includes both parity and disk striping across multiple arrays. RAID 50 is best implemented on two RAID 5 disk arrays with data striped across both disk groups.

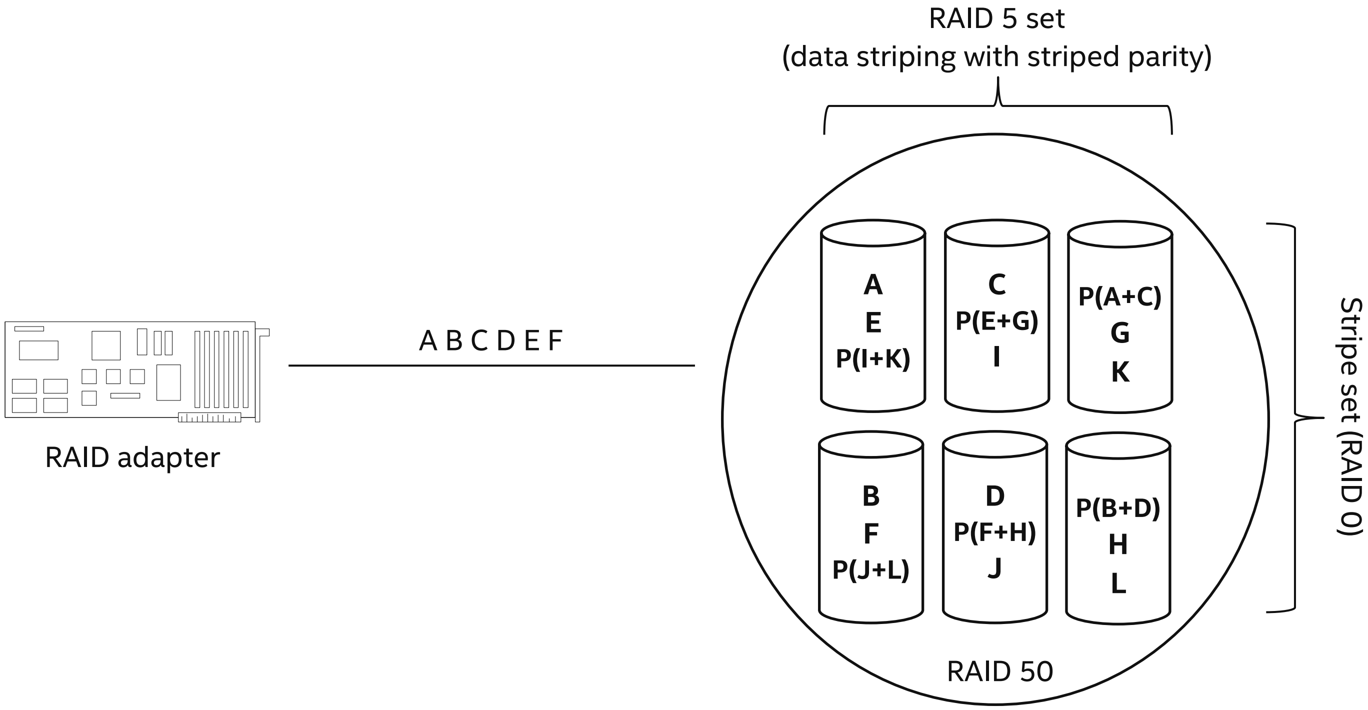


Figure 7. RAID 50 – combination of RAID 5 and RAID 0

RAID 50 breaks up data into smaller blocks and then stripes the blocks of data to each RAID 5 disk set. RAID 5 breaks up data into smaller blocks, calculates parity by performing an exclusive-or on the blocks and then writes the blocks of data and parity to each drive in the array. The size of each block is determined by the stripe size parameter, which is set during the creation of the RAID set.

RAID level 50 supports up to eight spans and tolerates up to eight drive failures, though less than total disk drive capacity is available. Though multiple drive failures can be tolerated, only one drive failure can be tolerated in each RAID 5 level array.

Table 8 provides an overview of RAID 50.

Table 8. RAID 50 overview

Uses	Appropriate when used with data that requires high reliability, high request rates, high data transfer, and medium to large capacity.
Strong points	• Provides high data throughput, data redundancy, and very good performance.
Weak points	• Requires 2 to 8 times as many parity drives as RAID 5.
Drives	6 to 32
Capacity	(N*C)(N-1)/N, where N is number of disks and C is disk capacity.

2.2.8 RAID 60 - Combination of RAID 6 and RAID 0

RAID 60 provides the features of both RAID 0 and RAID 6, and includes both parity and disk striping across multiple arrays. RAID 6 supports two independent parity blocks per stripe.

A RAID 60 virtual disk can survive the loss of two disks in each of the RAID 6 sets without losing data. RAID 60 is best implemented on two RAID 6 disk groups with data striped across both disk groups.

The following figure shows a RAID 6 data layout. The second set of parity drives are denoted by Q. The P drives follow the RAID 5 parity scheme.

Note: When only three hard drives are available for RAID 6, the situation has to be that P equals Q equals original data, which means that the three hard drives have the same original data, which can afford two disk failures.

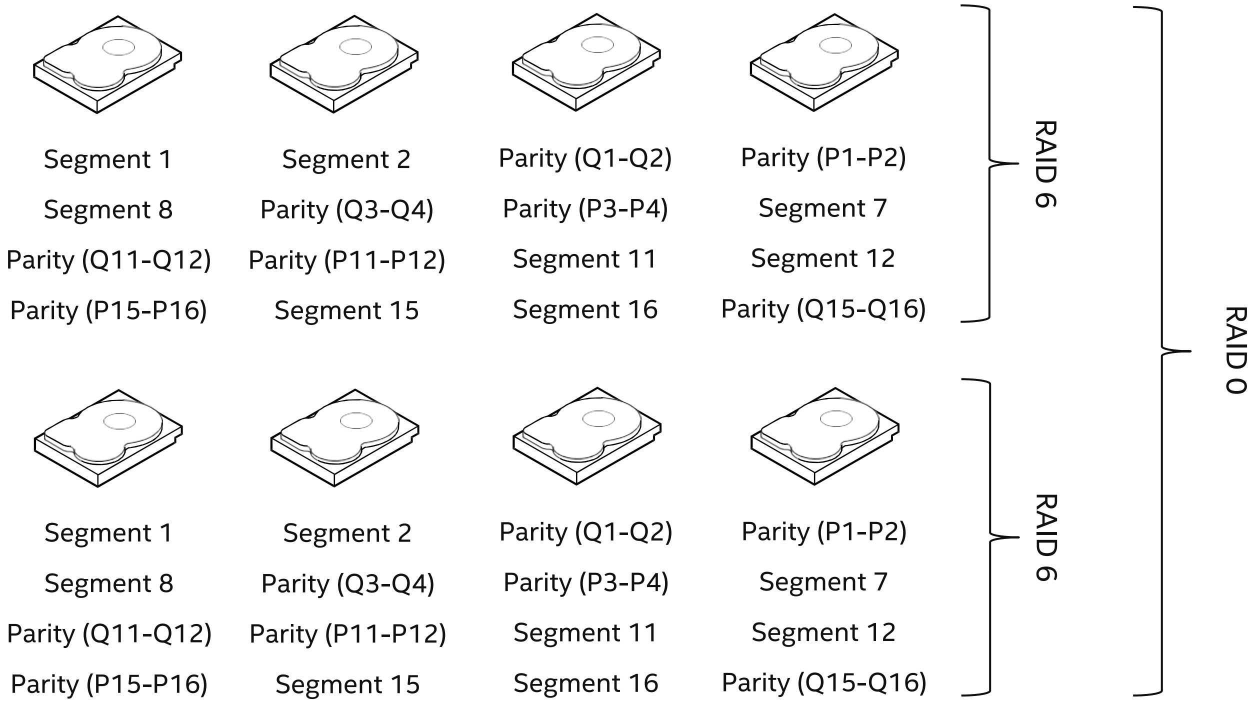


Figure 8. RAID 60 – combination of RAID 6 and RAID 0

Note: Parity is distributed across all drives in the array.

RAID 60 breaks up data into smaller blocks, and then stripes the blocks of data to each RAID 6 disk set. RAID 6 breaks up data into smaller blocks, calculates parity by performing an exclusive-or on the blocks and then writes the blocks of data and parity to each drive in the array. The size of each block is determined by the stripe size parameter, which is set during the creation of the RAID set.

RAID 60 supports up to eight spans and tolerates up to 16 drive failures, though less than total disk drive capacity is available. Each RAID 6 level can tolerate two drive failures.

Table 9 provides an overview of RAID 60.

Table 9. RAID 60 overview

Uses	Provides a high level of data protection through the use of a second parity block in each stripe. Use RAID 60 for data that requires a very high level of protection from loss. In the case of a failure of one drive or two drives in a RAID set in a virtual disk, the RAID controller uses the parity blocks to recreate all the missing information. If two drives in a RAID 6 set in a RAID 60 virtual disk fail, two drive rebuilds are required, one for each drive. These rebuilds do not occur at the same time. The controller rebuilds one failed drive, and then the other failed drive. Use for office automation, online customer service that requires fault tolerance or for any application that has high read request rates but low write request rates.
Strong points	• Provides data redundancy, high read rates, and good performance in most environments. • Each RAID 6 set can survive the loss of two drives or the loss of a drive while another drive is being rebuilt. • Provides the highest level of protection against drive failures of all of the RAID levels. • Read performance is similar to that of RAID 50, though random reads in RAID 60 might be slightly faster because data is spread across at least one more disk in each RAID 6 set.
Weak points	• Not well suited to tasks requiring a lot of writes. A RAID 60 virtual disk has to generate two sets of parity data for each write operation, which results in a significant decrease in performance during writes. • Disk drive performance is reduced during a drive rebuild. • Environments with few processes do not perform as well because the RAID overhead is not offset by the performance gains in handling simultaneous processes. • RAID 6 costs more because of the extra capacity required by using two parity blocks per stripe.
Drives	A minimum of 6.

2.3 RAID Configuration Strategies

The most important factors in RAID array configuration are virtual disk availability (fault tolerance), virtual disk performance, and virtual disk capacity.

A virtual disk cannot be configured to optimize all three factors, but it is easy to choose a virtual disk configuration that maximizes one factor at the expense of another factor. For example, RAID 1 (mirroring) provides excellent fault tolerance, but requires a redundant drive. The following subsections describe how to use the RAID levels to maximize virtual disk availability (fault tolerance), virtual disk performance, and virtual disk capacity.

2.3.1 Maximizing Fault Tolerance

Fault tolerance is achieved through the ability to perform automatic and transparent rebuilds using hot-spare drives and hot swaps. A hot-spare drive is an unused online available drive that the RAID controller instantly plugs into the system when an active drive fails. After the hot spare is automatically moved into the RAID array, the failed drive is automatically rebuilt on the spare drive. The RAID array continues to handle requests while the rebuild occurs.

A hot swap is the manual substitution of a replacement unit in a disk subsystem for a defective one, where the substitution can be performed while the subsystem is running hot-swap drives. Auto-Rebuild in the WebBIOS Configuration Utility allows a failed drive to be replaced and automatically rebuilt by “hot swapping” the drive in the same drive bay. The RAID array continues to handle requests while the rebuild occurs, providing a high degree of fault tolerance and zero downtime.

Table 10. RAID levels and fault tolerance

RAID Level	Fault Tolerance
0	Does not provide fault tolerance. All data is lost if any drive fails. Disk striping writes data across multiple disk drives instead of just one disk drive. It involves partitioning each drive storage space into stripes that can vary in size. RAID 0 is ideal for applications that require high bandwidth but do not require fault tolerance.
1 or IME	Provides complete data redundancy. If one drive fails, the contents of the other drive can be used to run the system and reconstruct the failed drive. The primary advantage of disk mirroring is that it provides 100 percent data redundancy. Since the contents of the drive are completely written to a second drive, no data is lost if one of the drives fails. Both drives contain the same data at all times. RAID 1 or IME is ideal for any application that requires fault tolerance and minimal capacity.
5	Combines distributed parity with disk striping. Parity provides redundancy for one drive failure without duplicating the contents of entire disk drives. If a drive fails, the RAID controller uses the parity data to reconstruct all missing information. In RAID 5, this method is applied to the entire drive or stripes across all disk drives in an array. Using distributed parity, RAID 5 offers fault tolerance with limited overhead.
6	Combines distributed parity with disk striping. RAID 6 can sustain two drive failures and still maintain data integrity. Parity provides redundancy for two drive failures without duplicating the contents of entire disk drives. If a drive fails, the RAID controller uses the parity data to reconstruct all missing information. In RAID 6, this method is applied to entire drives or stripes across all drives in an array. Using distributed parity, RAID 6 offers fault tolerance with limited overhead.
10	Provides complete data redundancy using striping across spanned RAID 1 arrays. RAID 10 works well for any environment that requires the 100 percent redundancy offered by mirrored arrays. RAID 10 can sustain a drive failure in each mirrored array and maintain drive integrity.
50	Provides data redundancy using distributed parity across spanned RAID 5 arrays. RAID 50 includes both parity and disk striping across multiple drives. If a drive fails, the RAID controller uses the parity data to recreate all missing information. RAID 50 can sustain one drive failure per RAID 5 array and still maintain data integrity.
60	Provides data redundancy using distributed parity across spanned RAID 6 arrays. RAID 60 can sustain two drive failures per RAID 6 array and still maintain data integrity. It provides the highest level of protection against drive failures of all of the RAID levels. RAID 60 includes both parity and disk striping across multiple drives. If a drive fails, the RAID controller uses the parity data to recreate all missing information.

2.3.2 Maximizing Performance

A RAID disk subsystem improves I/O performance. The RAID array appears to the host computer as a single storage unit or as multiple virtual units. I/O is faster because drives can be accessed simultaneously. Table 11 describes the performance for each RAID level.

Table 11. RAID levels and performance

RAID Level	Performance
0	RAID 0 (striping) offers the best performance of any RAID level. RAID 0 breaks up data into smaller blocks, then writes a block to each drive in the array. Disk striping writes data across multiple drives instead of just one drive. It involves partitioning each drive storage space into stripes that can vary in size from 8 KB to 128 KB. These stripes are interleaved in a repeated sequential manner. Disk striping enhances performance because multiple drives are accessed simultaneously.
1 or IME	With RAID 1 or IME (mirroring), each drive in the system must be duplicated, which requires more time and resources than striping. Performance is impaired during drive rebuilds.
5	RAID 5 provides high data throughput, especially for large files. Use this RAID level for any application that requires high read request rates, but low write request rates, such as transaction processing applications, because each drive can read and write independently. Since each drive contains both data and parity, numerous writes can take place concurrently. In addition, robust caching algorithms and hardware based exclusive-or assist make RAID 5 performance exceptional in many different environments. Parity generation can slow the write process, making write performance significantly lower for RAID 5 than for RAID 0 or RAID 1. Disk drive performance is reduced when a drive is being rebuilt. Clustering can also reduce drive performance. Environments with few processes do not perform as well because the RAID overhead is not offset by the performance gains in handling simultaneous processes.

6	RAID 6 works best when used with data that requires high reliability, high request rates, and high data transfer. It provides high data throughput, data redundancy, and very good performance. However, RAID 6 is not well suited to tasks requiring a lot of writes. A RAID 6 virtual disk has to generate two sets of parity data for each write operation, which results in a significant decrease in performance during writes. Disk drive performance is reduced during a drive rebuild. Environments with few processes do not perform as well because the RAID overhead is not offset by the performance gains in handling simultaneous processes.
10	RAID 10 works best for data storage that need the enhanced I/O performance of RAID 0 (striped arrays), which provides high data transfer rates. Spanning increases the size of the virtual volume and improves performance by doubling the number of spindles. The system performance improves as the number of spans increases (the maximum number of spans is eight). As the storage space in the spans is filled, the system stripes data over fewer and fewer spans and RAID performance degrades to that of a RAID 1 or RAID 5 array.
50	RAID 50 works best when used with data that requires high reliability, high request rates, and high data transfer. It provides high data throughput, data redundancy, and very good performance. Spanning increases the size of the virtual volume and improves performance by doubling the number of spindles. The system performance improves as the number of spans increases (the maximum number of spans is eight). As the storage space in the spans is filled, the system stripes data over fewer and fewer spans and RAID performance degrades to that of a RAID 1 or RAID 5 array.
60	RAID 60 works best when used with data that requires high reliability, high request rates, and high data transfer. It provides high data throughput, data redundancy, and very good performance. Spanning increases the size of the virtual volume and improves performance by doubling the number of spindles. The system performance improves as the number of spans increases (the maximum number of spans is eight). As the storage space in the spans is filled, the system stripes data over fewer and fewer spans and RAID performance degrades to that of a RAID 1 or RAID 6 array. RAID 60 is not well suited to tasks requiring a lot of writes. A RAID 60 virtual disk has to generate two sets of parity data for each write operation, which results in a significant decrease in performance during writes. Disk drive performance is reduced during a drive rebuild. Environments with few processes do not perform as well because the RAID overhead is not offset by the performance gains in handling simultaneous processes.

2.3.3 Maximizing Storage Capacity

Storage capacity is an important factor when selecting a RAID level. There are several variables to consider. Striping alone (RAID 0) requires less storage space than mirrored data (RAID 1 or IME) or distributed parity (RAID 5 or RAID 6). RAID 5, which provides redundancy for one drive failure without duplicating the contents of entire disk drives, requires less space than RAID 1. Table 12 explains the effects of the RAID levels on storage capacity.

Table 12. RAID levels and capacity

RAID Level	Storage Capacity
0	RAID 0 (disk striping) involves partitioning each drive storage space into stripes that can vary in size. The combined storage space is composed of stripes from each drive. RAID 0 provides maximum storage capacity for a given set of physical disks.
1 or IME	With RAID 1 (mirroring), data written to one disk drive is simultaneously written to another disk drive, which doubles the required data storage capacity. This is expensive because each drive in the system must be duplicated.
5	RAID 5 provides redundancy for one drive failure without duplicating the contents of entire disk drives. RAID 5 breaks up data into smaller blocks, calculates parity by performing an exclusive-or on the blocks, then writes the blocks of data and parity to each drive in the array. The size of each block is determined by the stripe size parameter, which is set during the creation of the RAID set.
6	RAID 6 provides redundancy for two drive failures without duplicating the contents of entire disk drives. However, it requires extra capacity because it uses two parity blocks per stripe. This makes RAID 60 more expensive to implement.
10	RAID 10 requires twice as many drives as all other RAID levels except RAID 1. RAID 10 works well for medium-sized databases or any environment that requires a higher degree of fault tolerance and moderate to medium capacity. Disk spanning allows multiple disk drives to function like one big drive. Spanning overcomes lack of disk space and simplifies storage management by combining existing resources or adding relatively inexpensive resources.

50	RAID 50 requires two to four times as many parity drives as RAID 5. This RAID level works best when used with data that requires medium to large capacity.
60	RAID 60 provides redundancy for two drive failures in each RAID set without duplicating the contents of entire disk drives. However, it requires extra capacity because a RAID 60 virtual disk has to generate two sets of parity data for each write operation. This makes RAID 60 more expensive to implement.

2.3.4 Array Purpose

Important factors to consider when creating RAID arrays include availability, performance, and capacity. Define the major purpose of the disk array by answering questions related to these factors, such as the following, which are followed by suggested RAID levels for each situation:

- Will this disk array increase the system storage capacity for general-purpose file and print servers? If so, use RAID 5, 6, 10, 50, or 60.
- Does this disk array support any software system that must be available 24 hours per day? If so, use RAID 1, IME, 5, 6, 10, 50, or 60.
- Will the information stored in this disk array contain large audio or video files that must be available on demand? If so, use RAID 0.
- Will this disk array contain data from an imaging system? If so, use RAID 0 or 10.

Refer to Table 14 to help plan the array configuration. Rank the requirements for the array, such as storage space and data redundancy, in order of importance, and then review the suggested RAID levels.

Table 13. Suggestions based on requirements for array configuration

Requirement	Suggested RAID Level
Storage space	RAID 0, RAID 5
Data redundancy	RAID 5, RAID 6, RAID 10, RAID 50, RAID 60
Physical disk performance and throughput	RAID 0, RAID 10
Hot spares (extra physical disks required)	RAID 1, RAID IME, RAID 5, RAID 6, RAID 10, RAID 50, RAID 60

2.3.5 Configuration Planning

Factors to consider when planning a configuration are the number of physical disks the RAID controller can support, the purpose of the array, and the availability of spare drives.

Each type of data stored in the disk subsystem has a different frequency of read and write activity. Knowing the data access requirements helps to successfully determine a strategy for optimizing the disk subsystem capacity, availability, and performance.

Servers that support video-on-demand typically read the data often, but write data infrequently. Both the read and write operations tend to be long. Data stored on a general-purpose file server involves relatively short read and write operations with relatively small files.

2.4 RAID Features

2.4.1 RAID Availability Concept

Data availability without downtime is essential for many types of data processing and storage systems. Businesses want to avoid the financial costs and customer frustration associated with failed servers. RAID helps maintain data availability and avoid downtime for the servers that provide that data. RAID offers several features, such as spare drives and rebuilds, that can be used to fix any physical disk problems, while keeping the servers running and data available. The following subsections describe these features.

2.4.2 Spare Drives

Spare drives can replace failed or defective drives in an array. A replacement drive must be at least as large as the drive it replaces. Spare drives include hot swaps, hot spares, and cold swaps.

A hot swap is the manual substitution of a replacement unit in a disk subsystem for a defective one, where the substitution can be performed while the subsystem is running (performing its normal functions). In order for the functionality to work, the backplane and enclosure must support hot swap.

Hot-spare drives are physical drives that power up along with the RAID drives and operate in a standby state. If a physical disk used in a RAID virtual disk fails, a hot spare automatically takes its place and the data on the failed drive is rebuilt on the hot spare. Hot spares can be used for RAID levels 1, IME, 5, 6, 10, 50, and 60.

Note: If a rebuild to a hot spare fails for any reason, the hot-spare drive is marked as failed. If the source drive fails, both the source drive and the hot-spare drive are marked as failed.

Before replacing a defective physical disk in a disk subsystem, a cold swap requires that the system be powered down.

2.4.3 Rebuild

If a physical disk fails in an array that is configured as a RAID 1, IME, 5, 6, 10, 50, or 60 virtual disk, the lost data can be recovered by rebuilding the drive. The RAID controller automatically tries to use any configured hot spares to rebuild failed arrays. A manual rebuild is necessary if there are no hot spares available with enough capacity to rebuild the failed array. Before rebuilding the failed array, a drive with enough storage must be installed into the subsystem.

2.4.4 Drive in Foreign State

Sometimes newly inserted drives are not brand new and they were previously used in a RAID configuration, this may be because we purposely want to import a RAID virtual drive from another controller or we are just re-using a disk drive. The RAID controller detects this and puts the drive in Foreign State. Drives cannot be configured directly and the controller needs to be instructed on what to do with the drive(s) in foreign state, either import or clear the foreign configuration. The Configuration Utility or any Monitoring and configuration Utility can be used to detect, import and clear the Foreign Configuration. Once the Foreign Configuration is successfully imported, the drives will become Configured Good (or bad if the drive is found in a failed state). Once the Foreign Configuration is successfully cleared, the drives will become Unconfigured Good (or bad if the drive is found in a failed state).

2.4.5 Copyback

When a hot spare drive is used to replace a failed drive in a virtual drive, the hot spare drive temporary becomes a *configured good* drive and also becomes part of the array. When eventually the failed drive gets replaced, in order to maintain the original configuration, the data in the temporary *configured good* drive is copied to the new inserted drive (copy back operation) and when this operation is done, the new inserted drive becomes the definite replaced drive and the drive used as a temporary replacement reverts back to its original hot spare status. The Copyback operation is set to Automatic by default, but it can be turned to manual. This operation runs as a background activity and the virtual drive is still available online to the host.

Copyback is also initiated when the first Self-Monitoring Analysis and Reporting Technology (SMART) error occurs on a drive that is part of a virtual drive. The destination drive is a hot spare that qualifies as a rebuild drive. The drive with the SMART error is marked as failed only after the successful completion of the copyback. This avoids putting the drive group in degraded status.

Note: During a copyback operation, if the drive group involved in the copyback is deleted because of a virtual drive deletion, the destination drive reverts to an Unconfigured Good state or hot spare state.

2.4.5.1 Order of Precedence

In the following scenarios, rebuild takes precedence over the copyback operation:

- If a copyback operation is already taking place to a hot spare drive, and any virtual drive on the controller degrades, the copyback operation aborts, and a rebuild starts. The rebuild changes the virtual drive to the optimal state.
- The rebuild operation takes precedence over the copyback operation when the conditions exist to start both operations. For example:
  - Where the hot spare is not configured (or unavailable) in the system.
  - There are two drives (both members of virtual drives), with one drive exceeding the SMART error threshold, and the other failed.
  - If a hot spare (assume a global hot spare) is added during a copyback operation, the copyback is aborted, and the rebuild operation starts on the hot spare.

2.4.6 UEFI 2.0 Support

UEFI 2.0 provides MegaRAID customers with expanded platform support. The MegaRAID UEFI 2.0 driver, a boot service device driver, handles block IO requests and SCSI pass-through (SPT) commands, and offers the ability to launch pre-boot MegaRAID management applications through a driver configuration protocol (DCP). The UEFI driver also supports driver diagnostic protocol, which allows administrators to access pre-boot diagnostics.

2.4.7 MegaRAID Fast Path

The MegaRAID Fast Path Premium Feature is a high performance IO Accelerator technology for Solid State Drive RAID Arrays connected to a MegaRAID adapter. There are two levels to this feature. Level 1 Fast Path is enabled by default without a premium feature key (PFK). The Level 1, or standard, Fast Path pertains to general IO path improvements to write through data transfers. Additionally, controller cache tuning has resulted in improvements to configurations leveraging write back mode.

Level 2 Fast Path is enabled automatically with Intel® RAID Premium Feature Key AXXRPFKSSD or AXXRPFKSSD2 installed. Level 2 Fast Path is solid state drive (SSD)-centric. This is where the premium feature kicks in by supporting full optimization of SSD virtual disk groups. With this premium feature enabled, SSD configurations tuned for small, random block-size IO activity – typical of transactional database applications – can sustain higher numbers of IO reads per second, compared with Level 1 Fast Path. The performance levels reached with this solution are equivalent to those of much costlier flash-based adapter card solutions.

Refer to *Intel® RAID Premium Feature Key AXXRPFKSSD, AXXRPFKDE, and AXXRPFKSNSH Installation Guide* (E88588-00x) or *Intel® RAID Premium Feature Keys AXXRPFKSSD2, AXXRPFKDE2, and AXXRPFKSNSH2 Installation Guide* (G29824-00x) for description of the PFK.

2.4.8 4K Sector Drive Support

All the modules and controllers listed in this guide (see Table 1) and newer have support for 512e and 4Kn drives; older firmware versions might not yet have this support. Refer to the next table for details on this support for a particular RAID module or controller.

Table 14. Advanced format support on Intel® RAID Modules and Controllers

R3LC[5]	**Yes**	**Yes**	**Yes**
R3LC5[6]	Yes	Yes	Yes
RS3PC[8]	Yes	Yes	Yes
R3YC[7]	Yes	Yes	Yes
RCS25ZB040	Yes[2]	Yes[2]	Yes[2]
RCS25ZB040LX	Yes[2]	Yes[2]	Yes[2]
RMS25CB040	Yes[2]	Yes[2]	Yes[2]
RMS25CB080	Yes[2]	Yes[2]	Yes[2]
RMS25CB080N	Yes[2]	Yes[2]	Yes[2]
RMS25PB040	Yes[2]	Yes[2]	Yes[2]
RMS25PB080	Yes[2]	Yes[2]	Yes[2]
RMS25PB080N	Yes[2]	Yes[2]	Yes[2]
RMS3CC040	Yes	Yes	Yes
RMS3CC080	Yes	Yes	Yes
RMS3HC040	Yes	Yes	Yes
RMS3HC080	Yes	Yes	Yes
RMT3CB080	Yes[2,4]	Yes[2]	N/A
RMT3PB080	Yes[2,4]	Yes[2]	N/A
RS25AB080	Yes[2]	Yes[2]	Yes[2]
RS25DB080	Yes[2]	Yes[2]	Yes[2]
RS25GB008	Yes	Yes	Yes
RS25NB008	Yes[2]	Yes[2]	Yes[2]
RS25SB008	Yes[2]	Yes[2]	Yes[2]
RS3DC040	Yes	Yes	Yes
RS3DC080	Yes	Yes	Yes
RS3GC008	Yes	Yes	Yes
RS3MC044	Yes	Yes	Yes
RS3SC008	Yes	Yes	Yes
RS3UC080	Yes	Yes	Yes
RS3WC040	Yes	Yes	Yes
RS3WC080	Yes	Yes	Yes

[2] From MR 5.5 (firmware version 3.230.05-2100 in FWPKG-v23.11.0-0021).
[4] Only SATA.
[5] RAID controller for the Intel® AHWKPTP12GBGB bridge board for the HWFF systems.
[6] RAID controller for the Intel® AHWKPTP12GBGBR5 bridge board for the HWFF systems.
[7] Onboard LSI 3008 SAS RAID controller for the Intel® Server Boards S2600CW2S and S2600CW2SR.
[8] RAID controller for the Intel® FHWKPTPBGB24 bridge board for the HWFF systems.

All new Tri-Mode modules and controllers have full support for 512e and 4Kn drives.

2.4.9 Larger than 2 TB Drive Support

All the modules and controllers listed in this guide (see Table 1) and newer can fully recognize and configure the volume of disk drives larger than 2 TB; however, there might be limitations on the operating system used and normally a GUID Partition Table (GPT) type partition is required. Make sure the OS has support for GPT partitions.

2.4.10 Error Handling

- Most commands are retried four or more times. The firmware is programmed to provide the best effort to recognize an error and recover from it if possible.
- Failures are logged and stored in NVRAM. Operating system-based errors are viewable from the event viewer in Intel RAID Web Console 2.
- RAID-related errors can be reported by the hard drive firmware, SCSI Accessed Fault-Tolerant Enclosure (SAF-TE) controller, or the RAID controller firmware. These errors may be reported to the operating system through the RAID management software, through SMART monitoring, or through the Common Information Model (CIM) Management Software. Some errors may also be reported by the SAF-TE controller and logged in the system event log (SEL) for the Intel® Server Board. In addition, the operating system may report access errors. Depending on the RAID controller and drive enclosure, the error may be evident by the color of LEDs, the flashing of LEDs, or audible alarms.

2.4.11 Shield State

Physical devices in RAID firmware transit between different states. If the firmware detects a problem or a communication loss for a physical drive, the firmware transitions the drive to a bad (Failed or Unconfigured Bad) state. To avoid transient failures, an interim state called the Shield State is introduced before marking the drive as being in a bad state.

The Shield State is an interim state of a physical drive for diagnostic operations. The results of the diagnostic tests determine if the physical drive is good or bad. If any of the diagnostic tests fail, the physical drive transitions to a bad state (Failed or Unconfigured Bad).

The three possible Shield States are:

- **Unconfigured** – Shielded
- **Configured** – Shielded
- **Hotspare** – Shielded

Physical View and Logical View in the Configuration Utility or any Monitoring and Management Utility can reflect drive Shield State. Other drive states include:

- Unconfigured Good
- Online
- Hotspare
- Failed
- Rebuilding
- Unconfigured Bad
- Missing
- Offline
- None

2.4.12 Dimmer Switch or Power Save feature

The controller conserves energy by placing certain unused drives into power save mode. The controller automatically spins up drives from power save mode when necessary. Drives that can be set to power save mode are: Unconfigured Drives, Hot Spare Drives, and Configured Drives. The power save mode is only supported by the full featured RAID modules and controllers.

2.4.13 Online capacity expansion

- Online capacity expansion (OCE) to add capacity to the virtual drive. The added capacity can be presented to the operating system as additional space for the operating system to partition it as an additional drive, or it may be added to an operating system drive, depending upon the capability of the operating system.
- Online RAID level migration allows for upgrading a RAID level. Options are to go from RAID 1 to RAID 0, RAID 5 to RAID 0, RAID 6 to RAID 0, RAID 6 to RAID 5. With OCE, options are to go from RAID 0 to RAID 1, RAID 0 to RAID 5, RAID 0 to RAID 6, RAID 1 to RAID 5, RAID 1 to RAID 6, RAID 5 to RAID 6. The following limitations apply:
  - No migrating or OCE on a spanned RAID array or disk group (RAID 10, RAID 50, or RAID 60).
  - No migration to a smaller capacity configuration.
  - No OCE when there is more than one virtual drive on a virtual array or disk group.
- Each controller allows 128 virtual drives.
- When five or more disks are used, smart initialization automatically checks consistency of virtual drives for RAID 5. This allows performance optimization by enabling read-modify-write mode of operation with five or more disks in a RAID 5 array or disk group. Peer read mode of operation is used when the RAID 5 array or disk group contains three or four physical drives.
- If the system shuts down, the initialization or rebuild process automatically resumes on the next boot. Auto resume must be enabled prior to virtual drive creation.
- Stripe size is user definable on a per drive basis and can be 8, 16, 32, 64, or 128 KB in size. The default is 256 KB, which is optimal for many data access types.
- Hot spares can be set as global or dedicated. A global hot spare automatically comes online to replace the first drive to fail on any array or disk group on the controller. A dedicated hot spare is assigned to a specific array or disk group and only comes online to rebuild this specific failed array or disk group. A hot spare only comes online if it is the same size or larger than the failing drive (see drive coercion in the next point), and if a drive has been marked as failed. If a drive is removed (and marked as failed) within a virtual drive, the hot spare automatically comes online. However, there must be disk activity (I/O to the drive) in order for a missing drive to be marked as failed.
- Drive coercion refers to the ability of the controller to recognize the size of the physical drives connected and then force the larger drives to use only the amount of space available on the smallest drive. Drive coercion allows an option to map out a reserved space to compensate for slightly smaller drive sizes that may be added later. The default is set to 1 GB. The coercion algorithm options are:
  - None – No coercion of size.
  - 128 MB – The software rounds the drive capacity down to the next 128 MB boundary and then up to the nearest 10 MB until the coerced capacity is larger than the actual drive size. It is then reduced by 10 MB.
  - 1 GB – The software rounds the drive capacity down to the nearest 1 GB boundary and then down by 1 MB. This corresponds to the terms most drive manufacturers use.

2.4.14 Fault Tolerant Features

- Configuration on Disk (COD) and NVRAM (Non-volatile Random Access Memory) storage of array and disk group configuration information. Array and disk group configuration information is stored both on the hard drive (COD) and in NVRAM. This helps protect against loss of the configuration due to adapter and/or drive failure.

- Failed drives are automatically detected and a transparent rebuild of the failed array automatically occurs using a hot-spare drive.
- Support for SCSI Accessed Fault-Tolerant Enclosure (SAF-TE) enabled enclosures allows enhanced drive failure and rebuild reporting through enclosure LEDs; support also includes hot swapping of hard drives.
- A battery backup for cache memory is available as an option. RAID controller firmware automatically checks for the presence of the battery module, and if found, allows the write back cache option. The adapter continuously tracks the battery voltage and reports if the battery is low. If low, the battery is first given a fast charge to replenish the charge and is then given a trickle charge to keep it at an optimal power level. Adapters that support the battery module include a “dirty cache” LED; when power is lost to the system and data remains in the cache memory that has not been written to disk, the LED signals that this operation needs to be completed. Upon reboot, the data in memory can then write to the hard disk drive.
- Although I/O performance may be lower, hard disk drive write-back cache is disabled by default because data can potentially be lost if a power outage occurs. Enabling the HDD write-back cache may improve performance; when enabled, use an uninterruptible power supply (UPS) device to prevent data loss during power outages.
- Battery life is about three years. Monitor the battery health and replace when needed.
- Self-Monitoring Analysis and Reporting Technology (SMART) technology is supported. This provides a higher level of predictive failure analysis of the hard disk drives by the RAID controller.

2.4.15 Cache Options and Settings

Cache options and settings can be unique for each virtual drive.

- Cache Write Policy
  - Write Through – I/O completion is signaled only after the data is written to hard disk.
  - Write Back with Battery Backup Unit (BBU) – I/O completion is signaled when data is transferred to cache.
  - Always Write Back – Write back is enabled even if BBU is bad or missing.
- Cache Policy
  - Direct I/O – When possible, no cache is involved for both reads and writes. The data transfers are directly from host system to the disk and from the disk to the host system.
  - Cached I/O – All reads first look at cache. If a cache hit occurs, the data is read from cache; if not, the data is read from disk and the read data is buffered into cache. All writes to drive are also written to cache.
- Read Policy
  - No Read Ahead – Provides no read ahead for the virtual drive.
  - Read Ahead – Reads and buffers additional consecutive stripes/lines into cache.
  - Adaptive – The read ahead automatically turns on and off depending upon whether the disk is accessed for sequential reads or random reads.

2.4.16 Background Tasks

- Rebuilding a failed drive is performed in the background. The rebuild rate is tunable from 0-100 %.
  - The rebuild rate controls the amount of system resources allocated to the rebuild.

Caution: It is not recommended to increase the rebuild rate to over 50%. A higher rebuild rate can result in operating system requests not being serviced in a timely fashion and causing an operating system error.

- A consistency check scans the consistency of data on a fault-tolerant disk to determine if data has been corrupted.
- Background initialization is a background check of consistency. It has the same functionality as the check consistency option but is automatic and can be canceled only temporarily. If it is canceled, it starts again in a few minutes. Background initialization is only performed on redundant volumes.
- RAID level migration and online capacity expansion are completed in the background.
- Patrol read is a user definable option available in Intel® RAID Web Console 2 that performs drive reads in the background and maps out any bad areas of the drive.

2.4.17 Audible Alarm

The following list of beep tones is used on Intel® RAID Controllers. These beeps usually indicate that a drive has failed.

- Degraded Array or Disk Group – Short tone (1 second on), 1 second off
- Failed Array or Disk Group – Long tone (3 seconds on), 1 second off
- Hot Spare Commissioned – Short tone (1 second on), 3 seconds off

During a rebuild, the tone alarm stays on. After the rebuild completes, an alarm with a different tone will sound.

It is possible to silence the alarm until a power cycle occurs using the Configuration Utility or any of the Monitoring and Management Utilities.

3 Intel® RAID Firmware

All the Intel RAID controllers come with a pre-installed firmware package. This firmware is fully tested and functional, however, Intel releases firmware updates. The firmware packages are available at http://downloadcenter.intel.com for your particular controller. Intel recommends to update the controller's firmware since newer firmware packages may provide additional features and fixes to defects.

Note: Firmware downgrade is not supported. In case a firmware downgrade is required, please contact Intel Support for guidance.

See the readme file that accompanies the firmware package, it has a list of the supported RAID controllers, new features and fixes.

The firmware packages consists of:

- A .rom file which is the actual firmware binary file.
- An .nsh file which is the EFI script to install the firmware.
- A readme file with important information regarding supported controllers, fixes and enhancements.
- Utilities requides to install the firmware.

The normal way to install a firmware package is booting the system into the UEFI mode and running the .nsh script file. Follow the instructions indicated by the script.

An on-line firmware upgrade (upgrading the controller's firmware from the OS) is possible using the CmdTool2, StorCli, RAID Web Console 2 or RAID Web Console 3 utilities (see the Intel RAID Utilities guide for details).

4 Intel® RAID Drivers

The drivers that Intel provides for Intel® RAID Controllers are not compatible with SCSI or SATA-only RAID controllers. The RAID driver files are available on the resource CD that accompanies the RAID controllers. The driver files are also available at http://downloadcenter.intel.com. Transfer the driver files to another system by copying them to a USB key.

Note: Intel updates software frequently and updated drivers may provide additional features.

See the readme file that accompanies the download for updated information. For operating systems that are not listed here, but are listed at the above Intel website, see the readme file that accompanies the download for installation steps.

The next sections provide brief instructions in order to install the drivers in the most commonly used operating systems. For a complete explanation please consult the Intel RAID Driver Installation Guide.

4.1 RAID Driver Installation for Microsoft Windows*

4.1.1 Installation in a New Microsoft Windows* Operating System

This procedure installs the RAID device driver system during the Microsoft Windows* 2003, Microsoft Windows 2000, or Microsoft Windows XP operating system installation. The system must contain an Intel® RAID Controller. Microsoft Windows 2003 automatically adds the driver to the registry and copies the driver to the appropriate directory.

1. Start the Microsoft Windows installation by booting from the Microsoft Windows CD-ROM disk. The system BIOS must support booting from a CD- ROM drive. The BIOS settings may need to be changed to allow CD-ROM booting. See the system documentation for instructions.
2. When the screen displays `Press F6 if you need to install...`, press **<F6>** for the system to recognize the new driver.
3. When the screen displays `Setup could not determine the type...`, choose <S> to specify an additional device.

Note: If this screen is not displayed as the first user input, then the setup program did not register that the **<F6>** key was pressed. Reboot the system and return to step 2.

4. When the system asks for the manufacturer-supplied hardware support disk, insert the Microsoft Windows driver disk and press **<Enter>**.
5. Select the appropriate Microsoft Windows driver from the menu by highlighting it and pressing **<Enter>** to proceed. The driver is added to the registry and copied to the appropriate directory.
6. Continue with the Microsoft Windows operating system installation procedure.

4.1.2 Installation in an Existing Microsoft Windows* Operating System

This procedure installs or upgrades the RAID device driver on an existing Microsoft Windows* 2003, Microsoft Windows 2000, or Microsoft Windows XP operating system. The system must contain an Intel® RAID controller.

1. Boot to the Microsoft Windows* operating system. The Found New Hardware Wizard is displayed. The program identifies the SAS controller and requests the driver disk.
2. Insert the Microsoft Windows* driver disk into the floppy drive.

3. For Microsoft Windows 2003 or Microsoft Windows XP, choose **Install Software Automatically**. In Microsoft Windows 2000, choose **Search for a Suitable Driver** and specify the floppy drive as the search location.
4. Click **Next**. A message that this driver is not digitally signed may be displayed with information that a nonsigned driver is being installed. If this message appears, click **Continue Anyway**.
5. The system loads the driver from the Microsoft Windows driver disk and copies the driver to the system disk. The Found New Hardware Wizard screen displays the message:

   ```
   The wizard has finished...
   ```

6. Click **Finish** to complete the driver upgrade.

4.2 RAID Driver Installation for Red Hat* Enterprise Linux*

This section describes the installation of the device driver on new Red Hat* Enterprise Linux* 3, 4, or 5 systems. The following are general installation guidelines. Refer to the release notes that accompany the driver for information on updating the driver on an existing Red Hat Linux system.

1. Boot to the CD-ROM with Disk 1 with the command `linux dd`.
2. Press **<Enter>** at the boot prompt on the Welcome screen.
3. Copy the Linux driver image from the resource CD to a USB drive formatted with the FAT32 file system.
4. Insert the disk with driver image.
5. Select **Yes**.
6. Scroll down to select Intel® RAID adapter driver. The utility locates and loads the driver for the device.
7. Follow the Red Hat Linux installation procedure to complete the installation.

4.3 RAID Driver Installation for SuSE* Linux*

SuSE* Linux* uses a program called YaST2 (Yet another System Tool) to configure the operating system during installation.

Note: For complex installations, select **Install Manually** at the first install screen to use a different program, linuxrc. This section assumes a straightforward installation using YaST2.

1. Insert CD-ROM disk 1 into the CD-ROM drive and the RAID controller driver diskette in the floppy drive.
2. Boot to the CD-ROM.
3. The operating system loads a minimal operating system from the CD-ROM onto a RAM disk. The operating system also loads any driver module found in the floppy drive.
4. At the Welcome to YaST2 screen, select a language and click **Accept**.
5. At the Installation Settings screen, set up the disk partitioning.
6. Continue with the SuSE Linux installation procedure.

5 Intel® RAID Configuration Utilities

5.1 Intel® RAID BIOS Console 2 for 6 Gb/s Intel® RAID Controllers

The Intel® RAID BIOS Console 2 Configuration Utility for 6 Gb/s Intel® RAID Controllers is used on the generation 2.5 Intel® RAID Controllers based on the MegaRAID* software stack, specifically RS25GB008, RS25NB008, RS25DB080, RS25AB080, RS25SB008, RMS25PB080, RMS25PB040, RMT3PB080, RMS25CB080, RMS25CB040, and RMT3CB080

The Intel® RAID BIOS Console 2 Configuration Utility provides full-featured, GUI-based configuration and management of RAID arrays. It resides in the controller firmware and is independent of the operating system. Use the configuration utility for the 6 Gb/s Intel RAID Controllers to

- Select an Intel RAID Controller.
- Choose a configuration method for physical arrays, disk groups, and virtual drives.
- Create drive arrays.
- Define virtual drives.
- Initialize virtual drives.
- Access controllers, virtual drives, and physical arrays to display their properties.
- Create hot-spare drives.
- Rebuild failed drives.
- Verify data redundancy in RAID 1, 5, 6, 10, 50, or 60 virtual drives.

This section provides the steps to configure arrays and disk groups, and virtual drives using the Intel® RAID BIOS Console 2 utility. The following sections describe how to perform each action using the Intel® RAID BIOS Console 2 utility. A summary of the steps are as follows:

1. Power on the system and start the Intel® RAID BIOS Console 2 utility.
2. Start the Configuration Wizard.
3. Choose a configuration method.
4. Using the available physical drives, create arrays and disk groups.
5. Using the space in the arrays and disk groups, define the virtual drive(s).
6. Initialize the new virtual drives.

Note: Some server boards have a BIOS SETUP option called "Port 60/64 Emulation" (or other similar name). Please ensure this option is enabled in order to use Intel® RAID BIOS Console 2 successfully.

5.1.1 Start Intel® RAID BIOS Console 2

1. Power on the system. When `Press <Ctrl><G> to enter the RAID BIOS Console` is displayed, press the **<Ctrl>** and **<G>** keys to open the Controller Selection screen.
2. Select a controller and click **Start** to begin the configuration.

Note: If there is a configuration mismatch between the disks and the NVRAM, the utility automatically displays the Select Configuration screen. Choose whether the configuration should be read from the RAID array or from NVRAM. For more information, see section 4.1.5.

5.1.2 Intel® RAID BIOS Console 2 Screens and Options

This section describes the Intel® RAID BIOS Console 2 screens and options.

5.1.2.1 Toolbar Options

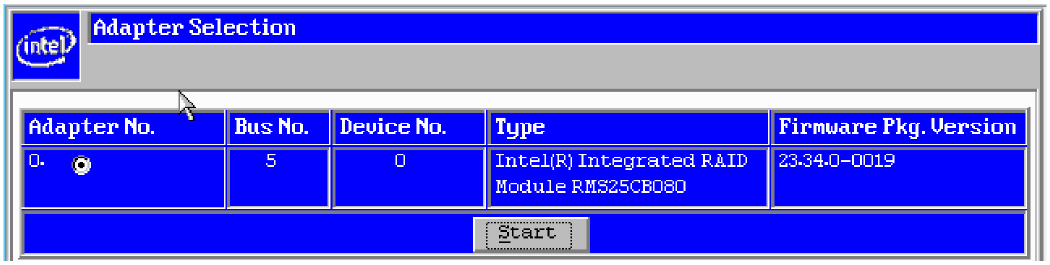
Table 16 describes the Intel® RAID BIOS Console 2 toolbar icons.

Table 15. Intel® RAID BIOS Console 2 toolbar icon descriptions

Icon	Description
⌂	Return to the main screen.
⬅	Return to the page accessed immediately before the current page.
⇥	Exit the Intel® RAID BIOS Console 2 utility.
🔈	Silence the alarm.

5.1.2.2 Controller Selection

Use controller selection to choose an Intel® RAID Controller installed in the system as shown in Figure 10.



Adapter Selection

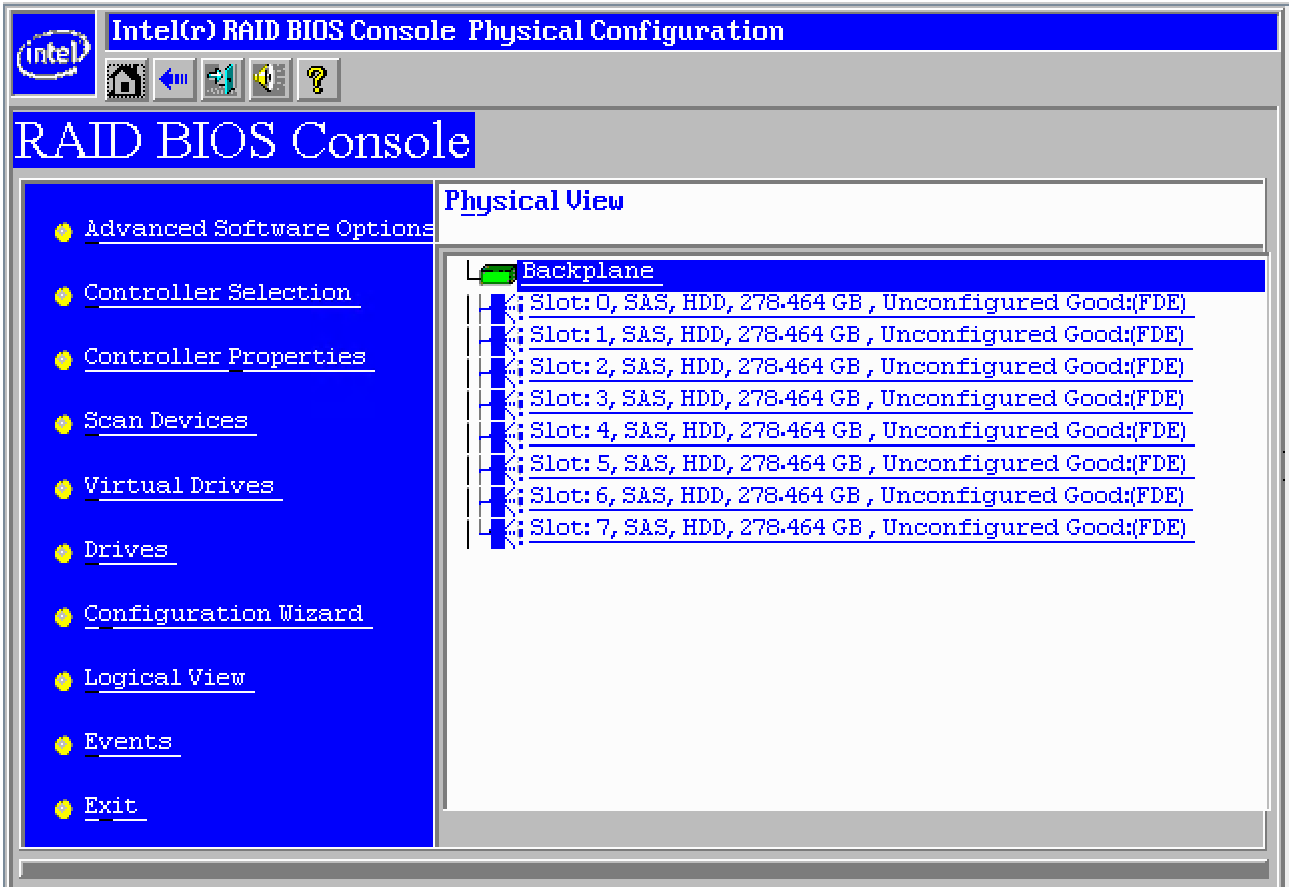
Adapter No.	Bus No.	Device No.	Type	Firmware Pkg. Version
0. ◉	5	0	Intel(R) Integrated RAID Module RMS25CB080	23.34.0-0019

Figure 9. Intel® RAID BIOS Console 2 – controller selection

5.1.2.3 Main Screen

The main screen provides options to scan the devices connected to the controller, select an Intel® RAID Controller, and switch between the Physical Drives view and Virtual Drives view. The main screen also provides access to additional screens and tools. The following options are available from the main screen:

- **Controller Selection** – Choose an Intel RAID Controller installed in the system (see section 5.1.2.2).
- **Controller Properties** – View and configure software and hardware of the selected controller (see section 5.1.2.4).
- **Scan Devices** – Check the physical and virtual drives for any changes in the drive status. The results of the scan are displayed in the physical and virtual drive descriptions.
- **Virtual Drives** – Manage virtual drives (see section 5.1.3).
- **Drives** – Manage physical drives (see section 5.1.4).
- **Configuration Wizard** – Open the Configuration Wizard to clear a configuration, create a new configuration or add a configuration. For detailed information on the Configuration Wizard, see section 5.1.6.
- **Physical View** – Toggle between the Physical View and the Logical View.
- **Events** – Display the events generated by physical drives, physical devices, enclosure, Intel® RAID Smart Battery, and SAS controller. For events and message descriptions, see Appendix B.
- **Exit** – Exit and reboot the system.

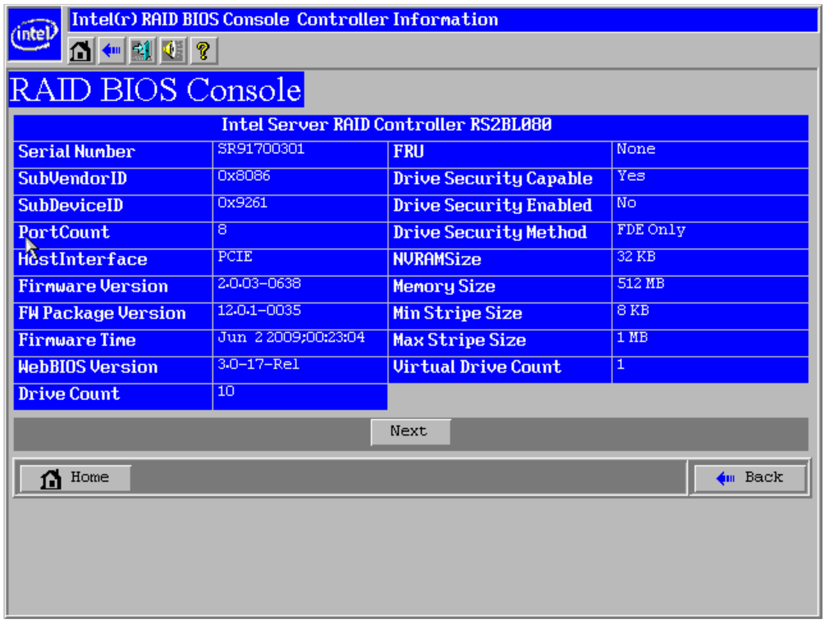


```
Backplane
Slot: 0, SAS, HDD, 278.464 GB , Unconfigured Good:(FDE)
Slot: 1, SAS, HDD, 278.464 GB , Unconfigured Good:(FDE)
Slot: 2, SAS, HDD, 278.464 GB , Unconfigured Good:(FDE)
Slot: 3, SAS, HDD, 278.464 GB , Unconfigured Good:(FDE)
Slot: 4, SAS, HDD, 278.464 GB , Unconfigured Good:(FDE)
Slot: 5, SAS, HDD, 278.464 GB , Unconfigured Good:(FDE)
Slot: 6, SAS, HDD, 278.464 GB , Unconfigured Good:(FDE)
Slot: 7, SAS, HDD, 278.464 GB , Unconfigured Good:(FDE)
```

Figure 10. Intel® RAID BIOS Console 2 main screen

5.1.2.4 Controller Properties Screen

Use the Controller Properties screen to view and configure the software and hardware of the selected controller.



Intel Server RAID Controller RS2BL080			
Serial Number	SR91700301	FRU	None
SubVendorID	0x8086	Drive Security Capable	Yes
SubDeviceID	0x9261	Drive Security Enabled	No
PortCount	8	Drive Security Method	FDE Only
HostInterface	PCIE	NVRAMSize	32 KB
Firmware Version	2.0.03-0638	Memory Size	512 MB
FW Package Version	12.0.1-0035	Min Stripe Size	8 KB
Firmware Time	Jun 2 2009;00:23:04	Max Stripe Size	1 MB
WebBIOS Version	3.0-17-Rel	Virtual Drive Count	1
Drive Count	10		

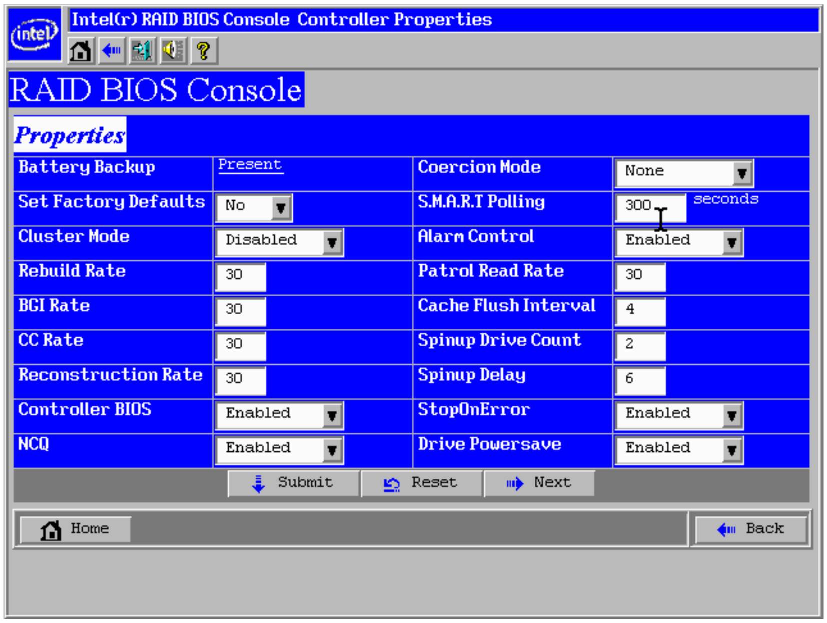
Figure 11. Intel® RAID BIOS Console 2 – controller properties

The following properties are viewable from the Controller Properties screen:

- **Firmware Version** – The firmware version.
- **Host Interface** – The host interface for the installed RAID controller.
- **NVRAM Size** – The NVRAM size on the RAID controller.
- **Firmware Time** – The firmware release date/time.
- **Min Stripe Size** – The minimum stripe size used to read and write data.
- **WebBIOS Version** – The BIOS version for the Intel® RAID BIOS Console 2.
- **Sub Device ID** – The sub-device ID (identification) for the RAID controller.
- **Sub Vendor ID** – The sub-vendor ID (identification) for the RAID controller.
- **Port Count** – Number of ports available.
- **Memory Size** – The memory size of the installed DIMM (Dual In-Line Memory Module).
- **Max Stripe Size** – The maximum stripe size.
- **Physical Disk Count** – The number of physical disks connected to the RAID controller.

5.1.2.5 Additional Controller Properties

To access additional controller properties, click **Next** on the Controller Properties screen. To change a property, select the new value and click **Submit**.



Battery Backup	Present	Coercion Mode	None
Set Factory Defaults	No	S.M.A.R.T Polling	300 seconds
Cluster Mode	Disabled	Alarm Control	Enabled
Rebuild Rate	30	Patrol Read Rate	30
BGI Rate	30	Cache Flush Interval	4
CC Rate	30	Spinup Drive Count	2
Reconstruction Rate	30	Spinup Delay	6
Controller BIOS	Enabled	StopOnError	Enabled
NCQ	Enabled	Drive Powersave	Enabled

Figure 12. Intel® RAID BIOS Console 2 – additional controller properties

The following additional controller properties are available:

- **Battery Backup** – Indicates if a battery backup unit is installed.
- **Set Factory Defaults** – Change this field to Yes to reset the RAID controller settings to the factory defaults.
- **Cluster Mode** – Enable this field if the RAID controller is used in a cluster.
- **Rebuild Rate** – Enter a number between 0 and 100 to control the rate at which a future rebuild will be performed on a disk group.
- **Patrol Read Rate** – A patrol read is a preventive procedure that monitors physical disks to locate and resolve potential problems that could lead to disk failure. Enter a number between 0 and 100 to control the rate at which patrol reads are performed.
- **BGI Rate** (Background Initialization Rate) – Background initialization makes the virtual drive immediately available for use, even while initialization is occurring. Enter a number between 0 and 100 to control the rate at which virtual drives are initialized in the background.

- **CC Rate** (Check Consistency Rate) – A consistency check scans the consistency of data on a fault-tolerant disk to determine if the data is corrupted. Enter a number between 0 and 100 to control the rate at which a consistency check is done.
- **Reconstruction Rate** – Enter a number between 0 and 100 to control the rate at which the reconstruction of a virtual drive occurs.
- **Adapter BIOS** – Determines whether the Option ROM is loaded.
- **Coercion Mode** – Select one of the following options:
    - None – No coercion of size.
    - 128M – The software rounds the drive capacity down to the next 128 MB boundary and then up to the nearest 10 MB until the coerced capacity is larger than the actual drive size. It is then reduced by 10 MB.
    - 1G – The software rounds the drive capacity down to the nearest 1 GB boundary and then down by 1 MB. This corresponds to the terms most drive manufacturers use.
- **PDF Interval** – The PDF interval is the predictive disk failure polling interval. This is the time needed between disk polls to perform SMART polling.
- **Alarm Control** – Disable the alarm to turn off the on-board speaker alarm.
- **Interrupt Throttle Count and Interrupt Throttle Time** – Sets the interrupt throttle and count times. This is the number of times that interrupts are coalesced and the amount of time that firmware holds an interrupt before passing it to the host software. Set values lower for better performance—be aware that latency is impacted by these settings.
- **Cache Flush Interval** – This sets the cache flush interval. Valid settings are 2, 4, 6, 8, or 10 seconds.
- **Spinup Drive Count** – This setting controls the number of drives that spin up at one time.
- **Spinup Delay** – After the RAID controller completes its initialization process, the initial delay value defines the number of seconds before the first disk interrogation request is issued to the array or disk group. Do not change this value.
- **Stop On Error** – Stops system POST if any error is detected.
- **NCQ** – Enables NCQ (Native Command Queuing) to optimize physical drive performance and life.
- **Stop CC On Error** – Stops Consistency Check if any error is detected.
- **Schedule CC** – Schedules a Consistency Check.
- **Maintain PD Fail History** – Enables tracking of bad PDs across reboot.

5.1.3 Virtual Drives Screen

Access the Virtual Drives screen by clicking on a virtual drive in the virtual drive list on the main screen. The upper right section of the screen displays the virtual drives that currently exist. The Virtual Drives screen provides options to:

- Initialize the virtual drives – The Slow Initialize option initializes the selected virtual drive by writing zeroes to the entire volume. Initialize each new virtual drive before configuring.

Warning: Initializing a virtual drive deletes all information on the physical drives that compose the virtual drive.

- Check consistency (CC) – This option verifies the correctness of the redundancy data and is available for arrays and disk groups using RAID 1, 5, 6, 10, 50, or 60. If a difference in the data is found, Intel RAID BIOS Console 2 assumes that the data is accurate and automatically corrects the parity value.
- Display the virtual drive properties – This option includes the following actions:
    - Display the virtual drive properties (such as RAID level, virtual drive size, and stripe size).
    - Display the read, write, Access, Disk Cache, BGI (Background Initialization), and I/O policies.
    - Change the read, write, Access, Disk Cache, BGI, and I/O policies.
    - Select Write Through, Write Back with BBU, or Always Write Back.

- o Start initialization.
- o Start a consistency check.

After setting any property, click **Go** to perform the selected operation. Click **Change** to apply any policy changes.

5.1.4 Physical Drives Screen

The Physical Drives screen displays the physical drives for each channel or port. Use the options on this screen to rebuild the physical arrays or disk groups or to view the properties for a selected physical drive.

Click **Reset** to return to the configuration that existed before any changes.

Select **Properties** and click **Go** to view the properties. An unconfigured drive can be made into a hot spare from the physical drive properties.

5.1.5 Configuration Mismatch Screen

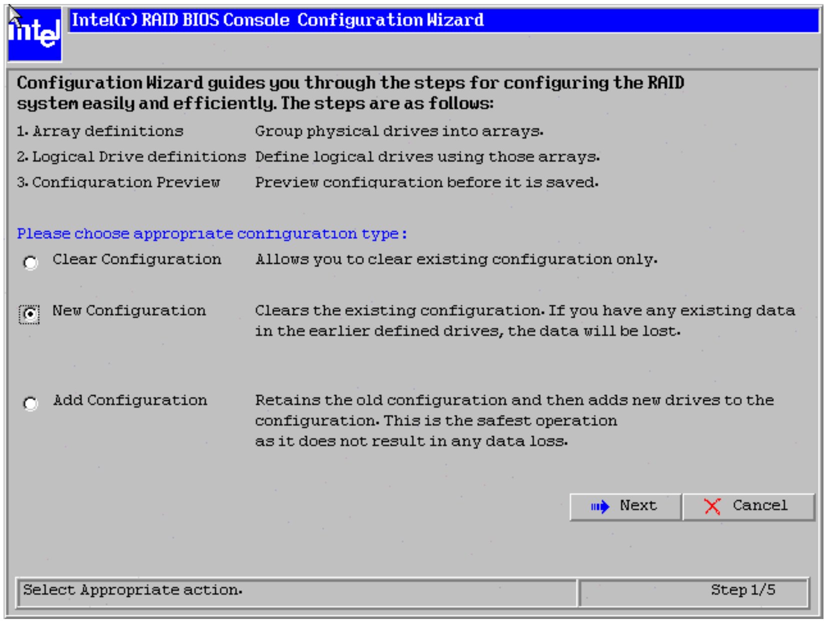
A configuration mismatch occurs when the data in the NVRAM and the hard disk drives are different. It automatically displays after POST when a configuration mismatch occurs. The following options are available on the Configuration Mismatch screen:

- Select Create New Configuration – Delete the previous configuration and create a new configuration.
- Select View Disk Configuration – Restore the configuration from the hard disk.
- Select View NVRAM Configuration – Restore the configuration from the NVRAM.

5.1.6 Setting Up a RAID Array Using the Configuration Wizard

This section provides detailed steps for using the Configuration Wizard to set up a RAID array.

1. Start the Configuration Wizard by selecting the **Configuration Wizard** option on the Intel® RAID BIOS Console 2 main screen.
2. Select **New Configuration** and click **Next**.



Intel(r) RAID BIOS Console Configuration Wizard

Configuration Wizard guides you through the steps for configuring the RAID system easily and efficiently. The steps are as follows:

1. Array definitions	Group physical drives into arrays.
2. Logical Drive definitions	Define logical drives using those arrays.
3. Configuration Preview	Preview configuration before it is saved.

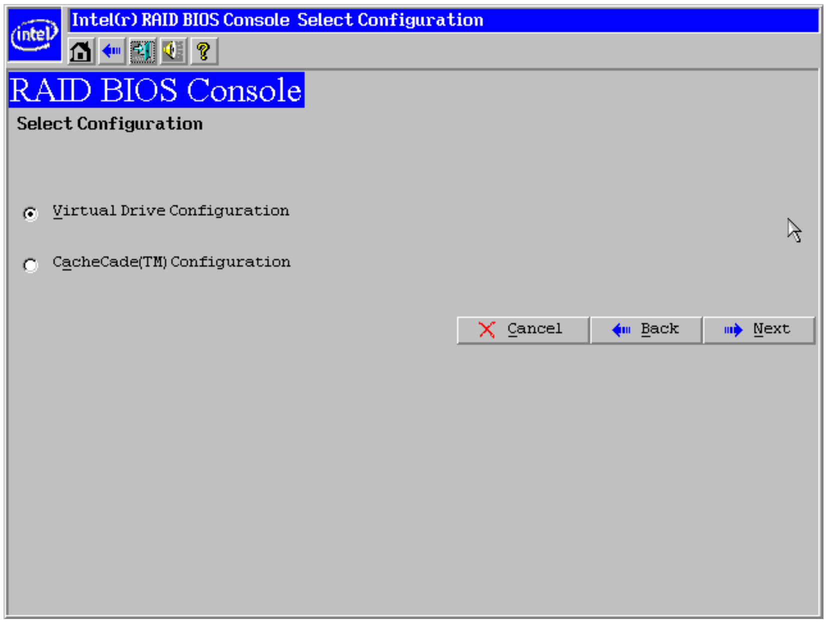
Please choose appropriate configuration type:

○ Clear Configuration	Allows you to clear existing configuration only.
● New Configuration	Clears the existing configuration. If you have any existing data in the earlier defined drives, the data will be lost.
○ Add Configuration	Retains the old configuration and then adds new drives to the configuration. This is the safest operation as it does not result in any data loss.

Select Appropriate action. Step 1/5

Figure 13. Intel® RAID BIOS Console 2 Configuration Wizard – configuration type

3. Select **Virtual Drive Configuration** and click **Next**.

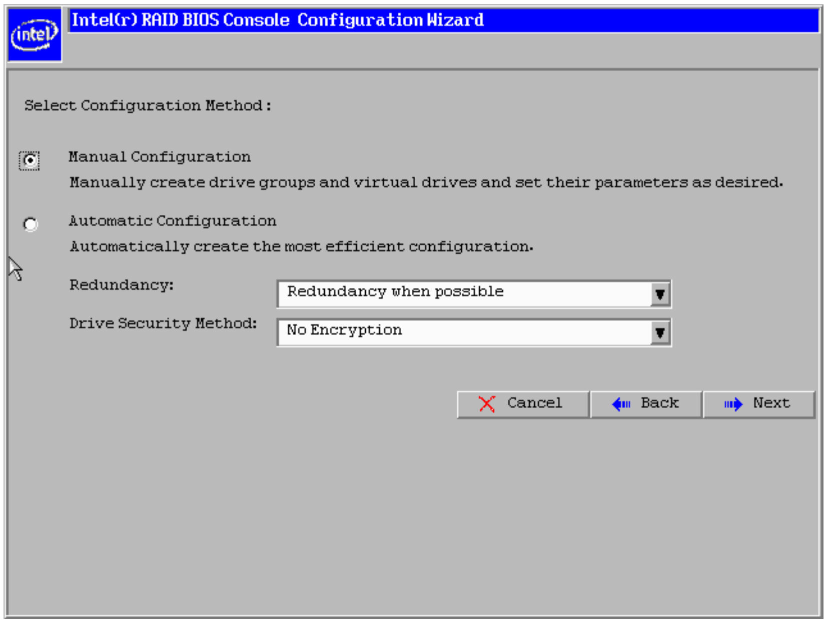


● Virtual Drive Configuration

○ CacheCade(TM) Configuration

Figure 14. Intel® RAID BIOS Console 2 Configuration Wizard – select configuration

4. Choose the configuration method and click **Next**. The following configuration methods options are provided: manual configuration and automatic configuration. If automatic configuration is selected, set the **Redundancy** to one of the following two options:
   - Redundancy When Possible – Configures RAID 1 for systems with two drives, RAID 5 for systems with three or more drives, or RAID 6 for systems with three or more drives. All available physical drives are included in the virtual drive using all available capacity on the disks.
   - No Redundancy – Configures all available drives as a RAID 0 virtual drive.



Select Configuration Method :

● Manual Configuration
Manually create drive groups and virtual drives and set their parameters as desired.

○ Automatic Configuration
Automatically create the most efficient configuration.

Redundancy: Redundancy when possible

Drive Security Method: No Encryption

Figure 15. Intel® RAID BIOS Console 2 Configuration Wizard – configuration method

Note: There is a Drive Security Method option which is reserved to be enabled in future.

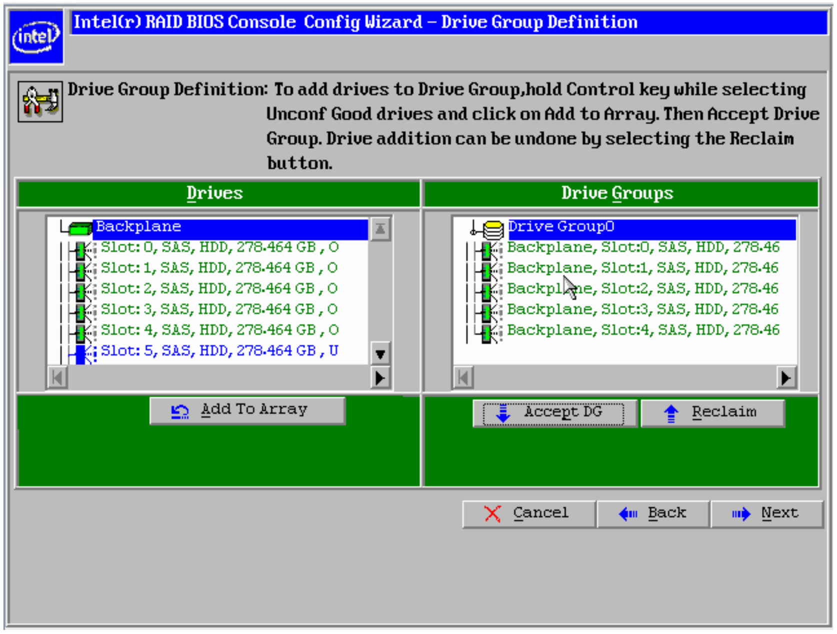
Note: Hot-spare drives must be designated before starting auto configuration using all available capacity on the disks.

Note: Automatic Configuration cannot be used for RAID 10, 50, or 60 or with mixed SATA and SAS drives.

5.1.7 Creating RAID 0, 1, 5, or 6 using Intel® RAID BIOS Console 2

This section describes the process to set up RAID modes using the custom configuration options.

1. Power on the system. When `Press <Ctrl><G> to enter the RAID BIOS Console` is displayed, press the **<Ctrl>** and **<G>** keys to open the Controller Selection screen.
2. Select a controller and click **Start** to begin the configuration.
3. Choose **Manual Configuration** and click **Next** (Figure 65).
4. In the Drive Group (DG) Definition screen (Figure 16), hold down the **<Ctrl>** key and select each drive to include in the drive group. See section 2.2 for information on the required minimum number of drives.



Intel(r) RAID BIOS Console Config Wizard – Drive Group Definition

Drive Group Definition: To add drives to Drive Group,hold Control key while selecting Unconf Good drives and click on Add to Array. Then Accept Drive Group. Drive addition can be undone by selecting the Reclaim button.

Drives

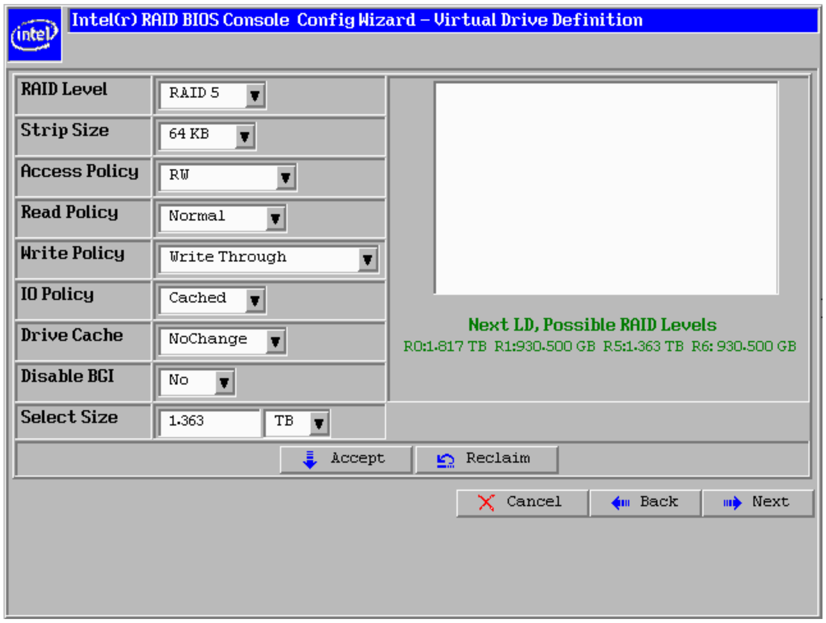
```
Backplane
  Slot: 0, SAS, HDD, 278.464 GB , O
  Slot: 1, SAS, HDD, 278.464 GB , O
  Slot: 2, SAS, HDD, 278.464 GB , O
  Slot: 3, SAS, HDD, 278.464 GB , O
  Slot: 4, SAS, HDD, 278.464 GB , O
  Slot: 5, SAS, HDD, 278.464 GB , U
```

Drive Groups

```
Drive Group0
  Backplane, Slot:0, SAS, HDD, 278.46
  Backplane, Slot:1, SAS, HDD, 278.46
  Backplane, Slot:2, SAS, HDD, 278.46
  Backplane, Slot:3, SAS, HDD, 278.46
  Backplane, Slot:4, SAS, HDD, 278.46
```

Figure 16. Intel® RAID BIOS Console 2 Configuration Wizard – drive group definition

5. Click **Add To Array**. To remove drives, click **Reclaim**.
6. When the desired drives have been added to the drive group, click **Accept DG**, then click **Next**.
7. In the next screen, click **Add to Span** and then click **Next**.
8. Set the parameter values for the virtual drive definition (Figure 17). Specifically, set the **RAID Level** to RAID 0, 1, 5, or 6 and the expected volume size in the **Select Size** field. Depending on the chosen RAID level, the volume size may need to be manually entered. The possible sizes for some RAID levels are listed on the right panel of the screen for reference. For information on setting these and other parameters, see section 5.1.9.



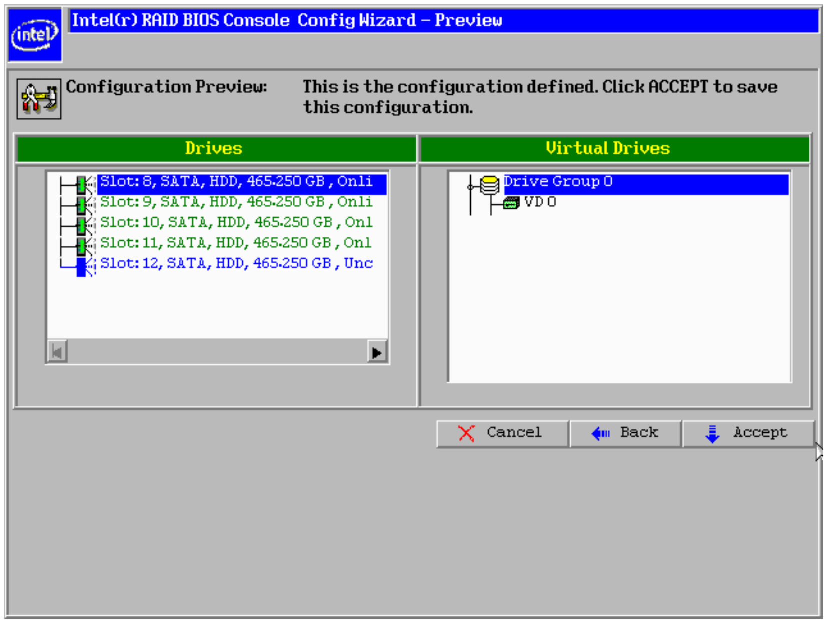
Intel(r) RAID BIOS Console Config Wizard – Virtual Drive Definition

RAID Level	RAID 5
Strip Size	64 KB
Access Policy	RW
Read Policy	Normal
Write Policy	Write Through
IO Policy	Cached
Drive Cache	NoChange
Disable BGI	No
Select Size	1.363 TB

Next LD, Possible RAID Levels
R0:1.817 TB R1:930.500 GB R5:1.363 TB R6: 930.500 GB

Figure 17. Intel® RAID BIOS Console 2 Configuration Wizard – virtual drive definition example for RAID 5

9. Click **Accept** to accept the changes or **Reclaim** to delete the changes and return to the previous settings. If accepted, the Intel® RAID BIOS Console 2 configuration utility displays a preview of the configuration (Figure 68).



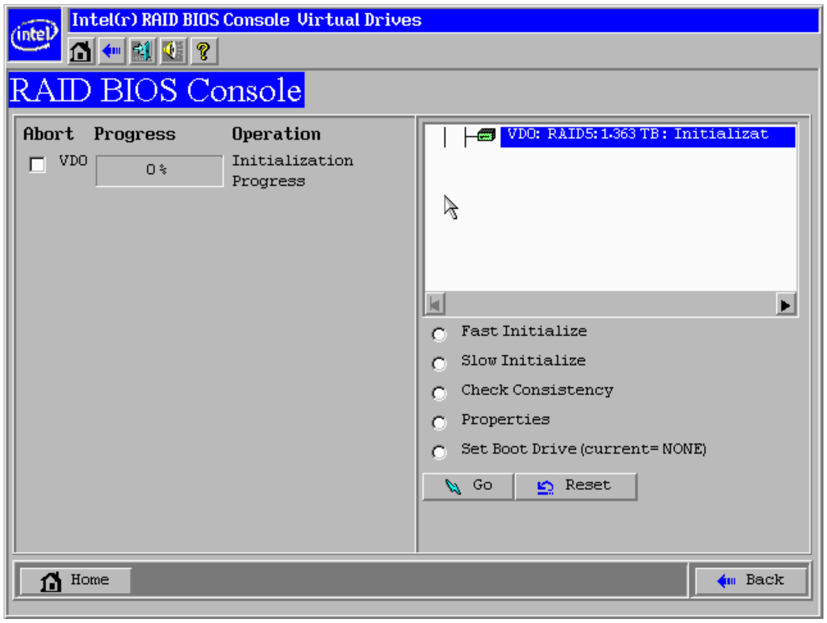
Intel(r) RAID BIOS Console Config Wizard – Preview

Configuration Preview: This is the configuration defined. Click ACCEPT to save this configuration.

Drives	Virtual Drives
Slot: 8, SATA, HDD, 465.250 GB, Onli Slot: 9, SATA, HDD, 465.250 GB, Onli Slot: 10, SATA, HDD, 465.250 GB, Onl Slot: 11, SATA, HDD, 465.250 GB, Onl Slot: 12, SATA, HDD, 465.250 GB, Unc	Drive Group 0 VD 0

Figure 18. Intel® RAID BIOS Console 2 Configuration Wizard – configuration preview

10. Click **Accept** to save the configuration or **Back** to return to the previous screens and change the configuration.
11. Click **No** or **Yes** as necessary in the screens that follow to save the configuration and initialize the virtual drive.
12. Select an initialization speed setting (Figure 69). Fast initialization runs a quick preliminary initialization and then runs a full initialization in the background after the OS is booted. Slow initialization may take several hours or even days to complete.
13. Click **Go** to begin the initialization process.



Abort	Progress	Operation
□ VD0	0 %	Initialization Progress

VD0: RAID5:1.363 TB: Initializat

○ Fast Initialize
○ Slow Initialize
○ Check Consistency
○ Properties
○ Set Boot Drive (current= NONE)

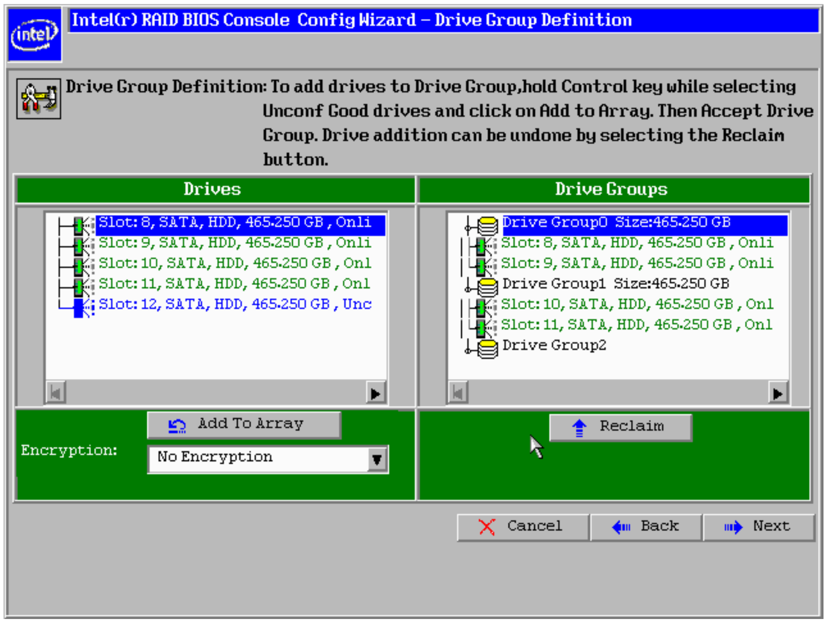
Figure 19. Intel® RAID BIOS Console 2 – initialization settings

14. Click **Home** to return to the main configuration screen.
15. Select an additional virtual drive to configure or exit the Intel® RAID BIOS Console 2 configuration utility and reboot the system.

5.1.8 Creating RAID 10, 50, or 60 using Intel® RAID BIOS Console 2

RAID 10, RAID 50, and RAID 60 require setting up multiple RAID arrays/disk groups.

1. Power on the system. When `Press <Ctrl><G> to enter the RAID BIOS Console` is displayed, press the **<Ctrl>** and **<G>** keys to open the Controller Selection screen.
2. Select a controller and click **Start** to begin the configuration.
3. Choose **Manual Configuration** and click **Next** (Figure 65).
4. In the Drive Group (DG) Definition screen (Figure 70), hold down the **<Ctrl>** key and select each drive to include in the first array.
   - For RAID 10, use two drives.
   - For RAID 50, use at least three drives.
   - For RAID 60, use at least three drives.
5. Click **Add To Array** and then click **Accept DG** in the right pane to confirm. The first group of drives appears as a disk group in the right pane. These drives are no longer available in the left pane.
6. From the drives that are available in the left pane, choose an additional group of drives and again click **Add To Array** and then click **Accept DG** to confirm. Each disk group must contain the identical quantity and size of drives.
7. Repeat step 6 for each additional array. Up to eight arrays can be added for RAID 10, 50, or 60.



Intel(r) RAID BIOS Console Config Wizard – Drive Group Definition

Drive Group Definition: To add drives to Drive Group,hold Control key while selecting Unconf Good drives and click on Add to Array. Then Accept Drive Group. Drive addition can be undone by selecting the Reclaim button.

Drives

- Slot: 8, SATA, HDD, 465.250 GB , Onli
- Slot: 9, SATA, HDD, 465.250 GB , Onli
- Slot: 10, SATA, HDD, 465.250 GB , Onl
- Slot: 11, SATA, HDD, 465.250 GB , Onl
- Slot: 12, SATA, HDD, 465.250 GB , Unc

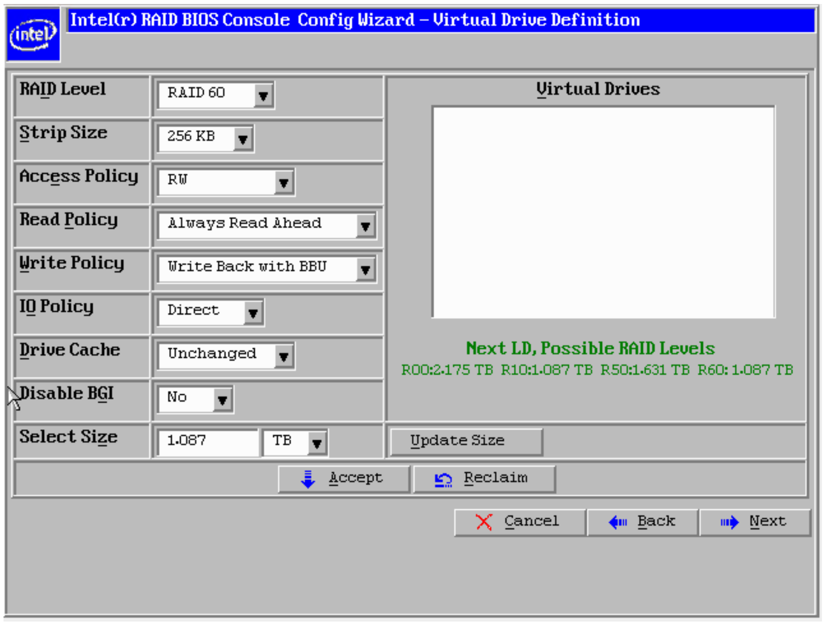
Drive Groups

- Drive Group0 Size:465.250 GB
  - Slot: 8, SATA, HDD, 465.250 GB , Onli
  - Slot: 9, SATA, HDD, 465.250 GB , Onli
- Drive Group1 Size:465.250 GB
  - Slot: 10, SATA, HDD, 465.250 GB , Onl
  - Slot: 11, SATA, HDD, 465.250 GB , Onl
- Drive Group2

Encryption: No Encryption

Figure 20. Intel® RAID BIOS Console 2 Configuration Wizard – definition of multiple drive groups

8. Select all arrays or disk groups that are to be spanned in the RAID 10, 50, or 60 array by holding down the **<Ctrl>** key and selecting each disk group in the right pane. Click **Next**.
9. In the next screen, click **Add to SPAN** to move all arrays from the left pane to the right pane. Use **<Ctrl>** to select all spans on the right pane. Click **Next**.
10. Set the parameter values for the virtual drive definition (Figure 21). Specifically, set the RAID Level to RAID 10, 50, or 60 and then click on **Update Size**. For information on setting these and other parameters, see section 5.1.9.



Intel(r) RAID BIOS Console Config Wizard – Virtual Drive Definition

RAID Level	RAID 60
Strip Size	256 KB
Access Policy	RW
Read Policy	Always Read Ahead
Write Policy	Write Back with BBU
IO Policy	Direct
Drive Cache	Unchanged
Disable BGI	No
Select Size	1.087 TB

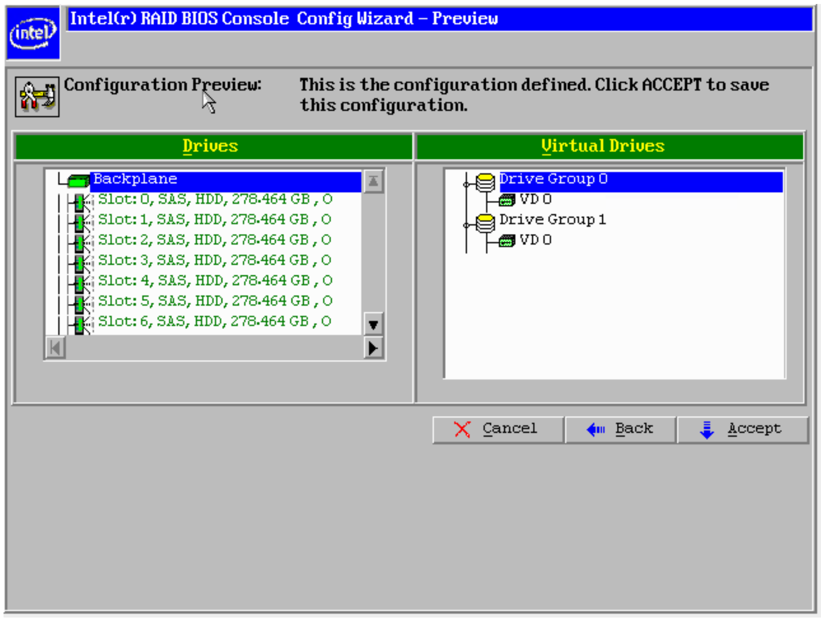
Virtual Drives

Next LD, Possible RAID Levels

R00:2.175 TB R10:1.087 TB R50:1.631 TB R60: 1.087 TB

Figure 21. Intel® RAID BIOS Console 2 Configuration Wizard – virtual drive definition example for RAID 10

11. Click **Accept**, then **Next**.
12. The configuration preview screen displays the virtual drive as shown in Figure 22. The configuration preview screen displays the virtual drive (RAID 1 for RAID 10, or RAID 50 or RAID 60). Click **Accept** to save the configuration.



Intel(r) RAID BIOS Console Config Wizard – Preview

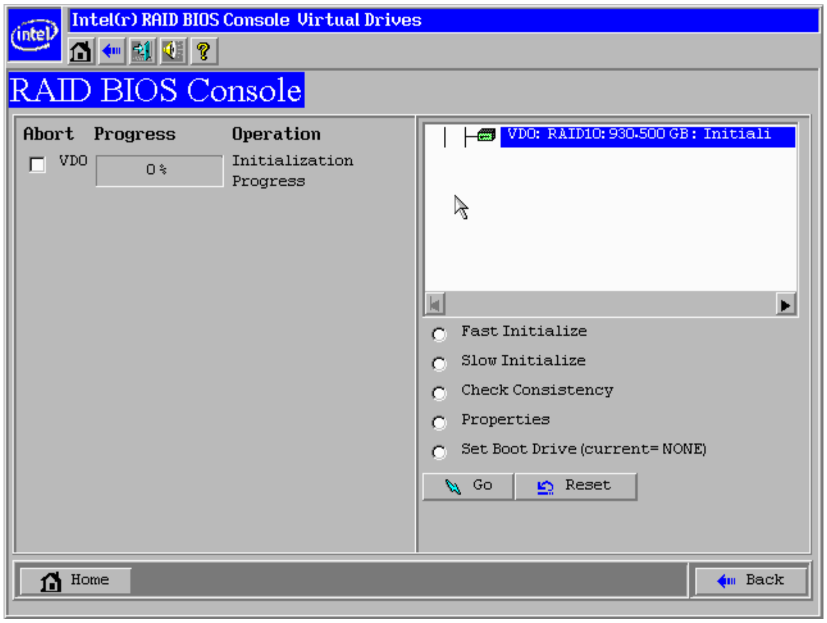
Configuration Preview: This is the configuration defined. Click ACCEPT to save this configuration.

Drives	Virtual Drives
Backplane	Drive Group 0
Slot: 0, SAS, HDD, 278.464 GB , O	VD 0
Slot: 1, SAS, HDD, 278.464 GB , O	Drive Group 1
Slot: 2, SAS, HDD, 278.464 GB , O	VD 0
Slot: 3, SAS, HDD, 278.464 GB , O	
Slot: 4, SAS, HDD, 278.464 GB , O	
Slot: 5, SAS, HDD, 278.464 GB , O	
Slot: 6, SAS, HDD, 278.464 GB , O	

Figure 22. Intel® RAID BIOS Console 2 Configuration Wizard – view virtual drive preview

13. When asked to save the configuration, click **Yes**. This stores the configuration in the RAID controller.
14. When asked to initialize the drive, click **Yes**.
15. Select **Fast Initialize** and click **Go** (Figure 23. The drives initialize based on the RAID settings.

Note: The Slow Initialize option initializes the entire drive and may take several hours to complete.



Intel(r) RAID BIOS Console Virtual Drives

RAID BIOS Console

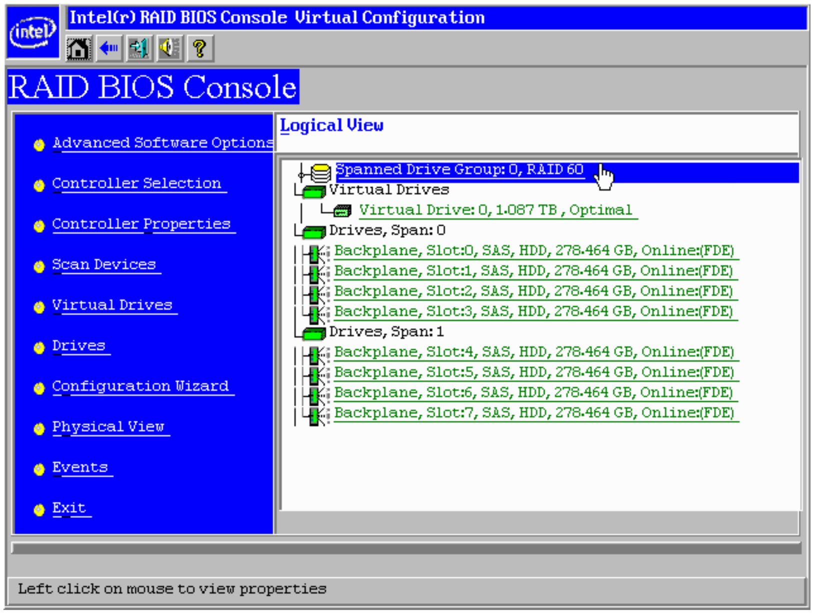
Abort	Progress	Operation
□ VD0	0 %	Initialization Progress

VD0: RAID10: 930.500 GB: Initiali

○ Fast Initialize
○ Slow Initialize
○ Check Consistency
○ Properties
○ Set Boot Drive (current= NONE)

Figure 23. Intel® RAID BIOS Console 2 – initialization settings

16. Click **Home** to return to the main screen. The RAID 10, RAID 50, or RAID 60 virtual drives are displayed. Figure 24 shows an example for RAID 10 virtual drives.

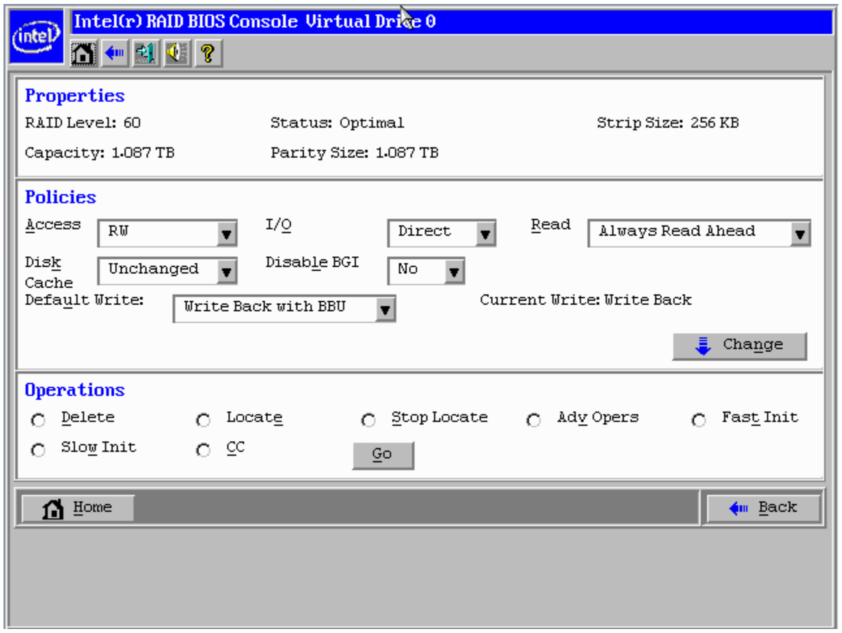


Spanned Drive Group: 0, RAID 60
Virtual Drives
Virtual Drive: 0, 1.087 TB , Optimal
Drives, Span: 0
Backplane, Slot:0, SAS, HDD, 278.464 GB, Online:(FDE)
Backplane, Slot:1, SAS, HDD, 278.464 GB, Online:(FDE)
Backplane, Slot:2, SAS, HDD, 278.464 GB, Online:(FDE)
Backplane, Slot:3, SAS, HDD, 278.464 GB, Online:(FDE)
Drives, Span: 1
Backplane, Slot:4, SAS, HDD, 278.464 GB, Online:(FDE)
Backplane, Slot:5, SAS, HDD, 278.464 GB, Online:(FDE)
Backplane, Slot:6, SAS, HDD, 278.464 GB, Online:(FDE)
Backplane, Slot:7, SAS, HDD, 278.464 GB, Online:(FDE)

Left click on mouse to view properties

Figure 24. Intel® RAID BIOS Console 2 – RAID 60 example of main screen logical view

17. Under the Virtual Drives section in the logical view, select the virtual drive you want see, select **Properties** and then **Go** to display the drive properties.



Properties

RAID Level: 60 Status: Optimal Strip Size: 256 KB

Capacity: 1.087 TB Parity Size: 1.087 TB

Policies

Access: RW I/O: Direct Read: Always Read Ahead

Disk Cache: Unchanged Disable BGI: No

Default Write: Write Back with BBU Current Write: Write Back

Operations

○ Delete ○ Locate ○ Stop Locate ○ Adv Opers ○ Fast Init

○ Slow Init ○ CC

Figure 25. Intel® RAID BIOS Console 2 – RAID 60 example of virtual drive properties screen

5.1.9 Setting Drive Parameters

The following fields are displayed in the Virtual Drive Definition screen (Figure 67 and Figure 71), which can be used to set the virtual drive parameters.

- **RAID Level** – Select the desired RAID level. For details on the available RAID levels, see chapter 2.
- **Stripe Size** – Specify the size of the segment written to each disk. Available stripe sizes are 4, 8, 16, 32, 64, 128, 256, 512, and 1024 KB.
- **Access Policy** – Select the type of data access that is allowed for this virtual drive. The choices are Read/Write, Read Only, or Blocked.
- **Read Policy** – Select the read-ahead feature for the virtual drive. Adaptive is the default setting.

  - Normal – The controller does not use read-ahead for the current virtual drive.
  - Read-ahead – Additional consecutive stripes are read and buffered into cache. This option will improve performance for sequential reads.
  - Adaptive – The controller begins using read-ahead if the two most recent disk accesses occurred in sequential sectors.
- **Write Policy** – Select when the transfer complete signal is sent to the host. Write-through caching is the default setting.
  - Write-back caching – This option is further classified as Write Back with BBU or Always Write Back, which means Write Back is always enabled even if BBU is bad or missing. The controller sends a data transfer completion signal to the host when the controller cache receives all of the data in a transaction. Write-back caching has a performance advantage over write-through caching, but it should only be enabled when the optional battery backup module is installed. The risk of using Always Write Back should be fully recognized.
  - Write-through caching – The controller sends a data transfer completion signal to the host after the disk subsystem receives all the data in a transaction. Write- through caching has a data security advantage over write-back caching.

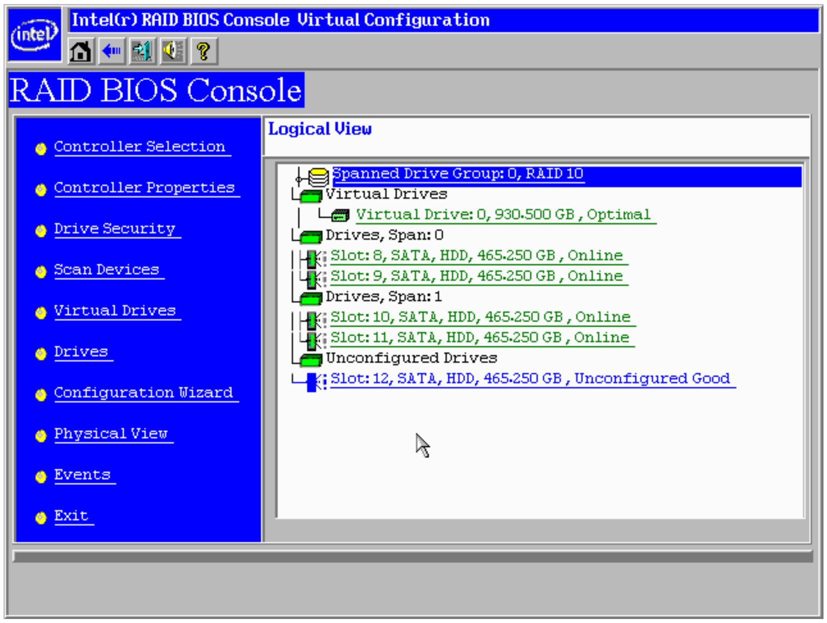
Caution: Do not use write-back caching for any virtual drive in a Novell NetWare* volume.

- **IO Policy** – Applies to reads on a specific virtual drive. It does not affect the read- ahead cache.
  - Cached IO – All reads are buffered in cache memory.
  - Direct IO – Reads are not buffered in cache memory. Data is transferred to cache and to the host concurrently. If the same data block is read again, it comes from cache memory.
- **Disk Cache Policy** – The cache policy applies to the cache on physical drives of the current array.
  - Enable – Enable disk cache. Enabling the disk cache in Write-back mode provides little or no performance enhancement, while the risk of data loss due to power failure increases.
  - Disable – Disable disk cache.
  - NoChange – Leave the default disk cache policy unchanged.
- **Disable BGI** – Enable or disable background initialization. Set this option to Yes to disable background initialization.
- **Select Size** – Set the size of the virtual drive. The right pane of the virtual drive configuration window lists the maximum capacity that can be selected, depending on the RAID level chosen.

5.1.10 Creating a Hot Spare

To create a hot spare, follow these steps:

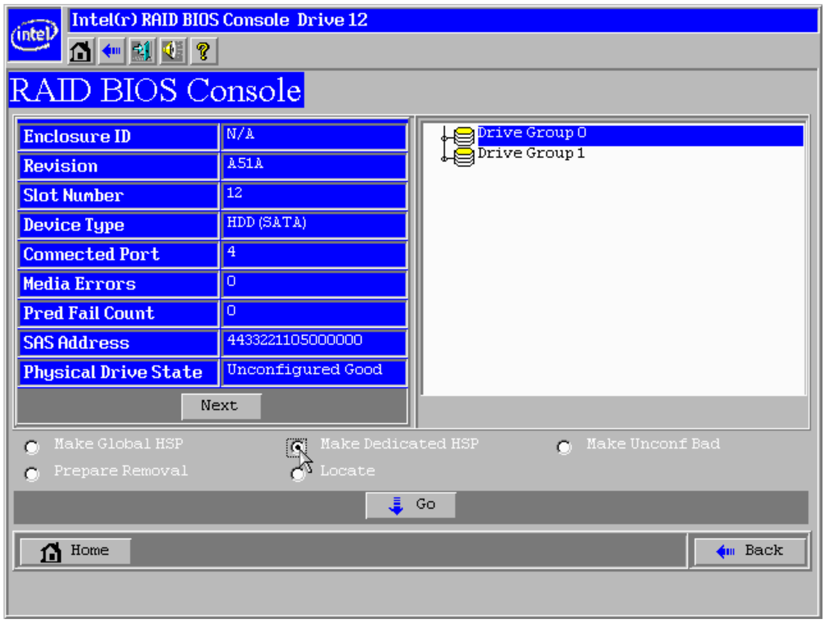
1. On the main screen, select the drive that should be used as the hot spare.



```
Spanned Drive Group: 0, RAID 10
Virtual Drives
    Virtual Drive: 0, 930.500 GB , Optimal
Drives, Span: 0
    Slot: 8, SATA, HDD, 465.250 GB , Online
    Slot: 9, SATA, HDD, 465.250 GB , Online
Drives, Span: 1
    Slot: 10, SATA, HDD, 465.250 GB , Online
    Slot: 11, SATA, HDD, 465.250 GB , Online
Unconfigured Drives
    Slot: 12, SATA, HDD, 465.250 GB , Unconfigured Good
```

Figure 26. Intel® RAID BIOS Console 2 – choosing a hot spare drive

2. On the next screen, select the disk group (Figure 27).
3. Select one of the following options:
    - **Make Dedicated HSP** – Add the drive as a hot spare dedicated for certain virtual drives.
    - **Make Global HSP** – Create a global hot spare for all disk groups.



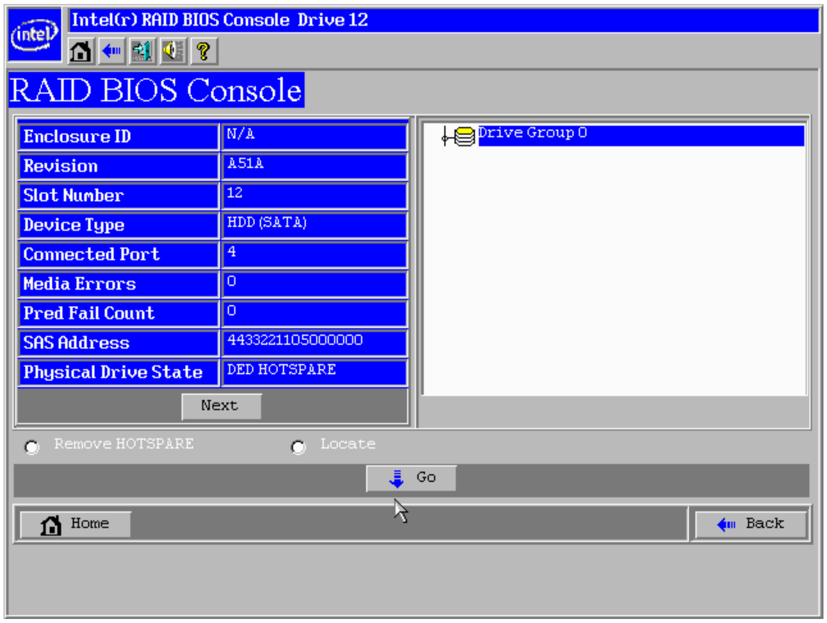
Enclosure ID	N/A
Revision	A51A
Slot Number	12
Device Type	HDD (SATA)
Connected Port	4
Media Errors	0
Pred Fail Count	0
SAS Address	4433221105000000
Physical Drive State	Unconfigured Good

Drive Group 0
Drive Group 1

○ Make Global HSP ● Make Dedicated HSP ○ Make Unconf Bad
○ Prepare Removal ○ Locate

Figure 27. Intel® RAID BIOS Console 2 – creating a hot spare drive

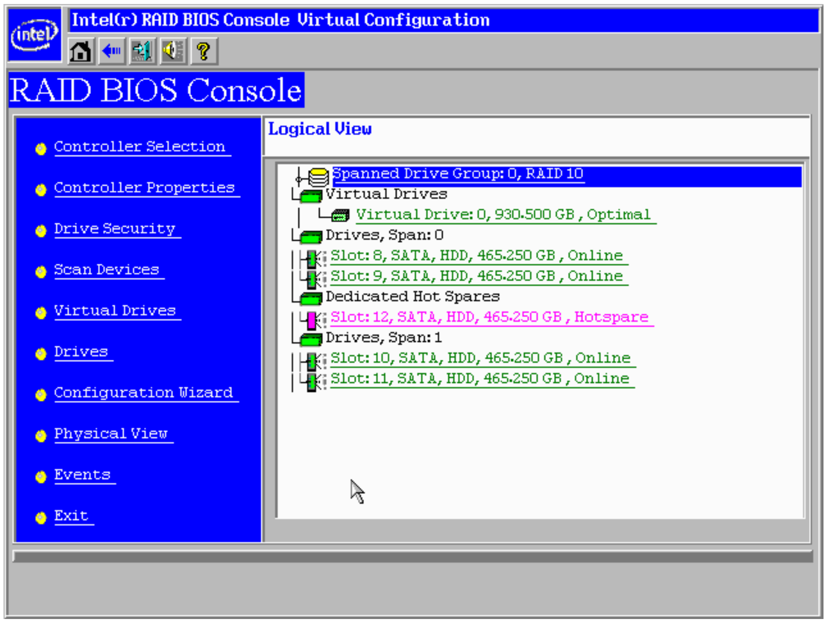
4. Click **Go** to create the hot spare. The Physical Drive State parameter changes to HOTSPARE, as shown in Figure 34.



Enclosure ID	N/A
Revision	A51A
Slot Number	12
Device Type	HDD (SATA)
Connected Port	4
Media Errors	0
Pred Fail Count	0
SAS Address	4433221105000000
Physical Drive State	DED HOTSPARE

Figure 28. Intel® RAID BIOS Console 2 – viewing a hot spare drive

5. Click **Home** to return to the main screen. The hot spare drive is listed in the main screen as shown in Figure 29.



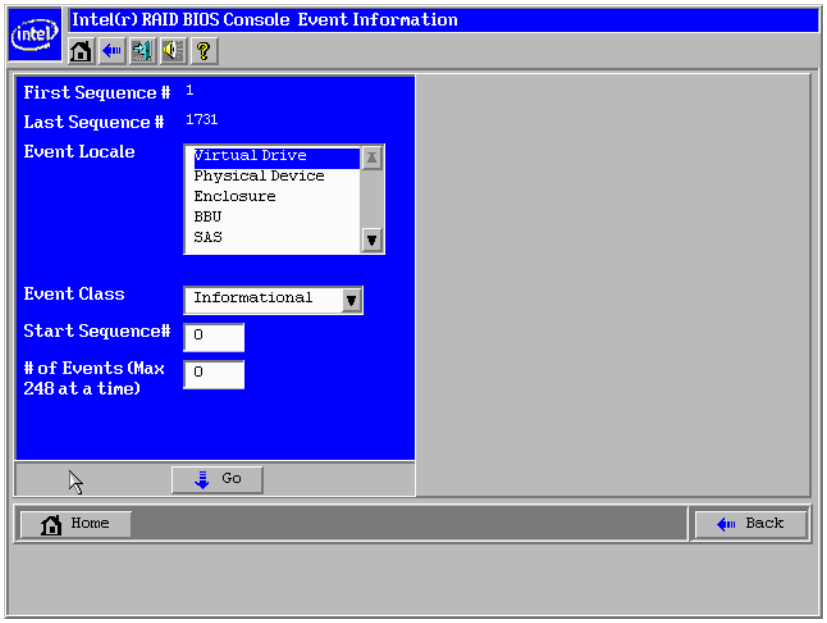
```
Spanned Drive Group: 0, RAID 10
Virtual Drives
    Virtual Drive: 0, 930.500 GB , Optimal
Drives, Span: 0
  Slot: 8, SATA, HDD, 465.250 GB , Online
  Slot: 9, SATA, HDD, 465.250 GB , Online
Dedicated Hot Spares
  Slot: 12, SATA, HDD, 465.250 GB , Hotspare
Drives, Span: 1
  Slot: 10, SATA, HDD, 465.250 GB , Online
  Slot: 11, SATA, HDD, 465.250 GB , Online
```

Figure 29. Intel® RAID BIOS Console 2 – hot spare drive listed in main screen

5.1.11 Viewing Event Details

Events contain information, warnings, and fatal events. Events can be captured on various RAID controller components, such as the battery, physical card, and within the configuration. View these using the following steps.

1. On the main screen, select the **Events** option from the menu at the left. The Event Information screen appears (Figure 30).



Intel(r) RAID BIOS Console Event Information

First Sequence # 1

Last Sequence # 1731

Event Locale: Virtual Drive, Physical Device, Enclosure, BBU, SAS

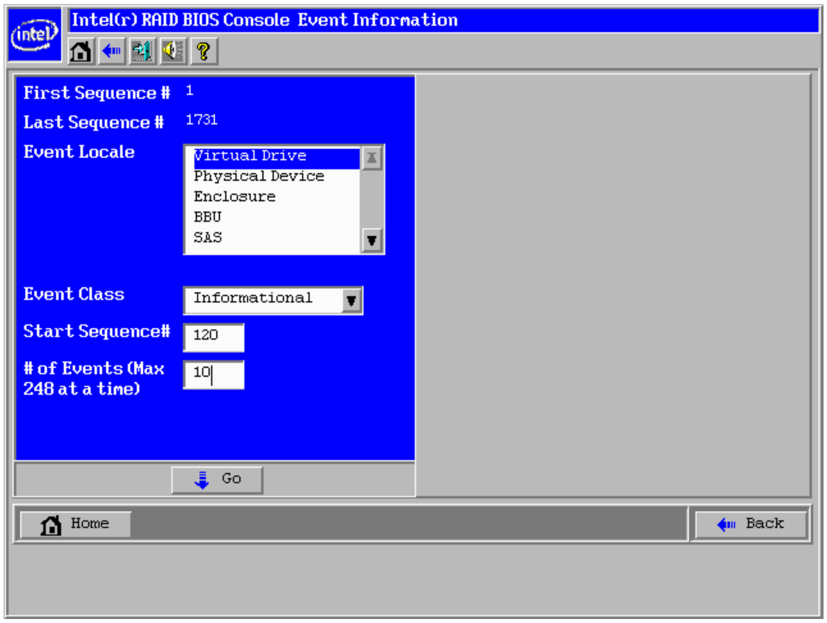
Event Class: Informational

Start Sequence# 0

# of Events (Max 248 at a time) 0

Figure 30. Intel® RAID BIOS Console 2 – event information screen

2. Select the component to display from the Event Locale list and the type of event to display from the Event Class drop-down. Enter the start sequence number and the number of events to display. Figure 31 shows a selection for informational events on the virtual drive, starting at sequence number 120 and displaying 10 events.



Intel(r) RAID BIOS Console Event Information

First Sequence # 1

Last Sequence # 1731

Event Locale: Virtual Drive, Physical Device, Enclosure, BBU, SAS

Event Class: Informational

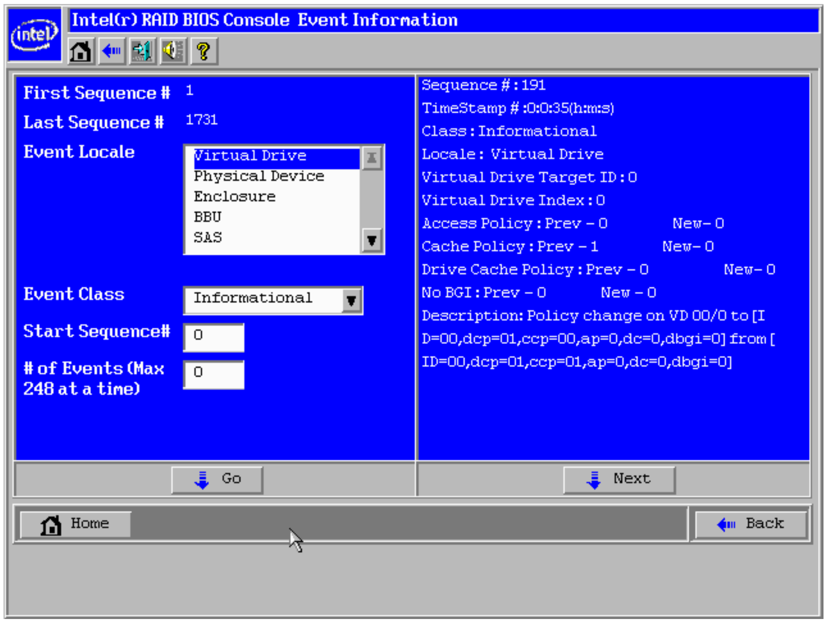
Start Sequence# 120

# of Events (Max 248 at a time) 10

Figure 31. Intel® RAID BIOS Console 2 – selecting events to view

3. Click **Go**. The Event Information screen displays the event information for the requested sequences on the right pane (Figure 83).

Note: In the example shown in Figure 83, the Start Sequence# and the # of Events fields are set 0. This is because clicking **Go** to display the events automatically resets these fields to 0.



First Sequence # 1

Last Sequence # 1731

Event Locale: Virtual Drive, Physical Device, Enclosure, BBU, SAS

Event Class: Informational

Start Sequence# 0

# of Events (Max 248 at a time) 0

```
Sequence # : 191
TimeStamp # :0:0:35(h:m:s)
Class : Informational
Locale : Virtual Drive
Virtual Drive Target ID : 0
Virtual Drive Index : 0
Access Policy : Prev - 0          New- 0
Cache Policy : Prev - 1          New- 0
Drive Cache Policy : Prev - 0          New- 0
No BGI : Prev - 0          New - 0
Description: Policy change on VD 00/0 to [I
D=00,dcp=01,ccp=00,ap=0,dc=0,dbgi=0] from [
ID=00,dcp=01,ccp=01,ap=0,dc=0,dbgi=0]
```

Figure 32. Intel® RAID BIOS Console 2 – viewing an event

4. Click **Next** to view the next message.

5.2 Integrated RAID M BIOS Configuration Utility for 12 Gb/s Intel® RAID Controllers

The Integrated RAID M BIOS Configuration Utility for 12 Gb/s Intel® RAID Controllers (RCU) is used on the generation 3 Intel® RAID Controllers based on the Mega RAID* software stack, specifically RS3SC008, RS3MC044, RS3DC040, RS3DC080, RS3WC080, RS3UC080, RS3FC044, RS3GC008 RMS3HC080 and RMS3AC160.

The Integrated RAID M BIOS Configuration Utility for 12 Gb/s Intel® RAID Controllers provides full-featured configuration and management of RAID arrays. It resides in the controller firmware and is independent of the operating system. Use the configuration utility for the 12 Gb/s Intel® RAID controllers to

- Select an Intel RAID Controller.
- Choose a configuration method for physical arrays, disk groups, and virtual drives.
- Create drive arrays.
- Define virtual drives.
- Initialize virtual drives.
- Access controllers, virtual drives, and physical arrays to display their properties.
- Create hot-spare drives.
- Rebuild failed drives.
- Verify data redundancy in RAID 1, 5, 6, 10, 50, or 60 virtual drives.
- Creating drive groups and virtual drives for storage configurations;
- Viewing controller, physical drive, virtual drive, enclosure, and battery backup unit (BBU) properties, and change parameters;
- Deleting virtual drives;
- Modifying power settings;
- Importing and clearing foreign configurations;
- Initializing virtual drives;
- Checking configurations for data consistency; and
- Creating SSD Cache virtual drives.

5.2.1 Starting the RCU

The RCU is invoked by pressing the **<Ctrl>** and **<R>** keys at the system power up.

If the system has only one SAS controller, the RCU opens the main menu screen.

If the system has multiple SAS controllers, a controller selection dialog appears. Using the keyboard arrows select a controller and press **Enter** to go to the RCU main menu screen.

5.2.2 Exiting the RCU

To exit the Ctrl-R Utility from a main menu screen, press **<Esc>**. To exit from a dialog, press **<Esc>** twice.

Click **OK** in the confirmation message.

5.2.3 RCU Keystrokes

The following table lists the keystrokes that can be used to navigate within the Ctrl-R Utility.

Table 16. RCU keystrokes

Keystroke	Action
<F1>	Display help for the particular screen that you are in.
<F2>	Display a list of commands that can be performed for the selected device. This key stroke is available only in the VD Mgmt, PD Mgmt, and Foreign View menus. The commands that are enabled are highlighted in white and the disabled commands are highlighted in black. Note that, based on the configurations, commands are enabled or disabled.

<F5>	Refresh the current screen.
<F11>	Switch between controllers.
<F12>	Display a list of all the available controllers or scroll to the next controller.
<Ctrl+N>	Display the next menu screen.
<Ctrl+P>	Display the previous menu screen.
<Ctrl+S>	Apply the settings in the Controller Settings screens.
<Tab>	Move the cursor to the next control.
<Shift+Tab>	Move the cursor to the previous control on a screen or a dialog.
<Enter>	Select a menu item, a button, a check box, or values in a list box.
<Esc>	Close a screen or a window. Press **<Esc>** twice to exit the Ctrl-R Utility.
Up Arrow	Move the cursor to the next menu selection.
Down Arrow	Move the cursor to the lower menu items or to a lower level menu.
Right Arrow	Open a submenu, move from a menu heading to the first submenu, or move to the first item in a submenu. The right arrow also closes a menu list in a popup window.
Left Arrow	Close a submenu, move from a menu item to the menu heading, or move from a submenu to a higher level menu.
Spacebar	Select a menu item, a button, or a check box.

5.2.4 RCU Menus

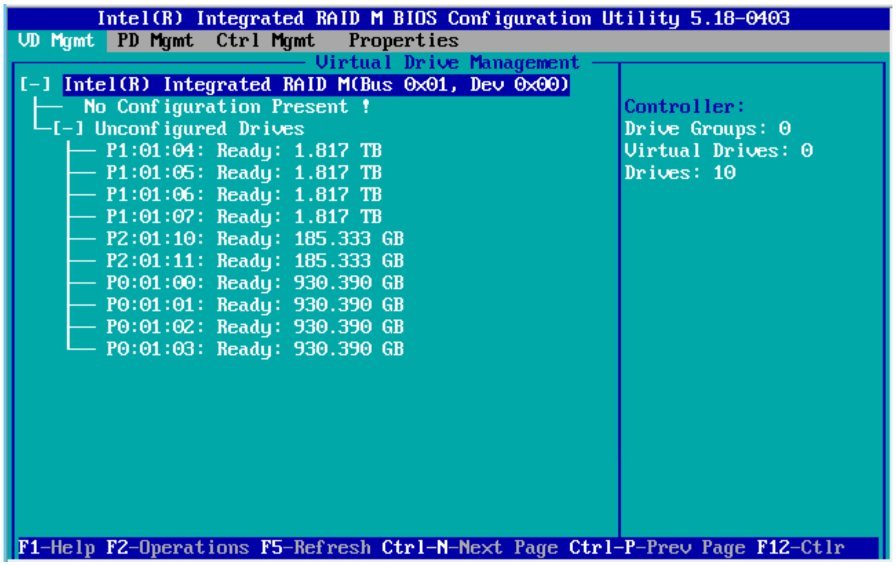
The RCU contains the following menus:

- VD Mgmt – Manage virtual drives.
- PD Mgmt – Manage physical drives.
- Ctrl Mgmt – Manage controllers.
- Properties – Set controller properties.
- Foreign View – View foreign configurations.

5.2.5 VD Mgmt Menu

The VD Mgmt menu is the first menu screen that appears when starting the RCU.

This screen shows information on the configuration of controllers, drive groups, and virtual drives. The right panel of the screen shows attributes of the selected device.



```
            Intel(R) Integrated RAID M BIOS Configuration Utility 5.18-0403
VD Mgmt  PD Mgmt  Ctrl Mgmt   Properties
                                  Virtual Drive Management
[-] Intel(R) Integrated RAID M(Bus 0x01, Dev 0x00)
 ├── No Configuration Present !                      Controller:
 └─[-] Unconfigured Drives                            Drive Groups: 0
     ├── P1:01:04: Ready: 1.817 TB                    Virtual Drives: 0
     ├── P1:01:05: Ready: 1.817 TB                    Drives: 10
     ├── P1:01:06: Ready: 1.817 TB
     ├── P1:01:07: Ready: 1.817 TB
     ├── P2:01:10: Ready: 185.333 GB
     ├── P2:01:11: Ready: 185.333 GB
     ├── P0:01:00: Ready: 930.390 GB
     ├── P0:01:01: Ready: 930.390 GB
     ├── P0:01:02: Ready: 930.390 GB
     └── P0:01:03: Ready: 930.390 GB

F1-Help F2-Operations F5-Refresh Ctrl-N-Next Page Ctrl-P-Prev Page F12-Ctlr
```

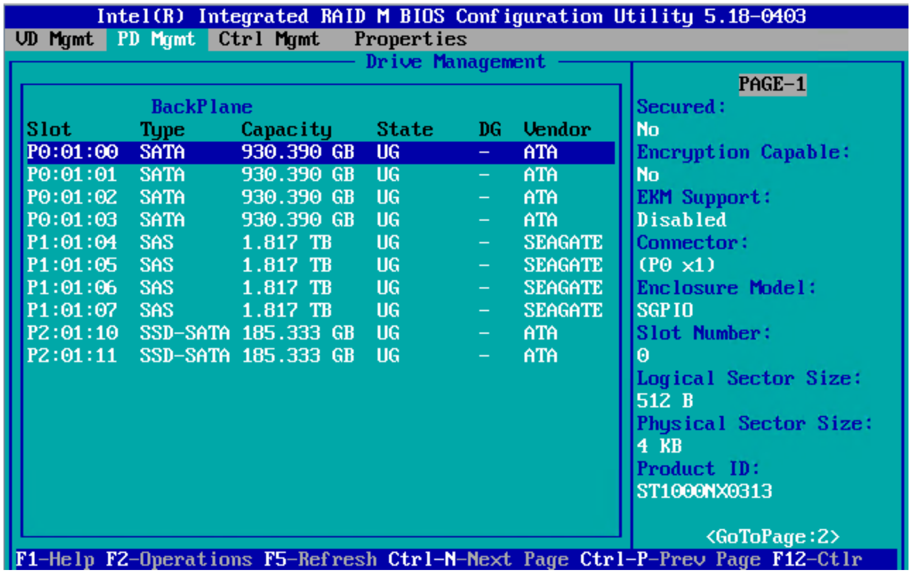
Figure 33. RCU – VD Mgmt menu screen

From this screen, perform tasks such as creating and initializing virtual drives; performing a consistency check; deleting, expanding, and erasing virtual drives; importing or clearing foreign configurations; and creating CacheCade* virtual drives.

Note: Based on the controller settings, options may be enabled or disabled.

5.2.6 PD Mgmt Menu

The PD Mgmt menu shows information about all the physical drives connected to the selected controller. This menu also shows information about enclosures, the number of physical drives in an enclosure, and all of the direct-attached drives under a backplane node. The right panel of the screen shows additional attributes of the selected device.



```
        Intel(R) Integrated RAID M BIOS Configuration Utility 5.18-0403
VD Mgmt  PD Mgmt  Ctrl Mgmt   Properties
                          Drive Management
                                                                PAGE-1
           BackPlane                                       Secured:
Slot       Type     Capacity    State    DG  Vendor        No
P0:01:00   SATA     930.390 GB  UG       -   ATA           Encryption Capable:
P0:01:01   SATA     930.390 GB  UG       -   ATA           No
P0:01:02   SATA     930.390 GB  UG       -   ATA           EKM Support:
P0:01:03   SATA     930.390 GB  UG       -   ATA           Disabled
P1:01:04   SAS      1.817 TB    UG       -   SEAGATE       Connector:
P1:01:05   SAS      1.817 TB    UG       -   SEAGATE       (P0 x1)
P1:01:06   SAS      1.817 TB    UG       -   SEAGATE       Enclosure Model:
P1:01:07   SAS      1.817 TB    UG       -   SEAGATE       SGPIO
P2:01:10   SSD-SATA 185.333 GB  UG       -   ATA           Slot Number:
P2:01:11   SSD-SATA 185.333 GB  UG       -   ATA           0
                                                           Logical Sector Size:
                                                           512 B
                                                           Physical Sector Size:
                                                           4 KB
                                                           Product ID:
                                                           ST1000NX0313

                                                               <GoToPage:2>
F1-Help F2-Operations F5-Refresh Ctrl-N-Next Page Ctrl-P-Prev Page F12-Ctlr
```

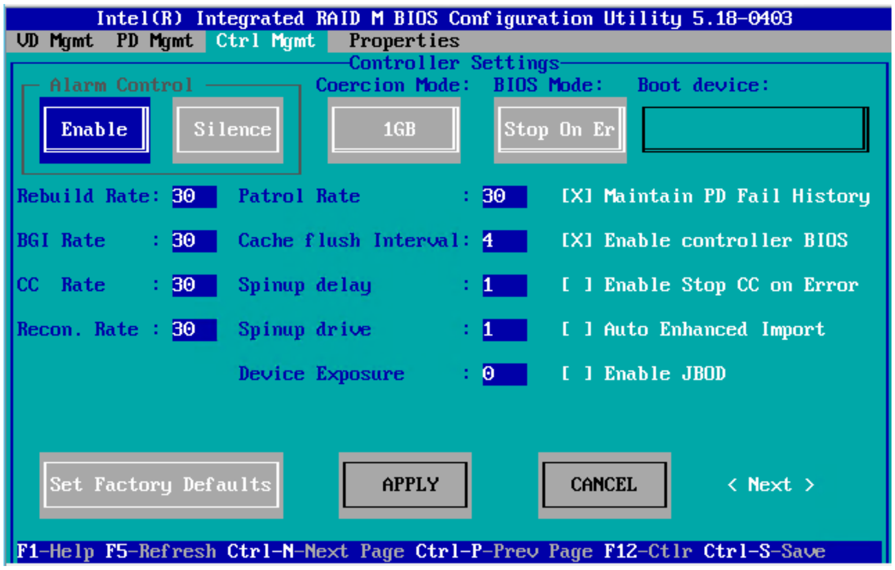
Figure 34. RCU – PD Mgmt menu screen

From this screen, perform tasks such as rebuilding a failed drive, making a drive offline, or making a drive a global hot spare drive.

5.2.7 Ctrl Mgmt Menu

The Ctrl Mgmt menu provides an interface to change the settings of the selected controller. The Ctrl Mgmt menu consists of two screens.

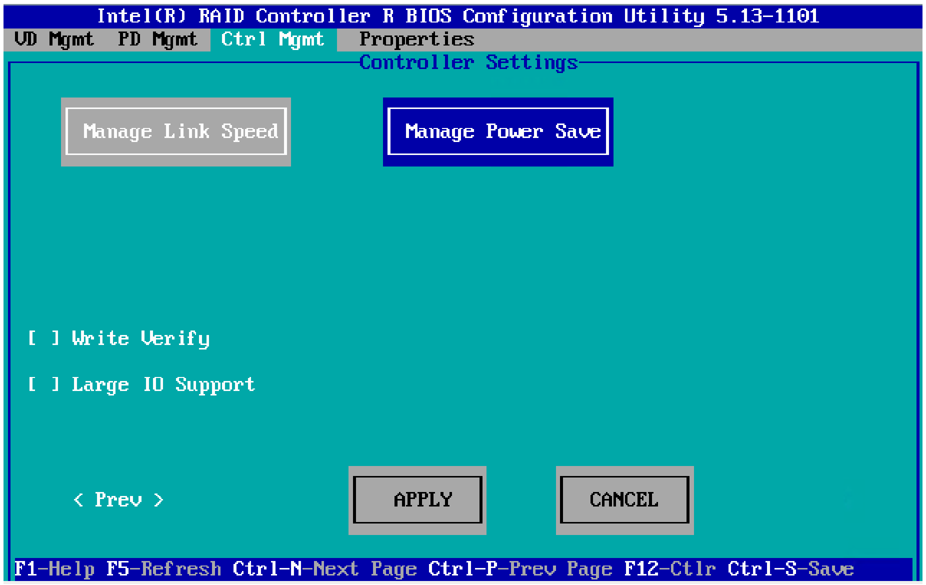
The first screen (Figure 16) provides options such as enabling controller BIOS, maintaining PD fail history, enabling Stop CC on Error, enabling or silencing an alarm, and entering values for Rebuild Rate and Patrol Rate.


Intel(R) Integrated RAID M BIOS Configuration Utility 5.18-0403
VD Mgmt
PD Mgmt
Ctrl Mgmt
Properties
Controller Settings
Alarm Control
Enable
Silence
Set Factory Defaults
APPLY
CANCEL
< Next >
F1-Help F5-Refresh Ctrl-N-Next Page Ctrl-P-Prev Page F12-Ctlr Ctrl-S-Save

```
Coercion Mode: 1GB     BIOS Mode: Stop On Er     Boot device:

Rebuild Rate: 30    Patrol Rate          : 30    [X] Maintain PD Fail History
BGI Rate    : 30    Cache flush Interval: 4      [X] Enable controller BIOS
CC  Rate    : 30    Spinup delay         : 1     [ ] Enable Stop CC on Error
Recon. Rate : 30    Spinup drive         : 1     [ ] Auto Enhanced Import
                    Device Exposure      : 0     [ ] Enable JBOD
```

Figure 35. SCU – Ctrl Mgmt menu first screen

In the second screen (Figure 36), changing the link speed and power save settings of the connected drives.


Intel(R) RAID Controller R BIOS Configuration Utility 5.13-1101
VD Mgmt
PD Mgmt
Ctrl Mgmt
Properties
Controller Settings
Manage Link Speed
Manage Power Save
< Prev >
APPLY
CANCEL
F1-Help F5-Refresh Ctrl-N-Next Page Ctrl-P-Prev Page F12-Ctlr Ctrl-S-Save

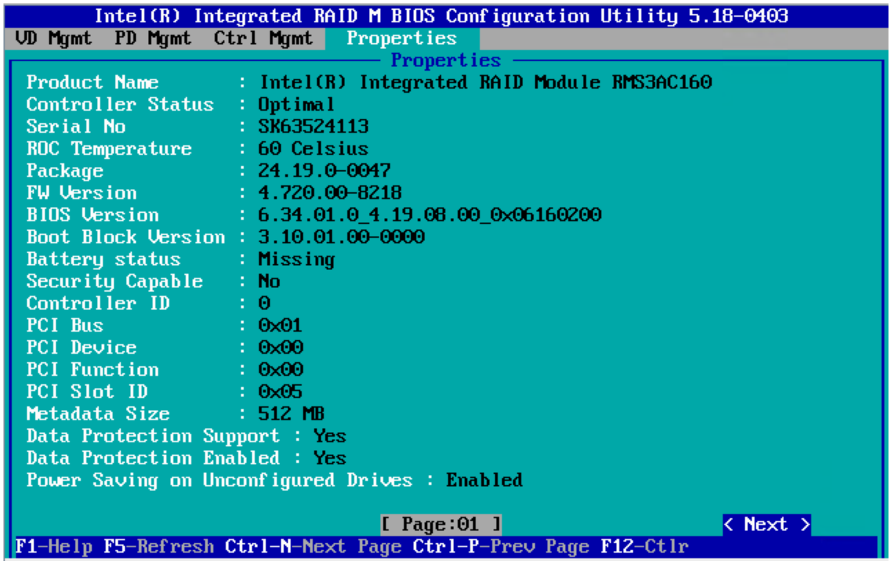
```
[ ] Write Verify
[ ] Large IO Support
```

Figure 36. RCU – Ctrl Mgmt menu second screen

5.2.8 Properties Menu

The Properties menu shows all of the properties of the active controller. The Properties menu consists of two screens. The information shown in these screens is read only.

The first screen (Figure 18) displays properties such as controller status, firmware version, BIOS version, and metadata size.



```
Intel(R) Integrated RAID M BIOS Configuration Utility 5.18-0403
VD Mgmt  PD Mgmt  Ctrl Mgmt  Properties
                        Properties
Product Name        : Intel(R) Integrated RAID Module RMS3AC160
Controller Status   : Optimal
Serial No           : SK63524113
ROC Temperature     : 60 Celsius
Package             : 24.19.0-0047
FW Version          : 4.720.00-8218
BIOS Version        : 6.34.01.0_4.19.08.00_0x06160200
Boot Block Version  : 3.10.01.00-0000
Battery status      : Missing
Security Capable    : No
Controller ID       : 0
PCI Bus             : 0x01
PCI Device          : 0x00
PCI Function        : 0x00
PCI Slot ID         : 0x05
Metadata Size       : 512 MB
Data Protection Support : Yes
Data Protection Enabled : Yes
Power Saving on Unconfigured Drives : Enabled

                              [ Page:01 ]             < Next >
F1-Help F5-Refresh Ctrl-N-Next Page Ctrl-P-Prev Page F12-Ctlr
```

Figure 37. RCU – Properties menu screen

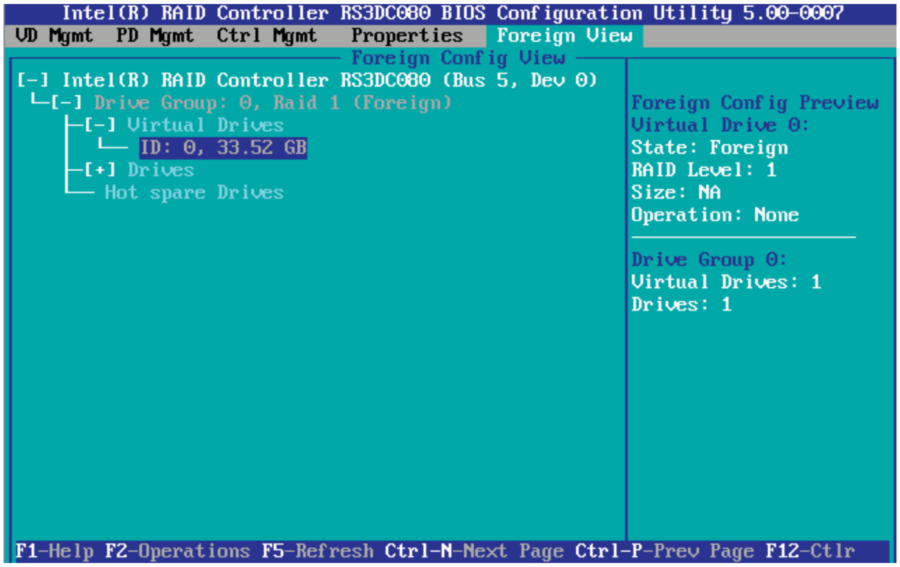
To view additional properties, navigate to **Next** and press **<Enter>**. The second properties screen displays information such as maximum cache size, drive standby time, and power saving properties.

To go back to the previous properties screen, navigate to **Prev**, and press **<Enter>**.

5.2.9 Foreign View Menu

If one or more physical drives in a configuration are removed and reinserted, the controller considers the drives as foreign configurations.

The Foreign View menu is shown only when the controller detects a foreign configuration. If no foreign configuration exists, the Foreign View menu is not shown.



```
Intel(R) RAID Controller RS3DC080 BIOS Configuration Utility 5.00-0007
VD Mgmt  PD Mgmt  Ctrl Mgmt  Properties  Foreign View
                          Foreign Config View
[-] Intel(R) RAID Controller RS3DC080 (Bus 5, Dev 0)
 └─[-] Drive Group: 0, Raid 1 (Foreign)          Foreign Config Preview
    ├─[-] Virtual Drives                          Virtual Drive 0:
    │  └── ID: 0, 33.52 GB                        State: Foreign
    ├─[+] Drives                                  RAID Level: 1
    └── Hot spare Drives                          Size: NA
                                                  Operation: None

                                                  Drive Group 0:
                                                  Virtual Drives: 1
                                                  Drives: 1

F1-Help F2-Operations F5-Refresh Ctrl-N-Next Page Ctrl-P-Prev Page F12-Ctlr
```

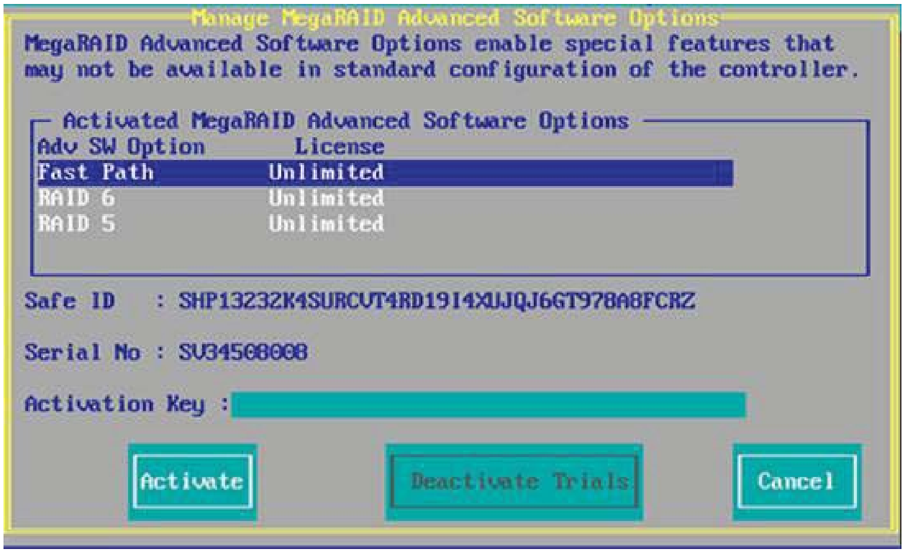
Figure 38. RCU – Foreign View menu screen

Use the Foreign View screen to view information about the foreign configuration, such as drive groups, virtual drives, physical drives, and hot spares or to import foreign configurations to the RAID controller and clear foreign configurations.

5.2.10 Controller Advanced Software Options

To access advanced software options

1. Select the controller in the VD Mgmt screen and press **<F2>**.
2. Navigate to the **Advanced Software Options** and press **<Enter>**. The Manage MegaRAID Advanced Software Options dialog appears showing a list of advanced software options available in the controller (Figure 20).

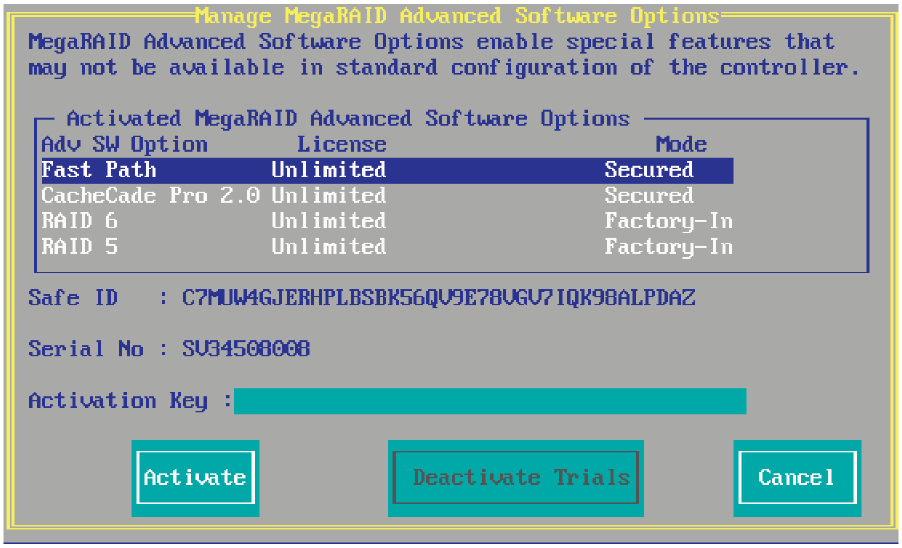


```
Manage MegaRAID Advanced Software Options
MegaRAID Advanced Software Options enable special features that
may not be available in standard configuration of the controller.

Activated MegaRAID Advanced Software Options
Adv SW Option        License
Fast Path          Unlimited
RAID 6             Unlimited
RAID 5             Unlimited

Safe ID    : SHP13232K4SURCUT4RD1914XUJQJ6GT978A8FCRZ

Serial No : SU34508008

Activation Key :
```

Figure 39. RCU – advanced software options

Note: Ignore the License column; the Safe ID, Serial No, and Activation Key fields; and Activate button. Intel RAID Controllers do not need software licenses to enable advanced software options.

Some premium features present in the RAID controller require Intel® RAID premium feature keys. For example, installing the premium feature key AXXRPFKSSD2 on the RAID controller adds the premium option CacheCade Pro 2.0 in the Adv SW Option column (Figure 40).



```
Manage MegaRAID Advanced Software Options
MegaRAID Advanced Software Options enable special features that
may not be available in standard configuration of the controller.

Activated MegaRAID Advanced Software Options
Adv SW Option        License                  Mode
Fast Path          Unlimited                Secured
CacheCade Pro 2.0  Unlimited                Secured
RAID 6             Unlimited                Factory-In
RAID 5             Unlimited                Factory-In

Safe ID    : C7MUW4GJERHPLBSBK56QV9E78VGV7IQK98ALPDAZ

Serial No : SV34508008

Activation Key :
```

Figure 40. RCU – advanced software options with key AXXRPFKSSD2 installed

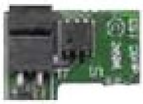
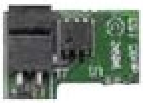
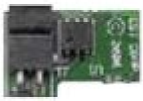
5.2.11 RAID Premium Feature Keys

Table 17 lists the available premium feature keys.

For the latest support information, refer to the Tested Hardware and Operating System List (THOL) of each RAID product available at http://www.intel.com/support.

For more details of premium feature key, refer to the *Intel® RAID Controller Configuration Guide* at http://www.intel.com/support.

Table 17. Intel® RAID premium feature keys

Product Image	Order Details		Description
	**iPC** **MM#** **UPC**	AXXRPFKSNSH 907051 00735858214377	Intel® RAID Rapid Recovery Snapshot
	**iPC** **MM#** **UPC**	AXXRPFKDE 907050 00735858214360	Intel® RAID Drive Encryption Management
	**iPC** **MM#** **UPC**	AXXRPFKSSD 918399 00735858214353	Intel® RAID SSD Cache with Fast Path *I/O
	iPC **MM#** **UPC**	AXXRPFKSNSH2 915318 00735858221481	Intel® RAID Rapid Recovery Snapshot (Gen 2*)
	iPC **MM#** **UPC**	AXXRPFKDE2 915317 00735858221474	Intel® RAID Drive Encryption Management (Gen 2*)
	iPC **MM#** **UPC**	AXXRPFKSSD2 919499 00735858221467	Intel® RAID SSD Cache with Fast Path *I/O (Gen 2*)

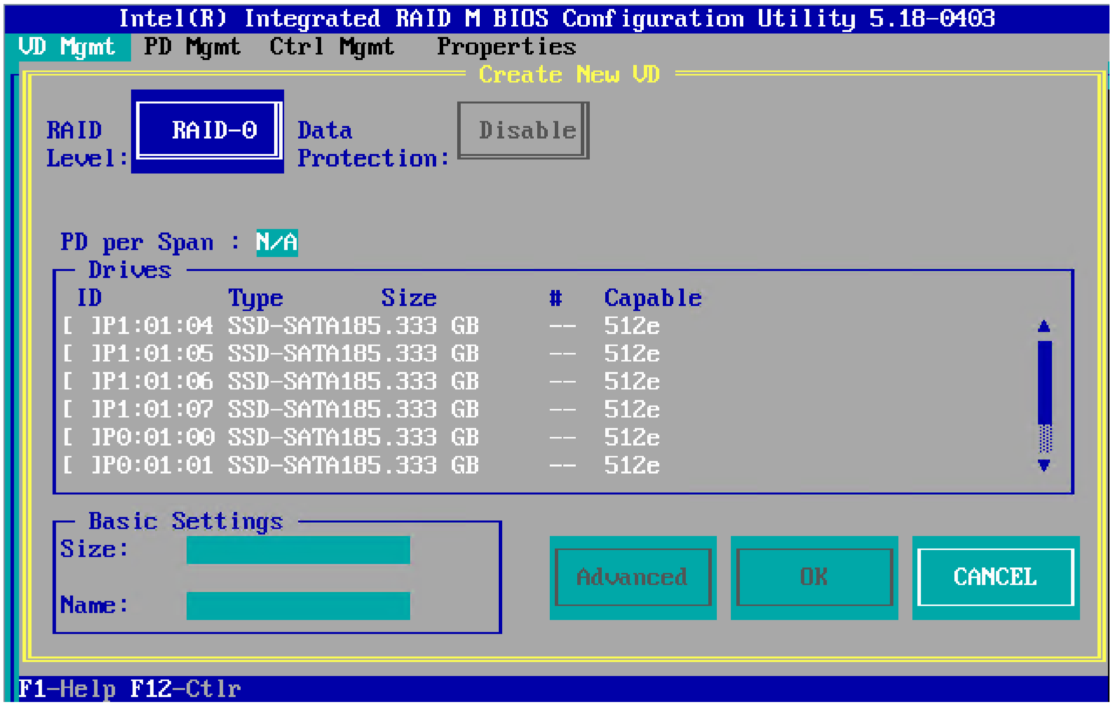
* Gen 2 RAID keys are supported by the Gen3 RAID controllers while the others are supported by the Gen2.5 RAID controllers.

5.2.12 Creating a Storage Configuration

Use the RCU to configure RAID drive groups and virtual drives to create storage configurations.

1. In the VD Mgmt screen, navigate to the controller and press the **<F2>** key.
2. Press **<Enter>**. The Create New VD screen appears (Figure 22).

Note: The Create New VD dialog can be used to create virtual drives for unconfigured good drives. To create virtual drives for existing drive groups, navigate to a drive group and press the **<F2>** key to view the Add VD in Drive Group dialog. The fields in the Add VD in Drive Group dialog are the same as in the Create New VD dialog.



```
        Intel(R) Integrated RAID M BIOS Configuration Utility 5.18-0403
VD Mgmt  PD Mgmt  Ctrl Mgmt   Properties
                                   Create New VD
 RAID    RAID-0   Data          Disable
 Level:           Protection:

  PD per Span : N/A
   Drives
  ID          Type         Size         #    Capable
[ ]P1:01:04 SSD-SATA185.333 GB          --   512e
[ ]P1:01:05 SSD-SATA185.333 GB          --   512e
[ ]P1:01:06 SSD-SATA185.333 GB          --   512e
[ ]P1:01:07 SSD-SATA185.333 GB          --   512e
[ ]P0:01:00 SSD-SATA185.333 GB          --   512e
[ ]P0:01:01 SSD-SATA185.333 GB          --   512e

   Basic Settings
  Size:
                                  Advanced     OK      CANCEL
  Name:

F1-Help F12-Ctlr
```

Figure 41. RCU – create a new virtual drive

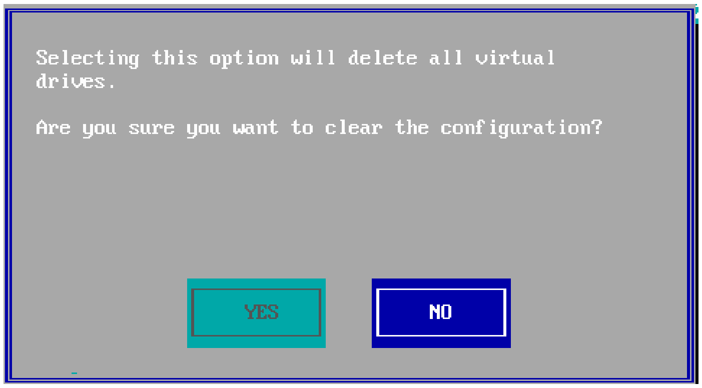
Note: If the system detects any JBOD drives the Convert JBOD to Unconfigured Good dialog (Figure 41) appears before the Create New VD dialog. The Convert JBOD to Unconfigured Good dialog provides an interface to convert the JBODs to unconfigured good drives.

3. Select a **RAID level** for the drive group.
4. Set the **Secure VD** field to **Yes** or **No**. The **Yes** option allows data encryption and uses drive-based key management for the data security solution. This option protects the data in the event of theft or loss of drives.
5. For controllers with data protection physical drives connected to it, set the **Data Protection** field to **Yes** or **No**. The **Yes** option uses the data protection feature on the newly created virtual drive. If the controller does not have data protection physical drives connected to it, the **Data Protection** field is disabled.
6. In the **Drives** list, change the sequence of the physical drives. All the available unconfigured good drives are listed. Select the physical drives in the preferred sequence. Based on the selection, the sequence number appears in the # column.
7. Set the virtual drive size in the **Size** field. The maximum size of the drive group appears automatically in the Size field. If creating other virtual drives on the same drive group, enter a size less than the maximum size of the drive group. Enter the size units (MB, GB, or TB) in uppercase.
8. Enter a name for the virtual drive in the **Name** field. The name given to the virtual drive cannot exceed 15 characters.
9. To set additional properties for the newly created virtual drive, click **Advanced**. For more information, see section 5.2.14.
10. Select **OK**. A dialog appears, asking whether to initialize the virtual drive just created.
11. To initialize the virtual drive, select **OK**. The VD Management screen appears again with the just created VD information updated.

5.2.13 Clearing the Configuration

Clear the existing configuration on virtual drives by deleting the virtual drives. Perform the following steps to clear configuration:

1. In the VD Mgmt screen, navigate to the controller and press the **<F2>** key.
2. Navigate to **Clear Configuration** and press **<Enter>**. The following dialog appears.



Selecting this option will delete all virtual drives.

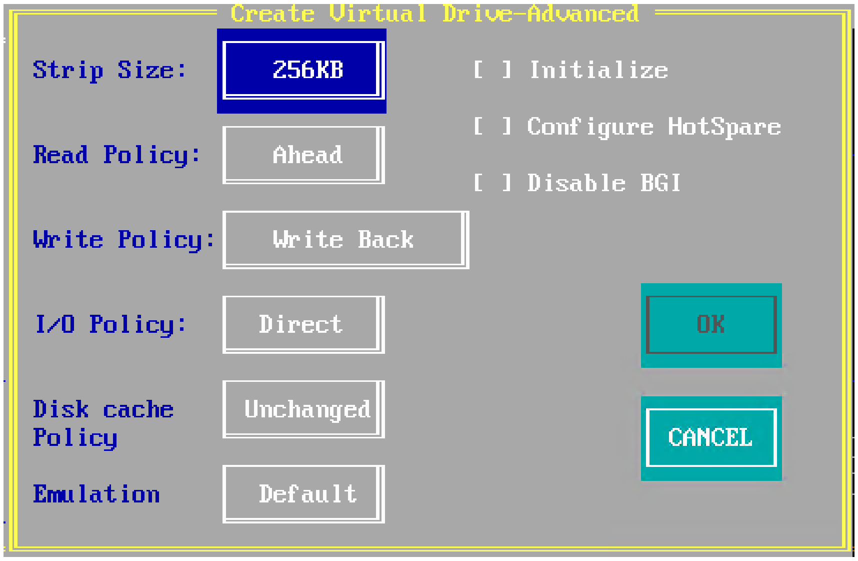
Are you sure you want to clear the configuration?

Figure 42. RCU– clear configuration dialog

3. Click **Yes** to delete all the virtual drives.

5.2.14 Setting Advanced Virtual Drive Properties

This section describes the advanced virtual drive properties that can be set when creating virtual drives. Change these parameters only with a specific reason for doing so. It is usually best to keep them at their default settings.



Create Virtual Drive-Advanced

Strip Size: 256KB

Read Policy: Ahead

Write Policy: Write Back

I/O Policy: Direct

Disk cache Policy: Unchanged

Emulation: Default

□ Initialize

□ Configure HotSpare

□ Disable BGI

Figure 43. RCU – create virtual drive advanced properties

- **Strip Size** – The strip size is the portion of the stripe that resides on a single virtual drive in the drive group. Strip sizes of 64 KB, 128 KB, 256 KB, 512 KB, or 1 MB are supported.
- **Read Policy** – Specify one of the following options to specify the read policy for this virtual drive:
  - Normal – Read ahead capability lets the controller read sequentially ahead of requested data and store the additional data in cache memory, thereby anticipating that the data will be

needed soon. This process speeds up reads for sequential data, but there is little improvement when the computer accesses random data.
    - Ahead – Disables the read ahead capability.
- **Write Policy** – Select one of the following options to specify the write policy for this virtual drive:
    - Write Thru – In this mode, the controller sends a data transfer completion signal to the host when the drive subsystem has received all the data in a transaction. This option eliminates the risk of losing cached data in case of a power failure.
    - Write Back – In this mode, the controller sends a data transfer completion signal to the host when the controller cache has received all the data in a transaction.
    - Write Back with BBU – In this mode, the controller enables write back caching when the BBU is installed and charged. This option provides a good balance between data protection and performance.

Note: The write policy depends on the status of the BBU. If the BBU is not present, is low, is failed, or is being charged, the current write policy switches to write through, which provides better data protection.

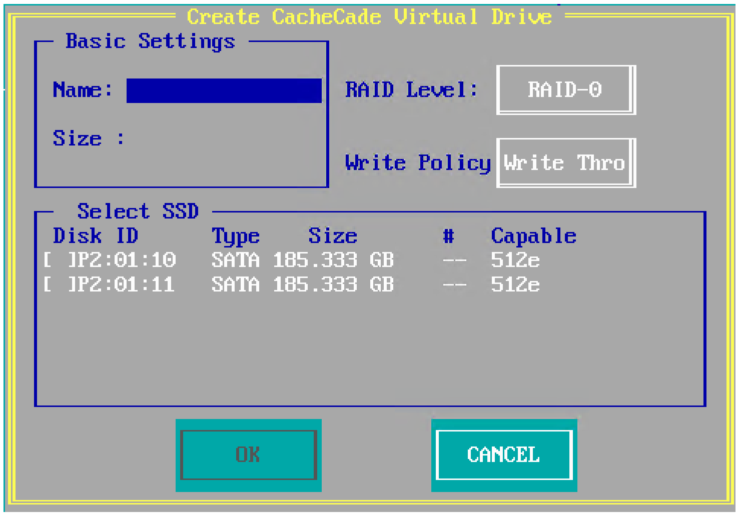
- **I/O Policy** – The I/O policy applies to reads on a specific virtual drive. It does not affect the read ahead cache.
    - Cached – In this mode, all reads are buffered in cache memory. Cached I/O provides faster processing.
    - Direct – In this mode, reads are not buffered in cache memory. Data is transferred to the cache and the host concurrently. If the same data block is read again, it comes from cache memory. Direct I/O makes sure that the cache and the host contain the same data.
- **Disk cache policy** – Select a cache setting for this virtual drive:
    - Enable – Enable the drive cache.
    - Disable – Disable the drive cache.
    - Unchanged – Updating the drive cache policy to Unchanged may enable/disable the drive cache based on the WCE (Write Cache Policy) bit of the save mode page of the drive.
- **Emulation** – Set the emulation type on a virtual drive. The possible options are Default, Disabled, or Forced. The Force option forces the emulation to be set on a controller even when MFC settings do not support it.
- **Initialize** – Select to initialize the virtual drive. Initialization prepares the storage medium for use. Fast initialization is performed on the virtual drive.
- **Configure Hot Spare** – Select to configure physical drives as hot spares for the newly created virtual drive. This option is enabled only if there are additional drives and if they are eligible to be configured as hot spares. This option is not applicable for RAID 0. If this option is selected, choose the physical drives to configure as hot spares in the resulting dialog.

5.2.15 Managing CacheCade Virtual Drives

5.2.15.1 Creating a CacheCade* Virtual Drive

The LSI* MegaRAID* CacheCade* software provides read caching capability. Perform the following steps to create a CacheCade virtual drive:

1. In the VD Mgmt screen, navigate to the controller and press the **<F2>** key.
2. Navigate to **Create CacheCade Virtual Drive**, and press **<Enter>**. The Create CacheCade Virtual Drive dialog appears (Figure 24).



```
Create CacheCade Virtual Drive

Basic Settings
Name:                      RAID Level:    RAID-0
Size :
                           Write Policy   Write Thro

Select SSD
Disk ID       Type     Size          #   Capable
[ ]P2:01:10   SATA  185.333 GB     --   512e
[ ]P2:01:11   SATA  185.333 GB     --   512e
```

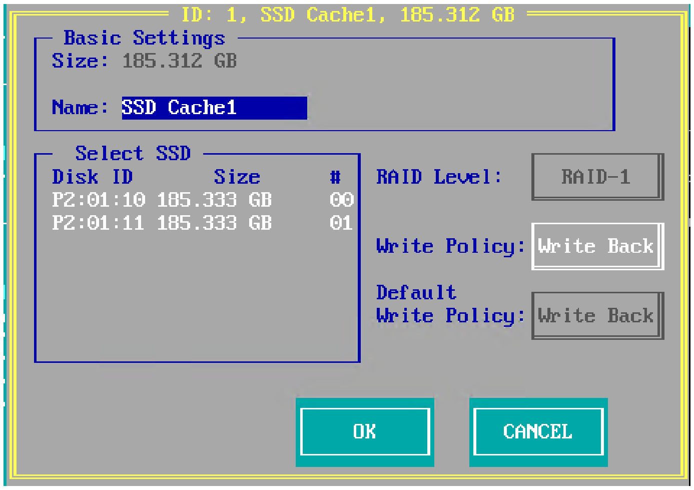
Figure 44. RCU – create CacheCade* virtual drive

3. Enter a name for the CacheCade virtual drive in the **Name** field.
4. Select a RAID level for the SSD Cache volume, either RAID-0 or RAID-1
5. Select the Write Policy either Write Through or Write back
6. Select the SSDs from the **Select SSD** box. The size of the SSD is reflected in the **Size** field (in the **Basic Settings** box).
7. Select **OK**. A message appears, stating that the CacheCade virtual drive has been created.

5.2.15.2 Modifying a CacheCade Virtual Drive

Modify an existing CacheCade virtual drive by renaming it. Perform the following steps to modify the CacheCade virtual drive:

1. In the VD Mgmt screen, navigate to the CacheCade virtual drive and press the **<F2>** key.
2. Navigate to **Properties** and press **<Enter>**. The following dialog appears.



```
ID: 1, SSD Cache1, 185.312 GB

Basic Settings
Size: 185.312 GB

Name: SSD Cache1

Select SSD
Disk ID      Size        #     RAID Level:      RAID-1
P2:01:10 185.333 GB     00
P2:01:11 185.333 GB     01     Write Policy:    Write Back

                               Default
                               Write Policy:    Write Back
```

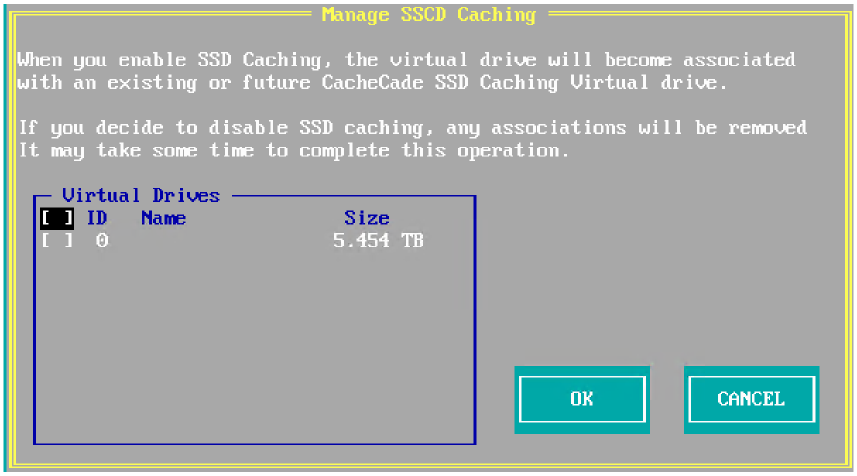
Figure 45. RCU – modify CacheCade* virtual drive

3. Rename the CacheCade virtual drive in the **CacheCade Virtual Drive Name** field.
4. Click **OK**.

5.2.15.3 Enabling SSD Cacheing on a Virtual Drive

After the SSD Cache VD is created, now it needs to be associated to a data VD:

1. In the VD Mgmt screen, navigate to the controller and press the **<F2>** key.
2. Navigate to **Manage SSD Caching** and press **<Enter>**. The Create CacheCade Virtual Drive dialog appears (Figure 45).



When you enable SSD Caching, the virtual drive will become associated with an existing or future CacheCade SSD Caching Virtual drive.

If you decide to disable SSD caching, any associations will be removed It may take some time to complete this operation.

```
Virtual Drives
[ ] ID   Name                Size
[ ]  0                     5.454 TB
```

Figure 46. RCU – Manage SSD Caching

3. Select the virtual drive to associate the SSD cache volume with (More than one VD can be associated if they exist).

12. Select **OK**. The VD Management screen appears again with the information updated.

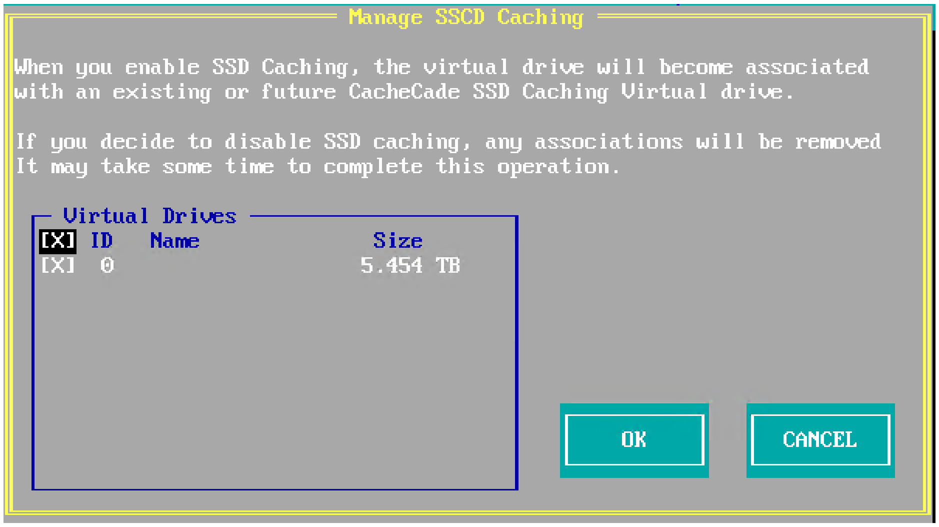
5.2.15.4 Disabling SSD Caching on a Virtual Drive

Disabling SSD caching on a virtual drive removes any associations that the selected virtual drive has with a CacheCade SSD Caching virtual drive. This option is only available when the virtual drive's caching is currently enabled.

Perform the following steps to disable SSD Caching on a virtual drive:

1. In the VD Mgmt screen, navigate to a virtual drive and press the **<F2>** key.

4. Select **Manage SSD Caching** and press **<Enter>**. The **Manage SSD Caching** screen appears showing all the associations (Figure 45).



```
When you enable SSD Caching, the virtual drive will become associated
with an existing or future CacheCade SSD Caching Virtual drive.

If you decide to disable SSD caching, any associations will be removed
It may take some time to complete this operation.

 Virtual Drives
[X] ID   Name                Size
[X]  0                      5.454 TB
```

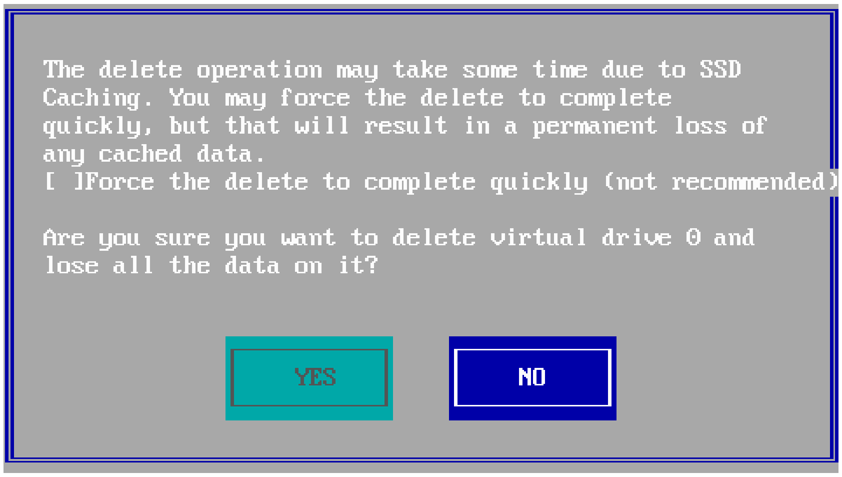
Figure 47. RCU – disabling SSD caching dialog

2. De-select the virtual drive and press OK.

5.2.15.5 Deleting a Virtual Drive with SSD Caching Enabled

Perform the following steps to delete a virtual drive that has SSD caching enabled:

1. In the VD Mgmt screen, navigate to a virtual drive and press the **<F2>** key.
2. Select **Delete VD** and click **Yes**. The following message dialog appears.



```
The delete operation may take some time due to SSD
Caching. You may force the delete to complete
quickly, but that will result in a permanent loss of
any cached data.
[ ]Force the delete to complete quickly (not recommended)

Are you sure you want to delete virtual drive 0 and
lose all the data on it?
```

Figure 48. Ctrl-R Utility – deleting a virtual drive dialog

Note: If the checkbox is selected for the Force delete to complete quickly option, the data is not flushed before deleting the virtual drive. In this scenario, if this virtual drive is created after deleting it, there is no data available.

3. Press **Yes** to proceed with the delete operation.

5.2.15.6 SSD Cache volume Sector Size

When creating SSD cache volumes, only 512n or 512e drives can be used but the sector size of the SSD cache volume must match the sector size of the data VD. Refer to Table 18 for sector size restrictions when creating an SSD cache volume.

Table 18. SSD cache Drive Sector Size

Data VD Sector Size	SSD Cache VD Sector Size
512n	512n
512e	512e
4Kn	Not supported

5.2.16 Using LSI* MegaRAID* SafeStore* Encryption Software

LSI* MegaRAID* SafeStore* encryption software enables the “Auto-Lock” feature on Self Encrypting Drives (SED) to provide data security on the data in rest. This solution protects data in the event of theft or loss of physical drives. Removing a self-encrypting drive from its storage system or the server in which it resides becomes useless to anyone who attempts to access it without appropriate security authorization since the data on that drive is encrypted.

5.2.17 Enabling Drive Security

This section describes how to enable, change, and disable the drive security and how to import a foreign configuration by using the SafeStore advanced software.

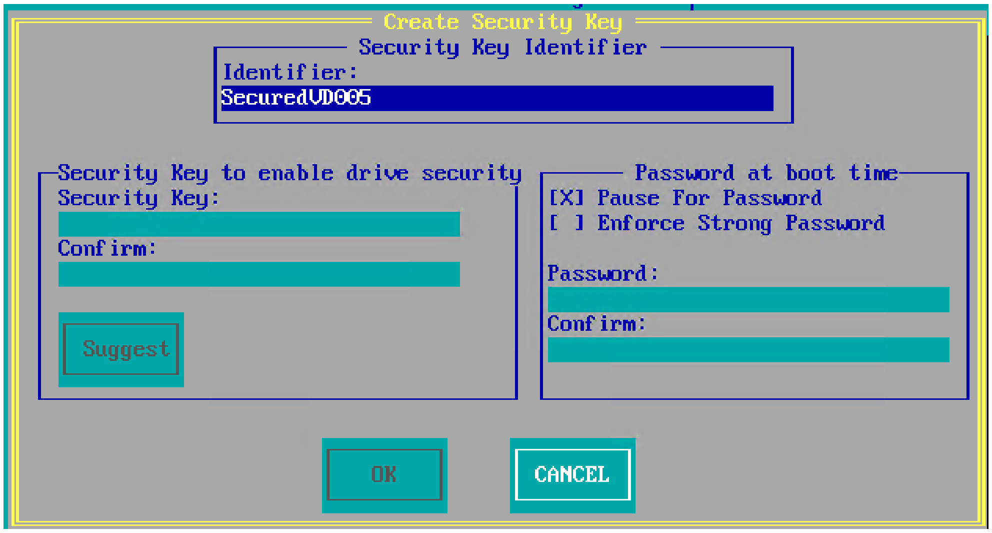
Enabling security on the drives requires a security key identifier and a security key as defined below.

- The security key identifier is a label for the security key and appears anytime the security key is requested.
- The security key is a password required to create secure virtual drives and to unlock the drives at power on. When the system is powered on, the RAID controller provides each drive the security key in order to unlock it and allow access to the stored data. The RAID controller encrypts the security key before storing it on its memory.

Security can be improved by entering a password. In this case when the server is powered on, the RAID controllers request for the password before passing the security key to the drives.

Perform the following steps to enable drive security on an existing VD:

1. In the VD Mgmt screen, navigate to the controller and press the **<F2>** key.
2. Navigate to **Drive Security**, and press **<Enter>**.
3. Navigate to **Enable Security** and press **<Enter>**. The Create Security Key dialog appears (Figure 34).



Identifier:
SecuredVD005

Security Key:

Confirm:

[X] Pause For Password
[ ] Enforce Strong Password

Password:

Confirm:

Figure 49. RCU – Create security key screen

4. Use the default security key identifier or enter a new one.

Note: After creating a security key, the Enable Security option is disabled. This option is reenabled only after deleting the existing key.

5. Enter a security key or click **Suggest** to automatically create one. The security is case sensitive; must be between 8 and 12 characters; and must contain at least one number, one lowercase letter, one uppercase letter, and one special character (for example, < > @ +). A space is not permitted.
6. Reenter the new security key to confirm it.
7. Optionally provide a Password that will be prompted at boot time.

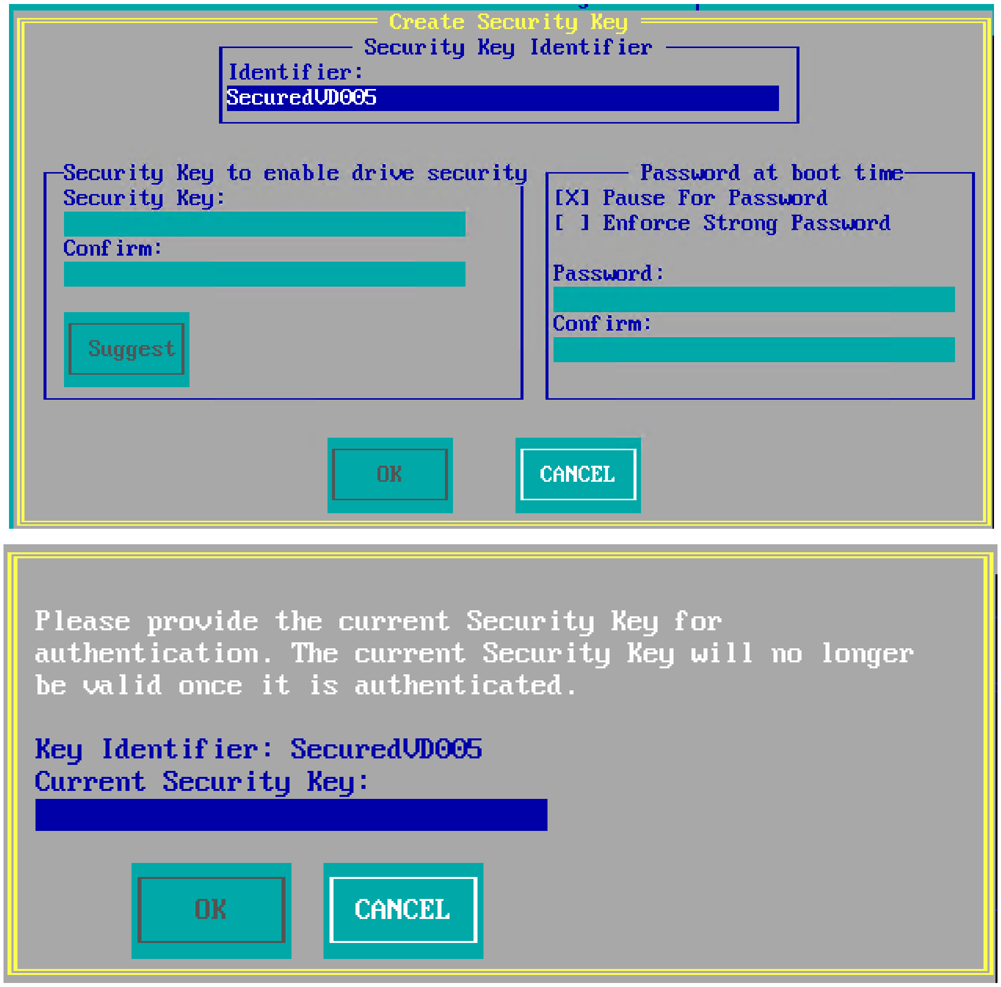
Caution: If the security key is forgotten, access to data is lost. Be sure to record the security key information.

Note: Non-U.S. keyboard users must be careful not to enter double-byte character set (DBCS) characters in the security key field. The firmware works with the ASCII character set only.

5.2.18 Changing Security Settings

Perform the following steps to change the encryption settings for the security key identifier, security key, and password:

1. In the VD Mgmt screen, navigate to the controller, and press the **<F2>** key.
2. Navigate to **Drive Security**, and press **<Enter>**.
3. Select **Change Security Settings** and press **<Enter>**. The Change Security Key dialog appears (Figure 35).



Identifier: SecuredVD005

[X] Pause For Password
[ ] Enforce Strong Password

Please provide the current Security Key for authentication. The current Security Key will no longer be valid once it is authenticated.

Key Identifier: SecuredVD005
Current Security Key:

Figure 50. RCU – change security key screen

4. Enter a new security key identifier. The security key identifier must be changed if the security key is changed in order to differentiate between the security keys.
5. Enter a new security key or click **Suggest** to automatically create one. See section 5.2.17 for security key requirements.
6. Reenter the new security key to confirm it.
7. After selecting OK, a dialog screen will pop up to enter the current Security Key. Enter the current Security Key and select OK.

5.2.19 Disabling Drive Security

After disabling drive security, the existing data is not secure and no new secure virtual drives can be created. Disabling drive security does not affect data security on foreign drives. If any drives that were previously secured were removed, the password is still required when importing them to access their data.

If there are any secure drive groups on the controller, drive security cannot be disabled. A warning dialog appears if this is attempted. To disable drive security, first delete the virtual drives on all the secure drive groups.

Perform the following steps to disable drive security:

1. In the VD Mgmt screen, navigate to the controller and press the **<F2>** key.
2. Navigate to **Drive Security**, and press **<Enter>**.
3. Select **Disable Security**. A message box appears.
4. To disable drive security, press **Yes** to delete the security key.

Note: Disabling drive security prevents the creation of any new encrypted virtual drives and erases the data on all encrypted unconfigured drives. Disabling drive security does not affect the security or data of foreign drives.

5.2.20 Importing or Clearing a Foreign Configuration

A foreign configuration is a RAID configuration that already exists on a replacement set of drives installed in a computer system. The Ctrl-R Utility can be used to import the foreign configuration to the RAID controller or to clear the foreign configuration so that these drives can be used to create a new configuration.

To import a foreign configuration, perform the following tasks:

1. Enable security to permit importation of locked foreign configurations. Unsecured or unlocked configurations can be imported when security is disabled.
2. If a locked foreign configuration is present and security is enabled, enter the security key and unlock the configuration.
3. Import the foreign configuration.

If one or more drives are removed from a configuration by a cable pull or drive removal, for example, the configuration on those drives is considered a foreign configuration by the RAID controller.

Verify whether any drives are left to import because the locked drives can use different security keys. If any drives remain, repeat the import process for the remaining drives. After all the drives are imported, there is no configuration to import.

Note: When creating a new configuration, the Ctrl-R Utility shows only the unconfigured drives. Drives that have existing configurations, including foreign configurations, do not appear. To use drives with existing configurations, first clear the configuration on those drives.

Foreign configurations can be imported or cleared from the VD Mgmt menu or from the Foreign View menu.

Perform the following steps to import or clear a foreign configuration from the VD Mgmt menu:

1. In the VD Mgmt screen, navigate to the controller and press the **<F2>** key.
2. Navigate to **Foreign Config** and press **<Enter>**. The foreign configuration options **Import** and **Clear** appear.

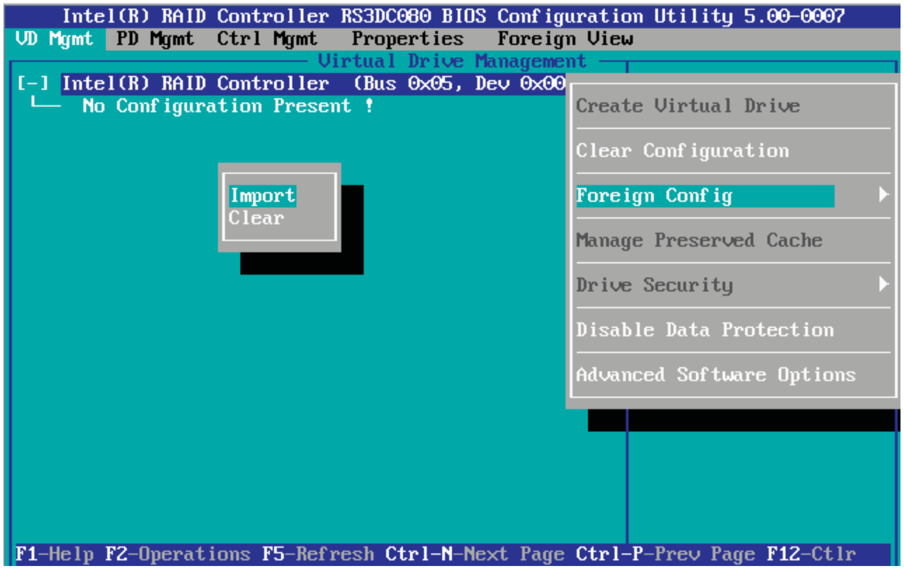
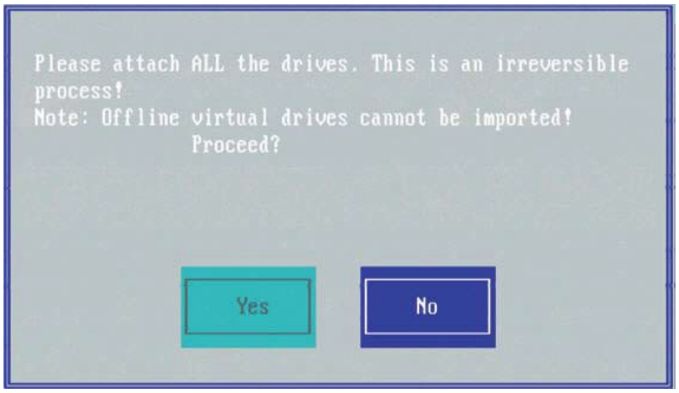

Intel(R) RAID Controller RS3DC080 BIOS Configuration Utility 5.00-0007
VD Mgmt
PD Mgmt
Ctrl Mgmt
Properties
Foreign View
Virtual Drive Management
[-] Intel(R) RAID Controller (Bus 0x05, Dev 0x00
No Configuration Present !
Import
Clear
Create Virtual Drive
Clear Configuration
Foreign Config
Manage Preserved Cache
Drive Security
Disable Data Protection
Advanced Software Options
F1-Help F2-Operations F5-Refresh Ctrl-N-Next Page Ctrl-P-Prev Page F12-Ctlr

Figure 51. RCU – foreign configuration options

3. To import a foreign configuration, select **Import** and press **<Enter>**. Select **Yes** in the resulting dialog (Figure 37) to import the foreign configuration from all the foreign drives. Repeat the import process for any remaining drives. Because locked drives can used different security keys, it is necessary to verify whether there are any remaining drives to be imported.

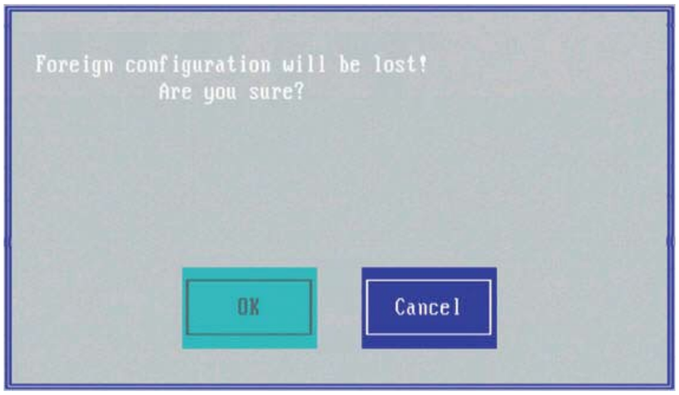


Please attach ALL the drives. This is an irreversible process!
Note: Offline virtual drives cannot be imported!
Proceed?

Figure 52. RCU – import foreign configuration

4. To clear a foreign configuration, select **Clear** and press **<Enter>**. Select OK in the resulting dialog (Figure 38) to clear the foreign configuration.

Note: The clear operation cannot be reversed after it is started. Imported drives appear as online in the Ctrl-R Utility.



Foreign configuration will be lost!
Are you sure?

Figure 53. RCU – clear foreign configuration

5.2.20.1 Foreign Configurations in Cable Pull and Drive Removal Scenarios

If one or more drives are removed from a configuration by a cable pull or drive removal, for example, the configuration on those drives is considered a foreign configuration by the RAID controller.

The following scenarios can occur with cable pulls or drive removals.

Note: To import the foreign configuration in any of the following scenarios, all the drives must be in the enclosure before performing the import operation.

- **Scenario 1**: If all or some the drives in a configuration are removed and reinserted, the controller considers the drives to have foreign configurations. Import or clear the foreign configuration. If import is selected, automatic rebuilds occur in redundant virtual drives.

Note: Start a consistency check immediately after the rebuild is complete to ensure data integrity for the virtual drives.

- **Scenario 2**: If all the drives in a virtual drive are removed, but at different times, and reinserted, the controller considers the drives to have foreign configurations. Import or clear the foreign configuration. If import is selected, all drives that were pulled before the virtual drive became offline are imported and automatically rebuilt. Automatic rebuilds occur in redundant virtual drives.
- **Scenario 3**: If the drives in a non-redundant virtual drive are removed, the controller considers the drives to have foreign configurations. Import or clear the foreign configuration. No rebuilds occur after the import operation because there is no redundant data to rebuild the drives.

5.2.21 Discarding Preserved Cache

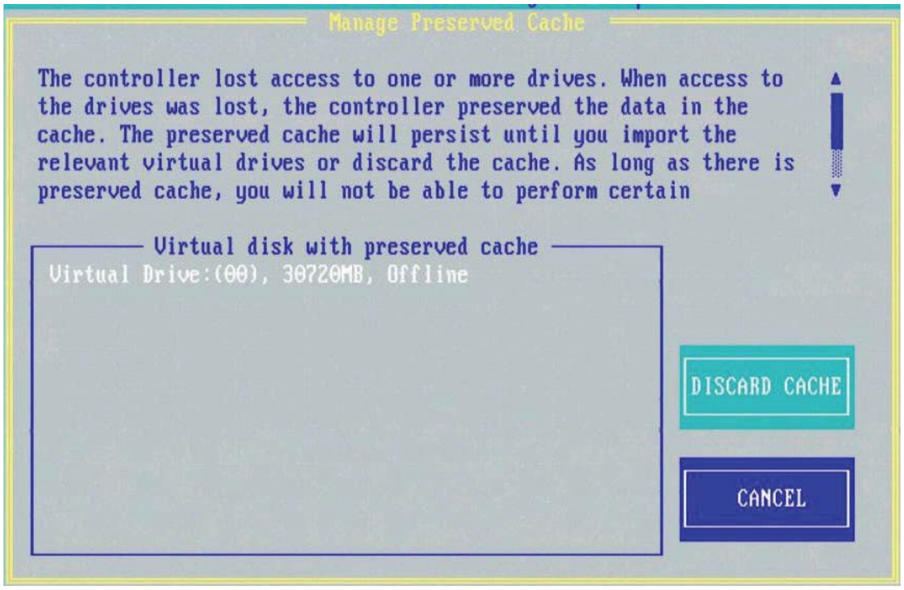
If the controller loses access to one or more virtual drives, the controller preserves the data from the virtual drive. This preserved cache, is preserved until importing the virtual drive or discard the cache.

Certain operations, such as creating a new virtual drive, cannot be performed if preserved cache exists.

Caution: If there are any foreign configurations, import the foreign configuration before discarding the preserved cache. Otherwise, data that belongs to the foreign configuration may be lost.

Perform the following steps to discard the preserved cache:

1. In the VD Mgmt screen, navigate to the controller and press the **<F2>** key.
2. Navigate to **Manage Preserved Cache** and press **<Enter>**. The Manage Preserved Cache dialog appears (Figure 54).


Manage Preserved Cache

The controller lost access to one or more drives. When access to the drives was lost, the controller preserved the data in the cache. The preserved cache will persist until you import the relevant virtual drives or discard the cache. As long as there is preserved cache, you will not be able to perform certain

Virtual disk with preserved cache

Virtual Drive:(00), 30720MB, Offline

Figure 54. RCU – manage preserved cache

3. Click **Discard Cache** to discard the preserved cache from the virtual drive.
4. Click **OK** to confirm.

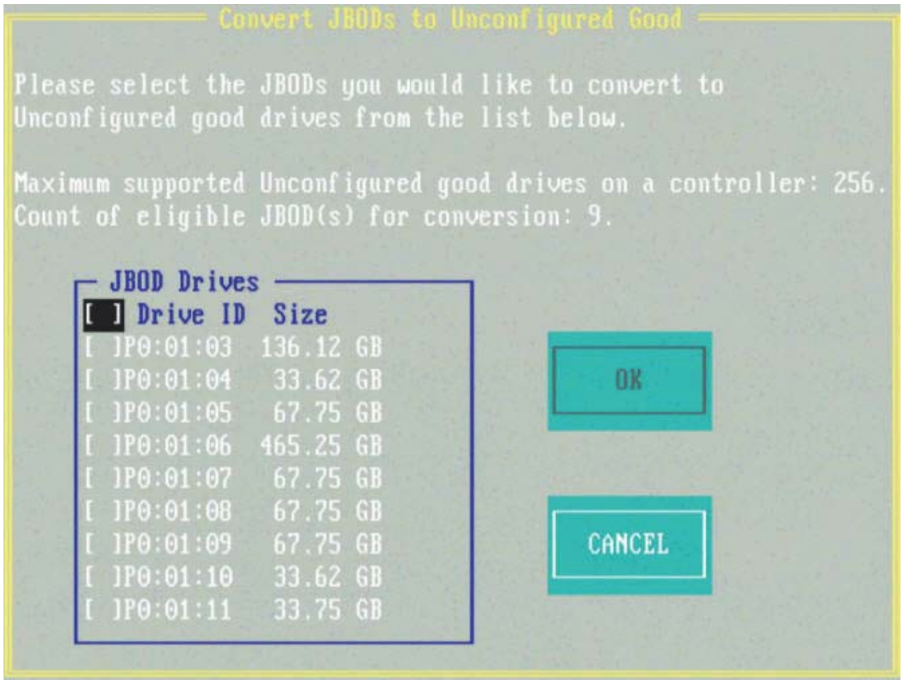
5.2.22 Converting JBOD Drives to Unconfigured Good Drives

When a drive is set to JBOD, the RAID controller presents the drive as is to the Operating System. A JBOD drive cannot be used in a RAID configuration.

Multiple JBOD drives can be converted to unconfigured good drives from the VD Mgmt screen or a particular JBOD drive can be converted to an unconfigured good drive from the Drive Management screen.

Perform the following steps to convert multiple JBODs to unconfigured good drives:

1. In the VD Mgmt screen, navigate to the controller and press the **<F2>** key.
2. Navigate to **Make Unconfigured Good** and press **<Enter>**. The Convert JBOD to Unconfigured Good dialog appears, which shows all JBODs available in the system (Figure 55).



```
Convert JBODs to Unconfigured Good

Please select the JBODs you would like to convert to
Unconfigured good drives from the list below.

Maximum supported Unconfigured good drives on a controller: 256.
Count of eligible JBOD(s) for conversion: 9.

JBOD Drives
[ ] Drive ID  Size
[ ]P0:01:03  136.12 GB
[ ]P0:01:04   33.62 GB
[ ]P0:01:05   67.75 GB
[ ]P0:01:06  465.25 GB
[ ]P0:01:07   67.75 GB
[ ]P0:01:08   67.75 GB
[ ]P0:01:09   67.75 GB
[ ]P0:01:10   33.62 GB
[ ]P0:01:11   33.75 GB
```

Figure 55. RCU – convert JBOD drives to unconfigured good drives

3. Select the desired JBODs to configure as unconfigured good drives. To select or deselect all the JBODs at once, select the top most square brackets in the **JBOD Drives** box.
4. Click **OK**. The selected JBODS are converted to unconfigured good drives.

Perform the following steps to convert a particular JBOD drive to an unconfigured good drive:

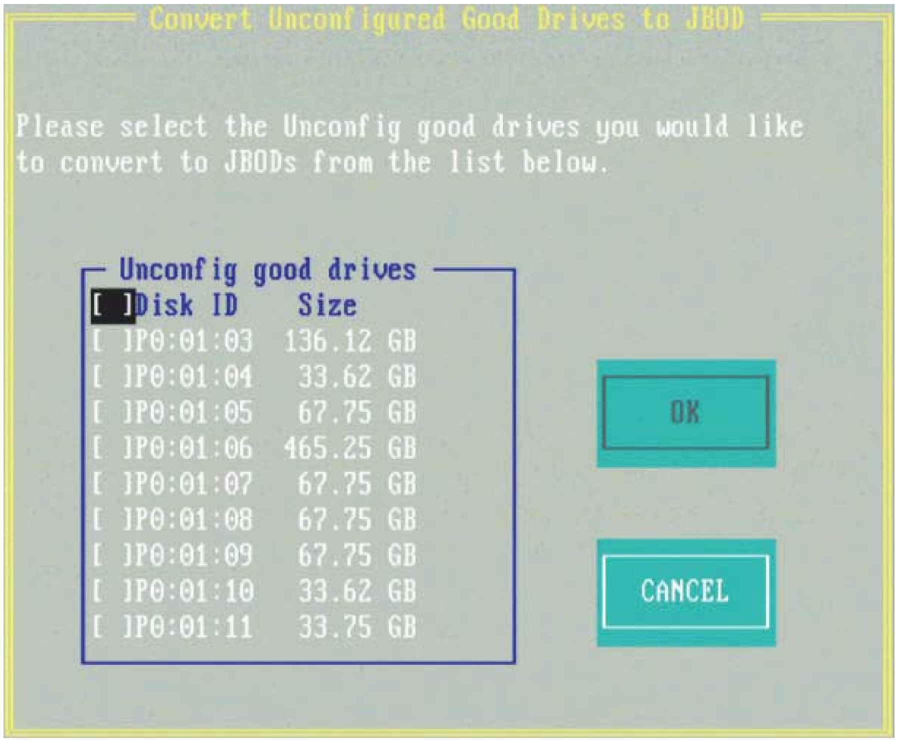
1. In the Drive Management screen, navigate to a JBOD drive and press the **<F2>** key.
2. Navigate to **Make Unconfigured Good** and press **<Enter>**.
3. Click **Yes** in the confirmation message box to proceed.

5.2.23 Converting Unconfigured Good Drives to JBOD Drives

Multiple unconfigured good drives can be converted to JBOD drives from the VD Mgmt screen or a particular unconfigured good drive can be converted to JBOD drive from the Drive Management screen.

Perform the following steps to convert multiple unconfigured good drives to JBOD drives:

1. In the VD Mgmt screen, navigate to the controller and press the **<F2>** key.
2. Navigate to **Make JBOD** and press **<Enter>**. The Convert Unconfigured Good to JBOD dialog appears showing all unconfigured good drives available in the system (Figure 41).



Convert Unconfigured Good Drives to JBOD

Please select the Unconfig good drives you would like to convert to JBODs from the list below.

```
Unconfig good drives
[ ]Disk ID    Size
[ ]P0:01:03  136.12 GB
[ ]P0:01:04   33.62 GB
[ ]P0:01:05   67.75 GB
[ ]P0:01:06  465.25 GB
[ ]P0:01:07   67.75 GB
[ ]P0:01:08   67.75 GB
[ ]P0:01:09   67.75 GB
[ ]P0:01:10   33.62 GB
[ ]P0:01:11   33.75 GB
```

Figure 56. RCU – convert unconfigured good drives to JBOD drives

3. Select the desired unconfigured good drives to configure as JBODs. To select or deselect all the unconfigured good drives at once, select the top most square brackets in the **Unconfig good drives** box.
4. Click **OK**. The selected unconfigured good drives are converted to JBOD drives.

Perform the following steps to convert a particular unconfigured good drive to a JBOD drive:

1. In the Drive Management screen, navigate to an unconfigured good drive and press the **<F2>** key.
2. Navigate to **Make JBOD** and press **<Enter>**.
3. Click **OK** in the message confirmation box to continue.

5.2.24 Viewing and Changing Device Properties

This section explains how to use the Ctrl-R Utility to view and change the properties for controllers, virtual drives, drive groups, physical drives, and BBUs.

5.2.25 Viewing Controller Properties

The Ctrl-R Utility shows information for one Intel RAID Controller at a time. If the system has multiple Intel RAID Controllers, view information for a different controller by pressing the **<F12>** key and selecting a controller from the list.

Navigate to the **Properties** menu to view the properties of the active controller. For more information on the Properties menu, see section 5.2.8.

5.2.26 Modifying Controller Properties

Modify controller properties in the Ctrl Mgmt menu. After changing property values on the first or second Ctrl Mgmt screen, press **Apply** to apply the changes. For more information on navigating the Ctrl Mgmt screen, see section 5.2.7.

The following table describes all entries and options listed on both Ctrl Mgmt screens. Leave these options at their default settings to achieve the best performance, unless there is a specific reason for changing them.

Table 19. RCU controller settings

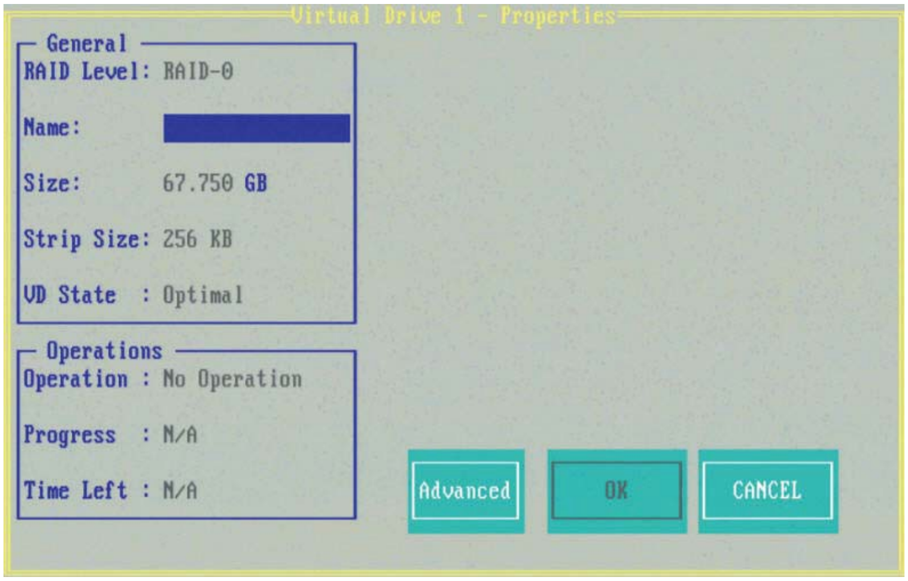
Option	Description
Alarm Control	Enable, disable, or silence the onboard alarm tone generator on the controller.
Coercion Mode	Force drives of varying capacities to the same size so they can be used in a drive group. The coercion mode options are None, 128MB-way, and 1GB-way. The chosen number depends on how much the drives from various vendors vary in their actual size.
BIOS Mode	Specifies one of the following options to set the BIOS boot mode: • Stop on Error – Shows the errors encountered during boot up and waits for your input. The firmware does not proceed with the boot process till you take some action • Ignore Error – Ignores errors and the firmware proceeds with boot. • Pause on Error – The firmware may halt due to hardware faults. If the firmware encounters no hardware faults, then the boot up continues. • SafeMode Error – Boots the controller to run in safe mode.
Boot Device	Select the boot device from the list of virtual drives and JBODs.
Rebuild Rate	Select the rebuild rate for drives connected to the selected controller. The rebuild rate is the percentage of system resources dedicated to rebuilding a failed drive. The higher the number, the more system resources that are devoted to a rebuild. The rebuild rate range is between 0 and 100 percent.
BGI Rate	Select the amount of system resources dedicated to background initialization (BGI) of virtual drives connected to the selected controller. The BGI rate range is between 0 and 100 percent.
CC Rate	Select the amount of system resources dedicated to consistency checks (CCs) of virtual drives connected to the selected controller. The CC rate range is between 0 and100 percent.
Recon. Rate	Select the amount of system resources dedicated to reconstruction of drives connected to the selected controller. The Recon rate range is between 0 and100 percent.
Patrol Rate	Select the rate for patrol reads for drives connected to the selected controller. The patrol read rate is the percentage of system resources dedicated to running a patrol read. The patrol read range is between 0 to 100 percent.
Cache Flush Interval	Control the interval in seconds at which the contents of the onboard data cache are flushed. The Cache Flush Interval range is between 0 to100 seconds.
Spinup Delay	Control the interval in seconds between spinup of drives connected to this controller. The delay prevents a drain on the system's power supply that would occur if all drives spun up at the same time. The Spinup Delay range is between 0 to 255 seconds.
Spinup Drive	Control the interval in seconds at which the contents of the onboard data cache are flushed. The Spinup Drive range is between 0 to 255 seconds.
Maintain PD Fail History	Maintain the history of all drive failures.
Enable Controller BIOS	Enable or disable the BIOS for the selected controller. If the boot device is on the selected controller, the BIOS must be enabled. Otherwise, the BIOS should be disabled to ensure a boot device can be used elsewhere.
Enable Stop CC on Error	Stop a consistency check when the controller BIOS encounters an error.
Auto Enhanced Import	Import automatically at boot time.
Set Factory Defaults	Load the default Ctrl-R Utility settings.
Manage Link Speed	Change the link speed between the controller and the expander, or between a controller and a drive that is directly connected to the controller.
Manage Power Save	Reduce the power consumption of drives that are not in use by spinning down the unconfigured good drives, hot spares, and configured drives.
Manage Battery	View information about the BBU, if the selected controller has a BBU.
Emergency Spare	Commission unconfigured good drives or global hotspares as emergency spare drives. Select from the options None, UG (Unconfigured Good), GHS (Global Hotspare), or UG and GHS (Unconfigured Good and Global Hotspare).
Enable Emergency for SMARTer	Commission emergency hot spare drives for predictive failure analysis events.

5.2.27 Viewing and Changing Virtual Drive Properties

The RCU shows the properties, policies, and the operations for virtual drives.

To view these items for the currently selected virtual drive and to change some of these settings, perform the following steps:

1. In the VD Mgmt screen, navigate to a virtual drive, and press the F2 key.
2. Press Enter. The Virtual Drive Properties dialog appears.



```
Virtual Drive 1 - Properties
General
RAID Level: RAID-0
Name:
Size:        67.750 GB
Strip Size: 256 KB
VD State   : Optimal
Operations
Operation : No Operation
Progress   : N/A
Time Left : N/A
```

Figure 57. RCU – virtual drive properties

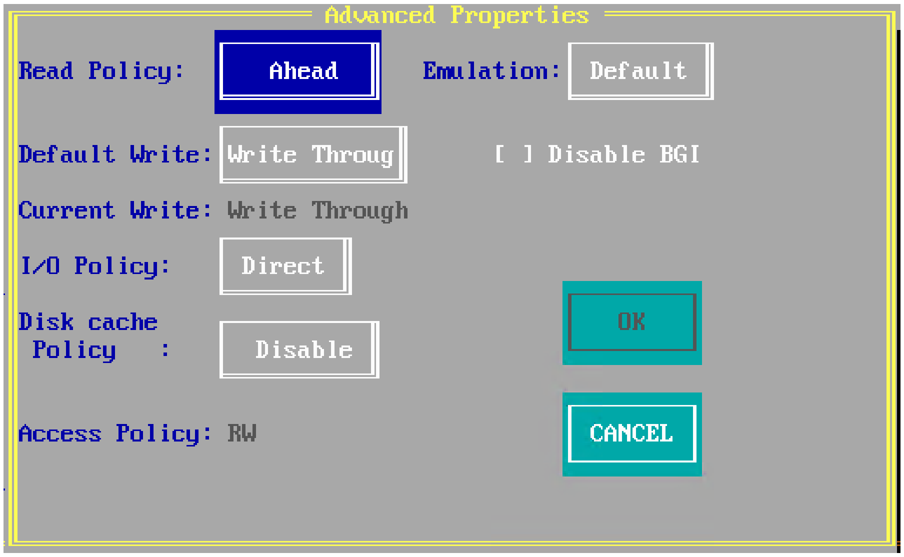
The General box shows the virtual drive's RAID level, name, state, size, and strip size.

The Operations box lists any operation (performed on the virtual drive) in progress, along with its progress status and the time remaining for the operation to be completed.

3. You may change the settings for the fields that are enabled in this dialog.

Caution: Before changing a virtual drive configuration, back up desired data on the virtual drive.

4. Press OK to save your changes.
5. Press Advanced to view additional virtual drive properties. The Create Virtual Drive – Advanced dialog appears.



Advanced Properties

Read Policy: Ahead

Emulation: Default

Default Write: Write Throug

[ ] Disable BGI

Current Write: Write Through

I/O Policy: Direct

Disk cache Policy : Disable

Access Policy: RW

Figure 58. RCU – advanced virtual drive properties

You can view the virtual drive policies that were defined when the storage configuration was created.

You can also select Initialize and/or Configure Hot Spare to initialize the newly created virtual drive or to configure the virtual drive as a hot spare, respectively.

If you select Initialize and/or Configure Hot Spare, messages pertaining to initializing the virtual drive or to configuring the virtual drive as a hot spare appear only after you exit the Virtual Drive Properties dialog.

5.2.28 Deleting a Virtual Drive

Any virtual drive on the controller can be deleted to reuse that space for a new virtual drive. The Ctrl-R Utility lists configurable drive groups where there is space to configure. If multiple virtual drives are defined on a single drive group, a virtual drive can be deleted without deleting the entire drive group.

Caution: Back up data before deleting a virtual drive.

Perform the following steps to delete a virtual drive:

1. In the VD Mgmt screen, navigate to the virtual drive, and press the **<F2>** key.
2. Navigate to **Delete VD**, and press **<Enter>**.
3. Press **OK** to confirm deletion of the virtual drive.

5.2.29 Deleting a Virtual Drive Group

Deleting a drive group also deletes all virtual drives in that drive group.

Caution: Back up data before deleting a virtual drive group.

Perform the following steps to delete a drive group:

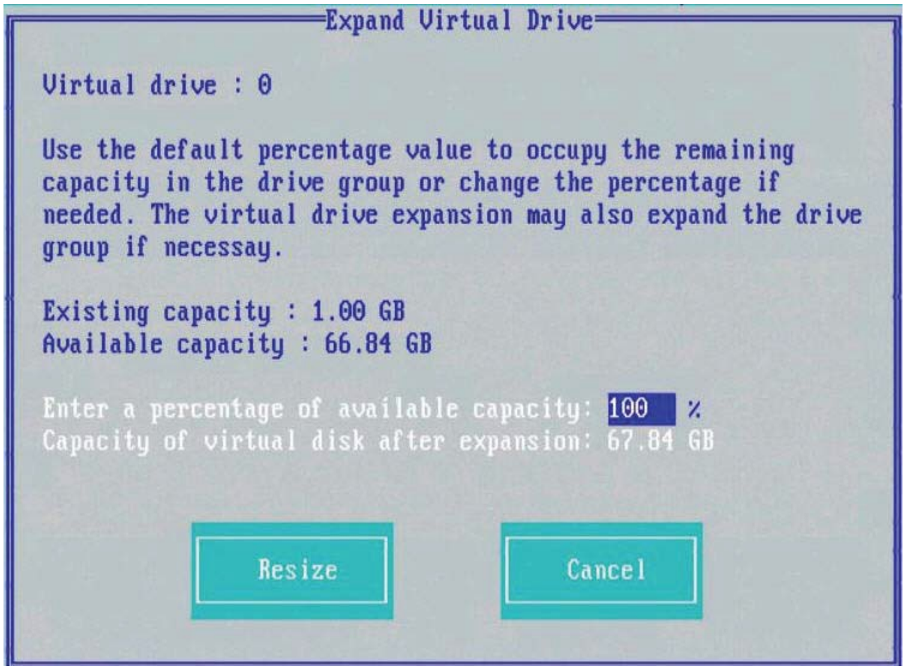
1. In the VD Mgmt screen, navigate to a drive group and press the **<F2>** key.
2. Navigate to **Delete Drive Group**, and press **<Enter>**. The drive group is deleted and is removed from the VD Mgmt screen.

5.2.30 Expanding a Virtual Drive

The size of a virtual drive can be increased to occupy the remaining capacity in a drive group.

Perform the following steps to expand the size of a virtual drive:

1. In the VD Mgmt screen, select the virtual drive to be expanded and press the **<F2>** key.
2. Navigate to **Expand VD**, and press **<Enter>**. The Expand Virtual Drive dialog appears (Figure 59).



```
Expand Virtual Drive

Virtual drive : 0

Use the default percentage value to occupy the remaining
capacity in the drive group or change the percentage if
needed. The virtual drive expansion may also expand the drive
group if necessary.

Existing capacity : 1.00 GB
Available capacity : 66.84 GB

Enter a percentage of available capacity: 100 %
Capacity of virtual disk after expansion: 67.84 GB
```

Figure 59. RCU – expand virtual drive

3. Enter the percentage of the available capacity for the virtual drive to use. For example, if 100 GB of capacity is available, select 30 percent to increase the size of the virtual drive by 30 GB.
4. Press **Resize** to determine the capacity of the virtual drive after expansion. The virtual drive expands by the selected percentage of the available capacity.

5.2.31 RAID migration

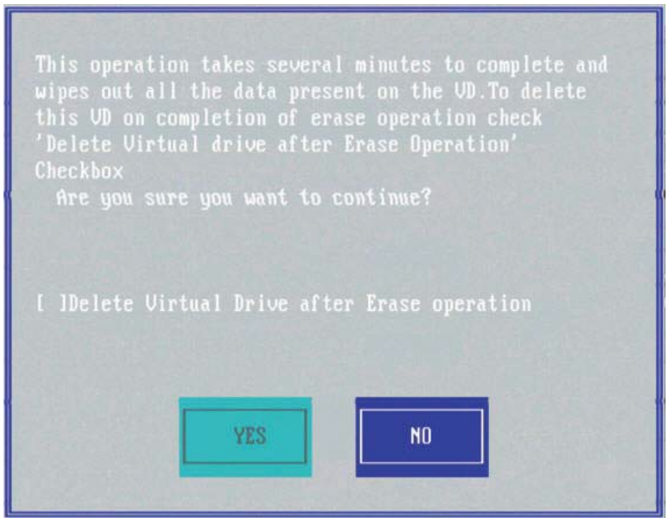
The RCU doesn't have an option to perform RAID migration. In order to achieve this, any Monitoring and Configuration Utility can be used. Refer to the RAID Utilities User Guide.

5.2.32 Erasing a Virtual Drive

Virtual drive erase operates on a specified virtual drive and overwrites all user-accessible locations. It supports nonzero patterns and multiple passes. Virtual drive erase optionally deletes the virtual drive and erases the data within the virtual drive's logical base address range. Virtual drive erase is a background operation that posts events to notify users of their progress.

Perform the following steps to perform the virtual drive erase operation:

1. In the VD Mgmt screen, select a virtual drive and press the **<F2>** key.
2. Navigate to **Erase VD** and press **Enter**. A menu appears displaying the following modes:
   - Simple – Specifies a single-pass erase operation that writes pattern A to the virtual drive.
   - Normal – Specifies a three-pass erase operation that first overwrites the virtual drive content with random values, then overwrites it with pattern A, and then overwrites it with pattern B.
   - Thorough – Specifies a nine-pass erase operation that repeats the Normal erase three times.
   - Stop Erase – Stops the erase operation that has already been started. This option is disabled at first. Once the erase operation begins, this option is enabled.
3. Select a mode and press **<Enter>**. A message box appears (Figure 45).



```
This operation takes several minutes to complete and
wipes out all the data present on the VD.To delete
this VD on completion of erase operation check
'Delete Virtual drive after Erase Operation'
Checkbox
  Are you sure you want to continue?


[ ]Delete Virtual Drive after Erase operation
```

Figure 60. RCU – erase virtual drive

4. To delete the virtual drive after the erase operation has been completed, select the **Delete Virtual Drive after Erase** operation check box.
5. Click **Yes** to start the erase operation. Once the Drive Erase operation has started, the Simple, Normal, and Thorough options are disabled and the Stop Erase option is enabled.

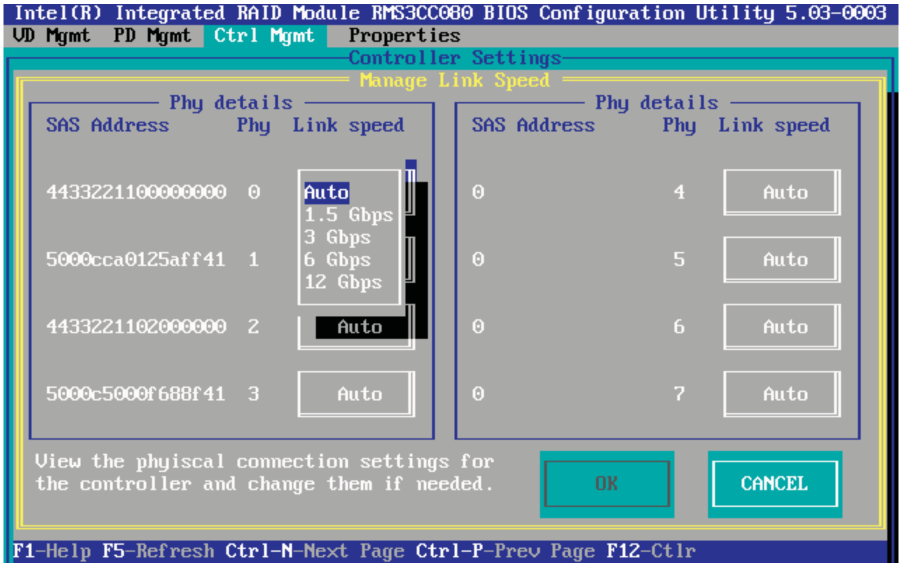
5.2.33 Managing Link Speed

Use the Managing Link Speed feature to change the link speed between the controller and an expander, or between the controller and a drive that is directly connected to the controller.

All phys in a SAS port can have different link speeds or can have the same link speed. However, if phys in a SAS port have different link speed settings and if a phy is connected to a drive or an expander, the firmware overrides the selected link speed setting. Instead, the firmware uses the common maximum link speed among all the phys.

Perform the following steps to change the link speed:

1. In the Ctrl Mgmt screen, press **Next** to navigate to the second Ctrl Mgmt screen.
2. Click **Manage Link Speed**. The Manage Link Speed dialog appears.



```
Intel(R) Integrated RAID Module RMS3CC080 BIOS Configuration Utility 5.03-0003
VD Mgmt  PD Mgmt  Ctrl Mgmt  Properties
                          Controller Settings
                            Manage Link Speed
          Phy details                            Phy details
SAS Address       Phy  Link speed      SAS Address       Phy  Link speed

4433221100000000   0   Auto             0                4    Auto
                       1.5 Gbps
                       3 Gbps
5000cca0125aff41   1   6 Gbps           0                5    Auto
                       12 Gbps

4433221102000000   2   Auto             0                6    Auto


5000c5000f688f41   3   Auto             0                7    Auto

View the phyiscal connection settings for
the controller and change them if needed.
F1-Help F5-Refresh Ctrl-N-Next Page Ctrl-P-Prev Page F12-Ctlr
```

Figure 61. RCU – manage link speed

- o The SAS Address column shows the SAS address that uniquely identifies a device in the SAS domain.
- o The Phy column shows the system-supported phy link values. The phy link values are from 0 through 7.
- o The Link Speed column shows the phy link speeds.

3. Select the desired link speed by using the drop-down list. The link speed values are Auto,1.5Gb/s, 3Gb/s, 6Gb/s, or 12Gb/s.

Note: By default, the link speed in the controller is Auto or the last saved value.

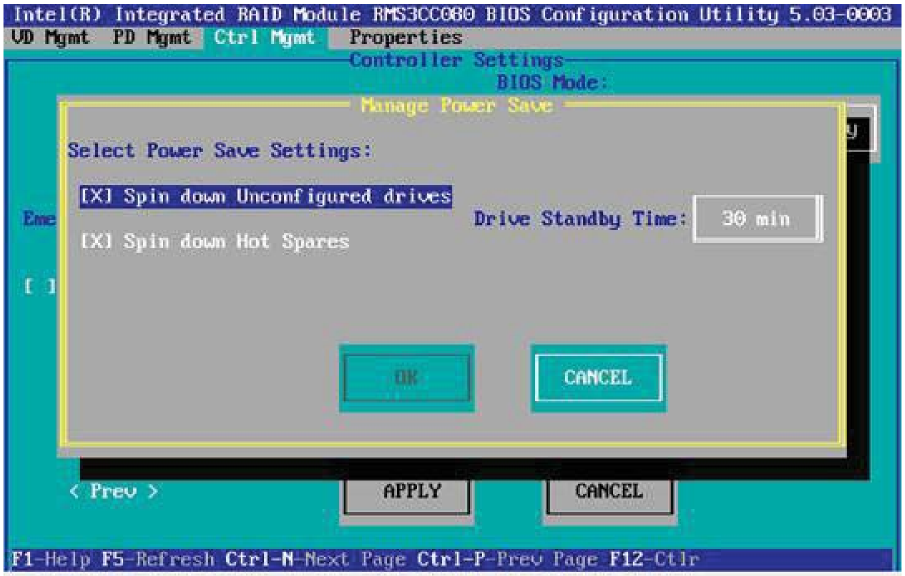
4. Click **OK**. A message box appears asking to restart the system for the changes to take effect.
5. Click **OK**. The link speed value is now reset. The change takes place after restarting the system.

5.2.34 Managing Power Save Settings for the Controller

Change the controller's power-save settings by using the Dimmer Switch enhancement (Power-Save mode).

Perform the following steps to change the power save settings:

1. In the Ctrl Mgmt screen, press **Next** to navigate to the second Ctrl Mgmt screen.
2. Navigate to **Manage Power Save** and press **<Enter>**. The Manage Power Save dialog appears (Figure 47).



Intel(R) Integrated RAID Module RMS3CC080 BIOS Configuration Utility 5.03-0003

Manage Power Save

Select Power Save Settings:

[X] Spin down Unconfigured drives

[X] Spin down Hot Spares

Drive Standby Time: 30 min

Figure 62. RCU – manage power save

3. Select the **Spin down Unconfigured drives** check box to let the controller enable the unconfigured drives to enter the Power-Save mode.
4. Select the **Spin down Hot Spares** check box to let the controller enable the hot spare drives to enter the Power-Save mode.
5. Select the drive standby time from the **Drive Standby Time** drop-down list.

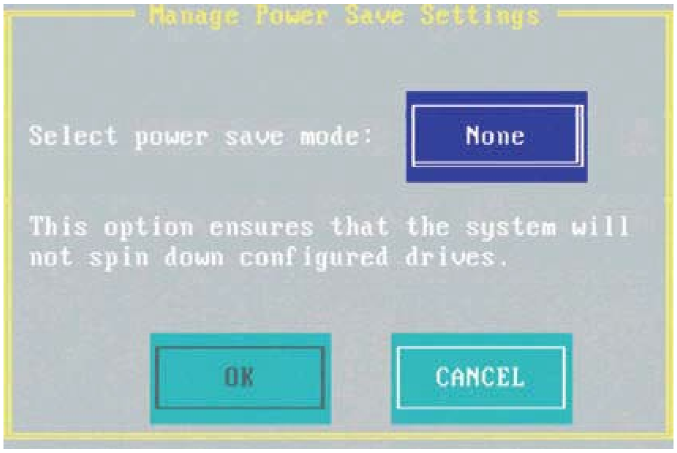
Note: The Drive Standby Time drop-down list is enabled only if any of the preceding check boxes are checked. The drive standby time can be 30 minutes, 1 hour, 90 minutes, or 2 hours through 24 hours.

6. Click **OK**. A message box appears, asking to save the power-save settings.
7. Click **Yes** to save the settings.

5.2.35 Managing Power Save Settings for the Drive Group

Perform the following steps to change the power save settings for a drive group:

1. Navigate to a drive group in the VD Mgmt screen and press the **<F2>** key.
2. Navigate to **Manage Power Save Settings** and press **<Enter>**. The Manage Power Save Settings dialog appears (Figure 63).



Select power save mode: None

This option ensures that the system will not spin down configured drives.

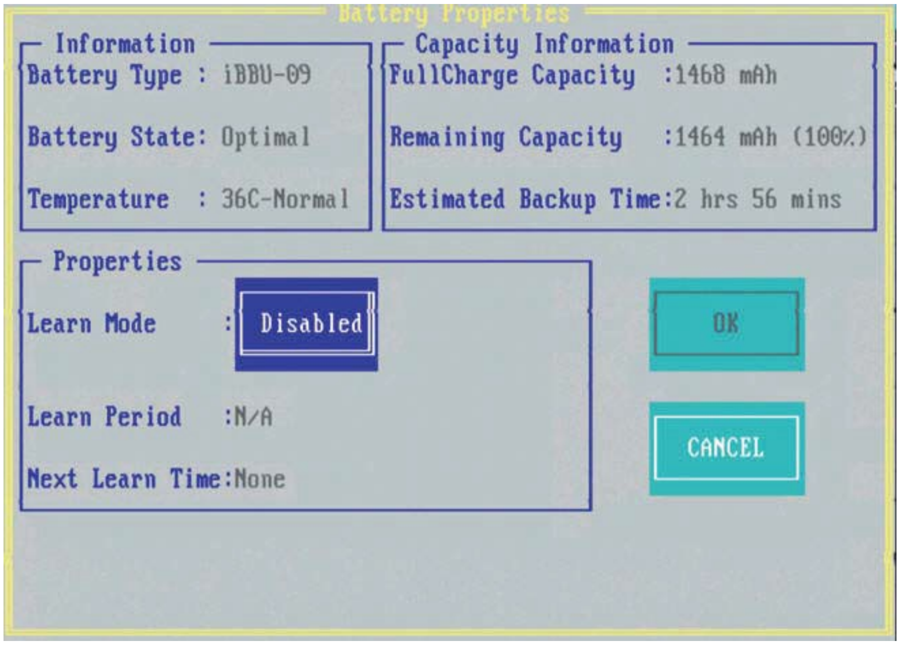
Figure 63. RCU – manage drive group power save settings

3. Select a power save mode from the **Select power save mode** drop-down list. A description of the selected mode appears in the dialog.
4. Click **OK**.

5.2.36 Managing BBU Information

Perform the following steps to view and change the battery settings in a controller with a BBU:

1. Navigate to the second Ctrl Mgmt screen and select **Manage Battery**. The Battery Properties dialog appears (Figure 49). Most of the battery properties are read only.



Information

Battery Type : iBBU-09

Battery State: Optimal

Temperature : 36C-Normal

Capacity Information

FullCharge Capacity :1468 mAh

Remaining Capacity :1464 mAh (100%)

Estimated Backup Time:2 hrs 56 mins

Properties

Learn Mode : Disabled

Learn Period :N/A

Next Learn Time:None

Figure 64. RCU – battery properties window

Note: If the Battery State field has a value other than Optimal, the Non-Optimal Reason field appears at the bottom of the Battery Properties dialog. The Non- Optimal Reason field is a read-only field and states a reason for the non optimal state of the battery.

2. Select a battery learn mode from the **Learn Mode** drop-down list. The values in the drop-down list differ based on whether the battery supports transparent learn cycles. A learning cycle is a battery calibration operation that the controller performs periodically to determine the condition of the battery.

   If the battery supports transparent learn, the following learn modes are available:

   - **G Transparent** – The firmware tracks the time since the last learning cycle and performs a learn cycle when it is due.
   - **G Disabled** – The firmware does not monitor or initiate a learning cycle. Learning cycles can be scheduled manually.
   - **G Unknown** – The firmware warns about a pending learning cycle. You can start a learning cycle manually. After the learning cycle completes, the firmware resets the counter and warns you when the next learning cycle time is reached.

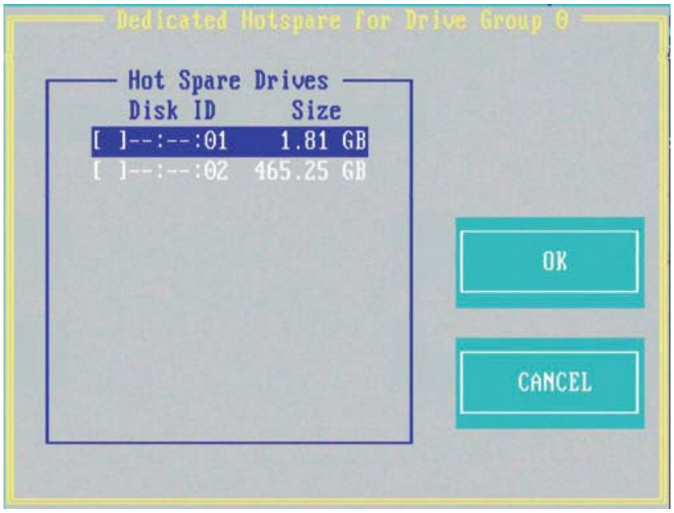
   If the battery does not support transparent learn, the following learn modes are available:

   - **G Automatic** – The firmware tracks the time since the last learning cycle and performs a learn cycle when due. Write caching need not be disabled.
   - **G Disabled** – The firmware does not monitor or initiate a learning cycle. Learning cycles can be scheduled manually.
   - **G Disabled (Warning Only)** – The firmware never initiates a battery learn cycle but notifies through events when a learn cycle is needed.
3. Click **OK** to change the learn mode.

5.2.37 Managing Dedicated Hot Spares

A dedicated hot spare is used to replace failed drives only in a selected drive group that contains the hot spare. Perform the following steps to create or delete dedicated hot spares:

1. Navigate to a drive group in the VD Mgmt screen and press the **<F2>** key.
2. Navigate to **Manage Dedicated Hotspare** and press **<Enter>**. The Dedicated Hotspare dialog appears showing a list of all hot spares that are available to create dedicated hot spares (Figure 50).



Dedicated Hotspare for Drive Group 0

```
Hot Spare Drives
Disk ID        Size
[ ]--:--:01    1.81 GB
[ ]--:--:02  465.25 GB
```

Figure 65. RCU – dedicated hot spare window

3. Perform one of these steps:

- o To create a dedicated hot spare, select a drive and press **OK**.
- o To delete a dedicated hot spare, deselect the hot spare and press **OK**.

5.2.38 Securing a Drive Group

If a drive group is created with FDE drives (security enabled drives) and at the security is set to No at the time of creation, the drive group can be secured later using encryption. Perform the following steps to secure a drive group:

1. From the VD Mgmt screen, navigate to the desired drive group and press the **<F2>** key.
2. Navigate to **Secure Drive Group** and press **<Enter>**. A message box appears asking for your confirmation.
3. Press **Yes** to confirm and secure the drive group.

Note: After a virtual drive is secured, the encryption cannot be removed without deleting the virtual drive.

5.2.39 Locating Physical Drives

The Locate option blinks the LEDs on the physical drives used by a virtual drive.

Perform the following steps to start or stop the locate mode:

1. From the PD Mgmt menu, navigate to the **Drive Management** screen.
2. Select a physical drive, and press the **<F2>** key.
3. Navigate to **Locate** and press **<Enter>**.
4. Perform one of these actions:
   - o Select **Start** and press **<Enter>** to start LED blinking in the locate mode.
   - o Select **Stop** and press **<Enter>** to stop LED blinking in the locate mode.

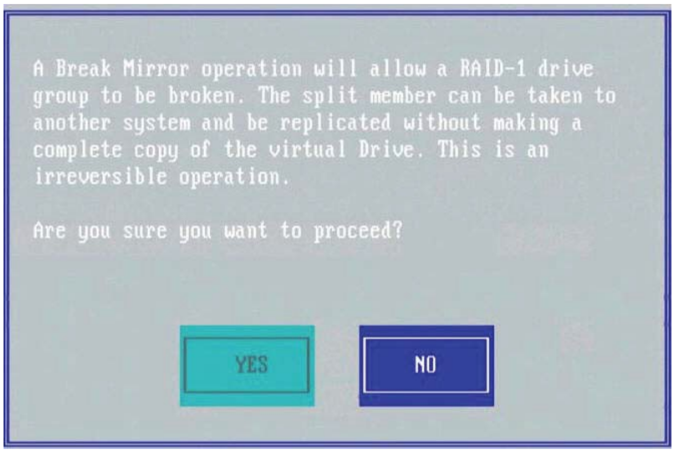
Note: Starting and stopping the locate mode only work if the drive is installed in a drive enclosure.

5.2.40 Performing a Break Mirror Operation

The Break Mirror operation enables a RAID 1 configured drive group to be broken into two volumes. One of the volumes can be used in another system and replicated without making a copy of the virtual drive.

Perform the following steps to perform a break mirror operation:

1. From the VD Mgmt screen, navigate to the desired drive group and press the **<F2>** key.
2. Navigate to **Break Mirror** and press **<Enter>**. The following confirmation message box appears.



A Break Mirror operation will allow a RAID-1 drive group to be broken. The split member can be taken to another system and be replicated without making a complete copy of the virtual Drive. This is an irreversible operation.

Are you sure you want to proceed?

Figure 66. RCU – break mirror message dialog

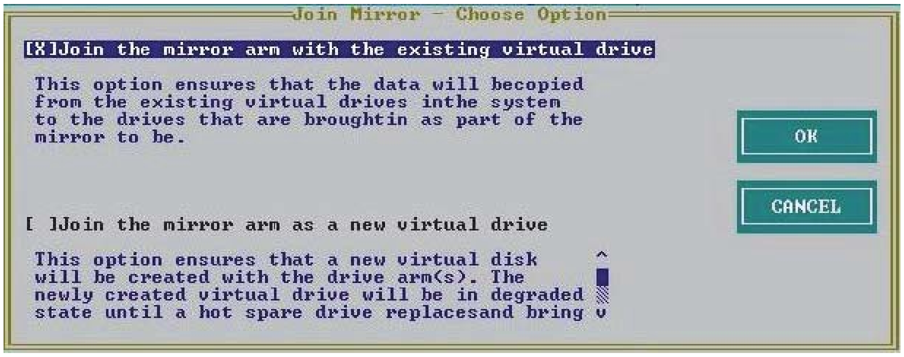
3. Click **Yes** to proceed.

5.2.41 Performing a Join Mirror Operation

Perform a join mirror operation on a drive group to continue using the modified virtual drive or to reuse the original virtual drive.

Perform the following steps to perform a join mirror operation:

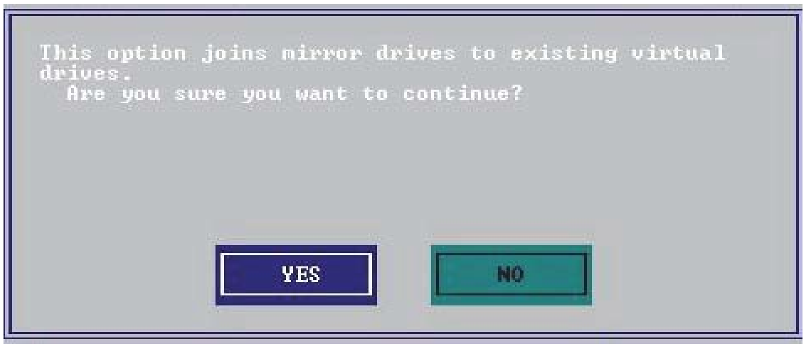
1. From the VD Mgmt screen, navigate to the desired drive group and press the **<F2>** key.
2. Navigate to **Join Mirror** and press **<Enter>**. The following dialog appears.



```
Join Mirror - Choose Option

[X]Join the mirror arm with the existing virtual drive

 This option ensures that the data will becopied
 from the existing virtual drives inthe system
 to the drives that are broughtin as part of the
 mirror to be.


[ ]Join the mirror arm as a new virtual drive

 This option ensures that a new virtual disk
 will be created with the drive arm(s). The
 newly created virtual drive will be in degraded
 state until a hot spare drive replacesand bring
```

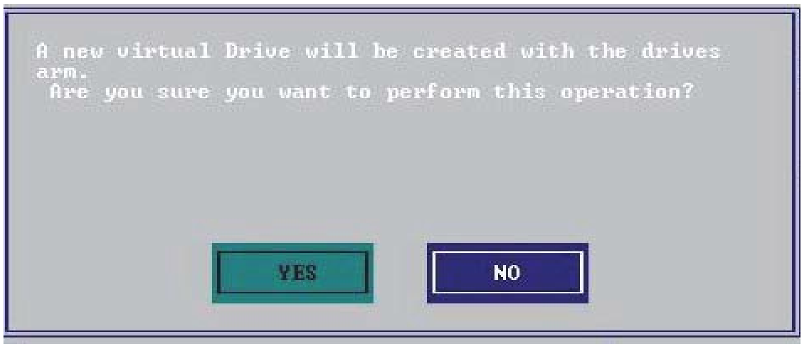
Figure 67. RCU – choose join mirror option

3. Select to either join the mirror arm with the existing virtual drive or join the mirror arm as a new virtual drive and press **OK**. A confirmation dialog appears (Figure 68 or Figure 69).



```
This option joins mirror drives to existing virtual
drives.
  Are you sure you want to continue?
```

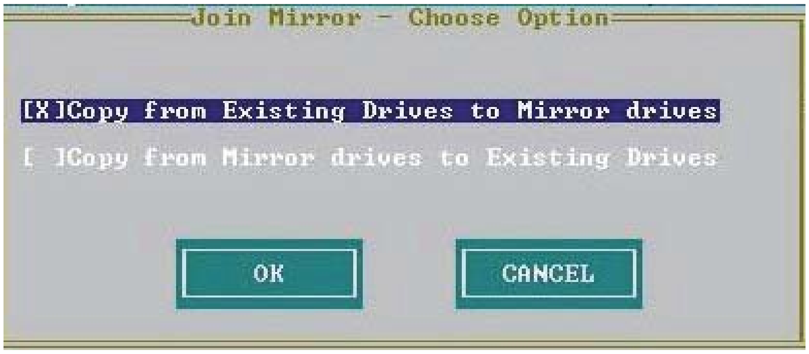
Figure 68. RCU – join mirror arm with existing virtual drive confirmation dialog



```
A new virtual Drive will be created with the drives
arm.
 Are you sure you want to perform this operation?
```

Figure 69. RCU – join mirror arm as new virtual drive confirmation dialog

4. Click **Yes** to proceed. The following dialog appears.



Join Mirror - Choose Option

[X]Copy from Existing Drives to Mirror drives

[ ]Copy from Mirror drives to Existing Drives

Figure 70. RCU – choose join mirror copy option

5. Select one of the options and press **OK**.

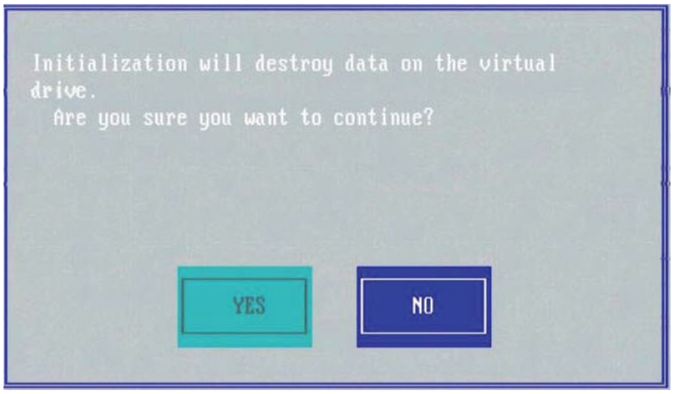
5.2.42 Managing Storage Configurations

This section describes how to use the RCU Utility to maintain and manage storage configurations.

5.2.42.1 Initializing a Virtual Drive

If a virtual drive is not initialized after creation, it can be initialized later. Perform the following steps to initialize a virtual drive:

1. From the VD Mgmt screen, navigate to a virtual drive and press the **<F2>** key.
2. Select **Initialization** and press **<Enter>**. The two initialization options, Fast Init and Slow Init, appear.
3. Select either **Fast Init** or **Slow Init** and and press **<Enter>**. A confirmation dialog appears (Figure 71).



Initialization will destroy data on the virtual drive.
Are you sure you want to continue?

Figure 71. RCU – initialize a virtual drive

4. Press **Yes** to begin initialization.

Caution: Initialization erases all data on the virtual drive. Make sure to back up data before you initializing a virtual drive. Make sure the operating system is not installed on the virtual drive being initialized.

5.2.42.2 Running a Consistency Check

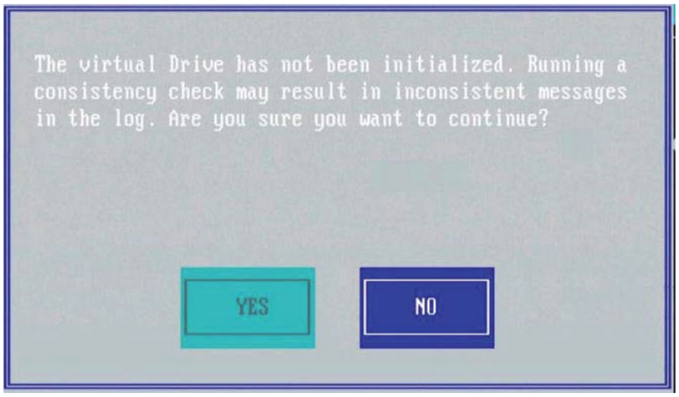
A consistency check should periodically be run on fault-tolerant virtual drives (RAID 1, 5, 6, 10, 50, or 60 configurations; RAID 0 does not provide data redundancy). A consistency check scans the virtual drive to determine whether the data has become corrupted and needs to be restored.

For example, in a system with parity, checking consistency means computing the data on one drive and comparing the results with the contents of the parity drive. A consistency check must be run if it is suspected that the data on the virtual drive might be corrupted.

Caution: Make sure to back up the data before running a consistency check, if the data might be corrupted.

Perform the following steps to run a consistency check:

1. Navigate to a virtual drive in the VD Mgmt screen and press the **<F2>** key.
2. Navigate to **Consistency Check** and press **<Enter>**.
3. Navigate to **Start** and press **<Enter>**. The consistency check starts and checks the redundant data in the virtual drive.
4. If a consistency check is attempted on a virtual drive that has not been initialized, a confirmation dialog appears asking for confirmation. Press **Yes** to run the consistency check.



The virtual Drive has not been initialized. Running a consistency check may result in inconsistent messages in the log. Are you sure you want to continue?

Figure 72. Consistency check

5.2.42.3 Rebuilding a Physical Drive

If a drive in a redundant virtual drive (RAID 1, 5, 6, 10, 50, or 60) fails, that drive must be rebuilt on a hot spare drive to prevent data loss. Perform the following steps to rebuild a physical drive:

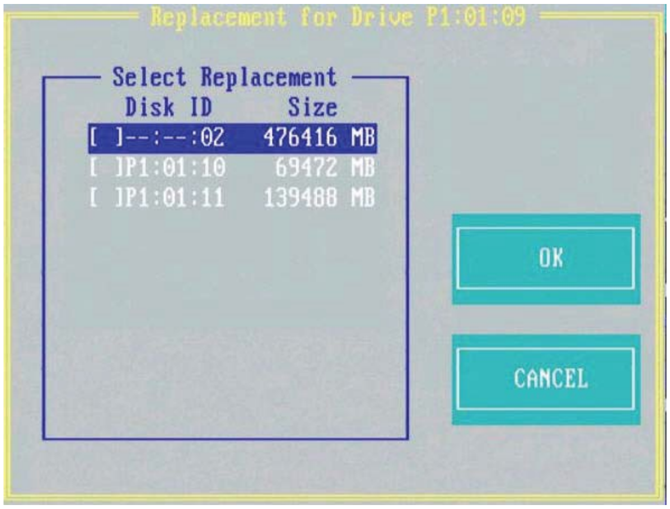
1. From the PD Mgmt screen, navigate to the **Drive Management** screen and press the **<F2>** key.
2. Select **Rebuild** and press **<Enter>**. The rebuild operation starts.

5.2.42.4 Performing a Copyback Operation

The Copyback operation copies data from a source drive of a virtual drive to a destination drive that is not a part of the virtual drive. The copyback operation often creates or restores a specific physical configuration for a drive group (for example, a specific arrangement of drive group members on the device I/O buses).

Perform the following steps to perform the Copyback operation:

1. From the PD Mgmt screen, navigate to the Drive Management screen, select a physical drive, and press the **<F2>** key.
2. Navigate to **Copyback** and press <Enter>. The following dialog appears.



```
Replacement for Drive P1:01:09

Select Replacement
Disk ID         Size
[ ]--:--:02     476416 MB
[ ]P1:01:10      69472 MB
[ ]P1:01:11     139488 MB
```

Figure 73. RCU – Copyback operation

3. Select the desired replacement drive.
4. Press **OK**. The copyback operation is performed on the selected drive.

5.2.42.5 Removing a Physical Drive

A non-failed drive connected to the controller may sometimes need to be removed. Preparing a physical drive for removal spins the drive into a power save mode. Perform the following steps to prepare a physical drive for removal:

1. From the PD Mgmt screen, navigate to the Drive Management screen and press the **<F2>** key.
2. Select **Prepare for Removal** and press **<Enter>**. The physical drive is now in a power save mode.

To reverse the process, navigate to **Undo Removal** and press **<Enter>**.

5.2.43 Creating Global Hot Spares

A global hot spare is used to replace a failed physical drive in any redundant array, as long as the capacity of the global hot spare is equal to or larger than the coerced capacity of the failed physical drive.

The hot spare can be designated to have enclosure affinity. In an enclosure affinity, if drive failures are present on a split backplane configuration, the hot spare first is used on the backplane in which it resides.

Perform the following steps to create global hot spares:

1. Navigate to the Drive Management screen, navigate to a physical drive to change to a hot spare, and press the **<F2>** key.
2. Select **Make Global HS** and press **<Enter>**. The physical drive is changed to a global hot spare. The status of the physical drive as a global hot spare appears in the Drive Management screen.

5.2.44 Removing a Hot Spare Drive

Perform these steps to remove a hot spare drive:

1. Navigate to the Drive Management screen, navigate to a hot spare drive to remove, and press the **<F2>** key.
2. Select **Remove Hot Spare Drive** and press **<Enter>**. The hot spare drive is removed.

5.2.45 Making a Drive Offline

If a drive is part of a redundant configuration, it can be removed and changed to an unconfigured good drive to be used in another configuration.

Caution: After performing this procedure, the virtual drive may become partially degraded, degraded or failed.

1. Navigate to the Drive Management screen, select a physical drive, and press the **<F2>** key.
2. Navigate to **Place Drive Offline** and press **<Enter>**. The drive status changes to **Unconfigured Good**.

5.2.46 Making a Drive Online

In an online state, the physical drive works normally and is a part of a configured virtual drive. Perform the following steps to make a physical drive online:

1. Navigate to the Drive Management screen, select a physical drive, and press the **<F2>** key.
2. Navigate to **Place Drive Online** and press **<Enter>**. The state of the physical drive changes to **Online**.

5.2.47 Instant Secure Erase

Perform the following steps to erase data on self-encrypting drives (SEDs):

1. Navigate to the Drive Management screen, select a physical drive, and press the **<F2>** key.
2. Navigate to **Instant Secure Erase** and press **<Enter>**.
3. Press **Yes** to confirm and proceed.

5.2.48 Erasing a Physical Drive

You can securely erase data on Non SEDs (normal HDDs) by using the Drive Erase option in the PD Mgmt menu.

For non-SEDs (normal HDDs), the erase operation consists of a series of write operations to a drive that overwrites every user-accessible sector of the drive with specified patterns. It can be repeated in multiple passes using different data patterns for enhanced security. The erase operation is performed as a background task.

Perform the following steps to erase data on non-SEDs:

1. Navigate to the Drive Management screen, select a physical drive, and press the **<F2>** key.
2. Navigate to **Drive Erase** and press **<Enter>**. A menu appears displaying the following modes:
    - Simple – Specifies a single-pass operation that writes pattern A to the physical drive.
    - Normal – Specifies a three-pass erase operation that first overwrites the physical drive content with random values, then overwrites it with pattern A, and then overwrites it with pattern B.
    - Thorough – Specifies a nine-pass erase operation that repeats Normal erase three times.
    - Stop Erase – This option is disabled until the erase operation begins.
3. Select a mode and press **<Enter>**.
4. Press **Yes** to confirm and proceed with the drive erase operation.

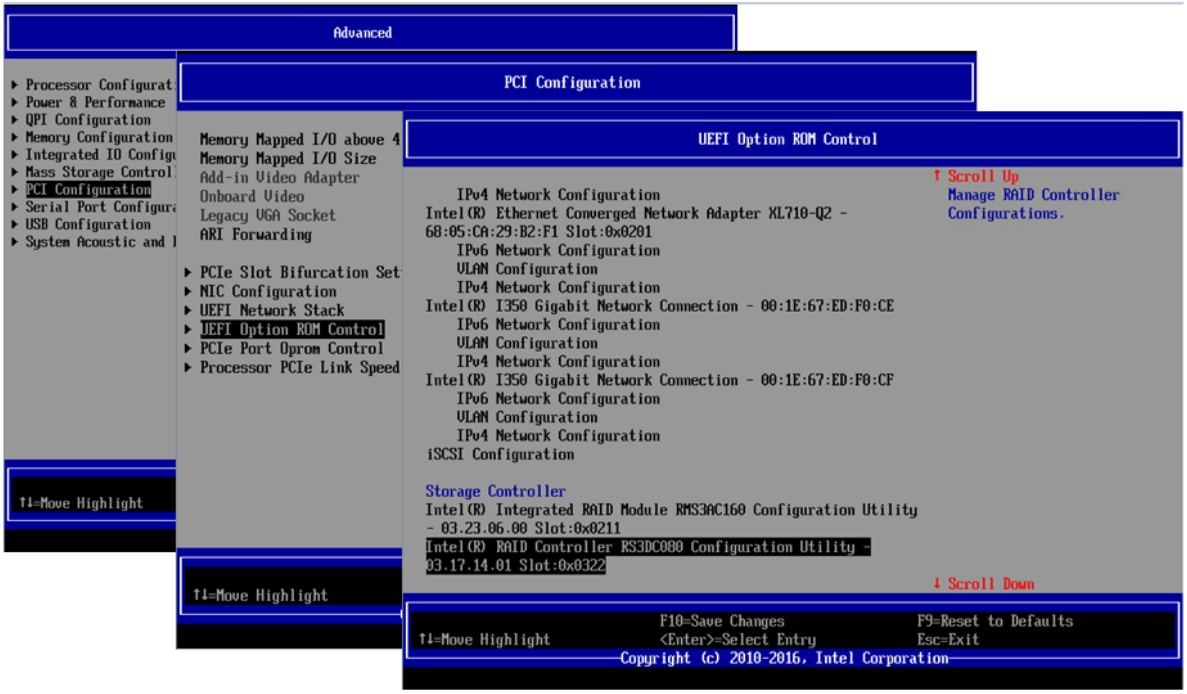
Once the Drive Erase operation has started, the progress of the operation is displayed and the Stop Erase option is enabled.

5.3 Human Interface Infrastructure (HII) Configuration Utility

The HII CU is the built-in configuration utility used in all the Intel® RAID Controllers based on the MR or iMR software stack when the system they are installed on is configured for UEFI boot mode. In UEFI boot mode, neither the Intel® RAID BIOS Console 2 CU (<Ctrl><G>) nor the Integrated RAID M BIOS CU (<Ctrl><R>) are available, so the HII CU is the only option in a pre-boot environment. There are RAID controllers like the Intel® Tri-Mode RAID controllers which don't have a Legacy mode CU and the HII CU is the only pre-boot option (although it is possible to configure them using the post-boot RAID configuration utilities).

In order to invoke the HII utility, the system must be configured for UEFI boot mode: At boot time, enter the BIOS setup by pressing F2, select the Setup Menu, then Boot Maintenance Manager, then Advanced Boot Options. In Boot Mode select "UEFI", then you can save and exit pressing F10 and confirming with "Y". Once the system is configured for UEFI not mode, enter again the BIOS Setup by pressing F2 at boot time. Select the Setup Menu, then Advanced, then PCI Configuration, then UEFI Option ROM Control. Then select the desired RAID controller to be managed (Figure 74. HII - Select RAID Controller)

The HII Configuration Utility supports the hot plug feature: you can add and remove devices to a computer while the computer is running and the utility recognizes the change.

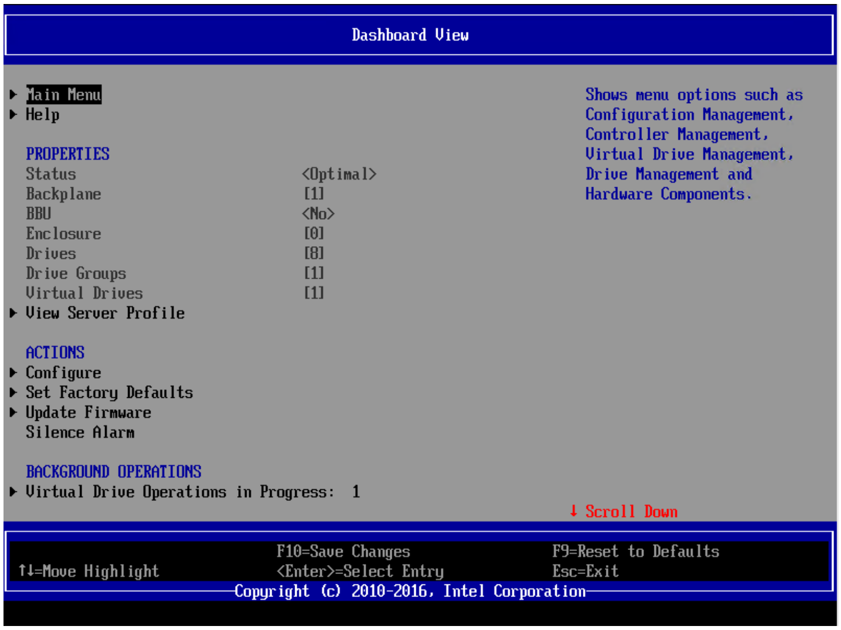


```
Advanced
▶ Processor Configurat
▶ Power & Performance
▶ QPI Configuration
▶ Memory Configuration
▶ Integrated IO Config
▶ Mass Storage Control
▶ PCI Configuration
▶ Serial Port Configur
▶ USB Configuration
▶ System Acoustic and I
↑↓=Move Highlight

PCI Configuration
Memory Mapped I/O above 4
Memory Mapped I/O Size
Add-in Video Adapter
Onboard Video
Legacy VGA Socket
ARI Forwarding

▶ PCIe Slot Bifurcation Set
▶ NIC Configuration
▶ UEFI Network Stack
▶ UEFI Option ROM Control
▶ PCIe Port Oprom Control
▶ Processor PCIe Link Speed
↑↓=Move Highlight

UEFI Option ROM Control
                                                          ↑ Scroll Up
    IPv4 Network Configuration                              Manage RAID Controller
Intel(R) Ethernet Converged Network Adapter XL710-Q2 -      Configurations.
68:05:CA:29:B2:F1 Slot:0x0201
    IPv6 Network Configuration
    VLAN Configuration
    IPv4 Network Configuration
Intel(R) I350 Gigabit Network Connection - 00:1E:67:ED:F0:CE
    IPv6 Network Configuration
    VLAN Configuration
    IPv4 Network Configuration
Intel(R) I350 Gigabit Network Connection - 00:1E:67:ED:F0:CF
    IPv6 Network Configuration
    VLAN Configuration
    IPv4 Network Configuration
iSCSI Configuration

Storage Controller
Intel(R) Integrated RAID Module RMS3AC160 Configuration Utility
- 03.23.06.00 Slot:0x0211
Intel(R) RAID Controller RS3DC080 Configuration Utility -
03.17.14.01 Slot:0x0322
                                                          ↓ Scroll Down
                           F10=Save Changes              F9=Reset to Defaults
↑↓=Move Highlight          <Enter>=Select Entry          Esc=Exit
                 Copyright (c) 2010-2016, Intel Corporation
```

Figure 74. HII CU - Select RAID Controller

5.3.1 Dashboard view

The first screen after entering the HII CU is the Dashboard View, here you can see an overview of the controller, BBU, enclosures, drives, drive groups and virtual drives. Here you can also view the main menu, the most common actions, the background operations and Advanced Software options.

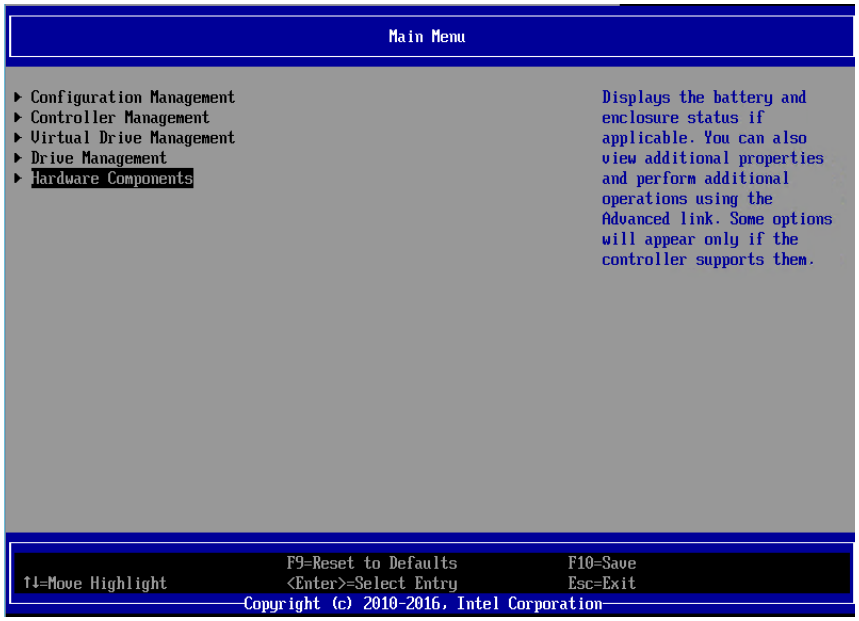


```
                              Dashboard View

▶ Main Menu                                         Shows menu options such as
▶ Help                                              Configuration Management,
                                                    Controller Management,
  PROPERTIES                                        Virtual Drive Management,
  Status                        <Optimal>           Drive Management and
  Backplane                     [1]                 Hardware Components.
  BBU                           <No>
  Enclosure                     [0]
  Drives                        [8]
  Drive Groups                  [1]
  Virtual Drives                [1]
▶ View Server Profile

  ACTIONS
▶ Configure
▶ Set Factory Defaults
▶ Update Firmware
  Silence Alarm

  BACKGROUND OPERATIONS
▶ Virtual Drive Operations in Progress:  1
                                                   ↓ Scroll Down

                    F10=Save Changes          F9=Reset to Defaults
↑↓=Move Highlight   <Enter>=Select Entry      Esc=Exit
              Copyright (c) 2010-2016, Intel Corporation
```

Figure 75. HII CU – Dashboard View

5.3.2 Main Menu

The Main Menu is the section where we can choose to create and delete RAID configurations (Configuration management), view and set the controller's properties (Controller Management), view and change properties of virtual drives (Virtual drive management), view the properties of the different drives installed (Drive management), configure and assign SSD cache volumes (when the SSD cache key is installed) and view the properties of the different hardware components like enclosures, temperature sensors, fans and power supplies (Hardware Components).

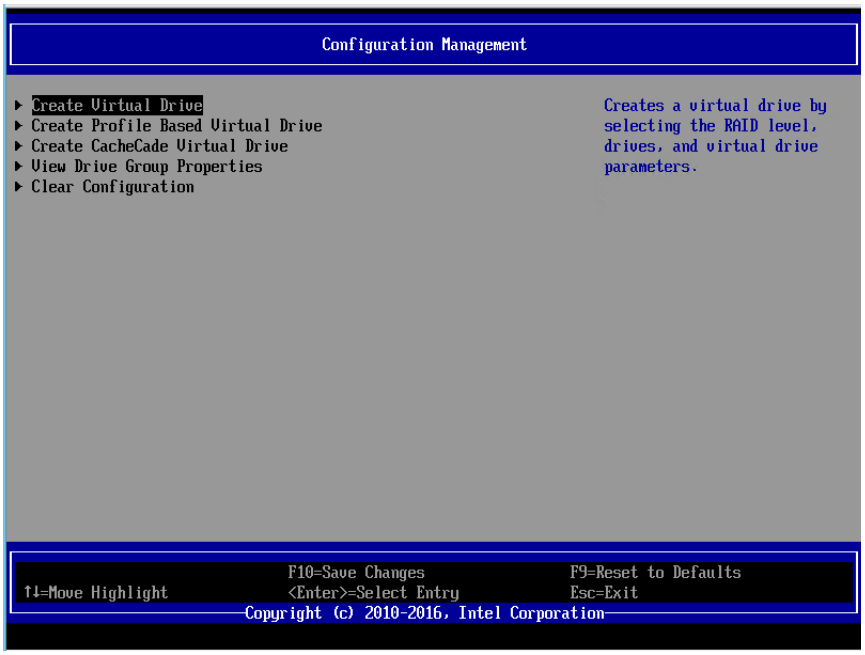


```
                                 Main Menu

▶ Configuration Management                          Displays the battery and
▶ Controller Management                             enclosure status if
▶ Virtual Drive Management                          applicable. You can also
▶ Drive Management                                  view additional properties
▶ Hardware Components                               and perform additional
                                                    operations using the
                                                    Advanced link. Some options
                                                    will appear only if the
                                                    controller supports them.

                    F9=Reset to Defaults        F10=Save
↑↓=Move Highlight   <Enter>=Select Entry        Esc=Exit
              Copyright (c) 2010-2016, Intel Corporation
```

Figure 76. HII CU – Main Menu

5.3.2.1 Configuration Management

In this section we can create and delete virtual drives. If the SSD cache key is installed, we can also create and assign SSD cache volumes. We can also view drive group properties and clear the RAID configuration.



Configuration Management

```
▸ Create Virtual Drive                                    Creates a virtual drive by
▸ Create Profile Based Virtual Drive                      selecting the RAID level,
▸ Create CacheCade Virtual Drive                          drives, and virtual drive
▸ View Drive Group Properties                             parameters.
▸ Clear Configuration
```

```
                          F10=Save Changes             F9=Reset to Defaults
↑↓=Move Highlight         <Enter>=Select Entry         Esc=Exit
              Copyright (c) 2010-2016, Intel Corporation
```

5.3.2.1.1 Creating Virtual Drives

This section provides detailed instructions to configure drive groups and virtual drives with the HII Configuration Utility.

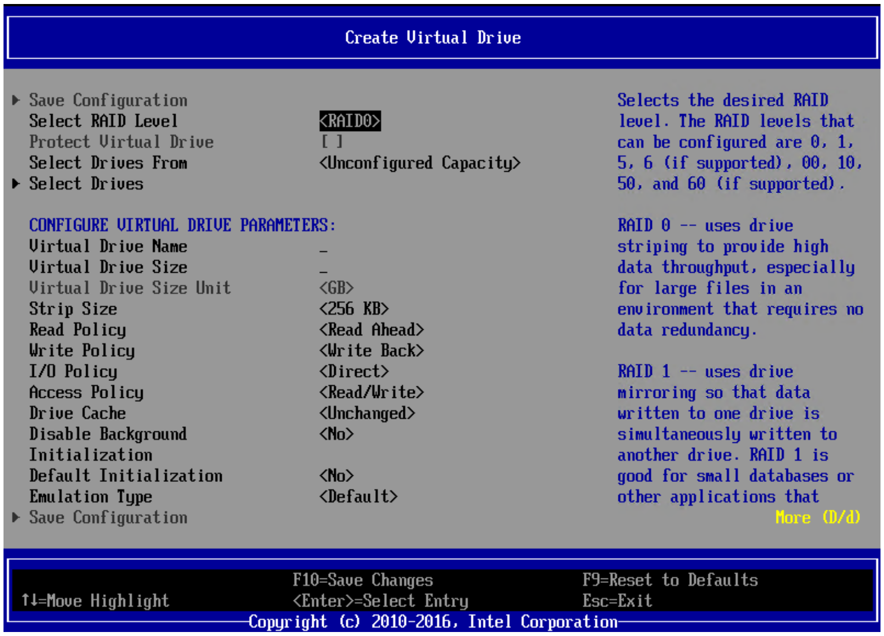
Use drives with the same capacity when you create a storage configuration. If you use drives with different capacities in the same drive group, the CU limits each drive to the capacity of the smallest drive.

The number of physical drives in a specific array determines the possible RAID levels that you can implement with the array.

- RAID 0 requires from one to eight physical drives.
- RAID 1 requires two physical drives.
- RAID 5 requires at least three physical drives.
- RAID 6 requires at least four physical drives.
- RAID 10 requires four, six, eight... or more physical drives (a pair number of disks).
- RAID 50 requires at least six physical drives.
- RAID 60 requires at least eight physical drives.

Follow these steps to access the **Virtual Drive Management** screen and create a virtual drive configuration.

1. Highlight **Create Virtual drive option** on the **Configuration Management** screen and press <Enter>.
   The **Create Virtual drive** screen appears, as shown in the following figure.



```
                              Create Virtual Drive

▶ Save Configuration                                       Selects the desired RAID
  Select RAID Level              <RAID0>                   level. The RAID levels that
  Protect Virtual Drive          [ ]                       can be configured are 0, 1,
  Select Drives From             <Unconfigured Capacity>   5, 6 (if supported), 00, 10,
▶ Select Drives                                            50, and 60 (if supported).

  CONFIGURE VIRTUAL DRIVE PARAMETERS:                      RAID 0 -- uses drive
  Virtual Drive Name             _                         striping to provide high
  Virtual Drive Size             _                         data throughput, especially
  Virtual Drive Size Unit        <GB>                      for large files in an
  Strip Size                     <256 KB>                  environment that requires no
  Read Policy                    <Read Ahead>              data redundancy.
  Write Policy                   <Write Back>
  I/O Policy                     <Direct>                  RAID 1 -- uses drive
  Access Policy                  <Read/Write>              mirroring so that data
  Drive Cache                    <Unchanged>               written to one drive is
  Disable Background             <No>                      simultaneously written to
  Initialization                                           another drive. RAID 1 is
  Default Initialization         <No>                      good for small databases or
  Emulation Type                 <Default>                 other applications that
▶ Save Configuration                                                         More (D/d)

                             F10=Save Changes              F9=Reset to Defaults
 ↑↓=Move Highlight           <Enter>=Select Entry          Esc=Exit
                    Copyright (c) 2010-2016, Intel Corporation
```

Figure 77. HII CU – Create Virtual Drive Screen

2. Select the RAID level from the drop down menu
3. Use the arrow keys to select any highlighted fields (one at a time) that you want to change the setting for and press <Enter>.
4. Select the setting for each property that you want to change from the default. Explanation for each property is on table 1.

You can change the settings for the following fields on this screen.

Table 20. Virtual Drive Management Property Settings

Property	Description
Select RAID Level	The possible RAID levels for the virtual drive. See Section 1.2, RAID Overview, on page 4, for more information about the RAID levels.
Select Drives From	The sources that you can use to select drives for the virtual drive. The options are **Unconfigured Capacity and Free Capacity**. By selecting Unconfigured Capacity the controller will show the Unconfigured good drives. By selecting Free Capacity the controller will show the unused or free capacity of the drives that are already part of a virtual drive if available.
Select Drives	Select this button and a screen appears that lists Unconfigured Good drives or free capacity, which depend on the value you selected in the **Select Drive From** field.
Virtual Drive Name	Enter the name of the virtual drive.
Virtual Drive Size	Enter the capacity of the virtual drive. Normally, this value is the full capacity of the drive. You can specify a smaller capacity if you want to create other virtual drives on the same drive group.
Virtual Drive Size Unit	Enter the unit of capacity you want to use for the virtual drive. The options are **MB**, **GB**, and **TB**.
Stripe Size	A stripe consists of the data segments that the RAID controller writes across multiple drives, not including parity drives. The default is **256 KB**. Possible values are 64KB, 128 KB, 256 KB, 512 KB and 1MB.
Read Ahead	When disk Read Ahead is **On**, extra data is read sequentially ahead of the data that is actually requested, and this extra data is stored in cache memory. If the additional read-ahead data is then requested, it can be read faster from the cache than from the disk directly.

Property	Description
Write Policy	This setting speeds up reads for sequential data, but there is little improvement when accessing random data. You can disable the Disk Write Cache option when you create a virtual drive, but you can enable this option later using the configuration utilities. When the Disk Write Cache is On, a write transaction is considered to be complete when all the data has been written to the disk cache. When Disk Write Cache is Off, the write transaction is complete only when the data has been written to the disk. Write Through – No write cache is enabled Write Back – Write cache is enabled but it depends on the state of the backup unit. When the controller detects that the BU unit is not fully charged or it's faulty, it automatically switches to Write Through. Always Write Back – Write cache is enabled no matter the state of the BU unit.
I/O Policy	
Access Policy	The access policy for the virtual drive. The options are Read/Write, Read Only and blocked.
Drive Cache	Some physical drives have their own cache memory, this setting is for enabling or disabling the drive's cache memory. Special care needs to be taken because the RMFBU unit does not protect this memory in the event of a power failure.
Disable Background Initialization	By disabling Background Initialization, the VD initialization will run in the foreground and no other activities will be allowed while it's running.
Default Initialization	Possible values are No, Fast and Full.

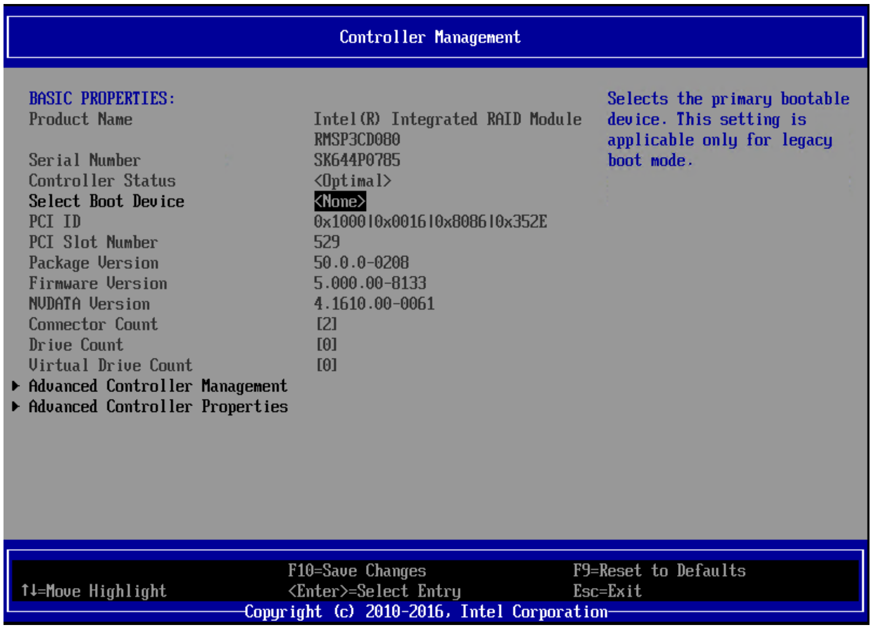
5.3.3 Controller Management

Some of the information on this screen is read-only. This screen presents basic information, such as the serial number, PCI ID, PCI slot number, details on the firmware package installed, connector count, drive count, etc. Here we can also set the boot device.

Entering the **Advanced Controller Management** it is possible to clear the controller events, manage link speed, schedule consistency check and set factory defaults.

Entering the **Advanced Controller Properties** it is possible to view the amount of the controller's memory and cache, manually start, suspend, resume and stop the patrol read operation, view and change the power save settings, view and change hot spare drive properties and view and change the controller's task rates.

The **Controller Management** screen appears, as shown in the following figure.



```
                              Controller Management

  BASIC PROPERTIES:                                            Selects the primary bootable
  Product Name                    Intel(R) Integrated RAID Module  device. This setting is
                                  RMSP3CD080                   applicable only for legacy
  Serial Number                   SK644P0785                   boot mode.
  Controller Status               <Optimal>
  Select Boot Device              <None>
  PCI ID                          0x1000|0x0016|0x8086|0x352E
  PCI Slot Number                 529
  Package Version                 50.0.0-0208
  Firmware Version                5.000.00-8133
  NVDATA Version                  4.1610.00-0061
  Connector Count                 [2]
  Drive Count                     [0]
  Virtual Drive Count             [0]
▶ Advanced Controller Management
▶ Advanced Controller Properties

                              F10=Save Changes             F9=Reset to Defaults
 ↑↓=Move Highlight            <Enter>=Select Entry         Esc=Exit
                      Copyright (c) 2010-2016, Intel Corporation
```

Figure 78. HII CU - Controller Management Screen

The following tables defines the basic and advanced controller properties. Note that different controllers may have different properties and not all of them necessarily are present on a particular controller.

Table 21. Basic Controller Properties

Property	Description
Product Name	The name of the controller
Serial Number	The controller's serial number
Controller Status	The current status of the controller (normally it should be optimal)
Select Boot Device	Selects the virtual drive to use as the boot device.
PCI ID	The ID number for the Peripheral Component Interconnect (PCI) local bus.
Host Interface	The type of interface used by the computer host system, such as PCI Express* (PCIe*).

Device Port Count	The maximum number of ports supported by the software RAID controller in which devices (such as CD-ROM and disks) can be connected.
PCI Slot Number	The number of the PCI slot in which the selected controller is installed.
Connector Count	The number of SFF-8643 connectors on the controller
Drive Count	The number of drives connected to the selected controller.
Virtual Drive Count	The number of virtual drives configured on the controller currently.
Encryption Capable	Indicates whether the controller offers the ability to encrypt data on the drives. This solution provides data protection in the event of theft or loss of physical drives.
Minimum Stripe Size	The minimum length of the data segments that the controller writes across multiple drives, not including the parity drives. The default minimum stripe size is 64 KB.
Maximum Stripe Size	The maximum length of the data segments that the controller writes across multiple drives, not including the parity drives. The default maximum stripe size is 64 KB.
Driver Version	The driver version of the EFI driver.
UEFI Driver Timestamp	The UEFI driver compilation time stamp.

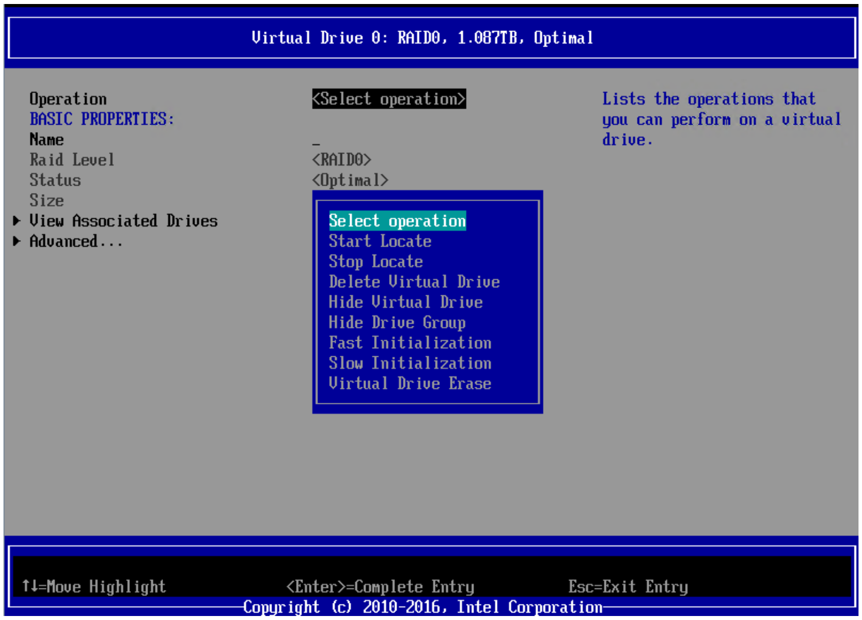
Table 22. Advanced Controller Properties

Property	Description
Profile Management	Some controllers have different profiles that define their behavior. This property is for future release.
Cache Flush Interval	The amount of seconds at which the contents of the controller's cache is flushed.
Patrol Read	Process that checks for physical disk errors that could lead to drive failure. This process starts only when the RAID controller is idle for a defined period of time and no other background tasks are active, although a patrol read check can continue to run during heavy I/O processes.
Patrol Read Mode	Defines if the Patrol read process is Automatic, Manual or Disabled.
Patrol Read Rate	Defines the percentage of system resources dedicated to perform a Patrol Read Process. The default is 30 which means that 30% of the resources will be dedicated to Patrol Read while 70% will be dedicated to I/O operations.
Patrol Read Setting for unconfigured space.	Defines whether or not the unconfigured space will be checked by Patrol Read.
Spin Down Unconfigured Good	Defines whether or not the Unconfigured Good drives will be put in power save mode (spun down).
Spin Down Hot Spare Drives	Defines whether or not the Hot Spare Drives will be put in power save mode (spun down).
Drive Standby Time	Defines the time needed to go by before the drives are spun down for power save.
Spinup Drive Count	The number of simultaneous drives that can be spun up at a time.
Spinup Delay	The delay in seconds between two successive drive spin up operations.
Set Factory Defaults	Resets factory default values for all of the controller properties.

Property	Description
Set Boot Devices	Selects the virtual drive to use as the boot device.
Rebuild Rate	The percentage of central processing unit (CPU) resources devoted to rebuilding data onto a new drive after a drive in a storage configuration has failed. The default value is 30 percent.
Background Initialization (BGI) Rate	Background initialization is a check for media errors on the drives when you create a virtual drive. It is an automatic operation that starts five minutes after you create the virtual drive. This check ensures that striped data segments are the same on all of the drives in the drive group. The default value is 30 percent.
Consistency Check Rate	A consistency check is an operation that verifies that all stripes in a virtual drive with a redundant RAID level are consistent and that it automatically fixes any errors. The consistency check rate is the rate at which consistency check operations are run on a computer system. The default value is 30 percent.
Disk Coercion	Drive coercion is a tool for forcing drives of varying capacities to the same capacity so they can be used in a drive group. The coercion mode options are None, 128MB- way, and 1GB-way. The number you choose depends on how much the drives from various vendors vary in their actual size.
Disk WC	You can disable the Disk Write Cache option when you create a virtual drive, but you can enable this option later using the configuration utilities. • When the Disk Write Cache is **On**, a write transaction is considered complete when all the data has been written to the disk cache. • When Disk Write Cache is **Off**, the write transaction is complete only when the data has been written to the disk.
Read Ahead	When Disk Read Ahead is **On**, extra data is read sequentially ahead of the data that is actually requested, and this extra data is stored in cache memory. If the additional read-ahead data is then requested, it can be read faster from the cache than from the disk directly. This setting speeds up read operations for sequential data, but there is little improvement when accessing random data.
Auto Rebuild	Auto-rebuild allows a failed drive to be replaced and the data automatically rebuilt by *hot-swapping* the drive in the same drive bay. The RAID drive group continues to handle requests while the rebuild occurs.
Auto Resume	When enabled, you can stop a consistency check, rebuild, or initialization, and resume it later where it left off, instead of aborting it and starting over.

5.3.3.1 Virtual Drive management

Using the Virtual drive Management option it is possible to change the properties of an existing VD, also it is possible to migrate (re-configure) from one RAID level to another, locate, hide, initialize and erase a virtual drive.

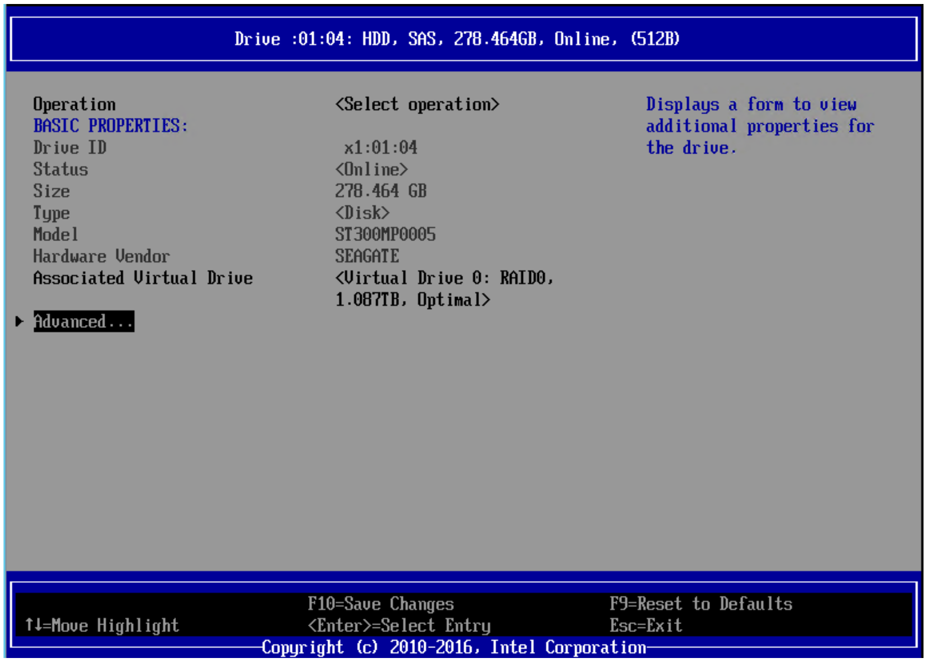


```
                     Virtual Drive 0: RAID0, 1.087TB, Optimal

  Operation                       <Select operation>          Lists the operations that
  BASIC PROPERTIES:                                           you can perform on a virtual
  Name                            _                           drive.
  Raid Level                      <RAID0>
  Status                          <Optimal>
  Size
▶ View Associated Drives           Select operation
▶ Advanced...                      Start Locate
                                   Stop Locate
                                   Delete Virtual Drive
                                   Hide Virtual Drive
                                   Hide Drive Group
                                   Fast Initialization
                                   Slow Initialization
                                   Virtual Drive Erase

 ↑↓=Move Highlight            <Enter>=Complete Entry           Esc=Exit Entry
                    Copyright (c) 2010-2016, Intel Corporation
```

Figure 79. HII CU – Virtual drive Management

5.3.3.2 Drive Management

Using the Drive Management option it is possible to see the properties of the physical drives connected to the RAID controller: Drive ID, size, type of drive, model, vendor, sector size, status, media erors, predicted fail count, SAS address, power state, cache settings, available size, used space, disk protocol, negotiated transfer speed, and temperature. Self-Encrypting Drives (SED)'s properties are also shown in this option.

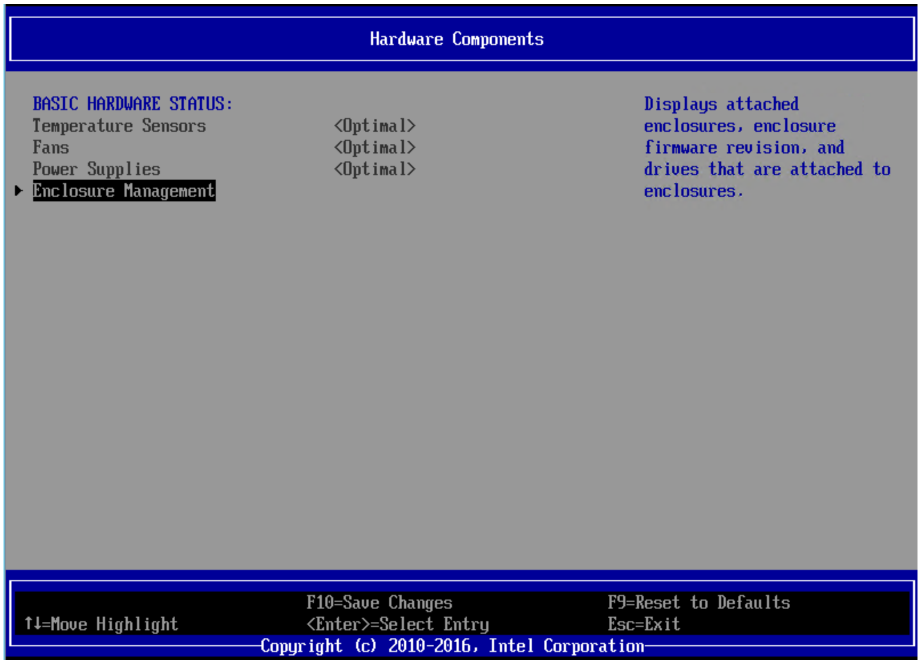


```
                    Drive :01:04: HDD, SAS, 278.464GB, Online, (512B)

 Operation                        <Select operation>         Displays a form to view
 BASIC PROPERTIES:                                           additional properties for
 Drive ID                          x1:01:04                  the drive.
 Status                           <Online>
 Size                             278.464 GB
 Type                             <Disk>
 Model                            ST300MP0005
 Hardware Vendor                  SEAGATE
 Associated Virtual Drive         <Virtual Drive 0: RAID0,
                                  1.087TB, Optimal>
▸ Advanced...

                              F10=Save Changes              F9=Reset to Defaults
↑↓=Move Highlight             <Enter>=Select Entry          Esc=Exit
                        Copyright (c) 2010-2016, Intel Corporation
```

Figure 80. HII CU – Drive Management

5.3.3.3 Hardware components

On the **Hardware Components** option it is possible to see the status of the temperature sensors, fans, power supplies and enclosures.



```
                         Hardware Components

BASIC HARDWARE STATUS:                               Displays attached
Temperature Sensors          <Optimal>               enclosures, enclosure
Fans                         <Optimal>               firmware revision, and
Power Supplies               <Optimal>               drives that are attached to
▶ Enclosure Management                               enclosures.

                         F10=Save Changes           F9=Reset to Defaults
↑↓=Move Highlight        <Enter>=Select Entry       Esc=Exit
                  Copyright (c) 2010-2016, Intel Corporation
```

Figure 81. HII CU – Hardware Components

6 Configuring the Tri-Mode RAID controllers

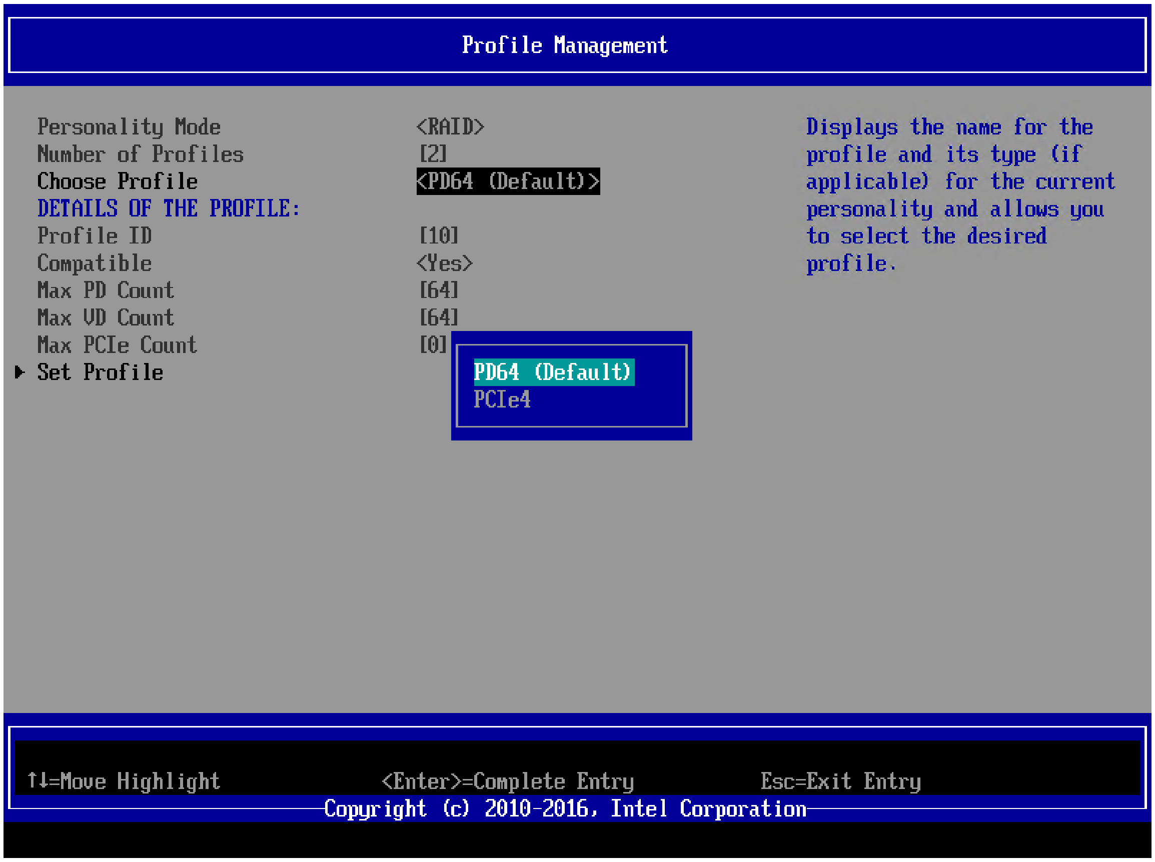
The Tri-Mode modules and controllers are designed to work in the optimized UEFI boot mode, the only way to configure them in a pre-boot environment is using the HII CU. Refer to Section 5.3 to see details on how to use the HII CU. They can also be configured using any of the post-boot configuration utilities, for more information on those utilities, please refer to the Intel RAID Configuration Utilities.

6.1 Operating modes

In order to select the operating modes between SAS/SATA only and NVMe only, the controller's profile needs to be switched. Use the **Profile Management** in the A**dvanced Controller Properties** in the HII Configuration Utility to select the appropriate profile:

Profile PD64 is for SAS/SATA drives and the profile PCIe4 is for NVMe drives.

Select the desired profile as shown in the Figure 82, then select "Set Profile" and reboot the system in order for the changes to take effect.



```
                              Profile Management

 Personality Mode              <RAID>              Displays the name for the
 Number of Profiles            [2]                 profile and its type (if
 Choose Profile                <PD64 (Default)>    applicable) for the current
 DETAILS OF THE PROFILE:                           personality and allows you
 Profile ID                    [10]                to select the desired
 Compatible                    <Yes>               profile.
 Max PD Count                  [64]
 Max VD Count                  [64]
 Max PCIe Count                [0]
▶ Set Profile                     PD64 (Default)
                                  PCIe4

 ↑↓=Move Highlight           <Enter>=Complete Entry           Esc=Exit Entry
                  Copyright (c) 2010-2016, Intel Corporation
```

Figure 82. HII CU – Profile Management

Appendix A. Glossary

Term	Definition
Absolute state of change	Predicted remaining battery capacity expressed as a percentage of Design Capacity. Note that the Absolute State of Charge operation can return values greater than 100 percent.
Access policy	A virtual drive property indicating what kind of access is allowed for a particular virtual drive. The possible values are Read/Write, Read Only, or Blocked.
Alarm enabled	A controller property that indicates whether the controller's onboard alarm is enabled.
Alarm present	A controller property that indicates whether the controller has an onboard alarm. If present and enabled, the alarm is sounded for certain error conditions.
Array	See **Drive group**
Auto learn mode	The controller performs the learn cycle automatically in this mode. This mode offers the following options: • BBU Auto Learn: Firmware tracks the time since the last learn cycle and performs a learn cycle when due. • BBU Auto Learn Disabled: Firmware does not monitor or initiate a learn cycle. You can schedule learn cycles manually. • BBU Auto Learn Warn: Firmware warns about a pending learn cycle. You can initiate a learn cycle manually. After the learn cycle is complete, the firmware resets the counter and warns you when the next learn cycle time is reached.
Auto learn period	Time between learn cycles. A learn cycle is a battery calibration operation performed periodically by the controller to determine the condition of the battery.
Average time to empty	One-minute rolling average of the predicted remaining battery life.
Average time to full	Predicted time to charge the battery to a fully charged state based on the one-minute rolling average of the charge current.
Battery module version	Current revision of the battery pack module.
Battery replacement	Warning issued by firmware that the battery can no longer support the required data retention time.
Battery retention time	Time, in hours, that the battery can maintain the contents of the cache memory.
Battery status	Operating status of the battery. Possible values are Missing, Optimal, Failed, Degraded (need attention), and Unknown.
Battery type	Possible values are intelligent Battery Backup Unit (BBU), intelligent Battery Backup Unit (iBBU), intelligent Transportable Battery Backup Unit (iTBBU), and ZCR Legacy.
BBU present	A controller property that indicates whether the controller has an on-board battery backup unit to provide power in case of a power failure.
BGI rate	A controller property indicating the rate at which the background initialization of virtual drives will be carried out.
BIOS	Basic Input/Output System. The computer BIOS is stored on a flash memory chip. The BIOS controls communications between the microprocessor and peripheral devices, such as the keyboard and the video controller, and miscellaneous functions, such as system messages.
Cache	Fast memory that holds recently accessed data. Use of cache memory speeds subsequent access to the same data. When data is read from or written to main memory, a copy is also saved in cache memory with the associated main memory address. The cache memory software monitors the addresses of subsequent reads to see whether the required data is already stored in cache memory. If it is already in cache memory (a cache hit), it is read from cache memory immediately and the main memory read is aborted (or not started). If the data is not cached (a cache miss), it is fetched from main memory and saved in cache memory.
Cache flush interval	A controller property that indicates how often the data cache is flushed.
Caching	The process of using a high-speed memory buffer to speed up a computer system's overall read/write performance. The cache can be accessed at a higher speed than a drive subsystem. To improve read performance, the cache usually contains the most recently accessed data, as well as data from adjacent drive sectors. To improve write performance, the cache can temporarily store data in accordance with its write back policies.

Capacity	A property that indicates the amount of storage space on a drive or virtual drive.
Coerced capacity	A drive property indicating the capacity to which a drive has been coerced (forced) to make it compatible with other drives that are nominally the same capacity. For example, a 4-GB drive from one manufacturer might be 4,196 MB, and a 4-GB from another manufacturer might be 4,128 MB. These drives could be coerced to a usable capacity of 4,088 MB each for use in a drive group in a storage configuration.
Coercion mode	A controller property indicating the capacity to which drives of nominally identical capacity are coerced (forced) to make them usable in a storage configuration.
Consistency check	An operation that verifies that all stripes in a virtual drive with a redundant RAID level are consistent and that automatically fixes any errors. For RAID 1 drive groups, this operation verifies correct mirrored data for each stripe.
Consistency check rate	The rate at which consistency check operations are run on a computer system.
Controller	A chip that controls the transfer of data between the microprocessor and memory or between the microprocessor and a peripheral device such as a drive. RAID controllers perform RAID functions such as striping and mirroring to provide data protection.
Copyback	The procedure used to copy data from a source drive of a virtual drive to a destination drive that is not a part of the virtual drive. The copyback operation is often used to create or restore a specific physical configuration for a drive group (for example, a specific arrangement of drive group members on the device I/O buses). The copyback operation can be run automatically or manually. Typically, a drive fails or is expected to fail, and the data is rebuilt on a hot spare. The failed drive is replaced with a new drive. Then the data is copied from the hot spare to the new drive, and the hot spare reverts from a rebuild drive to its original hot spare status. The copyback operation runs as a background activity, and the virtual drive is still available online to the host.
Current	Measure of the current flowing to (+) or from (-) the battery, reported in milliamperes.
Current write policy	A virtual drive property that indicates whether the virtual drive currently supports Write Back mode or Write Through mode. • In Write Back mode, the controller sends a data transfer completion signal to the host when the controller cache has received all of the data in a transaction. • In Write Through mode, the controller sends a data transfer completion signal to the host when the drive subsystem has received all of the data in a transaction.
Cycle count	The count is based on the number of times the near fully charged battery has been discharged to a level below the cycle count threshold.
Default write policy	A virtual drive property indicating whether the default write policy is Write Through or Write Back. • In Write Back mode, the controller sends a data transfer completion signal to the host when the controller cache has received all of the data in a transaction. • In Write Through mode, the controller sends a data transfer completion signal to the host when the drive subsystem has received all of the data in a transaction.
Design capacity	Designed charge capacity of the battery, measured in milliampere-hour units (mAh).
Design charge capacity remaining	Amount of the charge capacity remaining, relative to the battery pack design capacity.
Design voltage	Designed voltage capacity of the battery, measured in millivolts (mV).
Device chemistry	Possible values are NiMH (nickel metal hydride) and LiON (lithium ion).
Device ID	A controller or drive property indicating the manufacturer-assigned device ID.
Device port count	A controller property indicating the number of ports on the controller.
Drive cache policy	A virtual drive property indicating whether the virtual drive cache is enabled, disabled, or unchanged from its previous setting.
Drive group	A group of drives attached to a RAID controller on which one or more virtual drives can be created. All virtual drives in the drive group use all of the drives in the drive group.

Drive state	A drive property indicating the status of the drive. A drive can be in one of the following states: • Unconfigured Good – A drive accessible to the RAID controller but not configured as a part of a virtual drive or as a hot spare. • Hot Spare – A drive that is configured as a hot spare. • Online – A drive that can be accessed by the RAID controller and will be part of the virtual drive. • Rebuild – A drive to which data is being written to restore full redundancy for a virtual drive. • Failed – A drive that was originally configured as Online or Hot Spare, but on which the firmware detects an unrecoverable error. • Unconfigured Bad – A drive on which the firmware detects an unrecoverable error; the drive was Unconfigured Good or the drive could not be initialized. • Missing – A drive that was Online, but which has been removed from its location. • Offline – A drive that is part of a virtual drive but which has invalid data as far as the RAID configuration is concerned. • None – A drive with an unsupported flag set. An Unconfigured Good or Offline drive that has completed the prepare for removal operation.
Drive state drive subsystem	A collection of drives and the hardware that controls them and connects them to one or more controllers. The hardware can include an intelligent controller, or the drives can attach directly to a system I/O bus controller.
Drive type	A drive property indicating the characteristics of the drive.
EKM	External Key Management
Estimated time to recharge	Estimated time necessary to complete recharge of the battery at the current charge rate.
Expected margin of error	Indicates how accurate the reported battery capacity is in terms of percentage.
Fast initialization	A mode of initialization that quickly writes zeroes to the first and last sectors of the virtual drive. This allows you to immediately start writing data to the virtual drive while the initialization is running in the background.
Fault tolerance	The capability of the drive subsystem to undergo a single drive failure per drive group without compromising data integrity and processing capability. The Intel® RAID Controllers provide fault tolerance through redundant drive groups in RAID levels 1, 5, 6, 10, 50, and 60. They also support hot spare drives and the auto-rebuild feature.
Firmware	Software stored in read-only memory (ROM) or programmable ROM (PROM). Firmware is often responsible for the behavior of a system when it is first turned on. A typical example is a monitor program in a system that loads the full operating system from a drive or from a network and then passes control to the operating system.
Foreign configuration	A RAID configuration that already exists on a replacement set of drives that you install in a computer system. The GUI management utility software allows you to import the existing configuration to the RAID controller, or you can clear the configuration so you can create a new one.
Formatting	The process of writing a specific value to all data fields on a drive, to map out unreadable or bad sectors. Because most drives are formatted when manufactured, formatting is usually done only if a drive generates many media errors.
Full charge capacity	Amount of charge that can be placed in the battery. This value represents the last measured full discharge of the battery. This value is updated on each learn cycle when the battery undergoes a qualified discharge from nearly full to a low battery level.
Gas gauge status	Hexadecimal value that represents the status flag bits in the gas gauge status register.
Hole	In the GUI management utility, a hole is a block of empty space in a drive group that can be used to define a virtual drive.
Host interface	A controller property indicating the type of interface used by the computer host system; for example, PCIX.
Host port count	A controller property indicating the number of host data ports currently in use.
Host system	Any computer system on which the controller is installed. Mainframes, workstations, and standalone desktop systems can all be considered host systems.

Hot spare	A standby drive that can automatically replace a failed drive in a virtual drive and prevent data from being lost. A hot spare can be dedicated to a single redundant drive group or it can be part of the global hot spare pool for all drive groups controlled by the controller. When a drive fails, the GUI management utility software automatically uses a hot spare to replace it and then rebuilds the data from the failed drive to the hot spare. Hot spares can be used in RAID 1, 5, 6, 10, 50, and 60 storage configurations.
Initialization	The process of writing zeros to the data fields of a virtual drive and, in fault-tolerant RAID levels, generating the corresponding parity to put the virtual drive in a Ready state. Initialization erases all previous data on the drives. Drive groups work without initialization, but they can fail a consistency check because the parity fields have not been generated.
IO policy	A virtual drive property indicating whether Cached I/O or Direct I/O is being used. In Cached I/O mode, all reads are buffered in cache memory. In Direct I/O mode, reads are not buffered in cache memory. Data is transferred to cache and the host concurrently. If the same data block is read again, it comes from cache memory. (The IO Policy applies to reads on a specific virtual drive. It does not affect the read ahead cache.)
Learning cycle	A battery calibration operation performed by a RAID controller periodically to determine the condition of the battery. You can start battery learn cycles manually or automatically.
Learn delay interval	Length of time between automatic learn cycles. You can delay the start of the learn cycles for up to 168 hours (seven days).
Learn mode	Mode for the battery auto learn cycle. Possible values are Auto, Disabled, and Warning.
Learn state	Indicates that a learn cycle is in progress.
Load-balancing	A method of spreading work between two or more computers, network links, CPUs, drives, or other resources. Load balancing is used to maximize resource use, throughput, or response time.
Low-power storage mode	Storage mode that causes the battery pack to use less power, which saves battery power consumption.
LKM	Local Key Management
Manufacturing date	Date on which the battery pack assembly was manufactured.
Manufacturing name	Device code that indicates the manufacturer of the components used to make the battery assembly.
Max error	Expected margin of error (percentage) in the state of charge calculation. For example, when Max Error returns 10 percent and Relative State of Charge returns 50 percent, the Relative State of Charge is more likely between 50 percent and 60 percent. The gas gauge sets Max Error to 100 percent on a full reset. The gas gauge sets Max Error to 2 percent on completion of a learn cycle, unless the gas gauge limits the learn cycle to the +512/–256-mAh maximum adjustment values. If the learn cycle is limited, the gas gauge sets Max Error to 8 percent unless Max Error was already below 8 percent. In this case Max Error does not change. The gas gauge increments Max Error by 1 percent after four increments of Cycle Count without a learn cycle.
Maximum learn delay from current start time	The maximum length of time between automatic learn cycles. You can delay the start of a learn cycle for a maximum of 168 hours (7 days).
Media error count	A drive property indicating the number of errors that have been detected on the drive media.
Migration	The process of moving virtual drives and hot spare drives from one controller to another by disconnecting the drives from one controller and attaching them to another one. The firmware on the new controller will detect and retain the virtual drive information on the drives.
Mirroring	The process of providing complete data redundancy with two drives by maintaining an exact copy of one drive's data on the second drive. If one drive fails, the contents of the other drive can be used to maintain the integrity of the system and to rebuild the failed drive.
Multipathing	The firmware provides support for detecting and using multiple paths from the RAID controllers to the SAS devices that are in enclosures. Devices connected to enclosures have multiple paths to them. With redundant paths to the same port of a device, if one path fails, another path can be used to communicate between the controller and the device. Using multiple paths with load balancing, instead of a single path, can increase reliability through redundancy.
Name	A virtual drive property indicating the user-assigned name of the virtual drive.
Next learn time	Time at which the next learn cycle starts.
Non-redundant configuration	A RAID 0 virtual drive with data striped across two or more drives but without drive mirroring or parity. This provides for high data throughput but offers no protection in case of a drive failure.

NVRAM	Acronym for nonvolatile random access memory. A storage system that does not lose the data stored on it when power is removed. NVRAM is used to store firmware and configuration data on the RAID controller.
NVRAM present	A controller property indicating whether an NVRAM is present on the controller.
NVRAM size	A controller property indicating the capacity of the controller's NVRAM.
Offline	A drive is offline when it is part of a virtual drive but its data is not accessible to the virtual drive.
Patrol read	A process that checks the drives in a storage configuration for drive errors that could lead to drive failure and lost data. The patrol read operation can find and sometimes fix any potential problem with drives before host access. This enhances overall system performance because error recovery during a normal I/O operation might not be necessary.
Patrol read rate	The user-defined rate at which patrol read operations are run on a computer system.
Phy	Transceiver hardware that handles the communication between SAS devices.
Predicted battery capacity status (hold 24hr charge)	Indicates whether the battery capacity supports a 24-hour data retention time.
Product info	A drive property indicating the vendor-assigned model number of the drive.
Product name	A controller property indicating the manufacturing name of the controller.
RAID	A group of multiple, independent drives that provide high performance by increasing the number of drives used for saving and accessing data. A RAID drive group improves input/output (I/O) performance and data availability. The group of drives appears to the host system as a single storage unit or as multiple virtual drives. Data throughput improves because several drives can be accessed simultaneously. RAID configurations also improve data storage availability and fault tolerance. Redundant RAID levels (RAID levels 1, 5, 6, 10, 50, and 60) provide data protection.
RAID 0	Uses data striping on two or more drives to provide high data throughput, especially for large files in an environment that requires no data redundancy.
RAID 00	Uses data striping on two or more drives in a spanned drive group to provide high data throughput, especially for large files in an environment that requires no data redundancy.
RAID 1	Uses data mirroring on pairs of drives so that data written to one drive is simultaneously written to the other drive. RAID 1 works well for small databases or other small applications that require complete data redundancy.
RAID 5	Uses data striping and parity data across three or more drives (distributed parity) to provide high data throughput and data redundancy, especially for applications that require random access.
RAID 6	Uses data striping and parity data across three or more drives (distributed parity) to provide high data throughput and data redundancy, especially for applications that require random access. RAID 6 can survive the failure of two drives.
RAID 10	A combination of RAID 0 and RAID 1 that uses data striping across two mirrored drive groups. It provides high data throughput and complete data redundancy.
RAID 50	A combination of RAID 0 and RAID 5 that uses data striping across two drive groups with parity data. It provides high data throughput and complete data redundancy.
RAID 60	A combination of RAID 0 and RAID 6 that uses data striping across two drive groups with parity data. It provides high data throughput and complete data redundancy. RAID 60 can survive the failure of two drives in each RAID set in the spanned drive group.
RAID level	A virtual drive property indicating the RAID level of the virtual drive. Intel® RAID Controllers support RAID levels 0, 1, 5, 6, 10, 50, and 60.
RAID migration	A feature in RAID subsystems that allows changing a RAID level to another level without powering down the system.
Raw capacity	A drive property indicating the actual full capacity of the drive before any coercion mode is applied to reduce the capacity.
Read policy	A controller attribute indicating the current Read Policy mode. In Always Read Ahead mode, the controller reads sequentially ahead of requested data and stores the additional data in cache memory, anticipating that the data will be needed soon. This speeds up reads for sequential data, but there is little improvement when accessing random data. In No Read Ahead mode (known as Normal mode in WebBIOS), read ahead capability is disabled.

Rebuild	The regeneration of all data to a replacement drive in a redundant virtual drive after a drive failure. A drive rebuild normally occurs without interrupting normal operations on the affected virtual drive, though some degradation of performance of the drive subsystem can occur.
Rebuild rate	The percentage of central processing unit (CPU) resources devoted to rebuilding data onto a new drive after a drive in a storage configuration has failed.
Reclaim virtual drive	A method of undoing the configuration of a new virtual drive. If you highlight the virtual drive in the Configuration Wizard and click Reclaim, the individual drives are removed from the virtual drive configuration.
Reconstruction rate	The user-defined rate at which a drive group modification operation is carried out.
Redundancy	A property of a storage configuration that prevents data from being lost when one drive fails in the configuration.
Redundant configuration	A virtual drive that has redundant data on drives in the drive group can be used to rebuild a failed drive. The redundant data can be parity data striped across multiple drives in a drive group, or it can be a complete mirrored copy of the data stored on a second drive. A redundant configuration protects the data in case a drive fails in the configuration.
Relative state of charge	Predicted remaining battery capacity expressed as a percentage of Full Charge Capacity.
Remaining capacity	The amount of remaining charge capacity of the battery as stated in milliamp hours. This value represents the available capacity or energy in the battery at any given time. The gas gauge adjusts this value for charge, self-discharge, and leakage compensation factors.
Revertible hot spare	When you use the Replace Member procedure, after data is copied from a hot spare to a new drive, the hot spare reverts from a rebuild drive to its original hot spare status.
Revision level	A drive property that indicates the revision level of the drive's firmware.
Run time to empty	Predicted remaining battery life at the present rate of discharge in minutes.
SAS	Acronym for Serial-Attached SCSI. SAS is a serial, point-to-point, enterprise-level device interface that leverages the Small Computer System Interface (SCSI) protocol set. The SAS interface provides improved performance, simplified cabling, smaller connectors, lower pin count, and lower power requirements when compared to parallel SCSI.
SAS port	A virtual group of phys. It can be a narrow port (formed by one phy) or a wide port (formed by several phys).
SATA	Acronym for Serial Advanced Technology Attachment. A physical storage interface standard. SATA is a serial link that provides point- to-point connections between devices. The thinner serial cables allow for better airflow within the system and permit smaller chassis designs.
SCSI device type	A drive property indicating the type of the device, such as drive.
Serial no.	A controller property indicating the manufacturer-assigned serial number.
Strip size	The portion of a stripe that resides on a single drive in the drive group.
Stripe size	A virtual drive property indicating the length of the interleaved data segments that the RAID controller writes across multiple drives, not including parity drives. For example, consider a stripe that contains 64 KB of drive space and has 16 KB of data residing on each drive in the stripe. In this case, the stripe size is 64 KB and the strip size is 16 KB. The user can select the stripe size.
Striping	A technique used to write data across all drives in a virtual drive. Each stripe consists of consecutive virtual drive data addresses that are mapped in fixed-size units to each drive in the virtual drive using a sequential pattern. For example, if the virtual drive includes five drives, the stripe writes data to drives one through five without repeating any of the drives. The amount of space consumed by a stripe is the same on each drive. Striping by itself does not provide data redundancy. Striping in combination with parity does provide data redundancy.
Subvendor ID	A controller property that lists additional vendor ID information about the controller.
Temperature	Temperature of the battery pack, measured in Celsius.
Uncorrectable error count	A controller property that lists the number of uncorrectable errors detected on drives connected to the controller. If the error count reaches a certain level, a drive will be marked as failed.
Vendor ID	A controller property indicating the vendor-assigned ID number of the controller.
Vendor info	A drive property listing the name of the vendor of the drive.
Virtual drive	A storage unit created by a RAID controller from one or more drives. Although a virtual drive can be created from several drives, it is seen by the operating system as a single drive. Depending on the RAID level used, the virtual drive can retain redundant data in case of a drive failure.

Virtual drive state	A virtual drive property indicating the condition of the virtual drive. Examples include Optimal and Degraded.
Write-back	In Write-Back Caching mode, the controller sends a data transfer completion signal to the host when the controller cache has received all of the data in a drive write transaction. Data is written to the drive subsystem in accordance with policies set up by the controller. These policies include the amount of dirty/clean cache lines, the number of cache lines available, and elapsed time from the last cache flush.
Write policy	See **Default write policy**.
Write-through	In Write-Through Caching mode, the controller sends a data transfer completion signal to the host when the drive subsystem has received all of the data and has completed the write transaction to the drive.