USB 3.0, eSATA and iSCSI RAID Subsystem

User Manual

Revision 1.0

Table of Contents

Preface

About this manual

This manual provides information regarding the quick installation and hardware features of the **RAID subsystem**. This document also describes how to use the storage management software. Information contained in the manual has been reviewed for accuracy, but not for product warranty because of the various environment/OS/settings. Information and specifications will be changed without further notice.

This manual uses section numbering for every topics being discussed for easy and convenient way of finding information in accordance with the user's needs. The following icons are being used for some details and information to be considered in going through with this manual:

NOTES:
These are notes that contain useful information and tips that the user must give attention to in going through with the subsystem operation.

IMPORTANT!
These are the important information that the user must remember.

WARNING!
These are the warnings that the user must follow to avoid unnecessary errors and bodily injury during hardware and software operation of the subsystem.

CAUTION:
These are the cautions that user must be aware to prevent damage to the equipment and its components.

Copyright

Trademarks

All products and trade names used in this document are trademarks or registered trademarks of their respective holders.

Changes

The material in this document is for information only and is subject to change without notice.

Before You Begin

Before going through with this manual, you should read and focus to the following safety guidelines. Notes about the subsystem's controller configuration and the product packaging and delivery are also included.

Safety Guidelines

To provide reasonable protection against any harm on the part of the user and to obtain maximum performance, user is advised to be aware of the following safety guidelines particularly in handling hardware components:

Upon receiving of the product:

- Place the product in its proper location.
- To avoid unnecessary dropping out, make sure that somebody is around for immediate assistance.
- It should be handled with care to avoid dropping that may cause damage to the product. Always use the correct lifting procedures.

Upon installing of the product:

- Ambient temperature is very important for the installation site. It must not exceed 30°C. Due to seasonal climate changes; regulate the installation site temperature making it not to exceed the allowed ambient temperature.
- Before plugging-in any power cords, cables and connectors, make sure that the power switches are turned off. Disconnect first any power connection if the power supply module is being removed from the enclosure.
- Outlets must be accessible to the equipment.
- All external connections should be made using shielded cables and as much as possible should not be performed by bare hand. Using anti-static hand gloves is recommended.
- In installing each component, secure all the mounting screws and locks. Make sure that all screws are fully tightened. Follow correctly all the listed procedures in this manual for reliable performance.

Controller Configuration

This RAID subsystem supports single controller configuration.

Packaging, Shipment and Delivery

- Before removing the subsystem from the shipping carton, you should visually inspect the physical condition of the shipping carton.
- Unpack and verify that the contents of the shipping carton are complete and in good condition.
- Exterior damage to the shipping carton may indicate that the contents of the carton are damaged.

If any damage is found, do not remove the components; contact the dealer where you purchased the subsystem for further instructions.

Unpacking the Subsystem

The package contains the following items:

	RAID Subsystem Unit
	Two (2) power cords
	Two (2) RJ45 Ethernet cables
	One (1) external serial cables DB9-to-DB9
	One(1) USB Cable
	One(1) external SATA cable
	User Manual

NOTE: If any damage is found, contact the dealer or vendor for assistance.

Chapter 1 Introduction

The RAID Subsystem

Unsurpassed Value
- Most cost-effective SATA III RAID Subsystem

Application Flexibility
- Multiple interface, extends useful life by adapting to future IT requirements

Easy Installation, upgrade & Maintenance
- Provide a fast and easy way to install and upgrade the storage. Simplified maintenance reduces ongoing IT labor costs.

Exceptional Manageability
- Graphical User Interface (GUI) provides easy way for users to remotely manage and configure the storage
- Menu-driven interface make user a convenient way to maintain the storage by locally LCD front console

Green Power Concept
- Saves power by adopting the new technology "MAID" (Massive Arrays of Idle Disks).

1.1 Key Features

Subsystem Features:

- USB 3.0 (5Gbps) / eSATA (6Gbps) / GbE(x4) Host interface
- Multiple RAID selection
- Configurable stripe size up to 1024KB
- Online array roaming
- Online RAID level/stripe size migration
- Online capacity expansion and RAID level migration simultaneously
- Online volume set growth
- Support global and dedicated hot spare
- Support for native 4K and 512 byte sector SATA devices
- Multiple pairs SSD/HDD disk clone function
- Support HDD firmware update

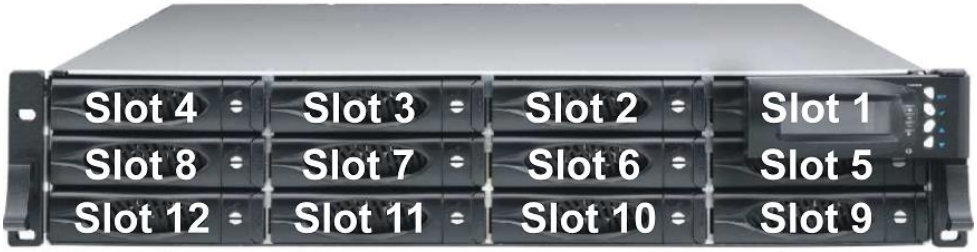
RAID Management:

- Smart-function LCD panel
- Environmental monitoring unit
- Real time drive activity and status indicators
- Web-based GUI management utility

1.2 Identifying Parts of the RAID Subsystem

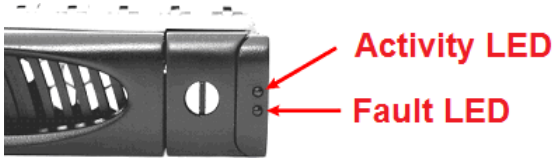
The illustrations below identify the various parts of the subsystem.

1.2.1 Front View



1.2.1.1 Disk Trays

HDD Status Indicator

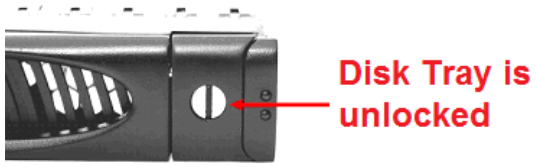


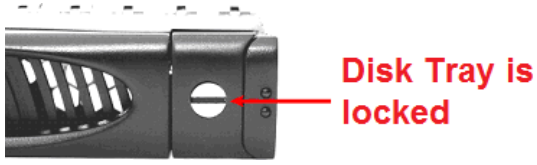
Part	Function
HDD Activity LED	This LED will blink blue when the hard drive is being accessed.
HDD Fault LED	Green LED indicates power is on and hard drive status is good for this slot. If hard drive is defective or failed, the LED is Red. LED is off when there is no hard drive.

Lock Indicator

Every Disk Tray is lockable and is fitted with a lock indicator to indicate whether or not the tray is locked into the chassis or not. Each tray is also fitted with an ergonomic handle for easy tray removal.

When the Lock Groove is horizontal, this indicates that the Disk Tray is locked. When the Lock Groove is vertical, then the Disk Tray is unlocked.





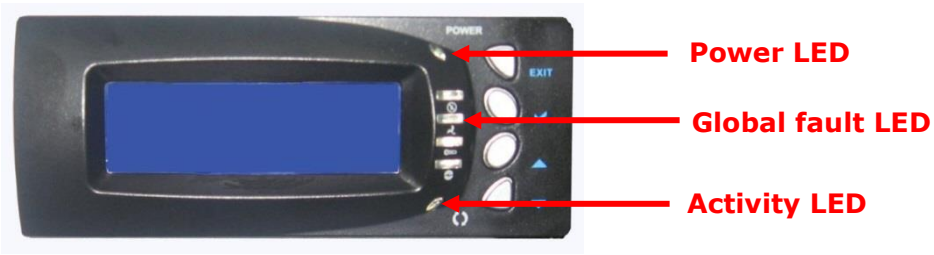
1.2.1.2 LCD Front Panel

Smart Function Front Panel

The smart LCD panel is an option to configure the RAID subsystem. If you are configuring the subsystem using the LCD panel, press the Select button to login and configure the RAID subsystem.

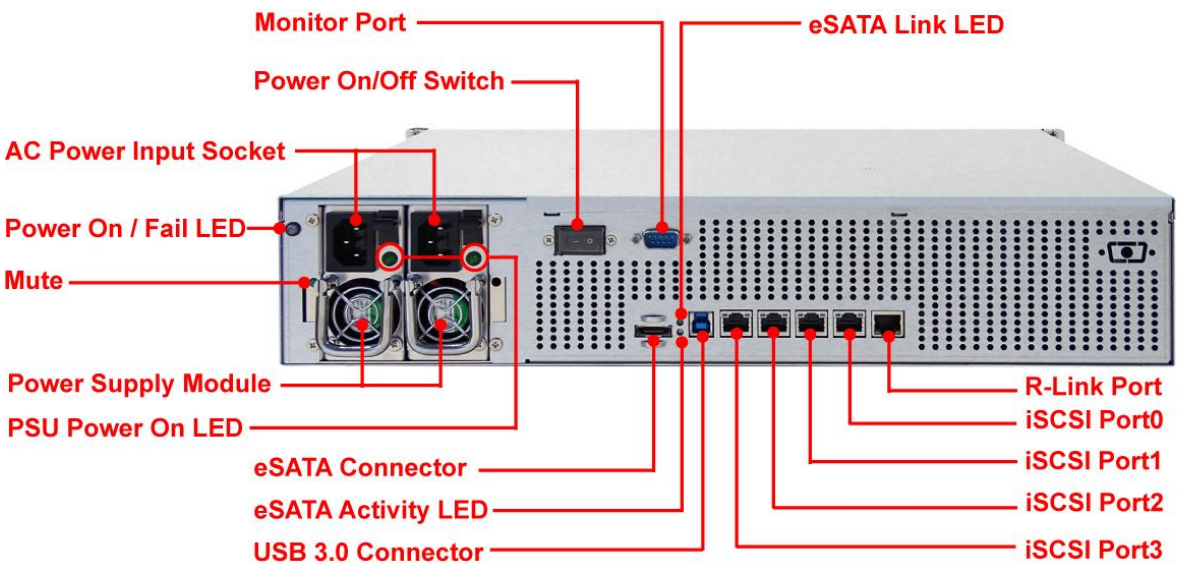
Parts	Function
Up and Down Arrow buttons ▲▼	Use the Up or Down arrow keys to go through the information on the LCD screen. This is also used to move between each menu when you configure the subsystem.
Select button ✔	This is used to enter the option you have selected.
Exit button **EXIT**	Press this button to return to the previous menu. **NOTE:** This button can also be used to reset the alarm beeper and turn off the Global fault LED.

Environment Status LEDs



Parts	Function
Power LED	Green LED indicates power is ON.
Global fault LED	Red LED indicates a problem within the internal subsystem, such as fan fail/power supply fail/disk fault.
Activity LED	This LED will blink blue when the Disk Array is busy or active.

1.2.2 Rear View



1. **Monitor Port -** The subsystem is equipped with a serial monitor port allowing you to connect a PC or terminal.

2. **AC Power Input Socket** – Use this to plug in the power cable connected from power source.

3. **Power On LED** – Green LED indicates power is ON.

4. **Power Supply Unit -** The subsystem has dual power supply units.

NOTE: After power on, the Power On/Fail LED is green, the PSU Power On/Fail LED is also green. When one Power Supply Module fails, the Power On/Fail LED will blink Green.

5. **eSATA Connector -** This external SATA II port for connecting to the host system or server.

   eSATA Link LED: Green LED indicates eSATA is linking.
   eSATA Activity LED: The LED will blink blue when the eSATA is being accessed.

6. **USB 3.0 Port -** The subsystem has one USB 3.0 port for connecting to the host system or server.

7. **R-Link Port : Remote Link through RJ-45 Ethernet for remote management -** The subsystem is equipped with one 10/100/1000 Ethernet RJ45 LAN port. You use a web browser to manage the RAID subsystem through Ethernet for remote configuration and monitoring.

8. **iSCSI Ports (Gigabit)**

   The subsystem is equipped with four LAN data ports (LAN0, LAN1, LAN2, and LAN3) for iSCSI connection.

1.3 Technical Specifications

Form-factor	2U 19-inch rackmount chassis
RAID processor	1.2GHz storage I/O processor
RAID level	0, 1, 10(1E), 3, 5, 6, 30, 50, 60, Single Disk or JBOD
Cache memory	2GB on-board DDR3-1200 SDRAM with ECC protection
No. of Channels (Host and Drive)	6 +12
Host bus interface	USB 3.0 x 1 / eSATA x 1 / GbE iSCSI x 4
Drive bus interface	6Gb/s SATA III
Data transfer rate	Support up to 5.0Gbps (USB 3.0) Support up to 6.0Gbps (eSATA) Support up to 1.0Gbps Ethernet
Hot-swap drive tray	Twelve (12)
Power supplies	400W x2 Redundant power supplies w/PFC
Cooling fan	2
Password protection	Yes
Audible alarm	Yes
Failed drive indicators	Yes
Failed drive auto rebuild	Yes
Online consistency check	Yes
Online expansion	Yes
Array Roaming	Yes
Online RAID level/ stripe size migration	Yes
Instant availability and background initialization	Yes
Environment monitor	Yes
Auto spare support	Yes
Bad block auto-remapping	Yes
Remote management	Yes
MAID support	Yes
Multiple RAID selection	Yes
Hot Spare	Global and Dedicated
Power requirements	AC 100V ~ 240V full range 8A ~ 4A, 47Hz ~ 63Hz
Relative Humidity:	10% ~ 85% Non-condensing
Operating Temp:	10°C ~ 40°C (50°F ~ 104°F)
Physical Dimensions:	88(H) x 482(W) x 500(D)mm
Weight	14.4 Kg (w/o Drives)

Note: Specifications are subject to change without notice. All company and product names are trademarks of their respective owners.

1.4 RAID Concepts

RAID Fundamentals

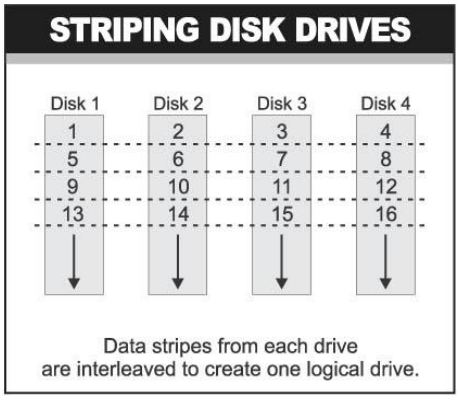
The basic idea of RAID (Redundant Array of Independent Disks) is to combine multiple inexpensive disk drives into an array of disk drives to obtain performance, capacity and reliability that exceeds that of a single large drive. The array of drives appears to the host computer as a single logical drive.

Five types of array architectures, RAID 1 through RAID 5, were originally defined; each provides disk fault-tolerance with different compromises in features and performance. In addition to these five redundant array architectures, it has become popular to refer to a non-redundant array of disk drives as a RAID 0 arrays.

Disk Striping

Fundamental to RAID technology is striping. This is a method of combining multiple drives into one logical storage unit. Striping partitions the storage space of each drive into stripes, which can be as small as one sector (512 bytes) or as large as several megabytes. These stripes are then interleaved in a rotating sequence, so that the combined space is composed alternately of stripes from each drive. The specific type of operating environment determines whether large or small stripes should be used.

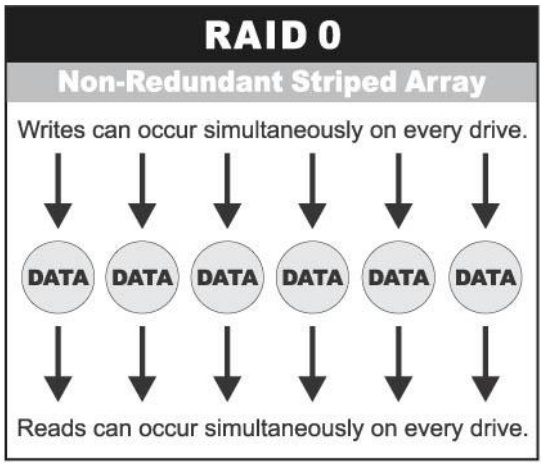
Most operating systems today support concurrent disk I/O operations across multiple drives. However, in order to maximize throughput for the disk subsystem, the I/O load must be balanced across all the drives so that each drive can be kept busy as much as possible. In a multiple drive system without striping, the disk I/O load is never perfectly balanced. Some drives will contain data files that are frequently accessed and some drives will rarely be accessed.



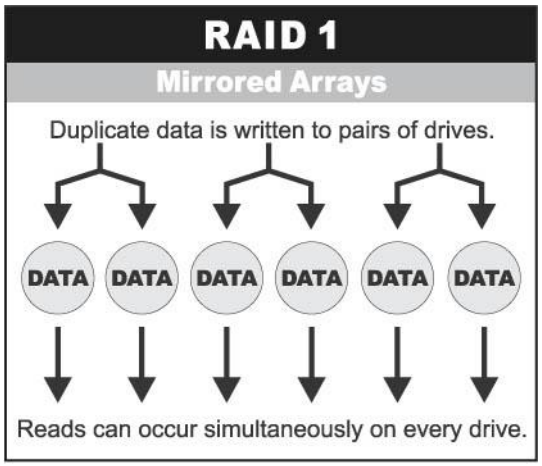
By striping the drives in the array with stripes large enough so that each record falls entirely within one stripe, most records can be evenly distributed across all drives. This keeps all drives in the array busy during heavy load situations. This situation allows all drives to work concurrently on different I/O operations, and thus maximize the number of simultaneous I/O operations that can be performed by the array.

Definition of RAID Levels

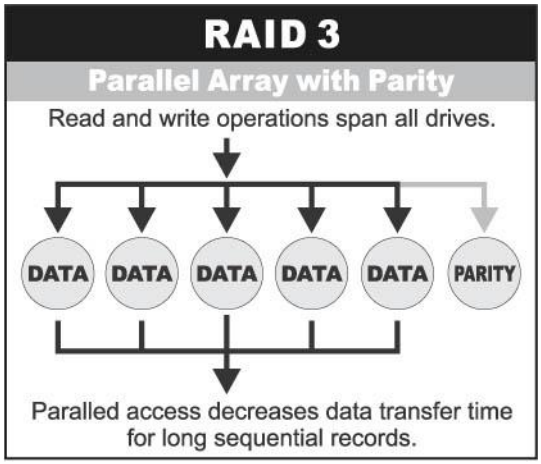
RAID 0 is typically defined as a group of striped disk drives without parity or data redundancy. RAID 0 arrays can be configured with large stripes for multi-user environments or small stripes for single-user systems that access long sequential records. RAID 0 arrays deliver the best data storage efficiency and performance of any array type. The disadvantage is that if one drive in a RAID 0 array fails, the entire array fails.



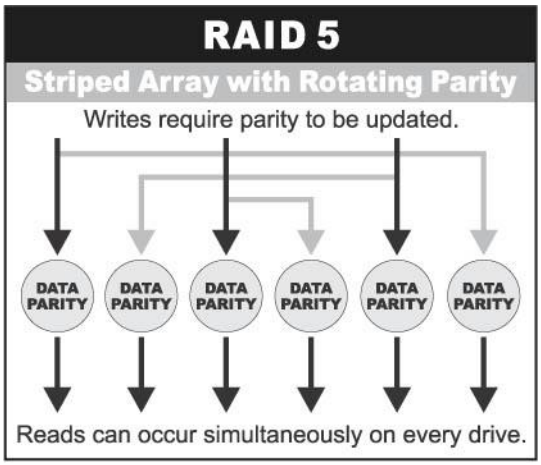
RAID 1, also known as disk mirroring, is simply a pair of disk drives that store duplicate data but appear to the computer as a single drive. Although striping is not used within a single mirrored drive pair, multiple RAID 1 arrays can be striped together to create a single large array consisting of pairs of mirrored drives. All writes must go to both drives of a mirrored pair so that the information on the drives is kept identical. However, each individual drive can perform simultaneous, independent read operations. Mirroring thus doubles the read performance of a single non-mirrored drive and while the write performance is unchanged. RAID 1 delivers the best performance of any redundant array type. In addition, there is less performance degradation during drive failure than in RAID 5 arrays.



RAID 3 sector-stripes data across groups of drives, but one drive in the group is dedicated to storing parity information. RAID 3 relies on the embedded ECC in each sector for error detection. In the case of drive failure, data recovery is accomplished by calculating the exclusive OR (XOR) of the information recorded on the remaining drives. Records typically span all drives, which optimizes the disk transfer rate. Because each I/O request accesses every drive in the array, RAID 3 arrays can satisfy only one I/O request at a time. RAID 3 delivers the best performance for single-user, single-tasking environments with long records. Synchronized-spindle drives are required for RAID 3 arrays in order to avoid performance degradation with short records. RAID 5 arrays with small stripes can yield similar performance to RAID 3 arrays.

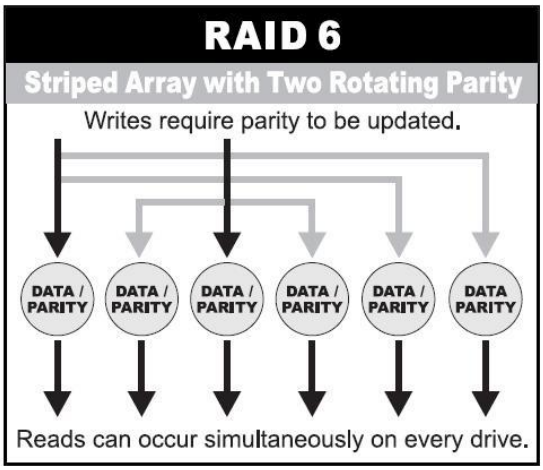


Under **RAID 5** parity information is distributed across all the drives. Since there is no dedicated parity drive, all drives contain data and read operations can be overlapped on every drive in the array. Write operations will typically access one data drive and one parity drive. However, because different records store their parity on different drives, write operations can usually be overlapped.



Dual-level RAID achieves a balance between the increased data availability inherent in RAID 1 and the increased read performance inherent in disk striping (RAID 0). These arrays are sometimes referred to as RAID 10.

RAID 6 is similar to RAID 5 in that data protection is achieved by writing parity information to the physical drives in the array. With RAID 6, however, ***two*** sets of parity data are used. These two sets are different, and each set occupies a capacity equivalent to that of one of the constituent drives. The main advantage of RAID 6 is High data availability – any two drives can fail without loss of critical data.



In summary:

- RAID 0 is the fastest and most efficient array type but offers no fault-tolerance. RAID 0 requires a minimum of one drive.
- RAID 1 is the best choice for performance-critical, fault-tolerant environments. RAID 1 is the only choice for fault-tolerance if no more than two drives are used.
- RAID 3 can be used to speed up data transfer and provide fault-tolerance in single-user environments that access long sequential records. However, RAID 3 does not allow overlapping of multiple I/O operations and requires synchronized-spindle drives to avoid performance degradation with short records. RAID 5 with a small stripe size offers similar performance.
- RAID 5 combines efficient, fault-tolerant data storage with good performance characteristics. However, write performance and performance during drive failure is slower than with RAID 1. Rebuild operations also require more time than with RAID 1 because parity information is also reconstructed. At least three drives are required for RAID 5 arrays.
- RAID 6 is essentially an extension of RAID level 5 which allows for additional fault tolerance by using a second independent distributed parity scheme (two-dimensional parity). Data is striped on a block level across a set of drives, just like in RAID 5, and a second set of parity is calculated and written across all the drives; RAID 6 provides for an extremely high data fault tolerance and can sustain multiple simultaneous drive failures. It is a perfect solution for mission critical applications.

RAID Management

The subsystem can implement several different levels of RAID technology. RAID levels supported by the subsystem are shown below.

RAID Level	Description	Min. Drives
0	Block striping is provide, which yields higher performance than with individual drives. There is no redundancy.	1
1	Drives are paired and mirrored. All data is 100% duplicated on an equivalent drive. Fully redundant.	2
3	Data is striped across several physical drives. Parity protection is used for data redundancy.	3
5	Data is striped across several physical drives. Parity protection is used for data redundancy.	3
6	Data is striped across several physical drives. Parity protection is used for data redundancy. Requires N+2 drives to implement because of two-dimensional parity scheme.	3
10(1E)	Combination of RAID levels 1 and 0. This level provides striping and redundancy through mirroring. RAID 10 requires the use of an even number of disk drives to achieve data protection, while RAID 1E (Enhanced Mirroring) uses an odd number of drives.	3
30	Combination of RAID levels 0 and 3. This level is best implemented on two RAID 3 disk arrays with data striped across both disk arrays.	6
50	RAID 50 provides the features of both RAID 0 and RAID 5. RAID 50 includes both parity and disk striping across multiple drives. RAID 50 is best implemented on two RAID 5 disk arrays with data striped across both disk arrays.	6
60	RAID 60 combines both RAID 6 and RAID 0 features. Data is striped across disks as in RAID 0, and it uses double distributed parity as in RAID 6. RAID 60 provides data reliability, good overall performance and supports larger volume sizes. RAID 60 also provides very high reliability because data is still available even if multiple disk drives fail (two in each disk array).	6

1.5 Array Definition

1.5.1 Raid Set

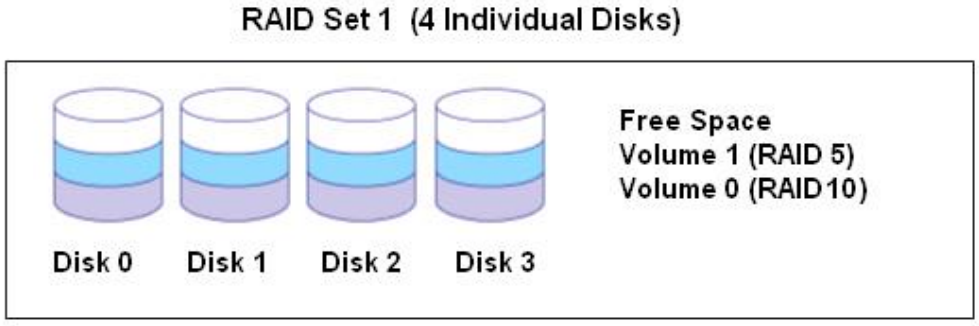
A Raid Set is a group of disk drives containing one or more logical volumes called Volume Sets. It is not possible to have multiple Raid Sets on the same disk drives.

A Volume Set must be created either on an existing Raid Set or on a group of available individual disk drives (disk drives that are not yet a part of a Raid Set). If there are existing Raid Sets with available raw capacity, new Volume Set can be created. New Volume Set can also be created on an existing Raid Set without free raw capacity by expanding the Raid Set using available disk drive(s) which is/are not yet Raid Set member. If disk drives of different capacity are grouped together in a Raid Set, then the capacity of the smallest disk will become the effective capacity of all the disks in the Raid Set.

1.5.2 Volume Set

A Volume Set is seen by the host system as a single logical device. It is organized in a RAID level with one or more physical disks. RAID level refers to the level of data performance and protection of a Volume Set. A Volume Set capacity can consume all or a portion of the raw capacity available in a Raid Set. Multiple Volume Sets can exist on a group of disks in a Raid Set. Additional Volume Sets created in a specified Raid Set will reside on all the physical disks in the Raid Set. Thus each Volume Set on the Raid Set will have its data spread evenly across all the disks in the Raid Set. Volume Sets of different RAID levels may coexist on the same Raid Set.

In the illustration below, Volume 1 can be assigned a RAID 5 level while Volume 0 might be assigned a RAID 10 level.



1.5.3 Easy to Use Features

1.5.3.1 Instant Availability/Background Initialization

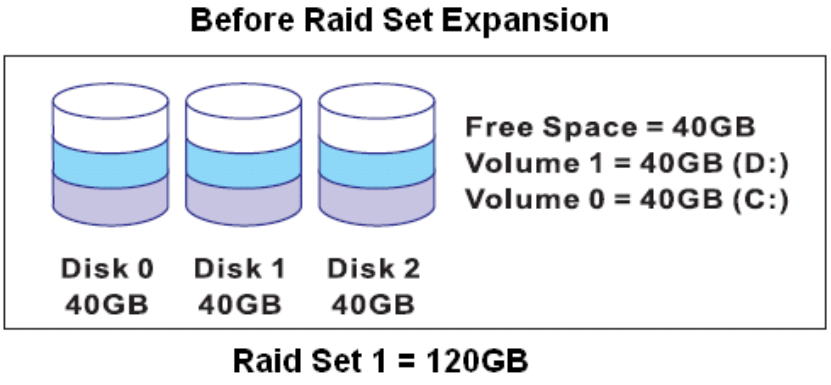
RAID 0 and RAID 1 Volume Set can be used immediately after the creation. But the RAID 3, 5 and 6 Volume Sets must be initialized to generate the parity. In the Background Mode initialization, the initialization proceeds as a background task, the Volume Set is fully accessible for system reads and writes. The operating system can instantly access to the newly created Volume Sets without waiting for the initialization to be completed. One disadvantage of this is that the initialization process takes longer time. In Foreground Mode initialization, the initialization process is faster but must be completed first before the Volume Set is ready for system access.

1.5.3.2 Array Roaming

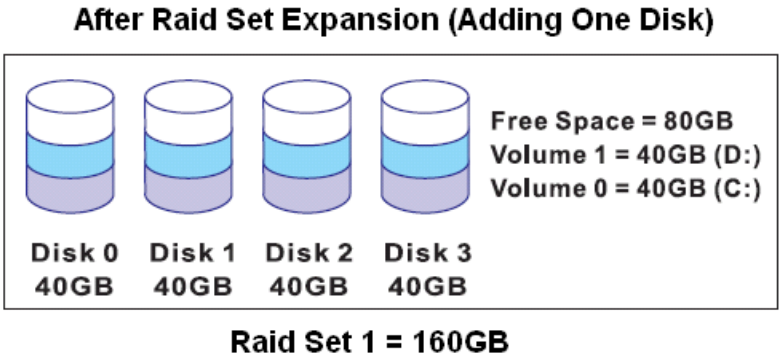
The RAID subsystem stores configuration information both in NVRAM and on the disk drives. This protects the configuration settings in the case of a disk drive or controller failure. Array roaming allows the administrator the ability to move a complete Raid Set to another system without losing RAID configuration and data on that Raid Set. If a RAID enclosure fails to work, the Raid Set disk drives can be moved to another enclosure and inserted in any order.

1.5.3.3 Online Capacity Expansion

Online Capacity Expansion makes it possible to add one or more physical drives to a Raid Set, while the server is in operation, eliminating the need to backup and restore after reconfiguring the Raid Set. When disks are added to a Raid Set, unused capacity is added at the end of the Raid Set. Data on the existing Volume Sets residing on that Raid Set is redistributed evenly across all the disks. A contiguous block of unused capacity is made available on the Raid Set. The unused capacity can be used to create additional Volume Set. The expansion process is illustrated as follows.



The RAID subsystem controller redistributes the original Volume Set over the original and newly added disks, using the same RAID level configuration. The unused capacity on the expand Raid Set can then be used to create an additional Volume Sets, with a different RAID level setting as needed by user.



1.3.3.4 Online RAID Level and Stripe Size Migration

User can do migration on both the RAID level and Stripe Size of an existing Volume Set while the server is online and the Volume Set is in use. Online RAID level/stripe size migration can prove helpful during performance tuning activities as well as in the event that additional physical disks are added to the RAID subsystem. For example, in a system using two drives in RAID level 1, you could add capacity and retain fault tolerance by adding one drive. With the addition of third disk, you have the option of adding this disk to your existing RAID logical drive and migrating from RAID level 1 to 5. The result would be parity fault tolerance and double the available capacity without taking the system off.

1.5.4 High Availability

1.5.4.1 Creating Hot Spares

A hot spare drive is an unused online available drive, which is ready to replace a failed disk drive. In a RAID level 1, 10, 3, 5 or 6 Raid Set, any unused online available drive installed but not belonging to a Raid Set can be defined as a hot spare drive. Hot spares permit you to replace failed drives without powering down the system. When the RAID subsystem detects a drive failure, the system will do automatic and transparent rebuild using the hot spare drives. The Raid Set will be reconfigured and rebuilt in the background while the RAID subsystem continues to handle system request. During the automatic rebuild process, system activity will continue as normal, however, the system performance and fault tolerance will be affected.

IMPORTANT: The hot spare must have at least the same or more capacity as the drive it replaces.

1.5.4.2 Hot-Swap Disk Drive Support

The RAID subsystem has built-in protection circuit to support the replacement of SATA III hard disk drives without having to shut down or reboot the system. The removable hard drive tray can deliver "hot swappable" fault-tolerant RAID solution at a price much less than the cost of conventional SCSI hard disk RAID subsystems. This feature is provided in the RAID subsystem for advance fault tolerant RAID protection and "online" drive replacement.

1.3.4.3 Hot-Swap Disk Rebuild

The Hot-Swap feature can be used to rebuild Raid Sets with data redundancy such as RAID level 1, 10, 3, 5 and 6. If a hot spare is not available, the failed disk drive must be replaced with a new disk drive so that the data on the failed drive can be rebuilt. If a hot spare is available, the rebuild starts automatically when a drive fails. The RAID subsystem automatically and transparently rebuilds failed drives in the background with user-definable rebuild rates. The RAID subsystem will automatically continue the rebuild process if the subsystem is shut down or powered off abnormally during a reconstruction process.

Chapter 2 Getting Started

2.1 Preparing the Subsystem and Powering On

Here are the basic steps to prepare the RAID subsystem for use.

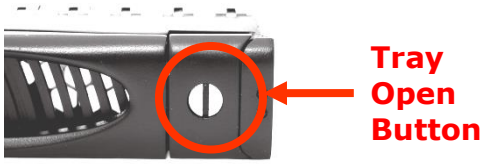
1. Attach network cable to the R-Link port and connect the other end of network cable to your network hub/switch. Or as alternative for configuration, you may connect the serial cable to the Monitor port and to the serial port of your host/server.
2. Connect the USB cable / eSATA cable to the USB port / eSATA port of the RAID subsystem and to the host system or server that will use the storage.
3. Connect the power cords to the AC input sockets. Plug the other ends of power cords to the power source.
4. Press the Power On/Off Switch at the rear of the subsystem.

2.2 Installing Hard Drives

This section describes the physical locations of the hard drives supported by the subsystem and gives instructions on installing a hard drive. The subsystem supports hot-swapping allowing you to install or replace a hard drive while the subsystem is running.

Each Drive Carrier has a locking mechanism. When the Lock Groove, which is located in carrier open button, is horizontal, the Drive Carrier is locked. When the Lock Groove is vertical, the Drive Carrier is unlocked. Lock and unlock the Drive Carriers by using a flat-head screw driver.

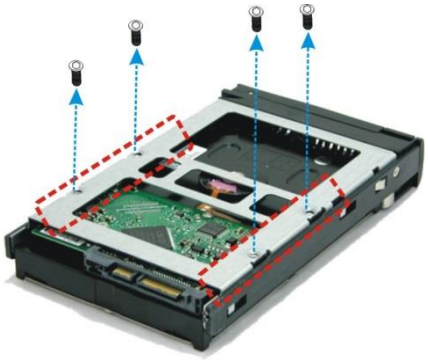
a. Make sure the lock indicator is in unlocked position. To pull out a disk tray, press the carrier open button.



b. Pull out an empty disk tray. Pull the lever handle outwards to remove the carrier from the enclosure.

c. Place the hard drive in the disk tray.

d. Install the mounting screws on the bottom part to secure the drive in the disk tray.



e. Slide the tray into a slot.

f. Close the lever handle until you hear the latch click into place.

Chapter 3 RAID Configuration

The subsystem has a setup configuration utility built in containing important information about the configuration as well as settings for various optional functions in the subsystem. This chapter explains how to use and make changes to the setup utility.

Configuration Methods

There are three methods of configuring the subsystem. You may configure through the following methods:

- VT100 terminal connected through the controller's serial port
- Telnet via the R-Link Ethernet port
- Web browser-based Remote RAID management via the R-Link Ethernet port

IMPORTANT! The subsystem allows you to access the utility using only one method at a time. You cannot use more than one method at the same time.

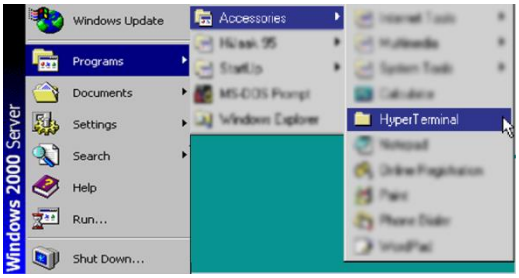
3.1 Configuring Through a Terminal

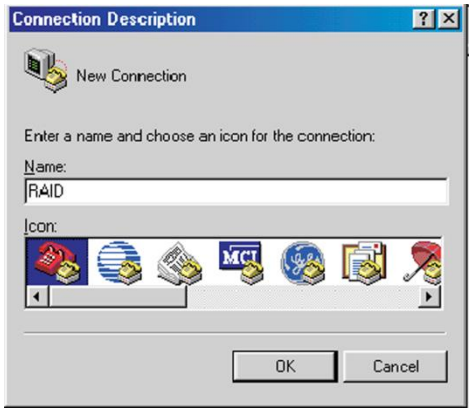
Configuring through a terminal will allow you to use the same configuration options and functions that are available from the LCD panel. To start-up:

1. Connect a VT100 compatible terminal or a PC operating in an equivalent terminal emulation mode to the monitor port located at the rear of the subsystem.

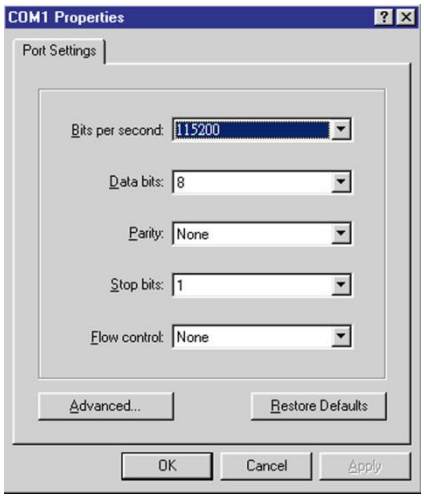
NOTE: You may connect a terminal while the subsystem's power is on.

2. Power-on the terminal.
3. Run the VT100 program or an equivalent terminal program.

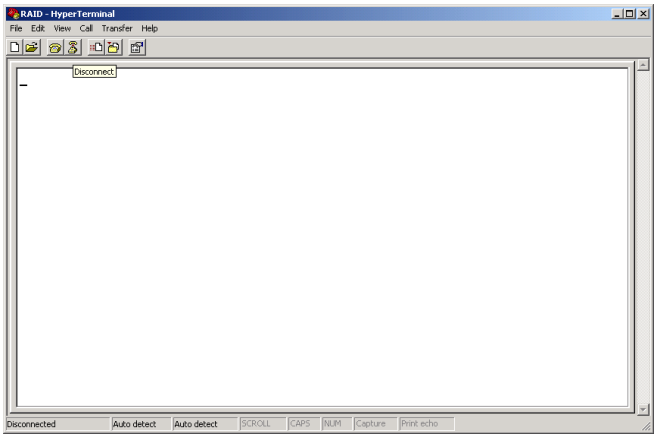




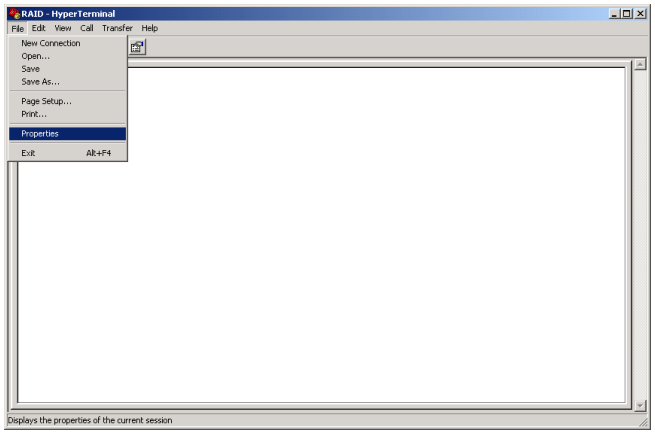
4. The default setting of the monitor port is **115200 baud rate, 8 data bit, non-parity, 1 stop bit** and **no flow control.**



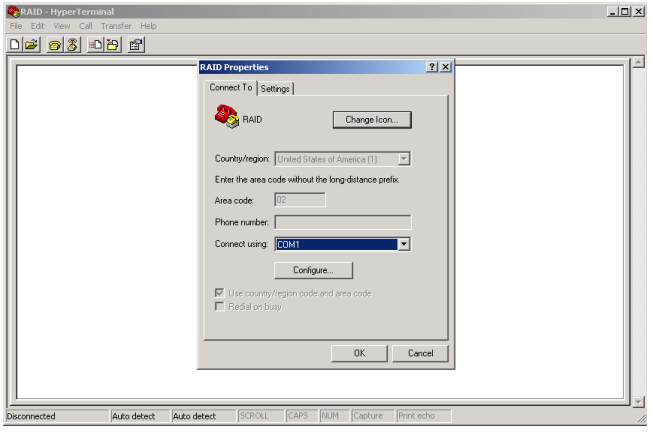
5. Click  disconnect button.



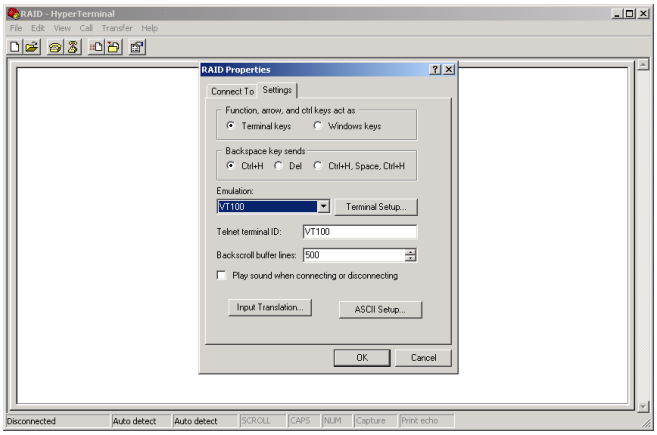
6. Open the File menu, and then open Properties.



7. Open the Settings Tab.

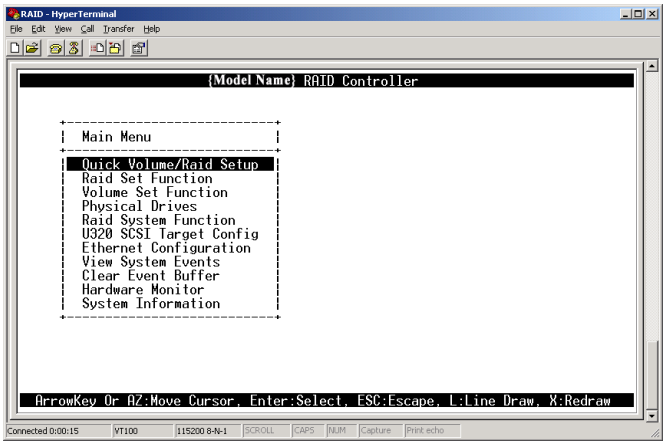


8. Configure the settings are follows:
   "Function, arrow and ctrl keys act as": Terminal Keys
   "Backspace key sends": Crtl + H
   "Emulation": VT100
   "Telnet terminal ID": VT100
   "Back scroll buffer lines": 500
   Click OK.



9. Now, the VT100 is ready to use. After you have finished the VT100 Terminal setup, you may press the "X" key (in your Terminal) to link the RAID subsystem and Terminal together. Press "X" key to display the disk array Monitor Utility screen on your VT100 Terminal.

10. The Main Menu will appear.



Keyboard Function Key Definitions

"A" key - to move to the line above

"Z" key - to move to the next line

"Enter" key - Submit selection function

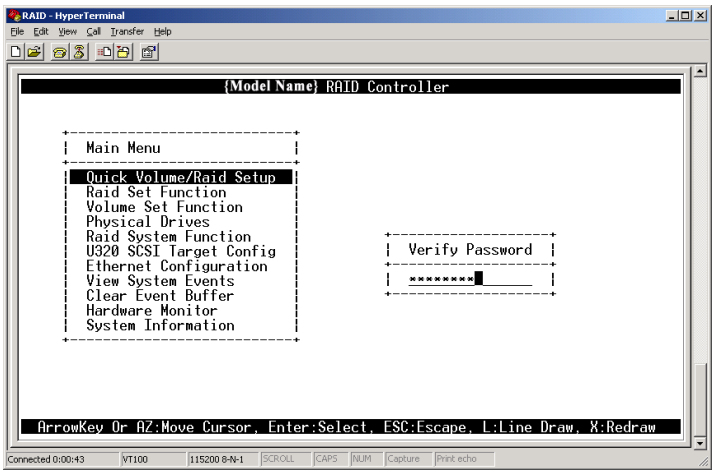
"ESC" key - Return to previous screen

"L" key - Line draw

"X" key – Redraw

3.2 Main Menu

The main menu shows all function that enables the customer to execute actions by clicking on the appropriate link.



NOTE: The password option allows user to set or clear the RAID subsystem's password protection feature. Once the password has been set, the user can only monitor and configure the RAID subsystem by providing the correct password. The password is used to protect the RAID subsystem from unauthorized access. The controller will check the password only when entering the Main menu from the initial screen. The RAID subsystem will automatically go back to the initial screen when it does not receive any command in twenty seconds. The RAID subsystem's factory default password is set to 00000000.

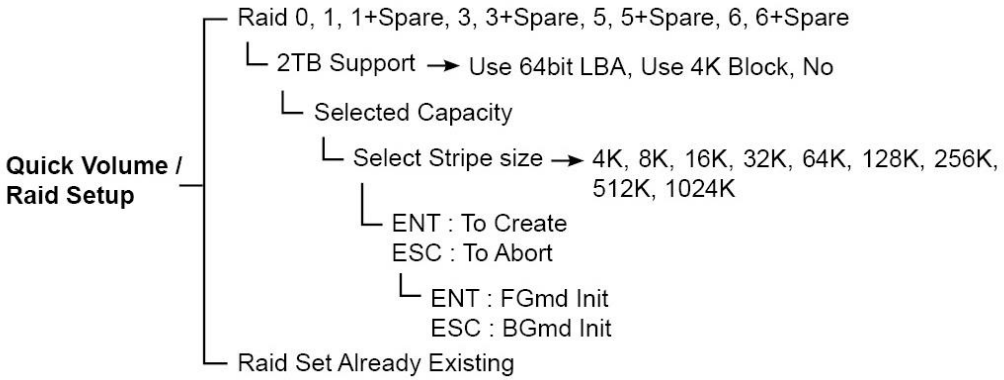
VT100 terminal configuration Utility Main Menu Options

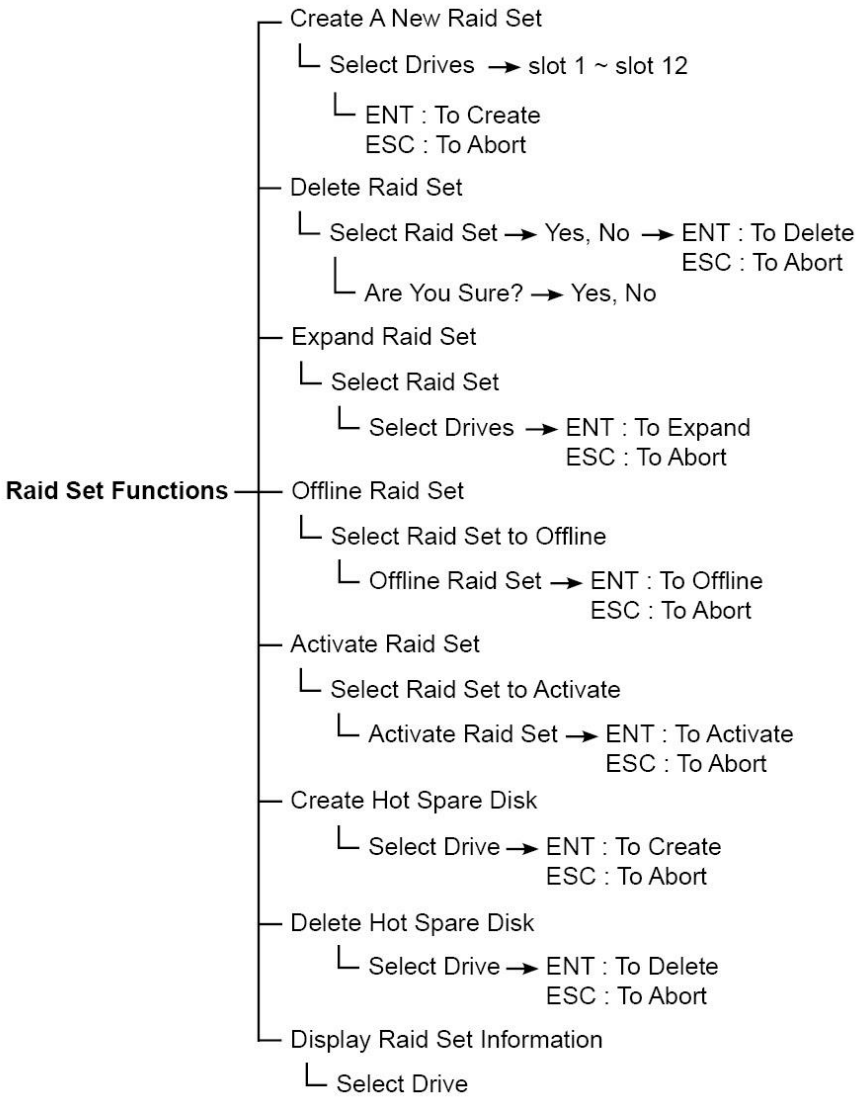
Select an option and the related information or submenu items display beneath it. The submenus for each item are shown in the next Section. The configuration utility main menu options are:

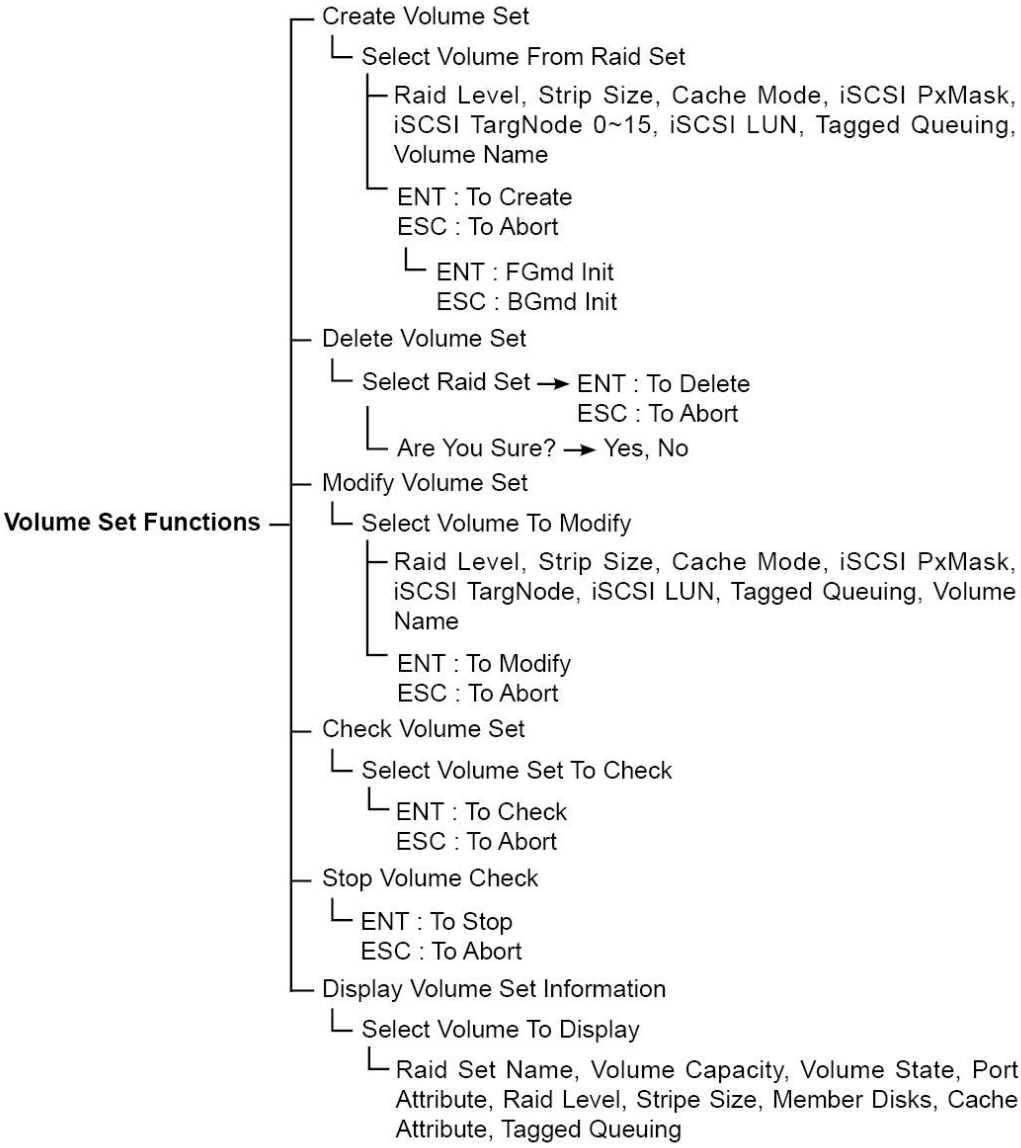
Menu Option	Description
Quick Volume And Raid Set Setup	Create a RAID configuration which consists of all physical disks installed
Raid Set Functions	Create a customized Raid Set
Volume Set Functions	Create a customized Volume Set
Physical Drive Functions	View individual disk information
Raid System Functions	Setting the Raid system configurations
Ethernet Configuration	Setting the Ethernet configurations
Views System Events	Record all system events in the buffer
Clear Event Buffer	Clear all event buffer information
Hardware Monitor	Show all system environment status
System Information	View the controller information

3.3 Menu Diagram

The following tree diagram is a summary of the various configurations and setting functions that can be accessed through the terminal monitor.





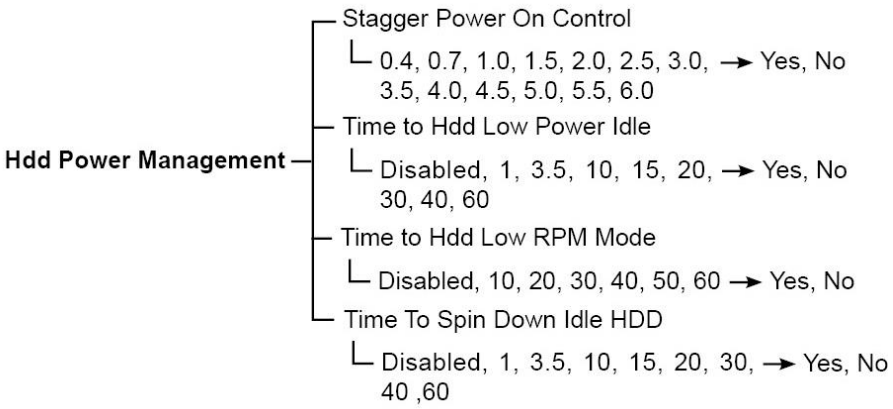

Volume Set Functions
Create Volume Set
Select Volume From Raid Set
Raid Level, Strip Size, Cache Mode, iSCSI PxMask, iSCSI TargNode 0~15, iSCSI LUN, Tagged Queuing, Volume Name
ENT : To Create
ESC : To Abort
ENT : FGmd Init
ESC : BGmd Init
Delete Volume Set
Select Raid Set → ENT : To Delete
ESC : To Abort
Are You Sure? → Yes, No
Modify Volume Set
Select Volume To Modify
Raid Level, Strip Size, Cache Mode, iSCSI PxMask, iSCSI TargNode, iSCSI LUN, Tagged Queuing, Volume Name
ENT : To Modify
ESC : To Abort
Check Volume Set
Select Volume Set To Check
ENT : To Check
ESC : To Abort
Stop Volume Check
ENT : To Stop
ESC : To Abort
Display Volume Set Information
Select Volume To Display
Raid Set Name, Volume Capacity, Volume State, Port Attribute, Raid Level, Stripe Size, Member Disks, Cache Attribute, Tagged Queuing

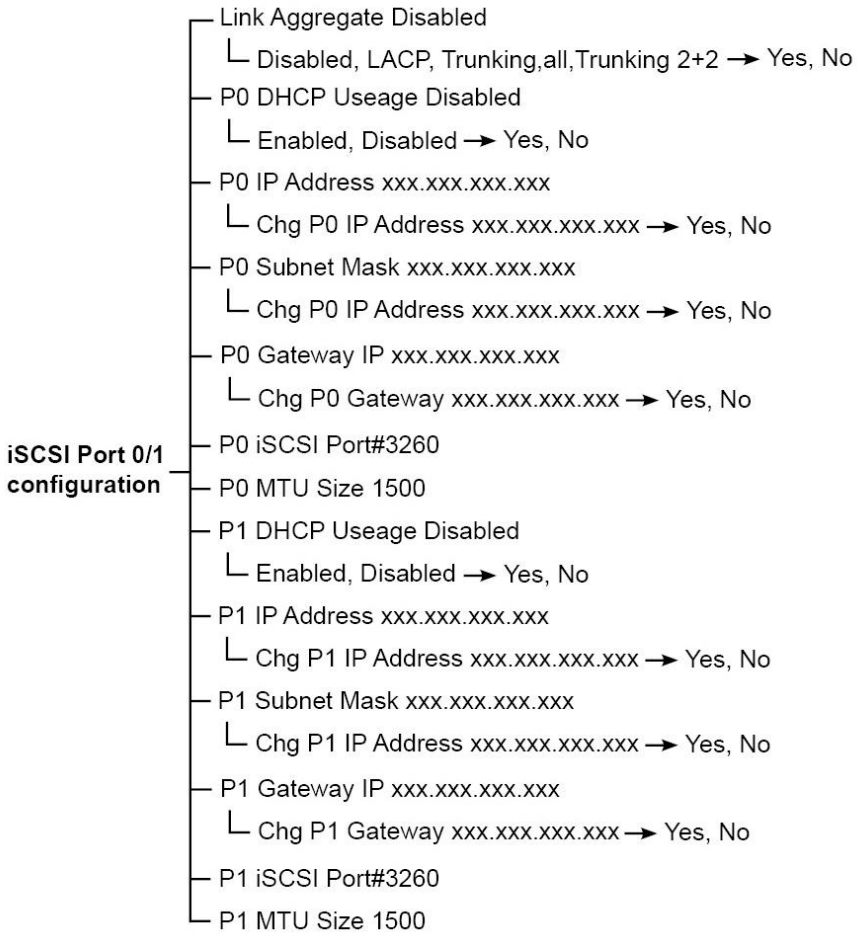
Physical Drive Function

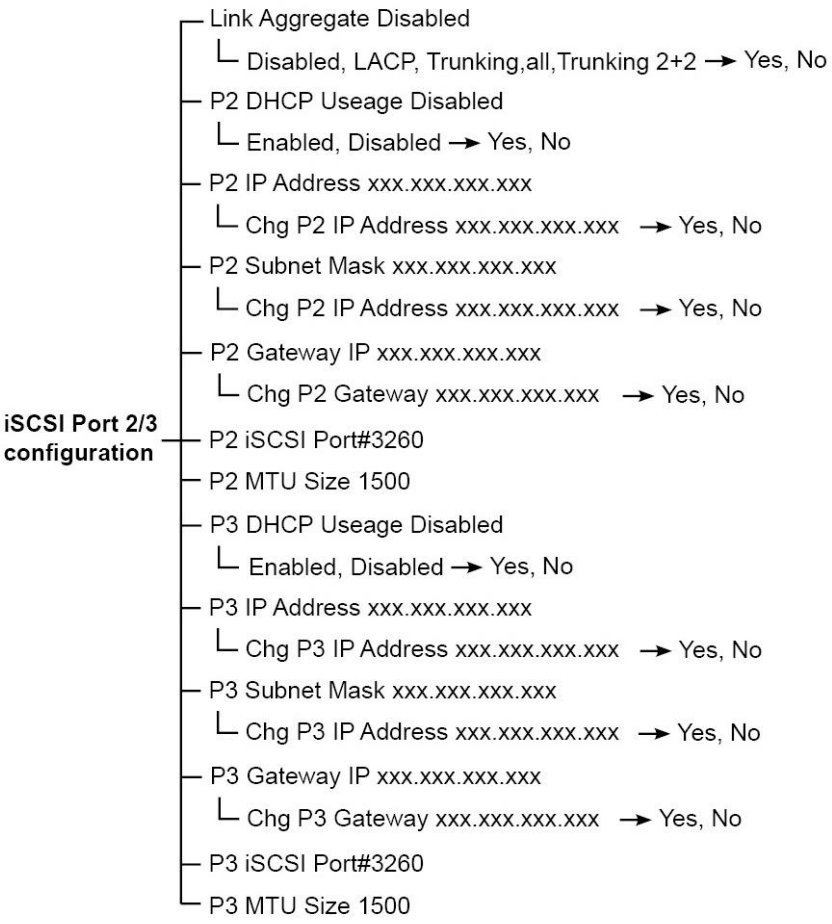
- Display Drive Information
  - Select Drive
    - Model Name, Serial Number, Firmware Rev, Device Capacity, Device State
- Create Pass Through Disk
  - Select Drive
    - Cache Mode, iSCSI PxMask, iSCSI TargNode, iSCSI LUN, Tagged Queuing
      - ENT : To Create
        ESC : To Abort
- Modify Pass Through Disk
  - Select Drive
    - Cache Mode, iSCSI PxMask, iSCSI TargNode, iSCSI LUN, Tagged Queuing
      - ENT : To Modify
        ESC : To Abort
- Delete Pass Through Disk
  - Select Drive E#1slot# 1
    - ENT : To Delete
      ESC : To Abort
- Identify The Selected Device
  - Select Drive E#1slot# 1

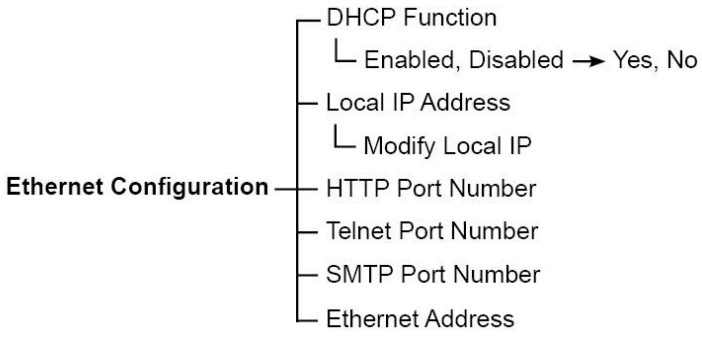
Raid System Function

- Mute The Alert Beeper → Yes, No
- Alert Beeper Setting
  - Save The Settings → Yes, No
- Change Password
  - New Password:_ → Yes, No
- JBOD/RAID Mode Configuration
  - JBOD/RAID Mode → Yes, No
- Raid Rebuild Priority
  - Rebuild Priority → Yes, No
- SATA NCQ Mode Supported
  - Enabled, Disabled → Yes, No
- HDD Read Ahead Cache
  - Enabled, Disabled → Yes, No
- Volume Data Read Ahead
  - Normal, Aggressive, Conservative, Disabled → Yes, No
- Empty HDD slot LED Control
  - On/Off → Yes, No
- Disk Write Cache HDD
  - Auto, Enabled, Disabled → Yes, No
- SATA Target speed
  - 6G/3G → Yes, No
- Disk Capacity & Truncation Mode
  - Cap. Trunc Mode Multiples Of 10G, 1G, No Truncation
    - Yes, No
- Shutdown The Controller
  - Confirm Shutdown → Yes, No
- Restart The Controller
  - Confirm Restart? → Yes, No


Hdd Power Management
Stagger Power On Control
0.4, 0.7, 1.0, 1.5, 2.0, 2.5, 3.0, 3.5, 4.0, 4.5, 5.0, 5.5, 6.0 → Yes, No
Time to Hdd Low Power Idle
Disabled, 1, 3.5, 10, 15, 20, 30, 40, 60 → Yes, No
Time to Hdd Low RPM Mode
Disabled, 10, 20, 30, 40, 50, 60 → Yes, No
Time To Spin Down Idle HDD
Disabled, 1, 3.5, 10, 15, 20, 30, 40 ,60 → Yes, No


iSCSI Port 0/1 configuration
Link Aggregate Disabled
Disabled, LACP, Trunking,all,Trunking 2+2 → Yes, No
P0 DHCP Useage Disabled
Enabled, Disabled → Yes, No
P0 IP Address xxx.xxx.xxx.xxx
Chg P0 IP Address xxx.xxx.xxx.xxx → Yes, No
P0 Subnet Mask xxx.xxx.xxx.xxx
Chg P0 IP Address xxx.xxx.xxx.xxx → Yes, No
P0 Gateway IP xxx.xxx.xxx.xxx
Chg P0 Gateway xxx.xxx.xxx.xxx → Yes, No
P0 iSCSI Port#3260
P0 MTU Size 1500
P1 DHCP Useage Disabled
Enabled, Disabled → Yes, No
P1 IP Address xxx.xxx.xxx.xxx
Chg P1 IP Address xxx.xxx.xxx.xxx → Yes, No
P1 Subnet Mask xxx.xxx.xxx.xxx
Chg P1 IP Address xxx.xxx.xxx.xxx → Yes, No
P1 Gateway IP xxx.xxx.xxx.xxx
Chg P1 Gateway xxx.xxx.xxx.xxx → Yes, No
P1 iSCSI Port#3260
P1 MTU Size 1500





Show System Events — View System Events

Clear All Event Buffer — Clear Event Buffer

→ ENT : To Clear
ESC : To Abort

Hardware Monitor Informaiton — The Hardware Monitor Informaiton

→ CPU Temperature, Controller Temp., 12V, 5V, 3.3V, IO Voltage+1.8V, DDR3+1.5V, CPU+1.05V, SATA Chip+1.0V, CPU VCore+0.9V, RTC+3.0V, Battery Status

Show System Information — The System Information

→ Main Processor, CPU ICache Size, CPU DCache Size, CPU SCache Size, System Memory, Firmware Version, BOOT ROM Version, Serial Number, Unit Serial #, Controller Name, Current IP Addr.

3.4 Web browser-based Remote RAID management via R-Link Port

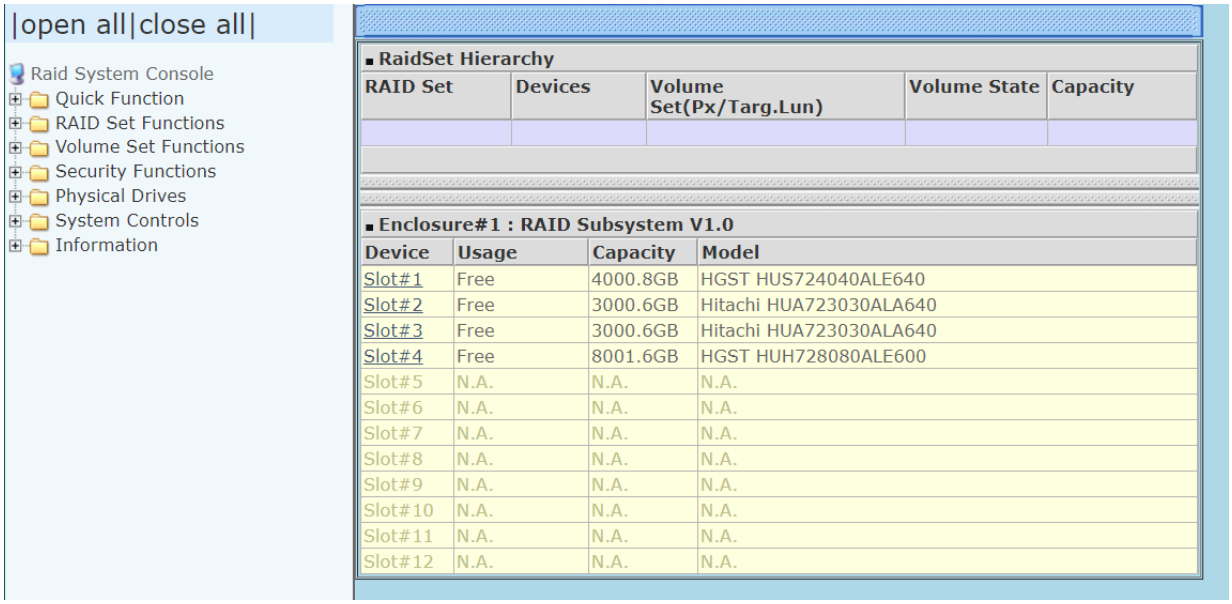
The RAID subsystem can be configured with RAID Manager, a web browser-based application which utilizes the web browser installed on your operating system. The web browser-based RAID Manager can be used to manage all the RAID function.

To configure the RAID subsystem on a remote machine, you need to know its IP Address. Launch your web browser by entering http://[IP Address] in the remote web browser.

IMPORTANT! The default IP address of R-Link Port is 192.168.1.100, and subnet mask is 255.255.255.0. DHCP client function is also enabled by default. You can reconfigure the IP Address or disable the DHCP client function through the LCD front panel or terminal "Ethernet Configuration" menu.

NOTE: If DHCP client function is enabled but a DHCP server is unavailable and the IP address is changed, a Controller Restart is necessary. If the DHCP client function is disabled and the IP address is changed, Controller Restart is not needed.

Note that you must be logged in as administrator with local admin rights on the remote machine to remotely configure it. The RAID subsystem controller default User Name is "admin" and the Password is "00000000".



Main Menu

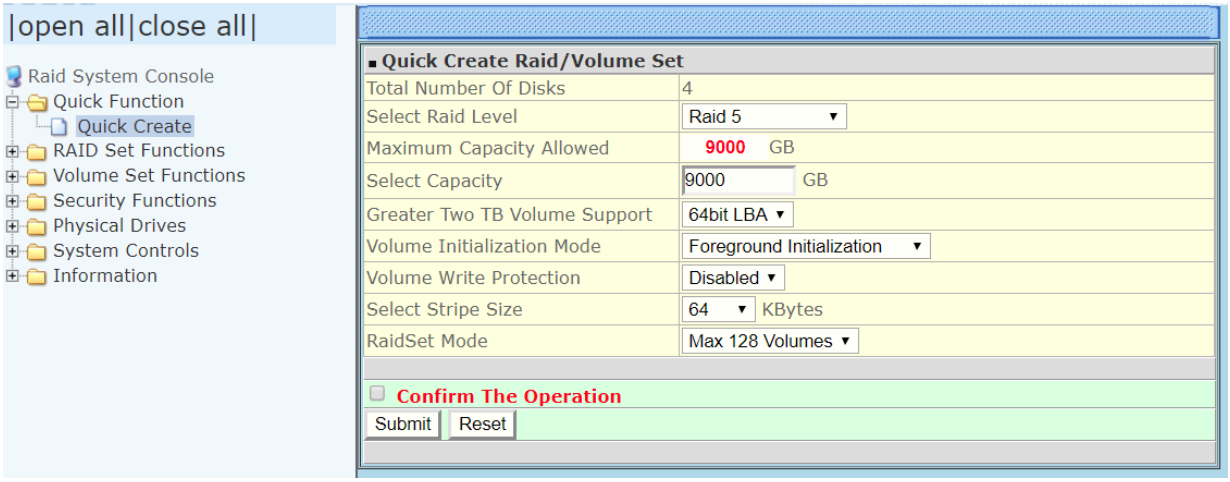
The main menu shows all function that enables the user to execute actions by clicking on the appropriate link.

Individual	Description
Quick Function	Create a RAID configuration, which consists of all physical disks installed. The Volume Set Capacity, Raid Level, and Stripe Size can be modified during setup.
Raid Set Functions	Create customized Raid Sets.
Volume Set Functions	Create customized Volume Sets and allow modification of parameters of existing Volume
Security Functions	Protect Drives with Self-Encrypting Drives (SED) and secure data from unauthorized
Physical Drives	Create pass through disks and allow modification of parameters of existing pass through drives. This also provides a function to identify a respective disk drive.
System Controls	For setting the RAID system configurations.
Information	To view the controller and hardware monitor information. The Raid Set hierarchy can also be viewed through the Raid Set Hierarchy item.

Configuration Procedures

Below are a few practical examples of concrete configuration procedures.

3.5 Quick Create



The number of physical drives in the RAID subsystem determines the RAID levels that can be implemented within the Raid Set. You can create a Raid Set associated with exactly one Volume Set. The user can change the RAID level, Capacity, Volume Initialization Mode and Stripe Size. A hot spare option is also created depending upon the existing configuration. Tick on the **Confirm The Operation** and click on the **Submit** button in the Quick Create screen, the Raid Set and Volume Set will start to initialize.

If the Volume Set size is over 2TB, an option "Greater Two TB Volume Support" will be automatically provided in the screen as shown in the example below. There are three options to select: "No", "64bit LBA", and "4K Block").

Greater Two TB Volume Support:

No: Volume Set capacity is set to maximum 2TB.

64bit LBA: This option use 16 bytes CDB instead of 10 bytes. The maximum volume capacity up to 512TB. For any hard disk drives working in the 4K native mode in the Raid set, the volume set directly sets and exposes 4KB sector size to the operating system. This option works on different OS which supports 16 bytes CDB. Such as: Windows 2003 with SP1 or later / Linux kernel 2.6.x or later.

4K Block: Use this option for Windows OS such as Windows 2000, 2003, or XP. The maximum Volume Set size is 16TB. Just use the Volume as "Basic Disk". Volume can't be used as "Dynamic Disk"; also can't be used in 512Bytes block service program.

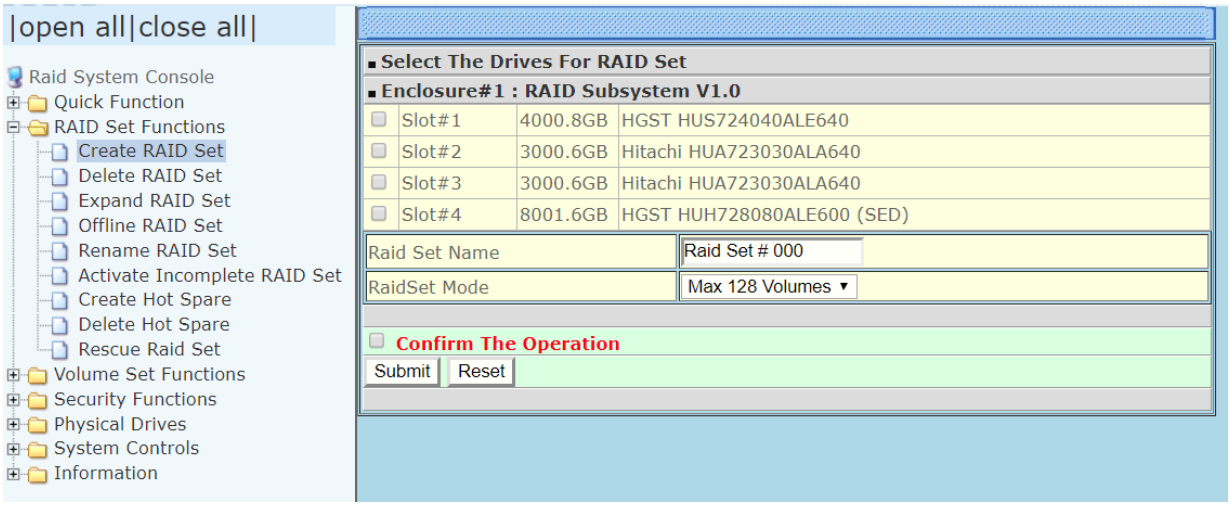
NOTE: In Quick Create, the Raid Set is automatically configured based on the number of disks in your system. Use the Raid Set Function and Volume Set Function if you prefer to customize your Raid Set and Volume Set.

NOTE: In Quick Create, the RAID Level options 30, 50, and 60 are not available. If you need to create Volume Set with RAID Level 30, 50, or 60, use the Create RAID Set function and Create Raid 30/50/60.

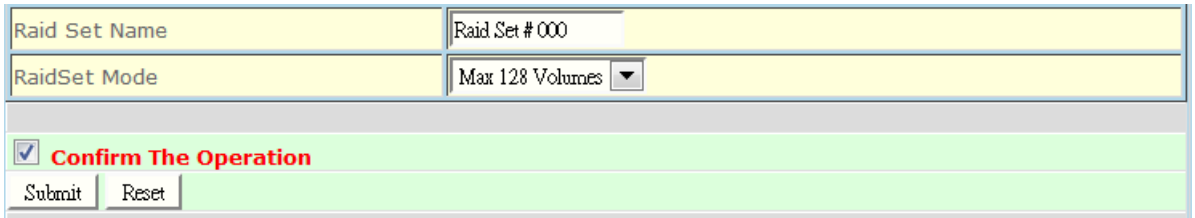
3.6 Raid Set Functions

Use the Raid Set Function and Volume Set Function if you prefer to create customized Raid Sets and Volume Sets. User can manually configure and take full control of the Raid Set settings, but it will take a little longer to setup than the Quick Create configuration. Select the Raid Set Function to manually configure the Raid Set for the first time or to delete existing Raid Set and reconfigure a Raid Set.

3.6.1 Create Raid Set



To create a Raid Set, click on the **Create RAID Set** link. A "Select The Drives For RAID Set" screen is displayed showing the disk drives in the system. Tick the box of each disk drive that will be included in Raid Set to be created. Enter the preferred Raid Set Name (1 to 16 alphanumeric characters) to define a unique identifier for the Raid Set. The default Raid Set name will always appear as **Raid Set # xxx**.



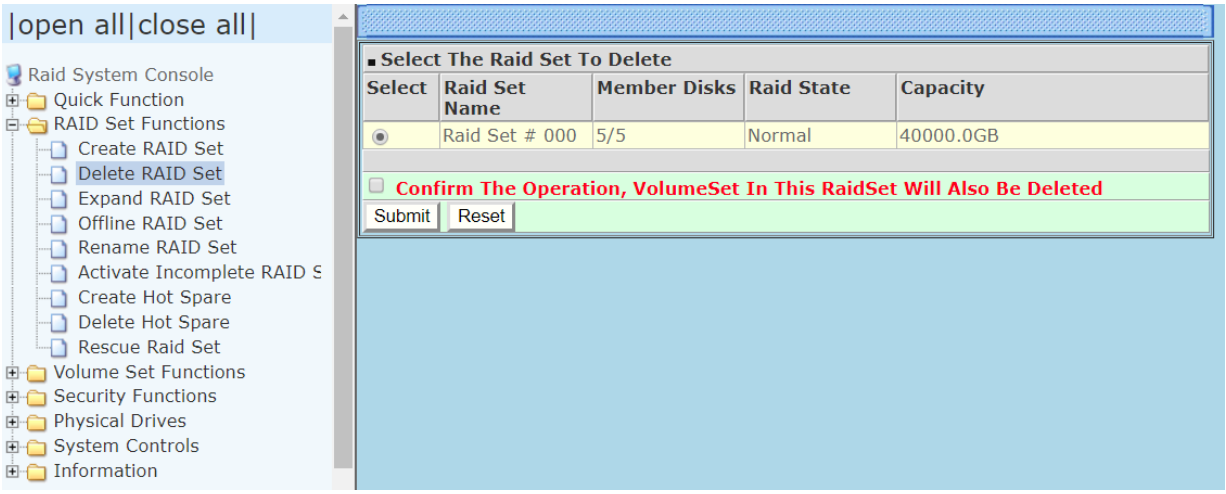
128 volumes is the default mode for SAS RAID controller, the 16 volumes mode is used for support roaming this raidset to SATA RAID controllers. The SATA RAID controller is designed to support up to 16 volumes only. You have to use "Max 16 volumes" on the raidset mode if you plan to roam this raidset between SAS RAID controller and SATA RAID controller.

Tick on the **Confirm The Operation** option and click on the **Submit** button in the screen.

3.6.2 Delete Raid Set

To delete a Raid Set, click on the **Delete Raid Set** link**.** A "Select The RAID SET To Delete" screen is displayed showing all Raid Sets existing in the current subsystem. Check the Raid Set number you want to delete in the Select column.

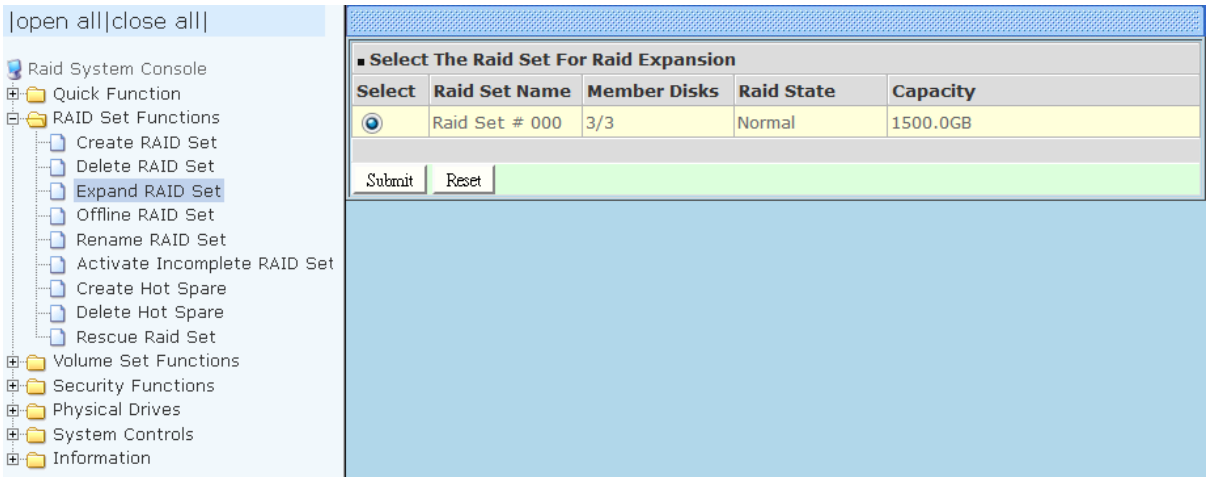
Tick on the **Confirm The Operation** option and click on the **Submit** button to process with deletion.



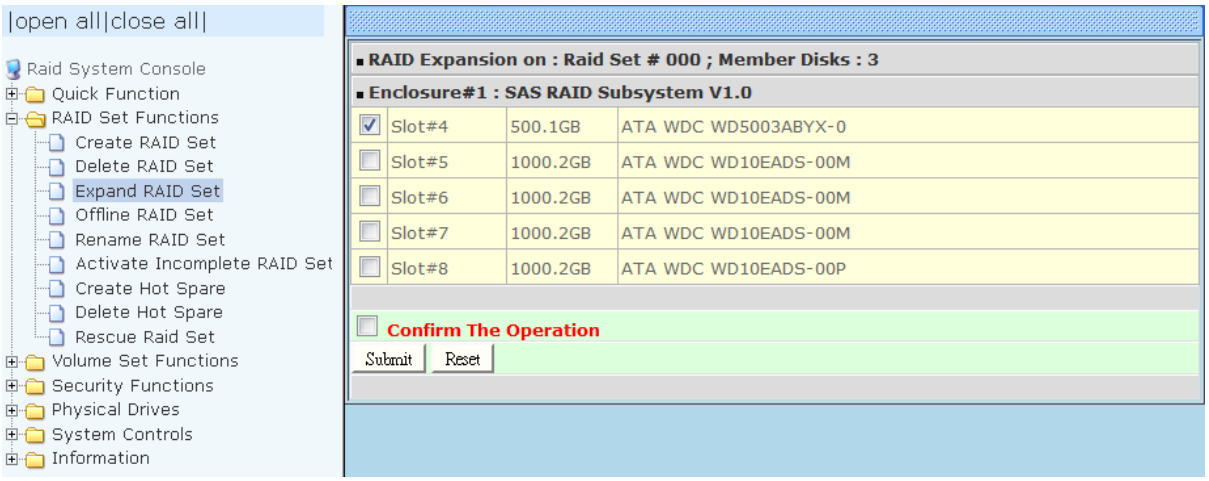
NOTE: You cannot delete a Raid Set containing a Raid 30/50/60 Volume Set. You must delete the Raid 30/50/60 Volume Set first.

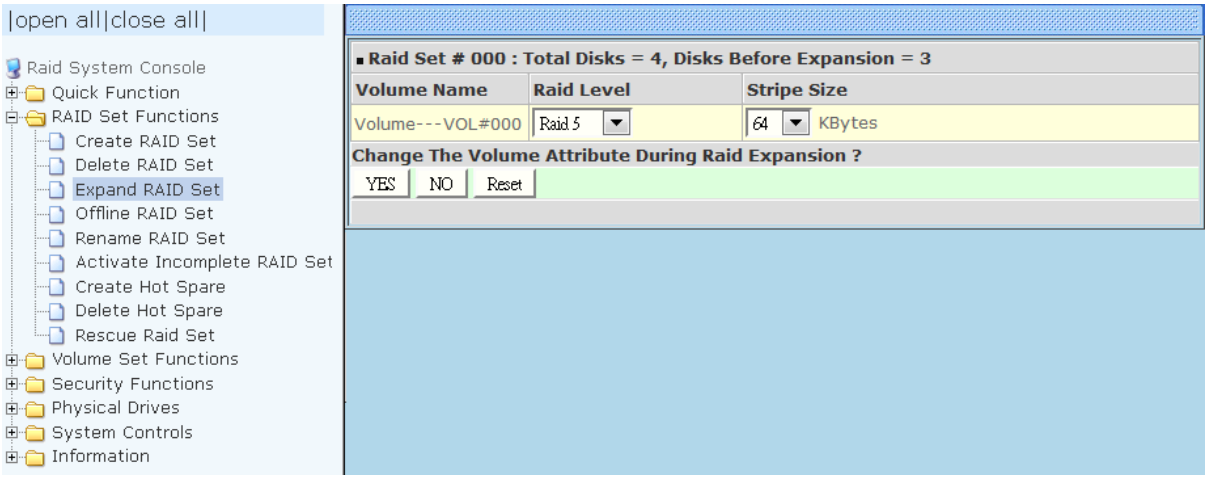
3.6.3 Expand Raid Set

Use this option to expand a Raid Set when one or more disk drives is/are added to the subsystem. This function is active when at least one drive is available.



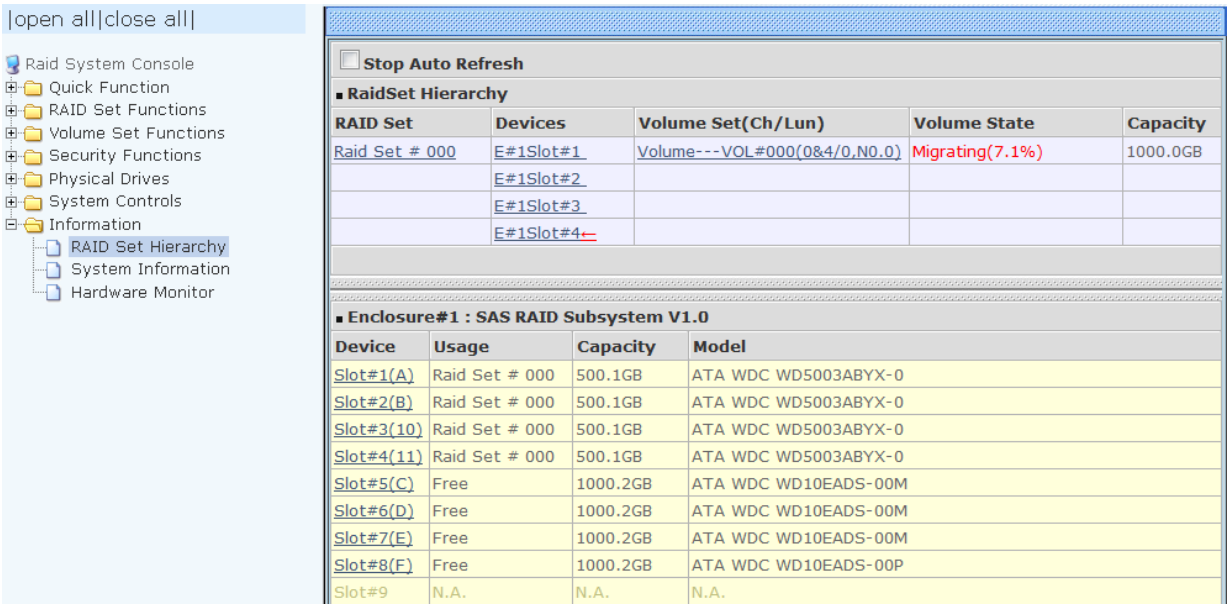
To expand a Raid Set, click on the **Expand Raid Set** link. Select the Raid Set which you want to expand.





Tick on the available disk(s) and check **Confirm The Operation.** Click on the **Submit** button to add the selected disk(s) to the Raid Set.

Migration occurs when a disk is added to a Raid Set. Migrating status is displayed in the Raid Set status area of the Raid Set information. Migrating status is also displayed in the Volume Set status area of the Volume Set Information for all Volume Sets under the Raid Set which is migrating.



The new additional capacity can be utilized by one or more volume sets. The volume sets associated with this RAID set appear for you to have chance to modify RAID level or stripe size. Follow the instruction presented in the "Modify Volume Set" to modify the volume sets; operation system specific utilities may be required to expand operating system partitions.

NOTE: Once the Expand Raid Set process has started, user cannot stop it. The process must be completed.

NOTE: If a disk drive fails during Raid Set expansion and a hot spare is available, an auto rebuild operation will occur after the Raid Set expansion is completed.

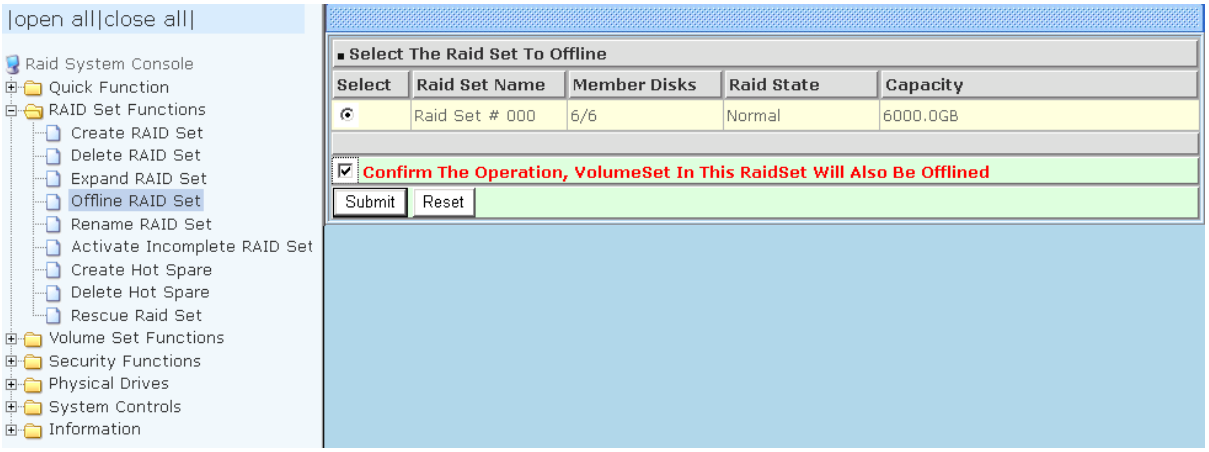
NOTE: A Raid Set cannot be expanded if it contains a Raid 30/50/60 Volume Set.

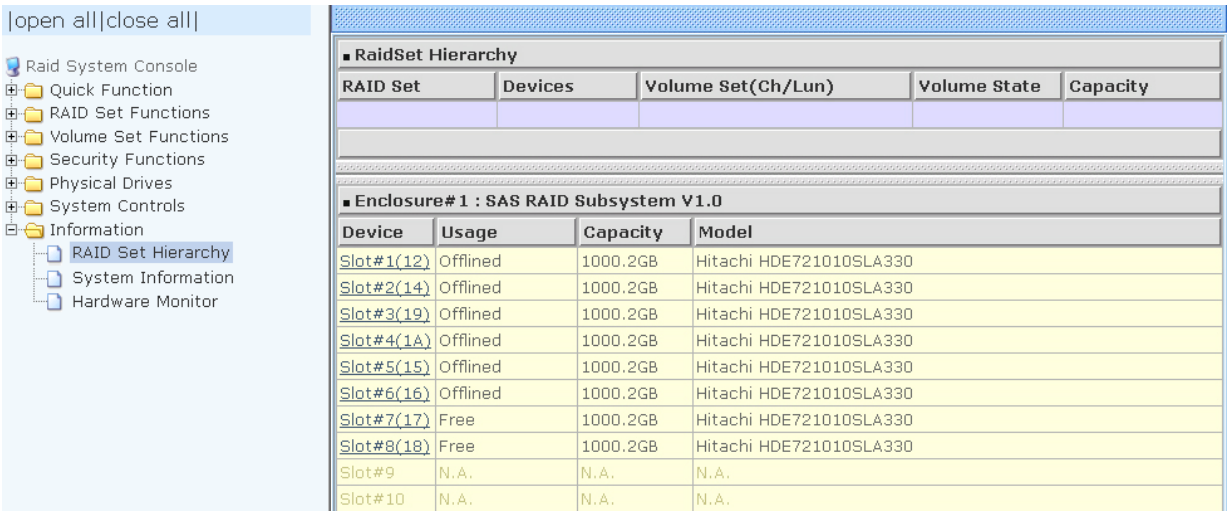
3.6.4 Offline Raid Set

If user wants to offline (and move) a Raid Set while the RAID subsystem is powered on, use the Offline Raid Set function. After completing the function, the HDD state will change to "Offlined" Mode.

To offline a Raid Set, click on the **Offline Raid Set** link**.** A "Select The RAID SET To Offline" screen is displayed showing all existing Raid Sets in the subsystem. Select the Raid Set which you want to offline in the Select column.

Tick on the **Confirm The Operation**, and then click on the **Submit** button to offline the selected Raid Set.

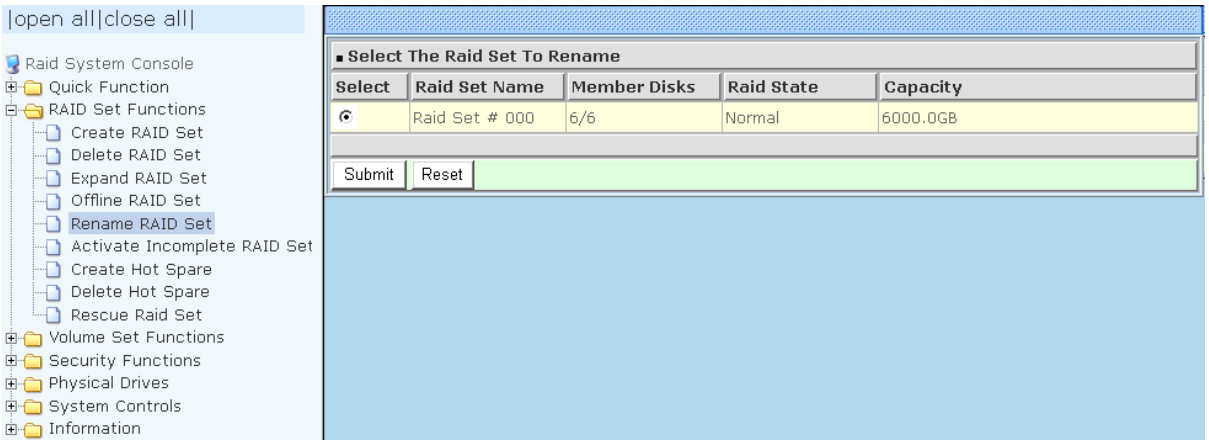




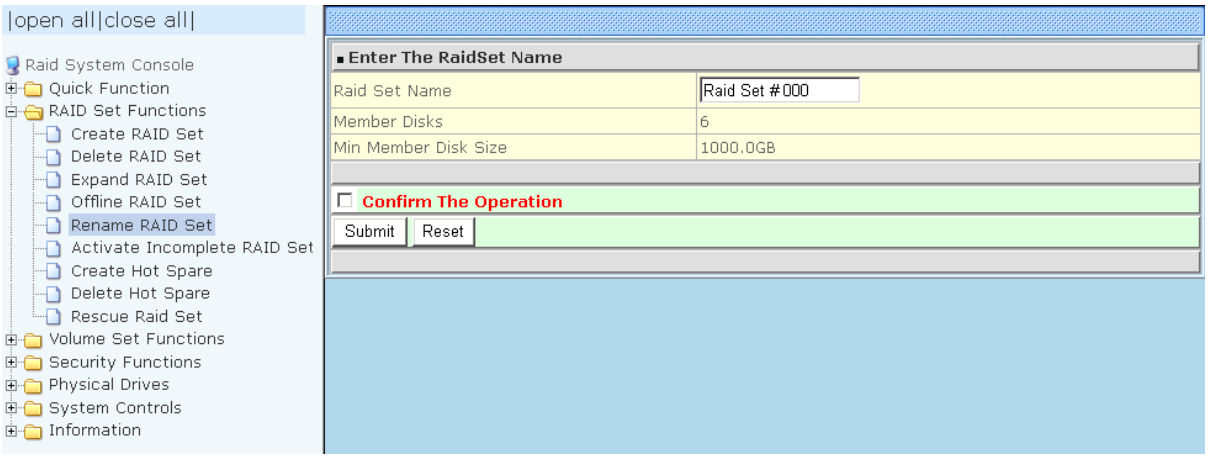
NOTE: After completing the Offline Raid Set Function, all the LEDs of the physical HDDs belonging to this Raid Set will be blinking red.

3.6.5 Rename RAID Set

Use this function to rename a RAID Set. Select the "**Rename RAID Set**" under the RAID Set Functions, and then select the Select the RAID Set to rename and click "**Submit**".



Enter the new name for the RAID Set. Tick the "**Confirm The Operation**" and click "**Submit**".



3.6.6 Activate Incomplete RAID Set

When Raid Set State is "**Normal**", this means there is no failed disk drive.

Raid Set Information	
Raid Set Name	Raid Set # 000
Member Disks	10
Total Raw Capacity	3200.0GB
Free Raw Capacity	756.7GB
Min Member Disk Size	320.0GB
Raid Set Power State	Operating
Raid Set State	Normal

When does "Incomplete" Raid Set State Happens?

If the RAID subsystem is powered off and one disk drive is removed or has failed in power off state, and when the subsystem is powered on, the Raid Set State will change to "**Incomplete**".

Raid Set Information	
Raid Set Name	Raid Set # 000
Member Disks	10
Total Raw Capacity	3200.0GB
Free Raw Capacity	3200.0GB
Min Member Disk Size	320.0GB
Raid Set Power State	Operating
Raid Set State	Incomplete

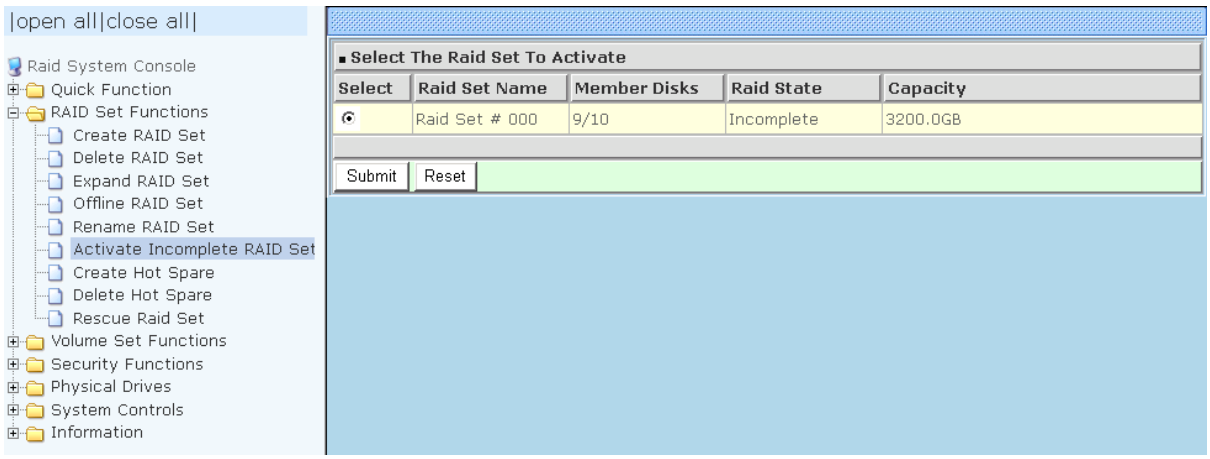
The Volume Set(s) associated with the Raid Set will not be visible and the failed or removed disk will be shown as "**Missing**". At the same time, the subsystem will not detect the Volume Set(s); hence the volume(s) is/are not accessible.

RaidSet Hierarchy				
RAID Set	Devices	Volume Set(Ch/Lun)	Volume State	Capacity
Raid Set # 000	E#1SLOT 01			
	E#1SLOT 02			
	Missing			
	E#1SLOT 04			
	E#1SLOT 05			
	E#1SLOT 06			
	E#1SLOT 07			
	E#1SLOT 08			
	E#1SLOT 09			
	E#1SLOT 10			

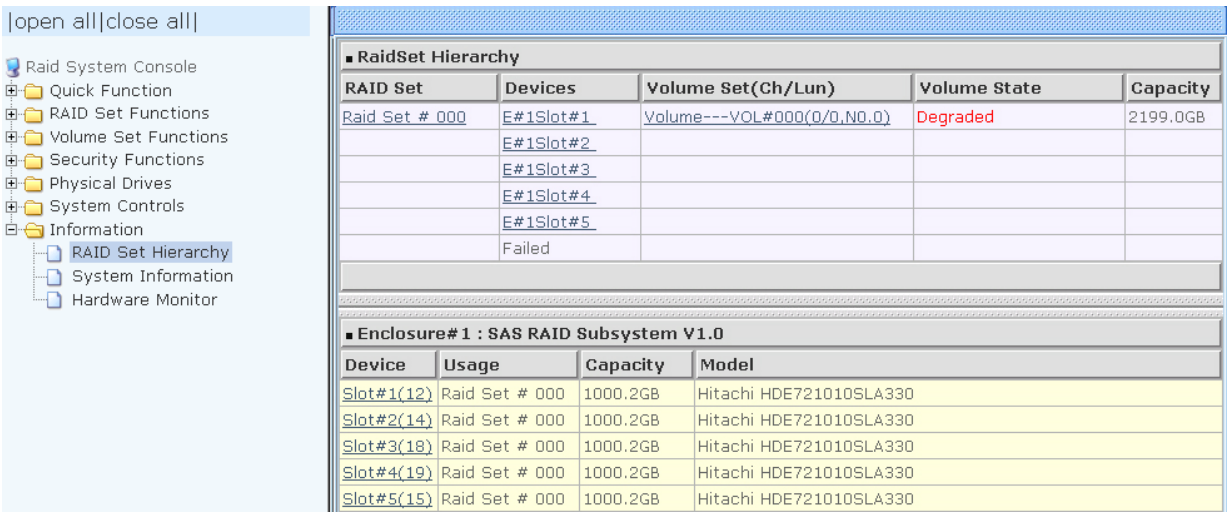
When can the "Activate Incomplete RAID Set" function be used?

In order to access the Volume Set and corresponding data, use the **Activate Incomplete RAID Set** function to active the Raid Set. After selecting this function, the Raid State will change to "**Degraded**" state.

To activate the incomplete the Raid Set, click on the **Activate Incomplete RAID Set** link**.** A "Select The Raid Set To Activate" screen is displayed showing all existing Raid Sets in the subsystem. Select the Raid Set with "**Incomplete**" state which you want to activate in the Select column.



Click on the **Submit** button to activate the Raid Set. The Volume Set(s) associated with the Raid Set will become accessible in "**Degraded**" mode.

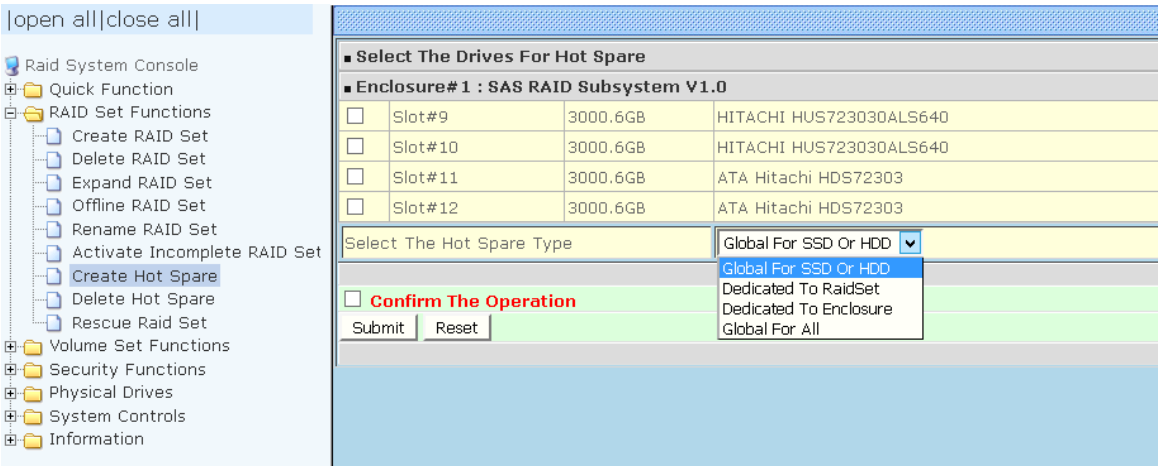


NOTE: The "Activate Incomplete RAID Set" function is only used when Raid Set State is "Incomplete". It cannot be used when Raid Set configuration is lost. In case Raid Set configuration is lost, contact your vendor for support.

3.6.7 Create Hot Spare

The Create Hot Spare option gives you the ability to define a global hot spare.

When you choose the **Create Hot Spare** option in the Raid Set Function, all unused (non Raid Set member) disk drives in the subsystem appear. Select the target disk drive by clicking on the appropriate check box. Select the Hot Spare Type. Tick on the **Confirm The Operation** and click on the **Submit** button to create hot spare drive(s).

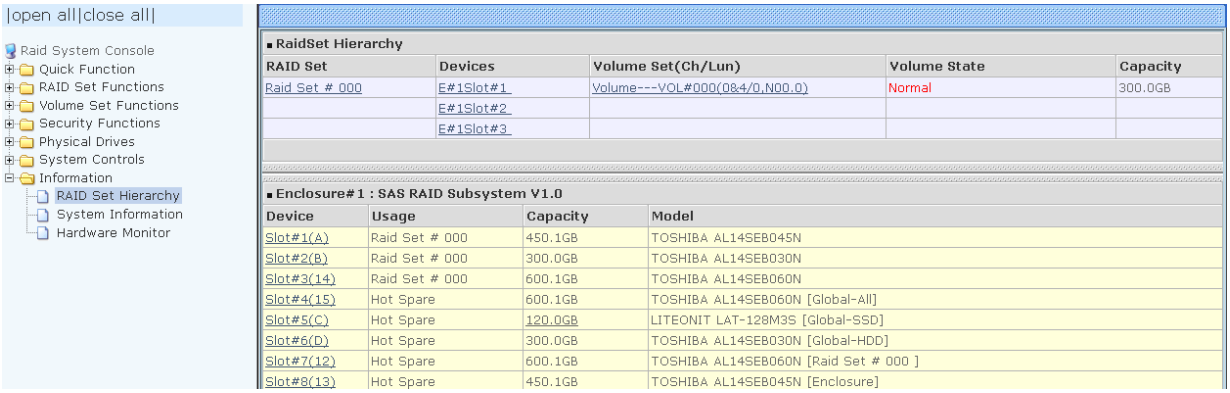


Hot Spare Type	Description
Global For SSD or HDD	If you are mixing SSD and HDD in a system, the Hot Spare SSD is a hot spare only to the SSD. This is to prevent possible drops in performance due to HDD using.
Global Hot Spare	The Hot Spare disk is a hot spare on all enclosures connected in daisy chain. It can replace any failed disk in any enclosure.
Dedicated to RaidSet	The Hot Spare disk is a hot spare dedicated only to the RaidSet where it is assigned. It can replace any failed disk in the RaidSet where it is assigned.
Dedicated to Enclosure	The Hot Spare disk is a hot spare dedicated only to the enclosure where it is located. It can replace any failed disk on the enclosure where it is located. NOTE: When the Raid Set status is in Degraded state, this option will not work.

NOTE: The capacity of the hot spare disk(s) must be equal to or greater than the smallest hard disk size in the subsystem so that it/they can replace any failed disk drive.

NOTE: The Hot Spare Type can also be viewed by clicking on Raid Set Hierarchy in the Information menu.

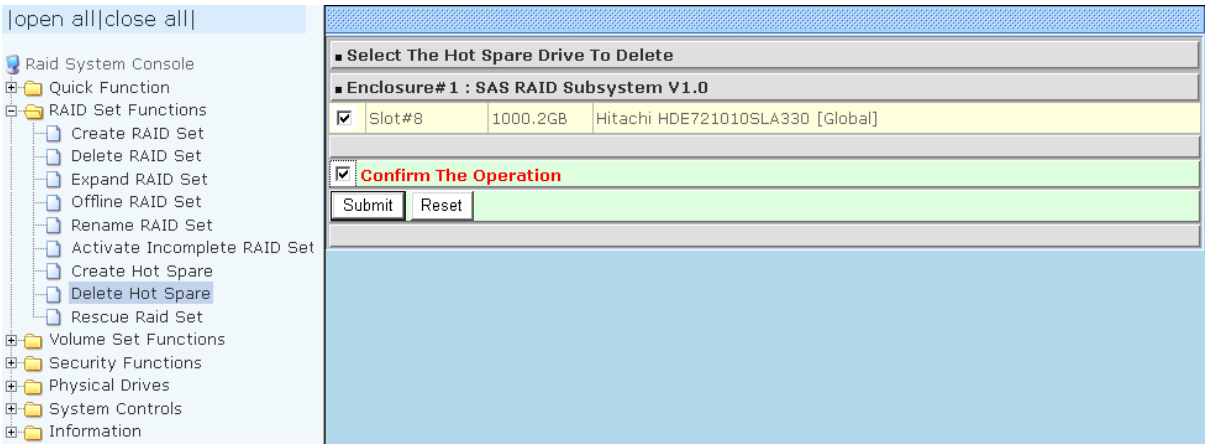
The hot spare type will be indicated in the "Model" area of the "RAID Set Hierarchy" screen. Select the **RAID Set Hierarchy** link from the **Information** menu to display the Raid Set Hierarchy screen.



3.6.8 Delete Hot Spare

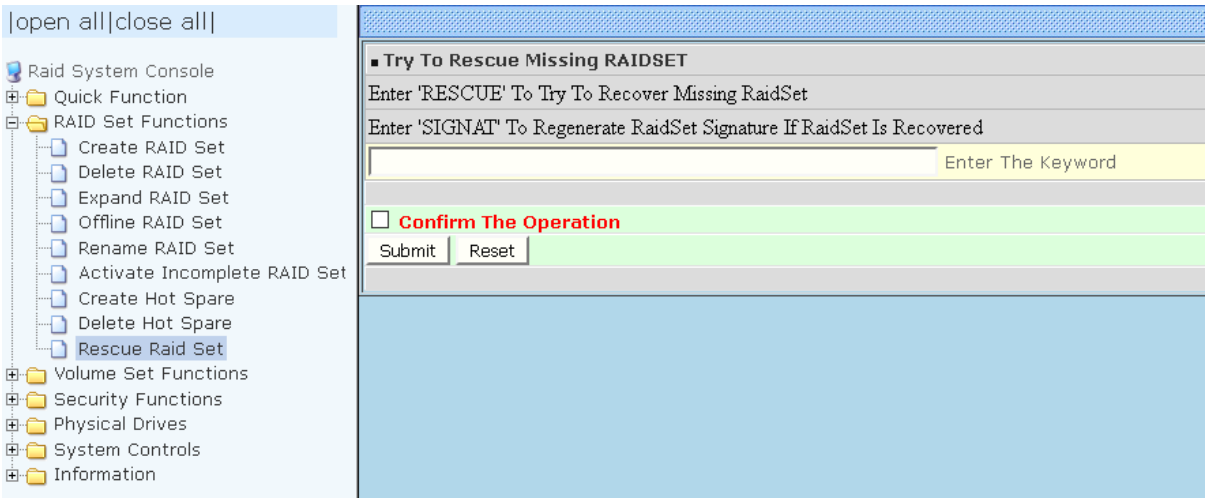
Select the target Hot Spare disk(s) to delete by clicking on the appropriate check box.

Tick on the **Confirm The Operation**, and click on the **Submit** button in the screen to delete the hot spare(s).



3.6.9 Rescue Raid Set

If you need to recover missing Raid Set configuration using the "Rescue Raid Set" function, please contact your vendor's support engineer for assistance.



3.7 Volume Set Function

A Volume Set is seen by the host system as a single logical device. It is organized in a RAID level with one or more physical disks. RAID level refers to the level of data performance and protection of a Volume Set. A Volume Set capacity can consume all or a portion of the raw capacity available in a Raid Set.

Multiple Volume Sets can exist on a group of disks in a Raid Set. Additional Volume Sets created in a specified Raid Set will reside on all the physical disks in the Raid Set. Thus each Volume Set on the Raid Set will have its data spread evenly across all the disks in the Raid Set.

3.7.1 Create Volume Set

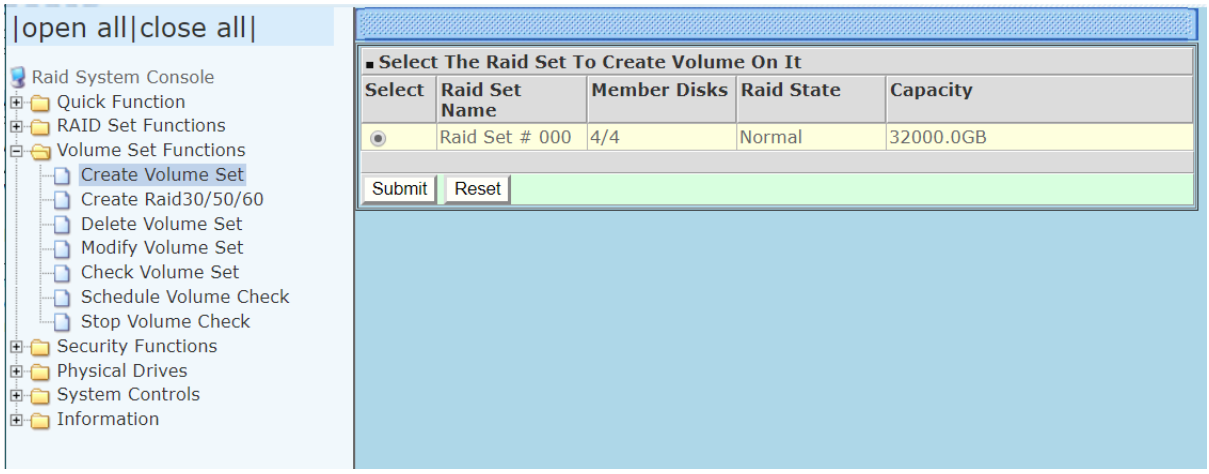
The following are the Volume Set features:

1. Volume sets of different RAID levels may coexist on the same Raid Set.

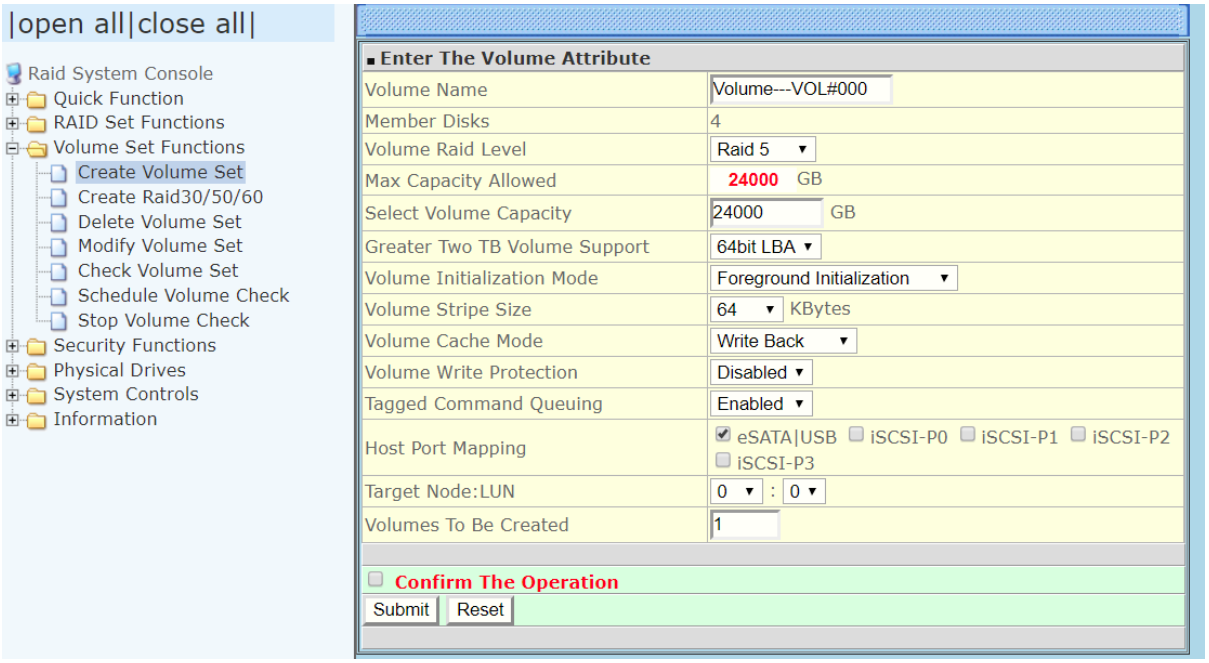
2. Up to 128 Volume Sets in a Raid Set can be created by the RAID controller.

3. The maximum addressable size of a single volume set is not lim ited to 2TB, because the controller is capable of 64-bit LBA mode. However the operating system itself may not be capable of addressing more than 2TB.

To create Volume Set from a Raid Set, expand the Volume Set Functions in the main menu and click on the **Create Volume Set** link. The **Select The Raid Set To Create On It** screen will show all existing Raid Sets. Tick on the Raid Set where you want to create the Volume Set and then click on the **Submit** button.



The Volume Set setup screen allows user to configure the Volume Name, Capacity, RAID level, Initialization Mode, Stripe Size, Cache Mode, Tagged Command Queuing, Host Port Mapping, Target Node:LUN, and Volume To Be Created.



Volume Name:
The default Volume Set name will always appear as Volume---VOL#00. You can rename the Volume Set name provided it does not exceed the 16 characters limit.

Raid Level:
Set the RAID level for the Volume Set. Click the down-arrow in the drop-down list. The available RAID levels for the current Volume Set are displayed. Select the preferred RAID level.

Capacity:
The maximum Volume Set size is displayed by default. If necessary, change the Volume Set size appropriate for your application.

Greater Two TB Volume Support:
If the Volume Set size is over 2TB, an option "Greater Two TB Volume Support" will be automatically provided in the screen as shown in the example above. There are three options to select: "No", "64bit LBA", and "4K Block").

No: Volume Set size is set to maximum 2TB limitation.

64bit LBA: This option use 16 bytes CDB instead of 10 bytes. The maximum volume capacity up to 512TB. For any hard disk drives working in the 4K native mode in the Raid set, the volume set directly sets and exposes 4KB sector size to the operating system. This option works on different OS which supports 16 bytes CDB. Such as: Windows 2003 with SP1 or later / Linux kernel 2.6.x or later.

4K Block: Use this option for Windows OS such as Windows 2000, 2003, or XP. The maximum Volume Set size is 16TB. Just use the Volume as "Basic Disk". Volume can't be used as "Dynamic Disk"; also can't be used in 512Bytes block service program.

Initialization Mode:
Set the Initialization Mode for the Volume Set. Initialization in Foreground mode is completed faster but must be completed before Volume Set becomes accessible. Background mode makes the Volume Set instantly available but the initialization process takes longer. No Init (To Rescue Volume) is used to create a Volume Set without initialization; normally used to recreate Volume Set configuration to recover data.

Stripe Size:
This parameter sets the size of the stripe written to each disk in a RAID 0, 1, 10(1E), 5, 6, 50 or 60 logical drive. You can set the stripe size to 4 KB, 8 KB, 16 KB, 32 KB, 64 KB, 128 KB, 256 KB, 512 KB, or 1024 KB.

A larger Stripe Size produces better read performance, especially if the host server does mostly sequential reads. However, if you are sure that the host server does random reads more often, select a small Stripe Size.

NOTE: Stripe Size in RAID level 3 can't be modified.

Cache Mode:

The RAID subsystem supports two types of write caching: Write-Through and Write-Back.

Write-Through: data are both written to the cache and the disk(s) before the write I/O is acknowledged as complete.

Write-Back: when data is written to cache, the I/O is acknowledged as complete, and some time later, the cached data is written or flushed to the disk(s). This provides better performance but requires a battery module support for the cache memory, or a UPS for the subsystem.

Volume Write Protection:

When "Volume Write Protection" is enabled on the "Create Volume Set", host commands fail if they are issued to a volume in that RAID controller and attempt to modify a volume's data or attributes. Volume Write Protection is used primarily for customer-initiated disaster recovery testing.

Tagged Command Queuing:

When this option is enabled, it enhances the overall system performance under multi-tasking operating systems by reordering tasks or requests in the command queue of the RAID system.

Tagged Command Queuing (TCQ) is a technology built into SAS hard drives. It allows the RAID controller to send multiple read and write requests to a hard drive. This function should normally remain "Enabled". "Disabled" this function only when using SATA drives that do not support command tag queuing.

Host Port Mapping & Target Node:LUN

There are three kinds of host interface connected to two internal channels for each volume. Different host interface can map and access to the same volume. But user can only write multiple hosts' volume through one host each time for data consistency.

eSATA/USB Host:

You can add both interfaces (eSATA & USB 3.0) connected to the host, but you can only use one connection at a time. Interface that is connected 1st has precedent.

eSATA: The eSATA lll host channel can access the volume set.

USB: The USB 3.0 host channel can access the volume set.
The following table is the map of host mapping, host interface and driver number assignment.

Host Port Mapping	Host	Target Node:LUN
eSATA / USB	eSATA	eSATA Host with Port Multiplier: Target Node=0~7/LUN=0
		eSATA Host without Port Multiplier: Target Node=0/LUN=0
	USB 3.0	Target Node=0~7/LUN=0

Target Node: Each SATA device attached to RAID controller must be assigned a unique ID number. A eSATA/USB 3.0 host port can connect up to 8 (Target Node=0~7:LUN=0) volume sets.

LUN: Each iSCSI Target Node can support up to 8 LUNs. The RAID controller treats each Target Node:LUN like an SATA disk.

iSCSI-P0/P1/P2/P3 Host:

iSCSI: The iSCSI host channel can access to the volume set.

The following table is the map of host mapping, host interface and driver number assignment.

Host Port Mapping	Host	Target Node:LUN
iSCSI-P0/P1/P2/P3	GbE P0~P3	Target Node=0~15/LUN=0~7

Target Node: A iSCSI host RAID controller can connect up to 16 Target Nodes. The iSCSI RAID controller is as a large SATA devices. You should assign a Target Node from a list of Target Nodes. A iSCSI channel can connect up to 128(16 Target Node * 8 LUN) volumes. Up to 128 volumes can support on each RAID controller.

LUN: Each Target Node can support up to 8 LUNs. The RAID controller treats each Target:LUN like a SATA disk.

Multiple Host:

Dual host channels can be applied to the same drive number volume. But user can only use one channel each time for data consistency.

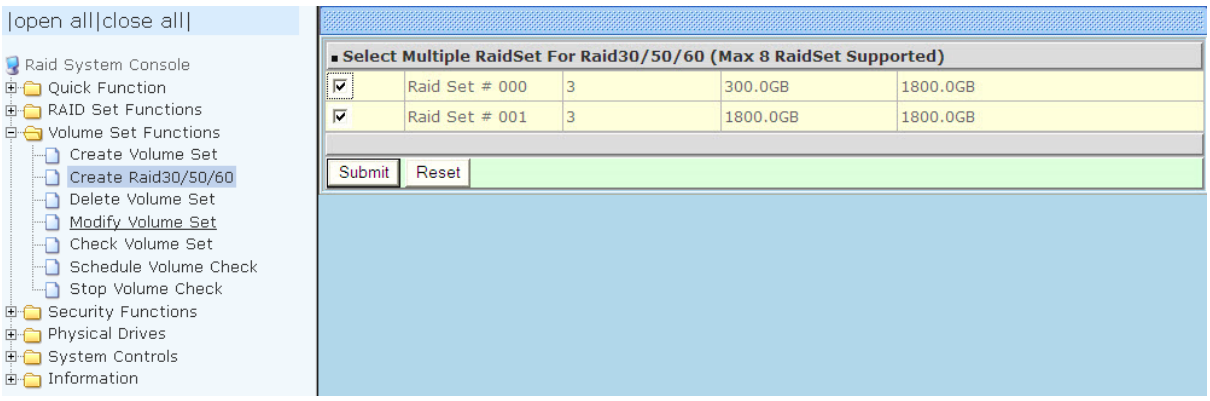
The following table is the map of host mapping, host interface and driver number assignment.

Host Port Mapping	Host	Target Node:LUN
eSATA / USB & iSCSI-P0~P3	eSATA & GbE P0~P3	eSATA Host with Port Multiplier:Target Node=0~7/LUN=0
		eSATA Host without Port Multiplier:Target Node=0/LUN=0
	USB 3.0 & GbE P0~P3	Target Node=0~7/LUN=0

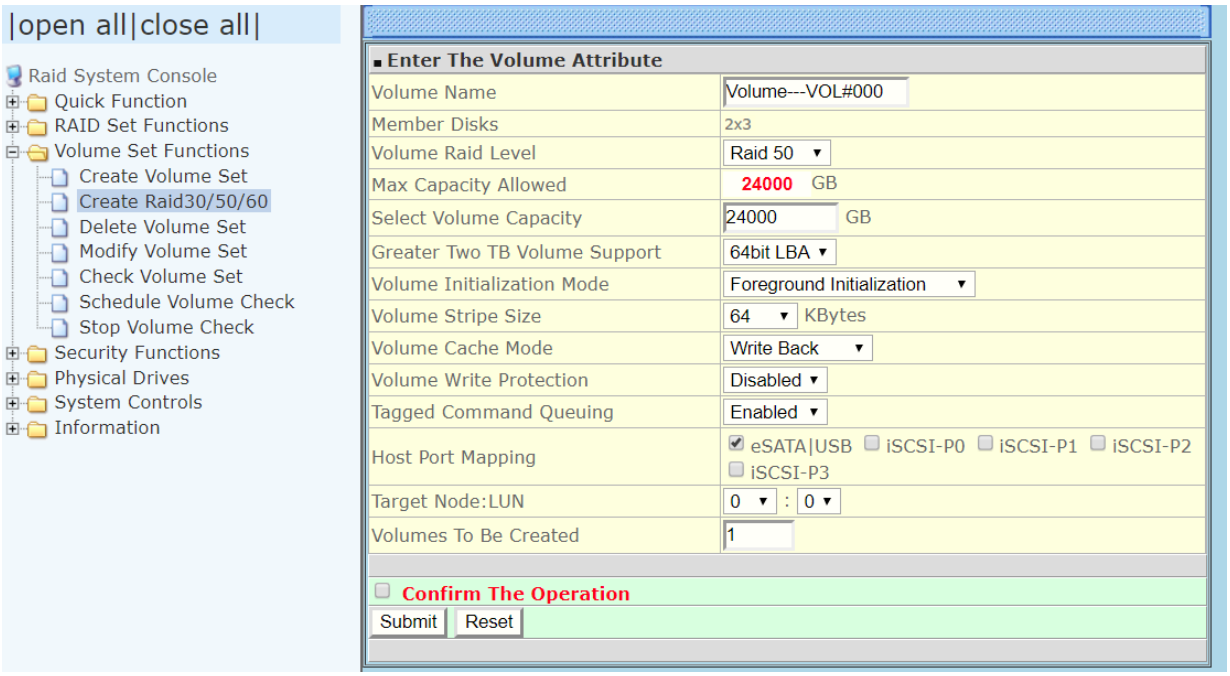
3.7.2 Create Raid 30/50/60

To create a Raid30/50/60 Volume Set, move the mouse cursor to the main menu and click on the **Create Raid30/50/60** link. The **Select Multiple RaidSet For Raid30/50/60** screen will show all Raid Sets. Tick on the Raid Sets that you want to include in the creation and then click on the **Submit** button.

NOTE: Maximum of 8 Raid Sets is supported. All Raid Sets must contain the same number of disk drives.



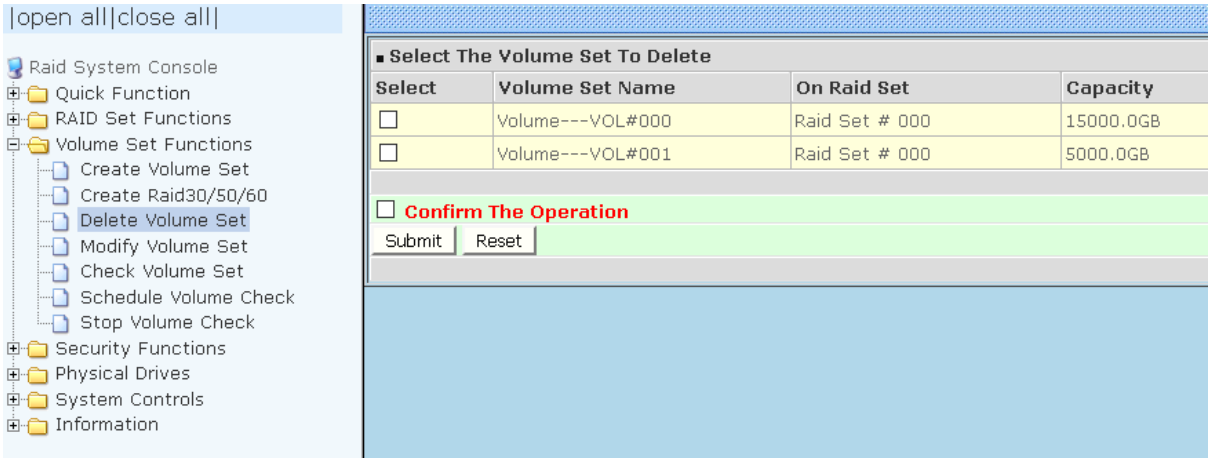
Configure the Volume Set attributes (refer to previous section for the Volume Set attributes). When done, tick **Confirm The Operation** and click on **Submit** button.



NOTE: Refer to Section 3.7.1 Create Volume Set for detailed information about the Volume Set settings.

3.7.3 Delete Volume Set

To delete a Volume Set, select the Volume Set Functions in the main menu and click on the **Delete Volume Set** link. The **Select The Volume Set To Delete** screen will show all available Raid Sets. Tick on a Raid Set and check the **Confirm The Operation** option and then click on the **Submit** button to show all Volume Sets in the selected Raid Set. Tick on a Volume Set and check the **Confirm The Operation** option. Click on the **Submit** button to delete the Volume Set.



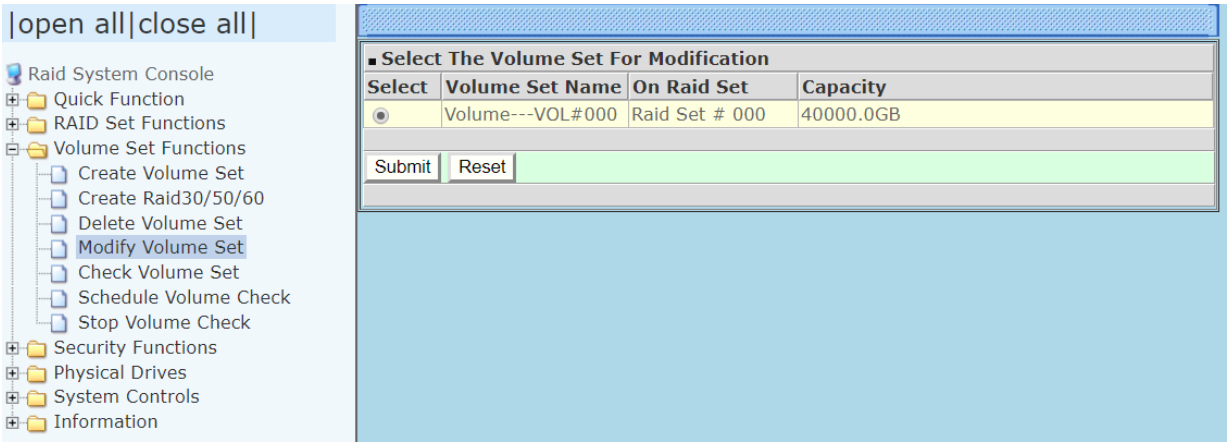
3.7.4 Modify Volume Set

Use this function to modify Volume Set configuration.

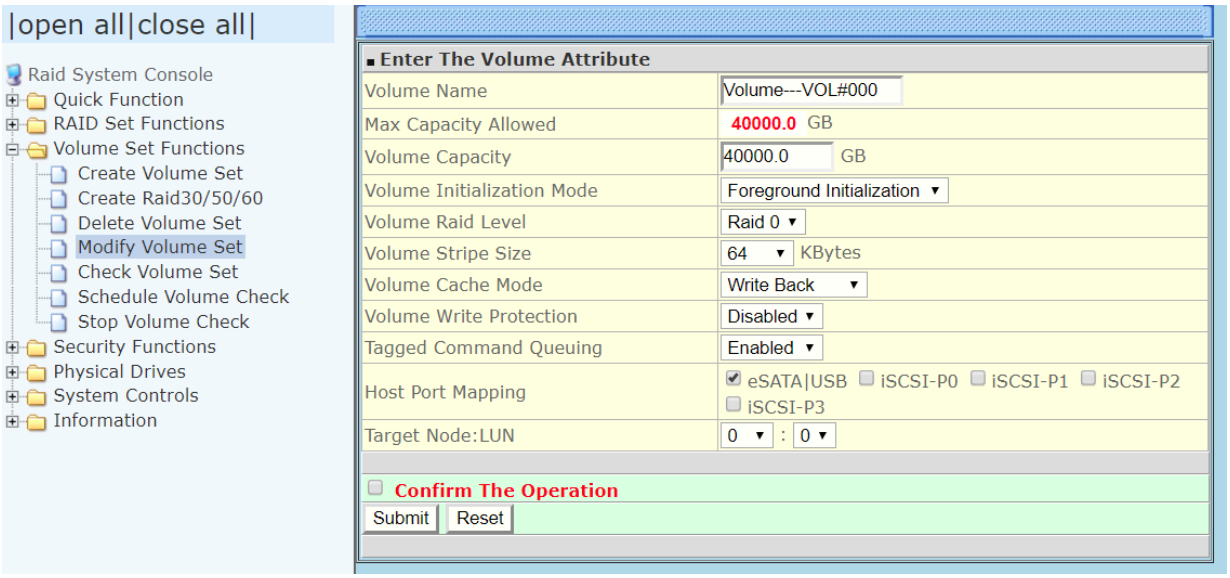
To modify the attributes of a Volume Set:

1. Click on the **Modify Volume Set** link.
2. Tick from the list the Volume Set you want to modify. Click on the **Submit** button.

The following screen appears.



To modify Volume Set attribute values, select an attribute item and click on the attribute value. After completing the modification, tick on the **Confirm The Operation** option and click on the **Submit** button to save the changes.



3.7.4.1 Volume Expansion

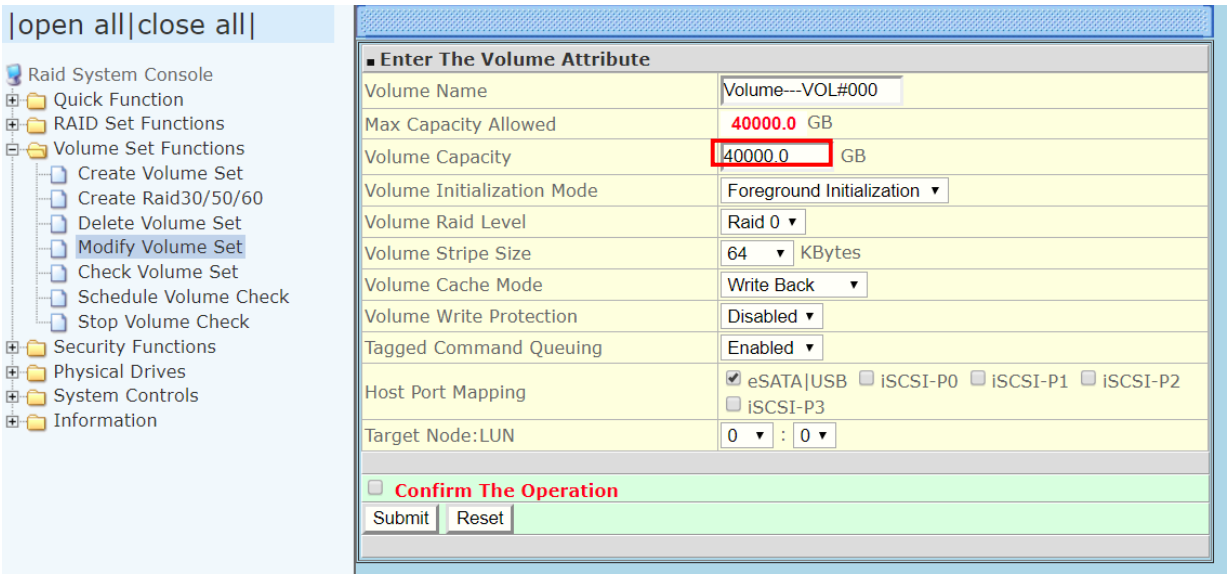
Volume Capacity (Logical Volume Concatenation Plus Re-stripe)

Use the Expand Raid Set function to expand a Raid Set when a disk is added to your subsystem. (Refer to Section 3.6.3)

The expanded capacity can be used to enlarge the Volume Set size or create another Volume Set. Use the Modify Volume Set function to expand the Volume Set capacity. Select the Volume Set and move the cursor to the **Volume Set Capacity** item and enter the capacity size.

Tick on the **Confirm The Operation** and click on the **Submit** button to complete the action. The Volume Set starts to expand.

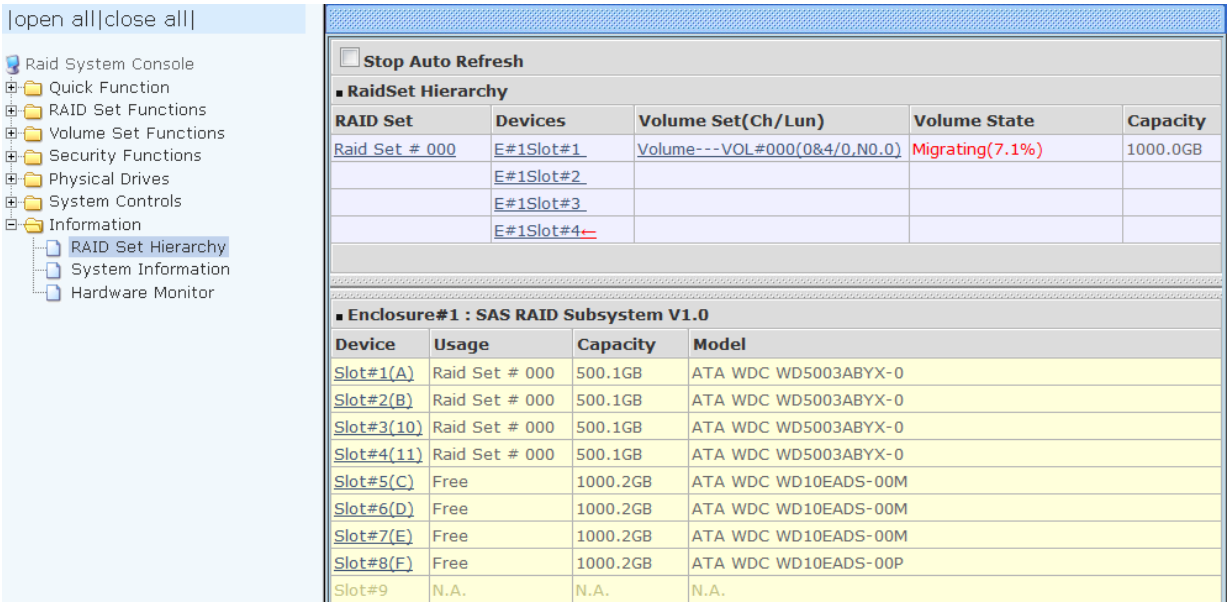
NOTE: The Volume Set capacity of RAID30/50/60 cannot be expanded.



3.7.4.2 Volume Set Migration

Migration occurs when a Volume Set migrates from one RAID level to another, a Volume Set stripe size changes, or when a disk is added to a Raid Set. Migrating status is displayed in the Volume Set status area of the RaidSet Hierarchy screen during migration.

NOTE: The Stripe Size of a Raid30/50/60 Volume Set cannot be modified.



3.7.5 Check Volume Set

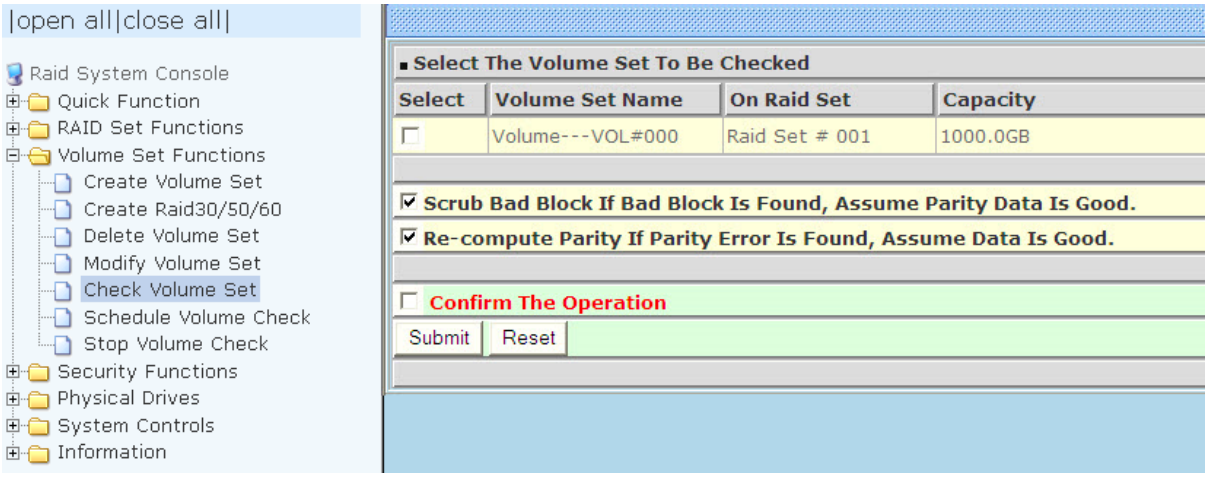
Use this function to perform Volume Set consistency check, which verifies the correctness of redundant data (data blocks and parity blocks) in a Volume Set. This basically means computing the parity from the data blocks and comparing the results to the contents of the parity blocks, or computing the data from the parity blocks and comparing the results to the contents of the data blocks.

NOTE: The Volume Set state must be Normal in order to perform Check Volume Set. Only RAID levels with parity (redundant data) such as RAID Levels 3, 5, 6, 30, 50 and 60, support this function.

To perform Check Volume Set function:

1. Click on the **Check Volume Set** link.

2. Tick from the list the Volume Set you want to check. Select the Check Volume Set options.



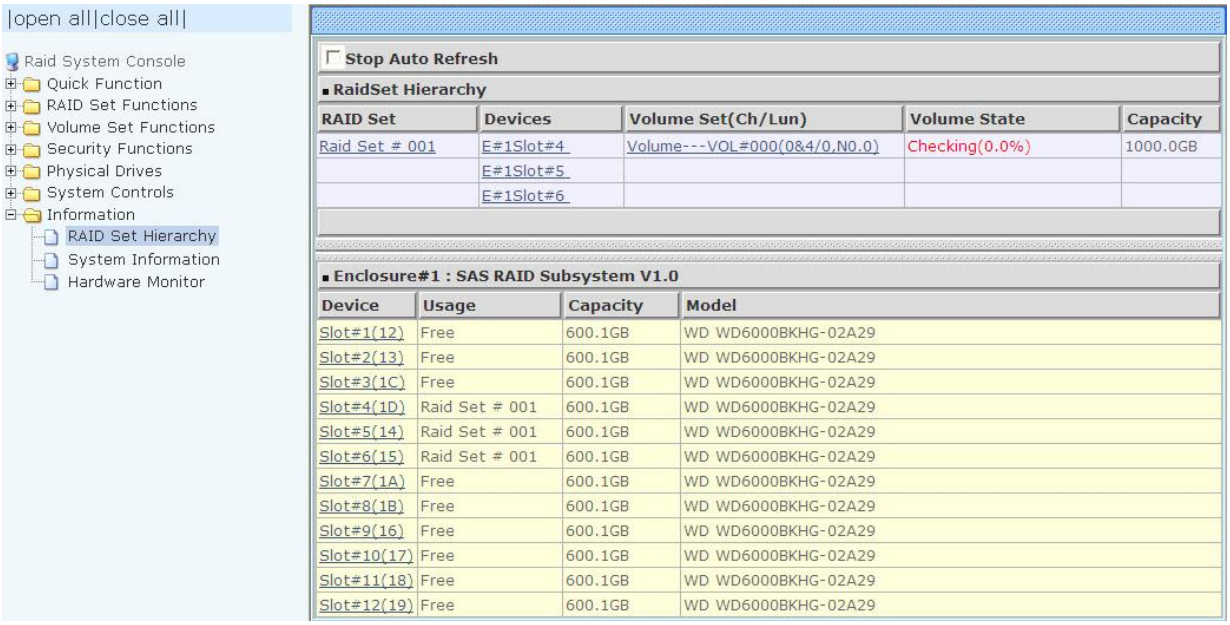
Check Volume Set Options:

- **Scrub Bad Block If Bad Block Found, Assume Parity Data is Good**
- **Re-compute Parity if Parity Error, Assume Data is Good**

NOTE: When the 2 options are not selected, it will only check for errors. It is recommended to perform Check Volume Set with the 2 options unselected at first. If the result shows error, the two options can be selected and redo Check Volume Set to correct the errors.

3. Tick on **Confirm The Operation** and click on the **Submit** button. The Checking process will be started.

The checking percentage can also be viewed by clicking on RaidSet Hierarchy in the Information menu.



NOTE: The result of Check Volume Set function is shown in System Events Information and Volume Set Information. In System Events Information, it is shown in the Errors column. In Volume Set Information, it is shown in Errors Found field.

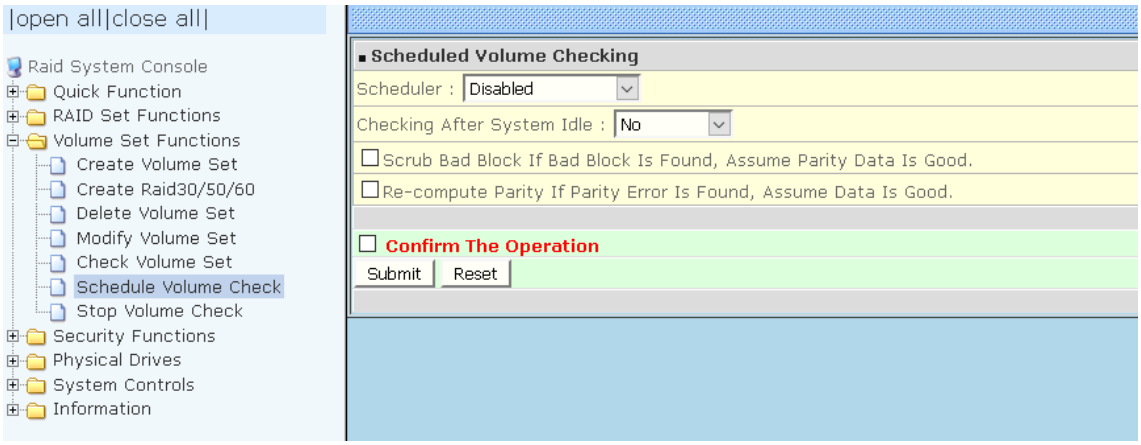
3.7.6 Schedule Volume Check

To perform Check Volume Set by schedule, follow these steps:

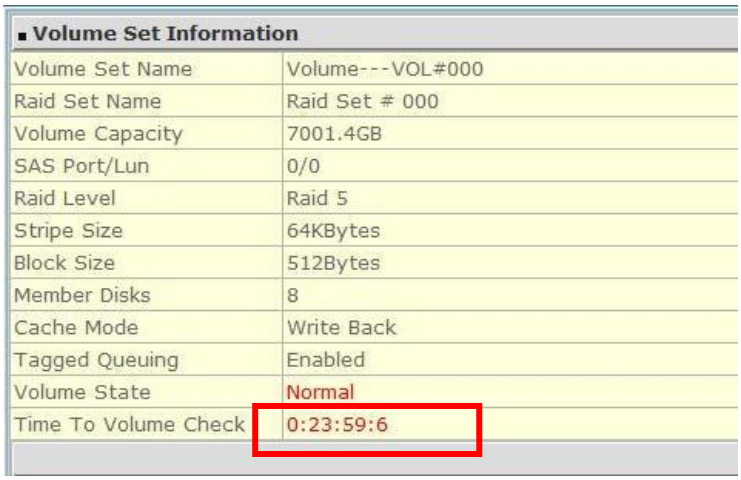
1. Click on the **Schedule Volume Check** link.
2. Select the desired schedule that you wish the Check Volume Set function to run. Tick on **Confirm The Operation** and click on the **Submit** button.

Scheduler: Disabled, 1Day (For Testing), 1Week, 2Weeks, 3Weeks, 4Weeks, 8Weeks, 12Weeks, 16Weeks, 20Weeks and 24Weeks.

Check After System Idle: No, 1 Minute, 3 Minutes, 5 Minutes, 10 Minutes, 15 Minutes, 20 Minutes, 30 Minutes, 45Minutes and 60 Minutes.



NOTE: To verify the Volume Check schedule, go to Information -> RAID Set Hierarchy -> select the Volume Set -> the Volume Set Information will be displayed.



Volume Set Information	
Volume Set Name	Volume---VOL#000
Raid Set Name	Raid Set # 000
Volume Capacity	7001.4GB
SAS Port/Lun	0/0
Raid Level	Raid 5
Stripe Size	64KBytes
Block Size	512Bytes
Member Disks	8
Cache Mode	Write Back
Tagged Queuing	Enabled
Volume State	Normal
Time To Volume Check	0:23:59:6

3.7.7 Stop Volume Check

Use this option to stop current running Check Volume Set process.

3.8 Security Functions

Protecting Drives with Self-Encrypting Drives (SED), a SED is a type of hard drive that automatically and continuously encrypts the data on the drive without any user interaction. The SED encryption is easy to use and manage with minimal impact on RAID controller performance that is invisible to the user, does not interfere in their workflow.

The SED function secures a volume's data from unauthorized access or modification in the event of drive theft, as well as more routine activities such as the return of defective drives for servicing or the decommission or repurposing of drives. The contents of a SED are always encrypted and the encryption keys are themselves encrypted and protected in hardware that cannot be accessed by other parts of the system. Local key management in the controller is designed to protect data from security breaches with minimal cost and complexity.

SEDs do all the cryptography within the disk drive internal controller, which means the disk encryption keys are never present in the RAID controller or memory, where they could be accessed by hackers. Encryption will conceal your volume's data and make accessing the files almost impossible for anyone who does not know your key. With this scramble process, no one can see and access into the hidden volume data without access key.

Note: SED security only works on logical drives composed of SED drives only.

How to enable SED functionality?

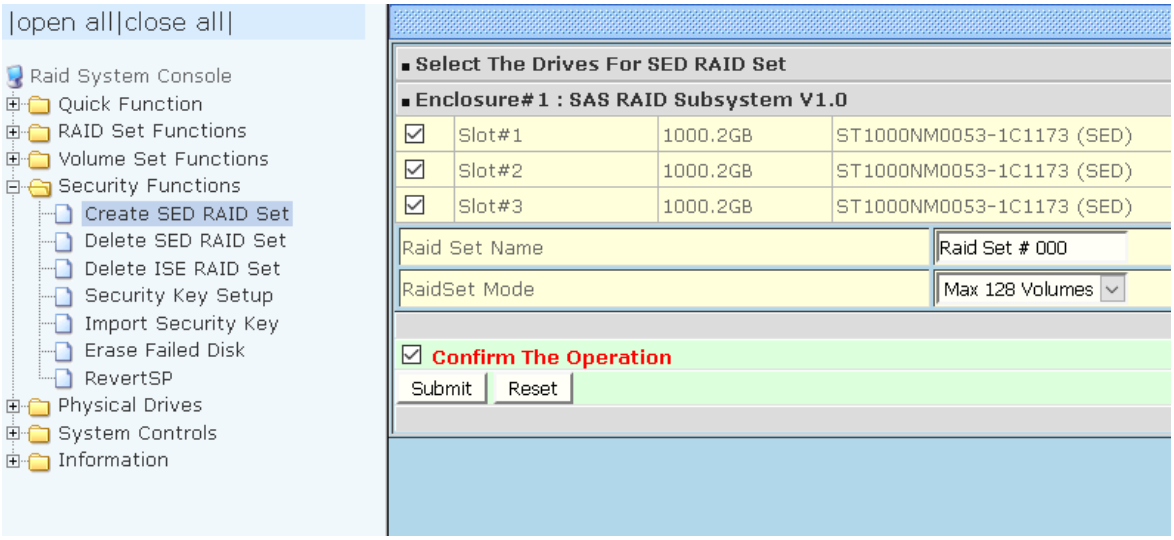
This Function is SED (self-encrypting drive technology) which support SED disks to provide Advanced Data Protection. The Security Key will enable the Disk Encryption at SED Raid Set.

1. Insert Self-Encrypting Drives (SEDs).
2. Login to storage management system. Please refer to Section 4.3 for more information.
3. Create SED Raid Set. See Section 5.4.1.
4. Create Volume Set. Refer to Section 5.3.1 Create Volume Set for detailed information about the Volume Set settings.
5. Create SED Key. See Section 5.4.4

NOTE: If SED Key "not enabled", then SED encryption is not enabled on that Raid Set.

3.8.1 Create SED RAID Set

Use the Create SED Raid Set function if you use SED (self-encryption drive) disks and need to encrypt the data, to use SED Raid Set to group SED drives. After Security Key is created, the SED Raid Set drives will automatically enable data encryption by Security Key. If Security Key is not enabled, the SED Raid Set will work as Normal Raid Set and disk data has no encryption.

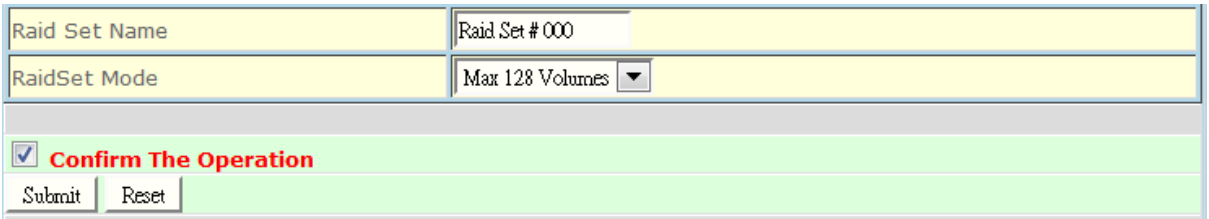


To create a SED Raid Set, click on the **Create SED RAID Set** link. A "Select The Drives For SED RAID Set" screen is displayed showing the Self-Encrypting Drives (SEDs) in the system.

NOTE:
The SED Raid Set can support below drive type. Can check the Supported Capability in the Device Information:

1. **Trusted Computing Group (TCG) SED**
2. **Secure Erase And Password (SATA)**
3. **Cryptographic Erase And Password (SATA)**

Tick the box of each Self-Encrypting Drives (SEDs) that will be included in Raid Set to be created.



Enter the preferred Raid Set Name (1 to 16 alphanumeric characters) to define a unique identifier for the Raid Set. Default Raid Set name always appear as **Raid Set # xxx**.

128 volumes is the default mode for SAS RAID controller, the 16 volumes mode is used for support roaming this raidset to SATA RAID controllers. The SATA RAID controller is designed to support up to 16 volumes only. You have to use "Max 16 volumes" on the raidset mode if you plan to roam this raidset between SAS RAID controller and SATA RAID controller.

Tick on the **Confirm The Operation** option and click on the **Submit** button in the screen.

NOTE: If SATA SED drives (with attached SAS bridge / MUX / dongle boards) are used in Dual Controller mode, the SED function cannot be used.

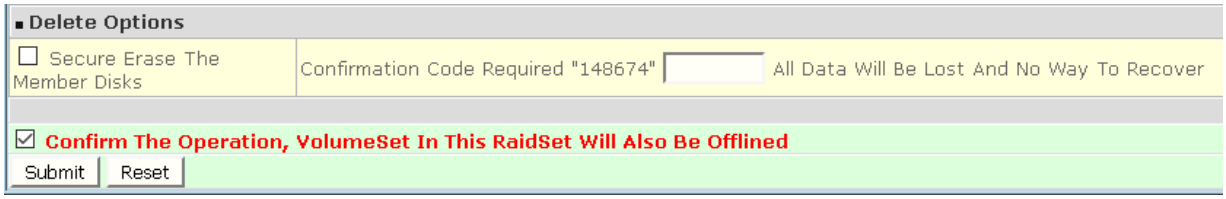
NOTE: Encryption in SED drives is enabled only when Create SED Raid Set. If create Normal Raid Set using SED drives, the Encryption is not enabled in those drives.

NOTE: In a SED Raid Set, the Rebuild/Expand/Clone/ Local Hot Spare can only select SED drive.

NOTE: For SSD with Block Erase Support: SATA SSD with Block Erase Support does not encrypt user data. It support Password Protect and "Instant Secure Erase" (may be longer erase time), it is included in SED Support. The difference is if Raid Set is deleted and NOT Secure Erased (Block Erase), the original data is still in the drive and accessible without Encryption.

3.8.2 Delete SED RAID Set

To delete a SED Raid Set, click on the **Delete SED RAID Set** link**.** A "Select The SED Raid Set To Delete" screen is displayed showing all Raid Sets existing in the system. Select the Raid Set you want to delete in the Select column.



If want to Security Erase the SED Raid Drive at Same Time, Tick On the **Secure erase the member disks** and Key In Correct **Confirmation Code.**

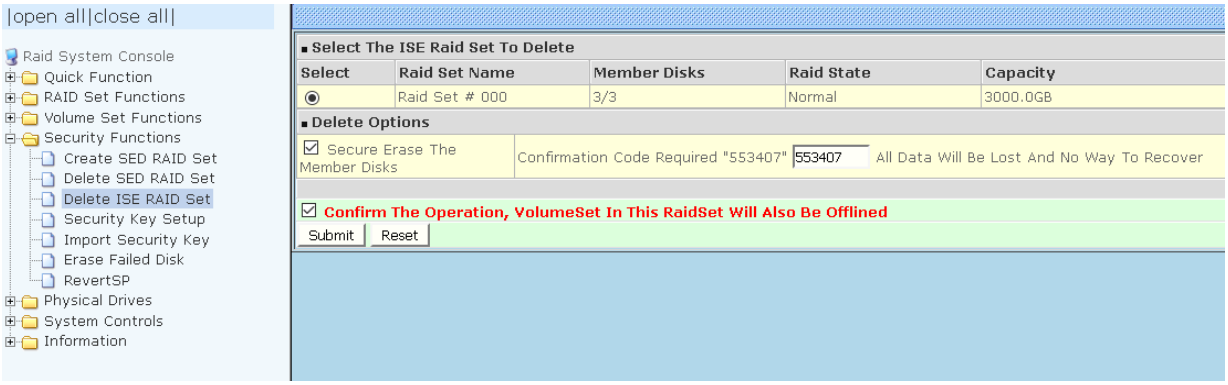
Confirmation Code:
Confirmation code is shown on the screen. This Code is produced by Controller. If tick on the "Secure Erase The Member Disks" but did not input the Confirmation Code or wrong Confirmation Code is entered, the Secure Erase will not be executed.

NOTE: Be careful when this options is selected, all data will be lost and no way to recover.

Tick on the **Confirm The Operation** and click on the **Submit** button to process with deletion.

NOTE: After Delete SED RAID Set, the Security Key will be disabled at same time in the SED RAID Set member disks, if Security Key was enabled before.

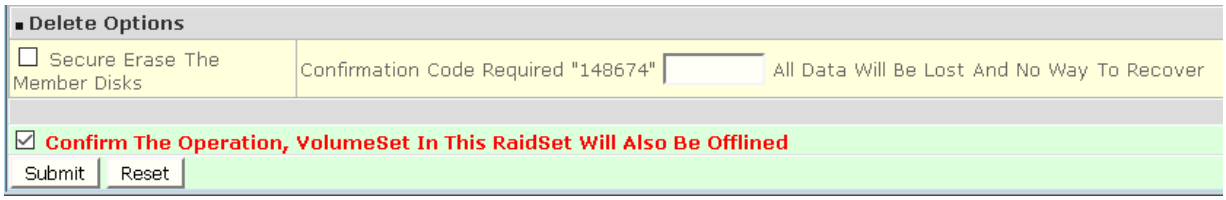
3.8.3 Delete ISE RAID Set



Instant Secure Erase (ISE) is designed to protect data on hard disk drives by instantly resetting the drive back to factory settings and changing the encryption key so that any data remaining on the drive is cryptographically erased. This means all data on the drive is permanently and instantly unreadable.

Non-SED drives (such as ISE-only drives) are supported in Normal Raid Set. If the Normal Raid Set, with some ISE member drives with Instant Secure Erase Capability, will be deleted, use the Delete ISE RAID Set.

To delete a ISE Raid Set, click on the **Delete ISE RAID Set** link**.** A "Select The ISE Raid Set To Delete" screen is displayed with Raid Set member disks including existing Instant Secure Erase capable drives. Select the Raid Set you want to delete in the Select column.



If want to Security Erase the ISE Raid Drive at Same Time, Tick On the **Secure erase the member disks** and Key In Correct **Confirmation Code.**

Confirmation Code:
Confirmation code is shown on the screen. This Code is produced by Controller. If tick on the "Secure Erase The Member Disks" but did not input the Confirmation Code or wrong Confirmation Code is entered, the Secure Erase will not be executed.

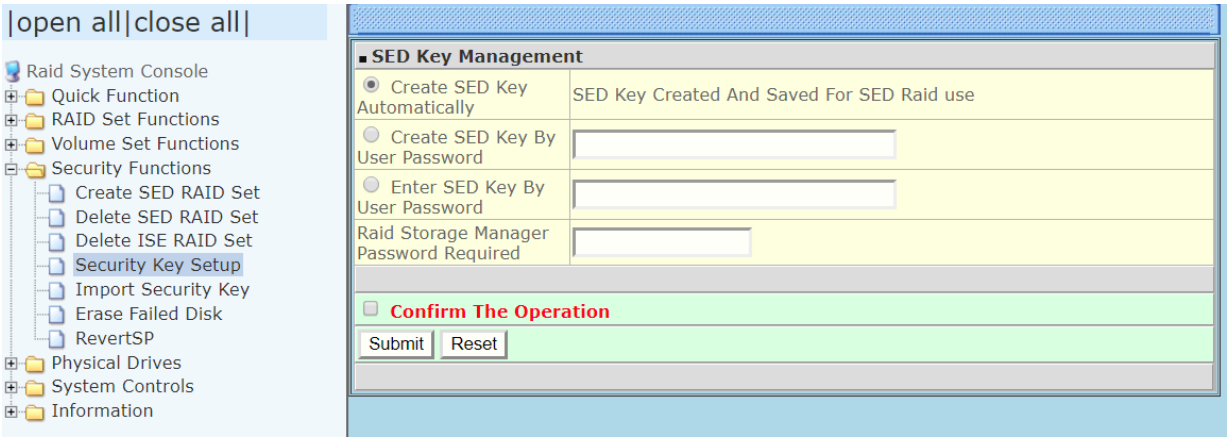
NOTE: Be careful when this options is selected, all data will be lost and no way to recover.

Tick on the **Confirm The Operation** and click on the **Submit** button to process with deletion.

3.8.4 Security Key Setup

Security Key Setup options are: Create / Disable / Change / Export - Security Key for SED Raid Set. The Security Key is global for all SED Raid Set. When SED Raid Set is created and Security Key is enabled, the Security Function will be enabled in the SED Raid Set member disks without any sequence.

To set the security key configuration options, click the **Security Key Setup** link under the **Security Functions** menu.



3.8.4.1 Create Security Key

There are three options to enable SED Key.

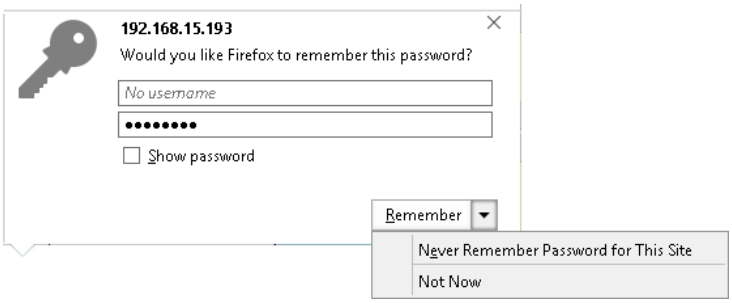
1. Create SED Key Automatically: the controller will automatically generate the SED Key.
2. Create SED Key By User Password: user defined password. The SED Key characters allowed are 'A' – 'Z', 'a' – 'z', and '0' – '9'. The minimum number of Password characters is 4.

NOTE: Once the SED Key has been set, the user can only lock and unlock the data by providing the correct SED Key.

3. Enter SED key is only allowed when no key is set in controller. So that next time power up again, it will need to input the key from the " Enter SED Key By User Password" again.

Enter the RAID Storage Manager Password (default is 00000000) to login. Tick the "**Confirm The Operation**" and click "**Submit**".

NOTE: The browser will prompt you to remember your password. We strongly recommend you not allow AutoComplete to save passwords. Do not store/save Raid Storage Manager Password in the web browser (cache). If Raid Storage Manager Password is saved in web browser and then configure Security Key Setup, the Raid Storage Manager Password will be automatically inputted by web browser. Suggestion is to enter the Raid Storage Manager Password every time for better security in the Security Key Setup.

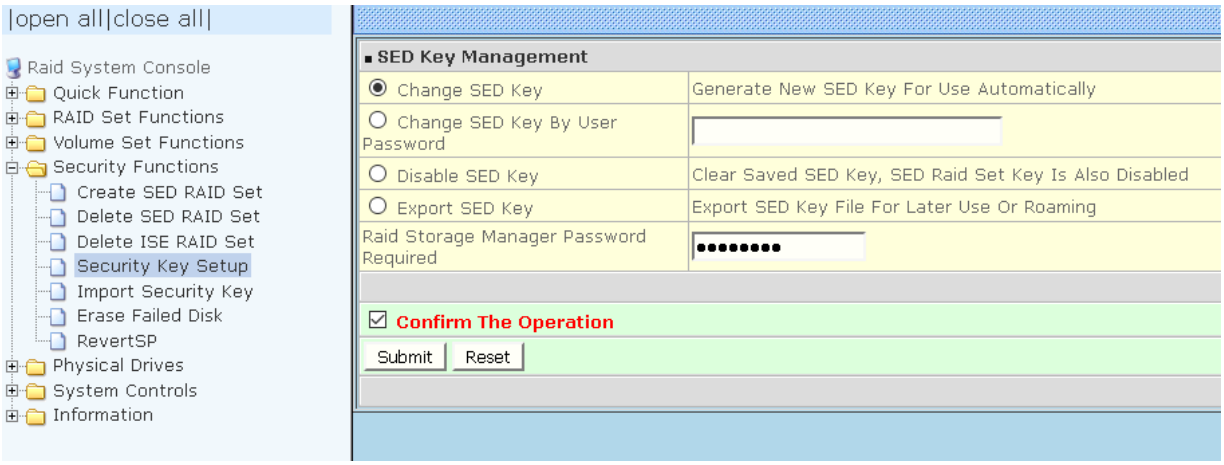


IMPORTANT: The SED Key must be exported regularly and add date and time at the exported Key filename. The default Key filename is SEDKEY256.BIN. Suggestion is to add date and time, e.g. 201702091210_SEDKEY256.BIN at every Export Key file. These Key file can provide more protection of the saved Key. Refer to next Section for exporting Key.

3.8.4.2 Modify Security Key

After create Security Key, next time to use the SED Key Management, the function will change to Change / Disable / Export Security Key for the global SED Raid Set.

To change, disable or export the SED Key, click the **Security Key Setup** link under the **Security Functions** menu.



Using "Change SED Key" and "Change SED Key By User Password" can change Security Password to new one.

NOTE: Create SED Key By User Password, the SED Key characters allowed are 'A' – 'Z', 'a' – 'z', and '0' – '9'. The minimum number of Password characters is 4.

NOTE: If need to change the SED Key, the RAID system and all device must be at Normal Status:

1. **No failed SED Disk**
2. **The SED Raid Set must not be in Offline status**
3. **In dual controller mode, other controller must not be at "Restarting Controller" status**
4. **In dual controller mode, both controllers must be operational and no failed controller**

If not, may be some disk's SED Key not matched will happen.

"Disable SED Key" is to disable Security key for all SED Raid Sets in the RAID unit. This will also clear saved SED key.

"Export SED Key" can store Security key to a file for later use or roaming.

After selecting an option, need to provide the "Raid Storage Manager Password Required" for security confirmation, and then tick on the "**Confirm The Operation**" and click **Submit.**

NOTE: The browser will prompt you to remember your password. We strongly recommend you not allow AutoComplete to save passwords. Do not store/save Raid Storage Manager Password in the web browser (cache). If Raid Storage Manager Password is saved in web browser and then configure Security Key Setup, the Raid Storage Manager Password will be automatically inputted by web browser. Suggestion is to enter the Raid Storage Manager Password every time for better security in the Security Key Setup.

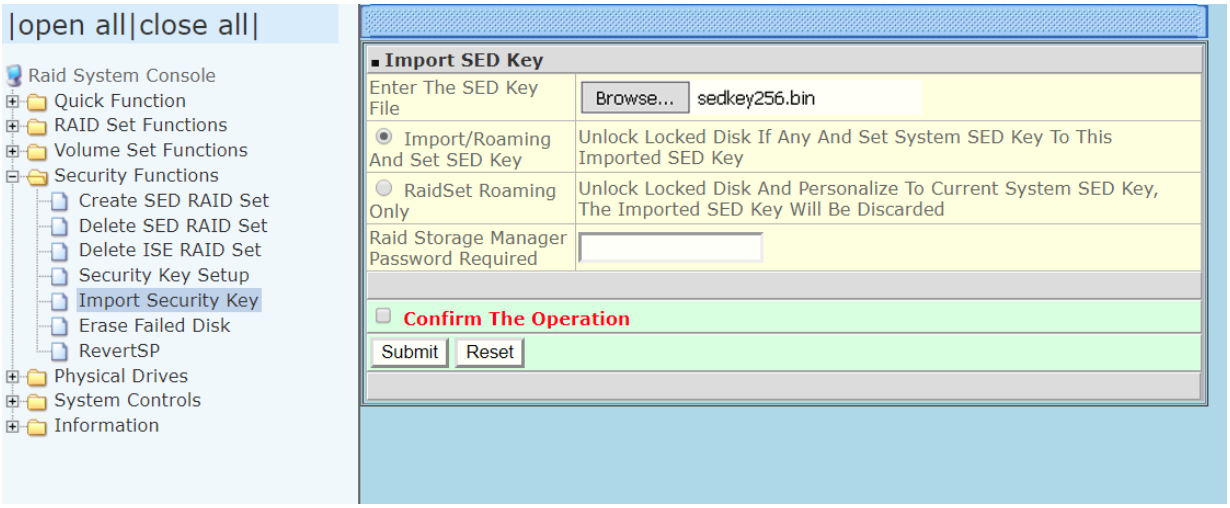
IMPORTANT: The SED Key must be exported regularly and add date and time at the exported Key filename. The default Key filename is SEDKEY256.BIN. Suggestion is to add date and time, e.g. 201902091210_SEDKEY256.BIN at every Export Key file. These Key file can provide more protection of the saved Key.

3.8.5 Import Security Key

SED RaidSet created on a RAID system can be migrated to another RAID system. If you are importing a RaidSet originally secured with a SED key, you need to import the foreign SED key files to secure or unlock that RaidSet. The "Import Security Key" file is for Raidset Roaming or Change SED Key function. If you roam a RaidSet from old system to another new (with Security Functions support), the foreign SED key file must be imported before it can be used.

Import Security Key provides function to import Security Key to unlock/Locked Disks.

To Import Security Key, click the **Import Security Key** link under the **Security Functions** menu.



Enter The SED Key File: Click the [Browse…] button and select SED Key File first, then choose a type to unlock Locked Disk.

Import Security Key supports 2 functions: **Import/Roaming And Set SED Key** and **RaidSet Roaming Only**.

1. Select the "Import/Roaming And Set SED Key" option to unlock the locked disk and change to foreign SED key.

2. Select the "RaidSet Roaming Only" option to unlock the locked disk and personalize to new controller's SED key. If there is an existing SED key on new controller, RaidSet is updated with the new security key. If there is not an existing SED key on new controller, RaidSet is updated to unlock RaidSet.

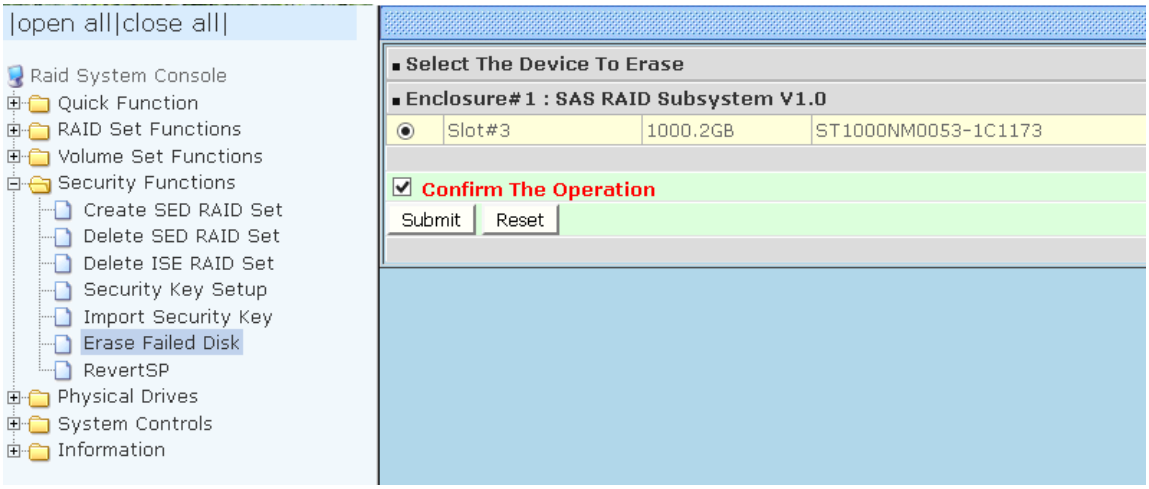
After selecting an option, need to provide the "Raid Storage Manager Password Required" for security confirmation, and then tick on the "**Confirm The Operation**" and click **Submit.**

NOTE: The browser will prompt you to remember your password. We strongly recommend you not allow AutoComplete to save passwords. Do not store/save Raid Storage Manager Password in the web browser (cache). If Raid Storage Manager Password is saved in web browser and then configure Security Key Setup, the Raid Storage Manager Password will be automatically inputted by web browser. Suggestion is to enter the Raid Storage Manager Password every time for better security in the Security Key Setup.

IMPORTANT: The SED Key must be exported regularly and add date and time at the exported Key filename. The default Key filename is SEDKEY256.BIN. Suggestion is to add date and time, e.g. 201702091210_SEDKEY256.BIN at every Export Key file. These Key file can provide more protection of the saved Key.

3.8.6 Erase Failed Disk

The Erase Failed Disk function can be used to securely erase a SED or ISE disk that is failed. User can select to erase its content. If failed disk is not accessible and this function fails, in this case, failed disk can be power cycled and try again.

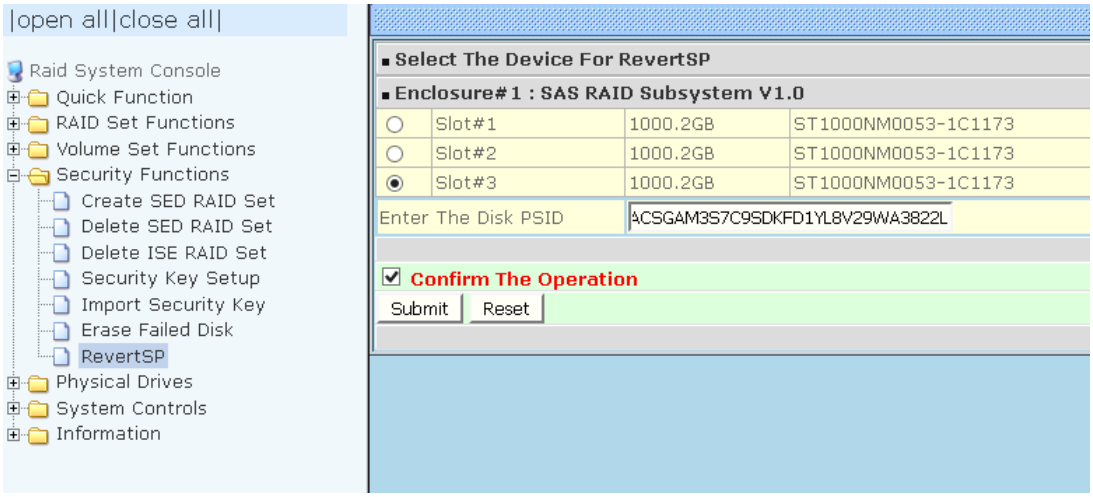


To securely erase the SED or ISE failed disk, choose and click the failed disk Slot# and tick on the "**Confirm The Operation**" and click **Submit**. After secure erase failed disk, there is no way to recover original data.

3.8.7 RevertSP

If a disk has been Locked and cannot be Unlocked, then need to use RevertSP to return disk to Factory Default. After execute RevertSP to reset disk to Factory Default, there is no way to recover original data.

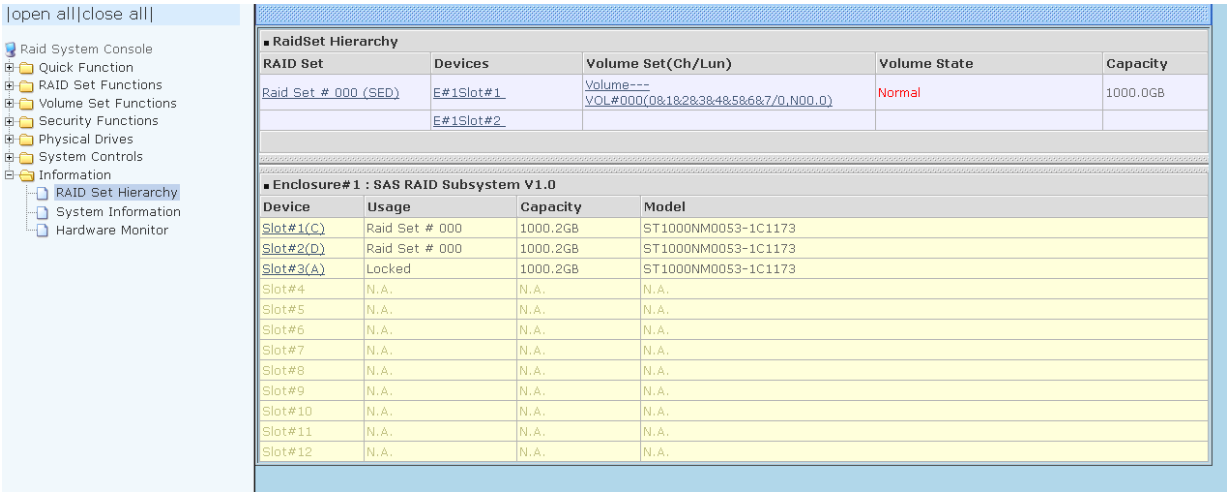
Please contact your vendor's support engineer for assistance.



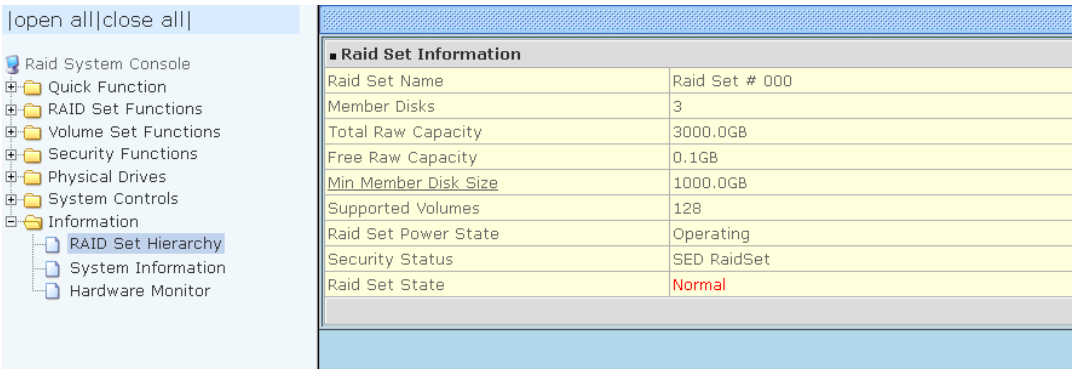
NOTE: Pass-Through Disk and JBOD mode do not support SED Function.

3.8.8 SED Information

Use this feature to view the RAID subsystem's existing SED Raid Set(s) and SED disk drive(s) configuration and information. Select the **RAID Set Hierarchy** link from the **Information** menu to display the Raid Set Hierarchy screen.



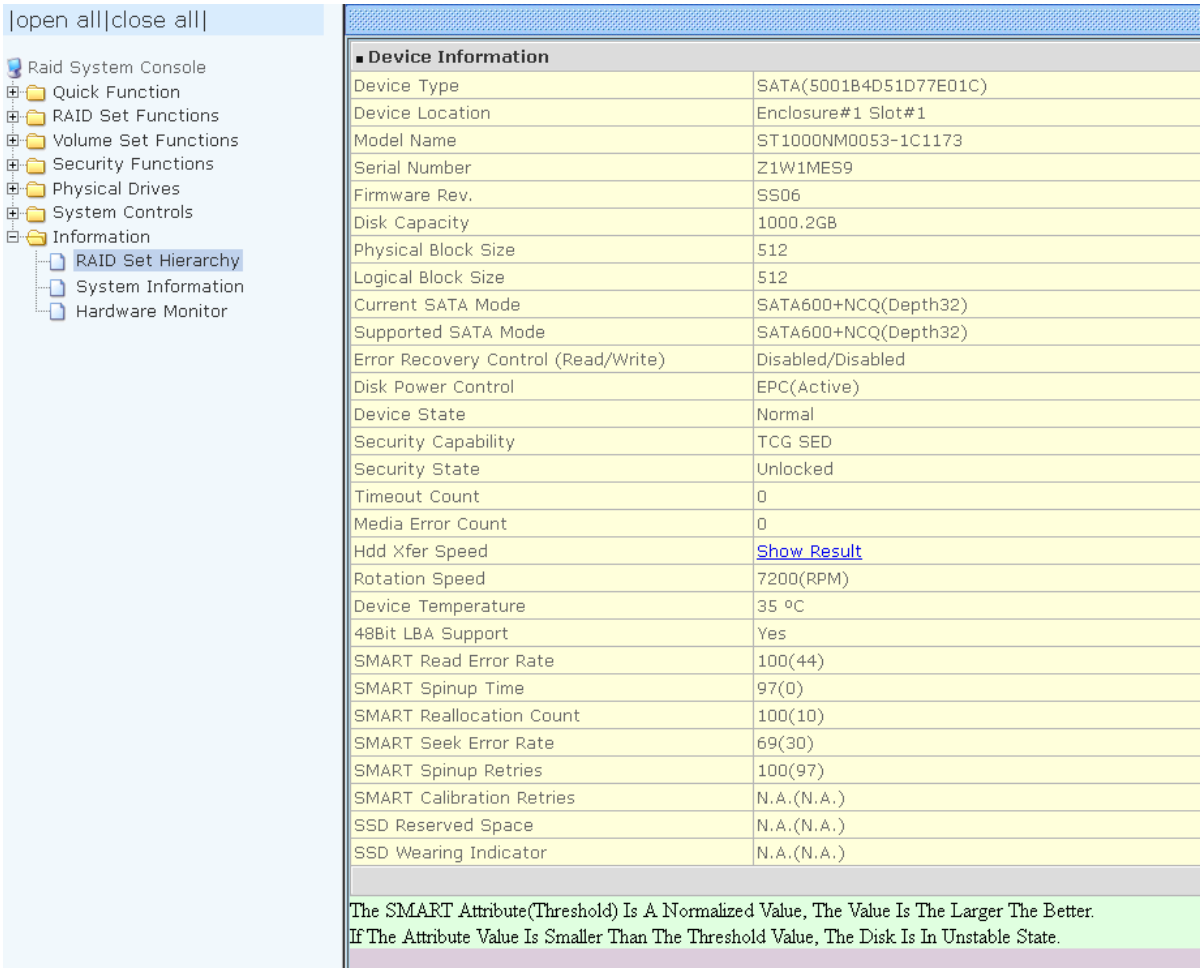
To view the Raid Set information, click the **Raid Set #** link from the Raid Set Hierarchy screen. The Raid Set Information screen appears.



The Raid Set Hierarchy can show SED Raid Sets, click the Raid Set name link and check the Raid Set Information for Security Status:

Security Status	Description
N/A	Non-SED or ISE Disk
x/y ISE Disks	Number of ISE disks included in the Raid Set x: ISE Disk Count; if SED Disk is used to create Normal Raid Set this will display ISE Disk. y: Total Disk Count.
SED Raid Set	SED Raid Set has member SED disks.

To view the disk drive information, click the **E# Slot#** link from the Raid Set Hierarchy screen. The Device Information screen appears. This screen shows various information such as disk drive model name, serial number, firmware revision, disk capacity, **Security Capability**, **Security State**, timeout count, media error count, Hdd Xfer Speed and SMART information.



Device Information has 2 fields displayed about disk Security Type and Status, which are:

1. Security Capability
2. Security State

Below table is the description.

Security Capability

Security Capability	Description	Shows the drive security capability, for example: Cryptographic Erase, TCG SED
N/A	Normal disk, Non-ISE disk	Can be used to create Normal Raid Set
Cryptographic Erase	ISE Secure Erase - Some SAS Disks Only Support Encryption without Password	Can be used to create Normal Raid Set
Cryptographic Erase And Password	ISE Sanitize with Crypto erase - Some SAS/SATA Support this Type of Operation	Can be used to create Normal Raid Set and also SED Raid Set
Secure Erase And Password	• Password & FDE (Full-Disk-Encryption) with Password Protect - Some SATA Disk Support Password and Encryption • SSD with Block Erase and Password	Can be used to create Normal Raid Set and also SED Raid Set
Block Erase	SSD with Block Erase	Can be used to create Normal Raid Set
TCG SED	Full SED Function Support	Can be used to create Normal Raid Set and also SED Raid Set

Security State

Security State	Description
N/A	Non-SED Disk
Disabled	Not Personalized, No SED Key Setup.
Unlocked	Personalized, Operational by SED Key enabled and Key is match
	Comment: Every time the SED Key is changed, it is necessary to export the SED Key and save by time record (Date and Time).
Locked	Personalized, SED Key is not match
	Comment: Import SED Key is required.

3.9 Physical Drive

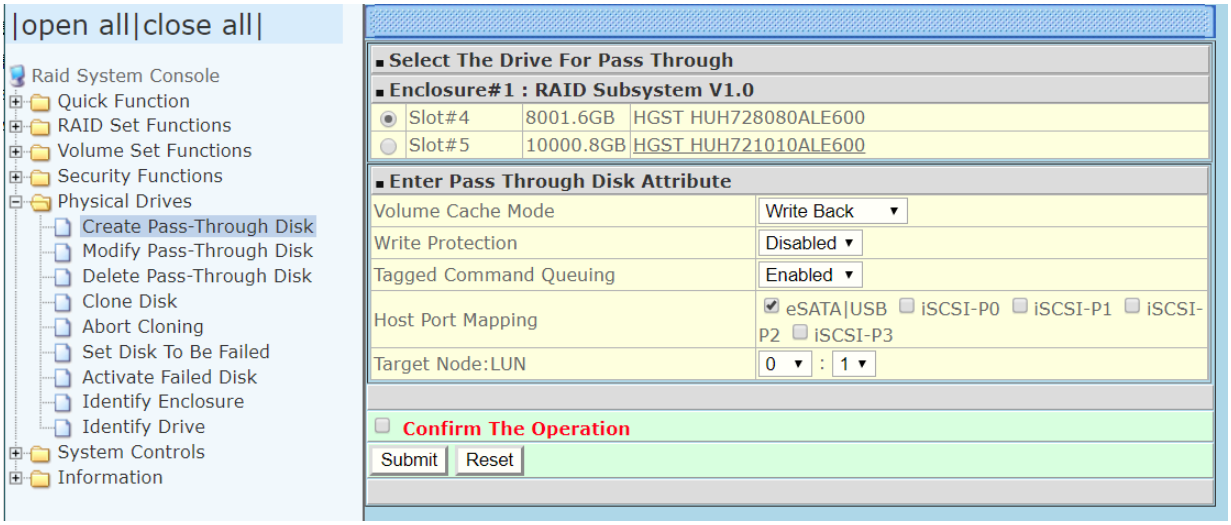
Choose this option from the Main Menu to select a disk drive and to perform the operations listed below.

3.9.1 Create Pass-Through Disk

A Pass-Through Disk is a disk drive not controlled by the internal RAID subsystem firmware and thus cannot be a part of a Volume Set. A Pass-Through disk is a separate and individual Raid Set. The disk is available to the host as an individual disk. It is typically used on a system where the operating system is on a disk not controlled by the RAID firmware.

To create pass-through disk, click on the **Create Pass-Through** link under the Physical Drives main menu. The setting function screen appears.

Select the disk drive to be made as Pass-Through Disk and configure the Pass-Through Disk attributes, such as the Cache Mode, Tagged Command Queuing, and Host Port Mapping/LUN for this volume.

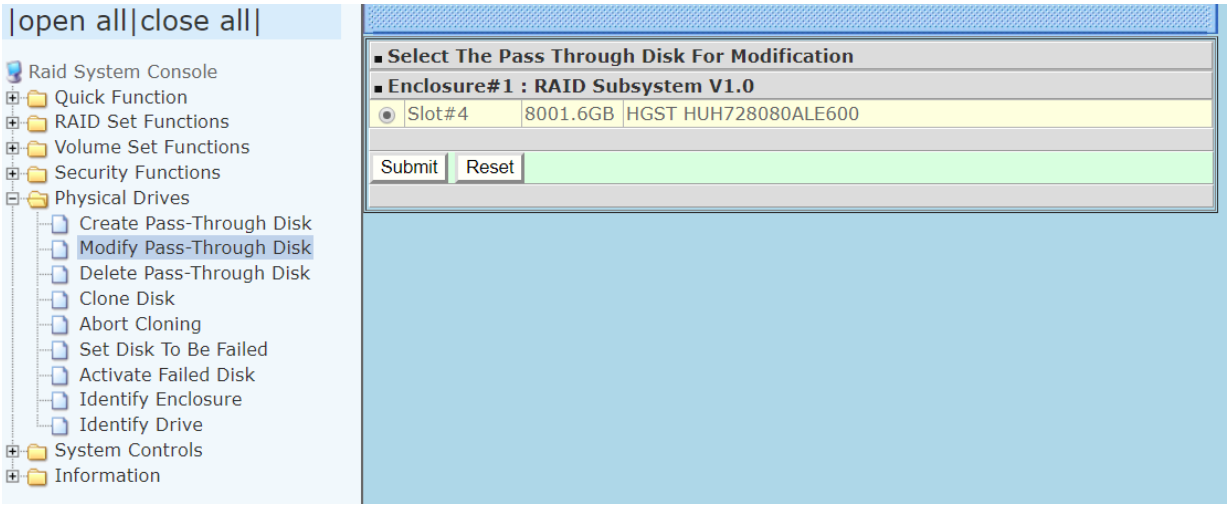


3.9.2 Modify Pass-Through Disk

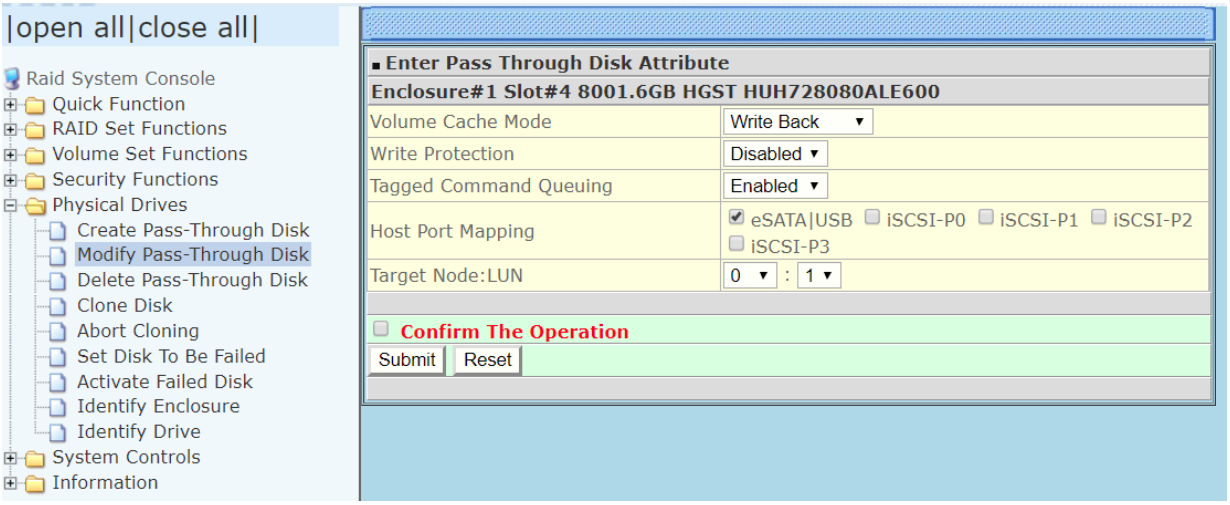
Use this option to modify the attribute of a Pass-Through Disk. User can modify the Cache Mode, Tagged Command Queuing, and SAS Port/LUN Base/LUN on an existing Pass-Through Disk.

To modify the Pass-Through drive attribute from the Pass-Through drive pool, click on the **Modify a Pass-Through Disk** link. The "Select The Pass-Through Disk For Modification" screen appears. Tick on the Pass-Through Disk from the Pass-Through drive pool and click on the **Submit** button to select the drive.

The Enter Pass-Through Disk Attribute screen appears. Modify the drive attribute values as you want.



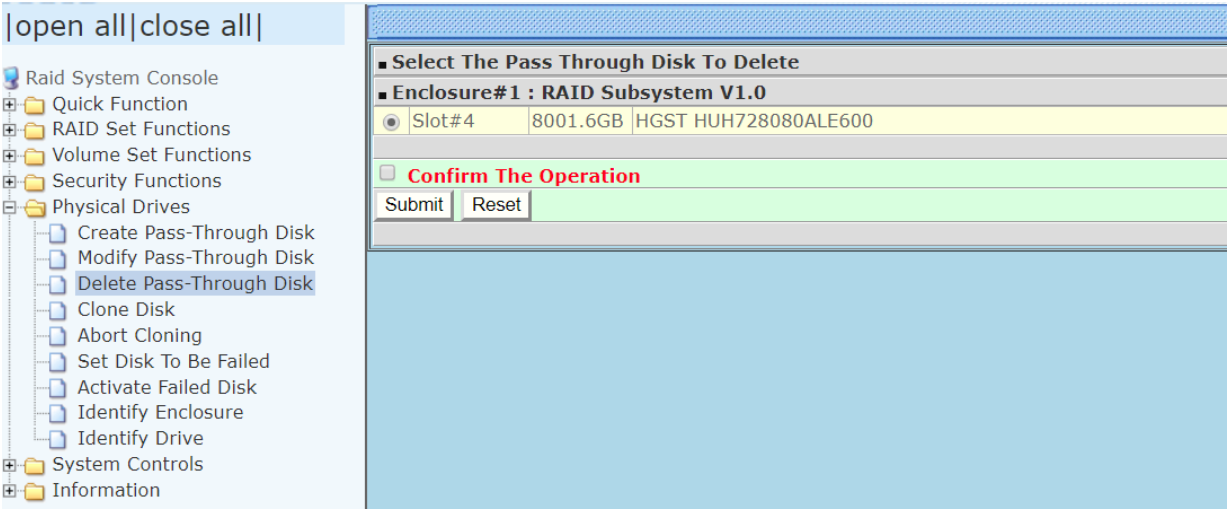
The Enter Pass-Through Disk Attribute screen appears. Modify the drive attribute values as you want.



To save changes, tick on **Confirm The Operation** and click on the **Submit** button.

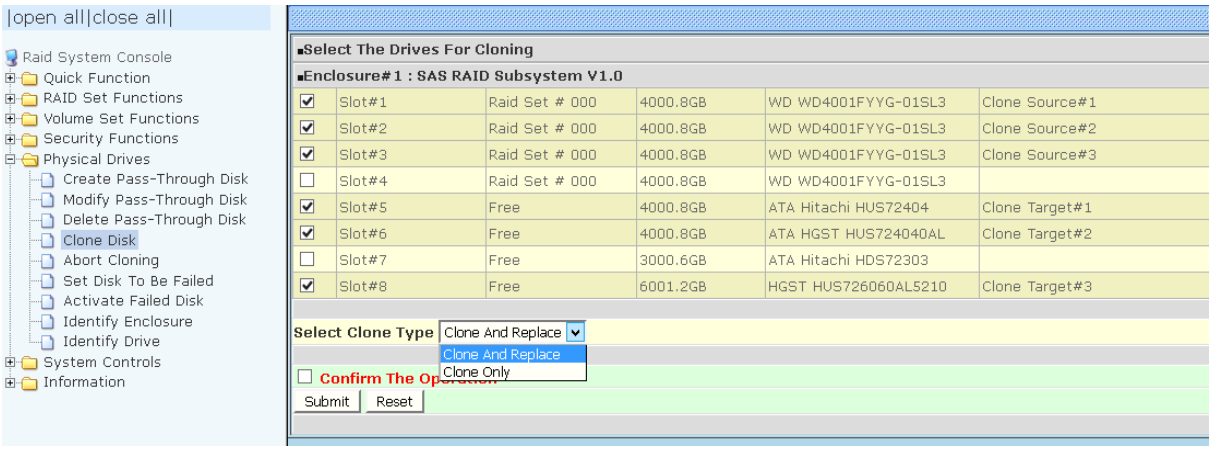
3.9.3 Delete Pass-Through Disk

To delete Pass-Through Disk from the Pass-Through drive pool, click on **Delete Pass-Through** link. Select a Pass-Through Disk, tick on the **Confirm The Operation** and click the **Submit** button to complete the delete action.



3.9.4 Clone Disk

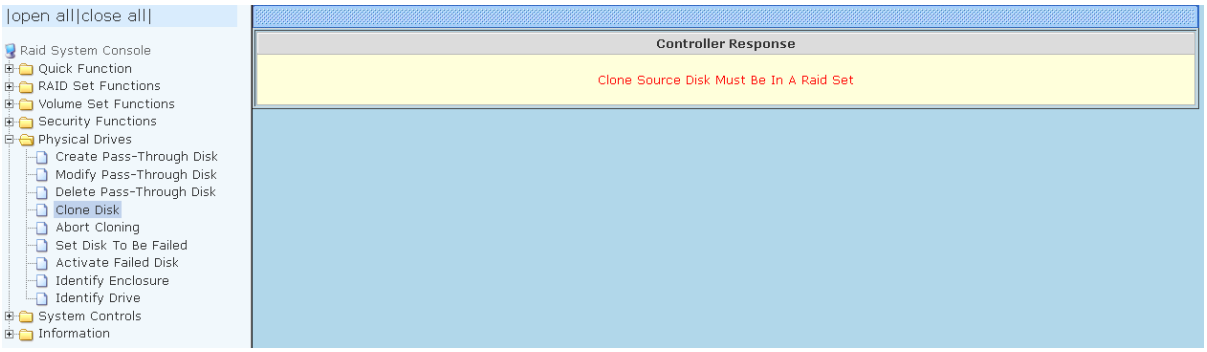
Instead of deleting a RAID set and recreating it with larger disk drives, the "Clone Disk" function allows the users to replace larger disk drives to the RAID set that have already been created. Click on the "Clone Disk" option on the "Physical Drives" link to enable the clone function. If there is an available disk, then the "Select The Drives For Cloning" screen appears. There are two "Clone Disk" function options: "Clone And Replace" and "Clone Only."



Clone Disk Procedure

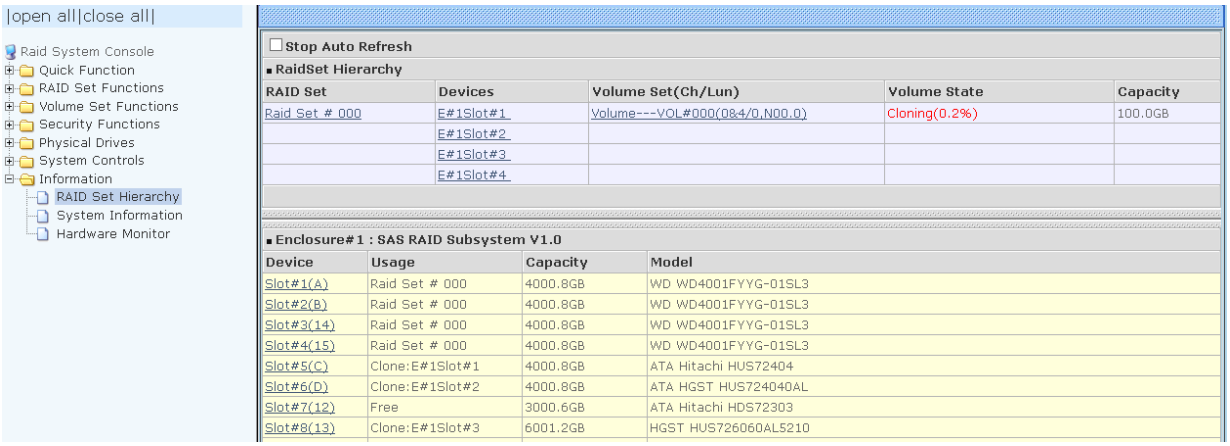
1. Select one of the members as the "Clone Source" (status indicated as Raid Set #) by clicking on the appropriate check box.

NOTE: An error message will be showed on the screen, when the selected disk is not in a Raid Set.



2. Select a "Clone Target" (status indicated as Free or Hot Spare) by clicking on the appropriate check box.
3. If you have available disk member, you can repeat above procedures to define another clone pair.
4. Select clone type.

The pair number for both the "Clone Source" and the "Clone Target" will be indicated in the screen. Tick on the "Confirm The Operation" check box and click on the "Submit" button on the screen; the controller will automatically start the cloning process using the existing "stand-by" (Free or Hot Spare drive) to clone the source drive (the Raid Set member drive). The cloning process percentage will be indicated in the "Volume State" area of the "RAID Set Hierarchy" screen. Completion of the Clone function process will be indicated by a notification message on the event log.



3.9.4.1 Clone And Replace

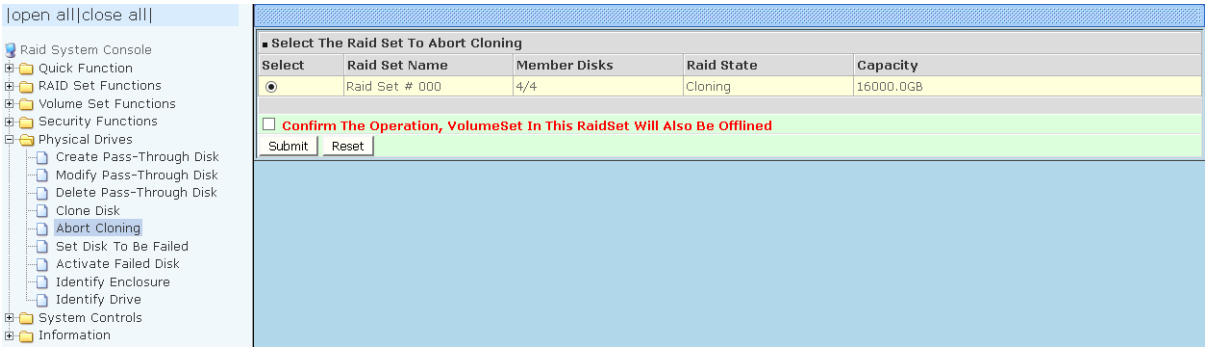
You can enlarge your logical drives by copying and replacing all member drives with drives of higher capacity. The existing data in the logical drives is copied onto the new drives, and then the original members are marked as "Offlined".

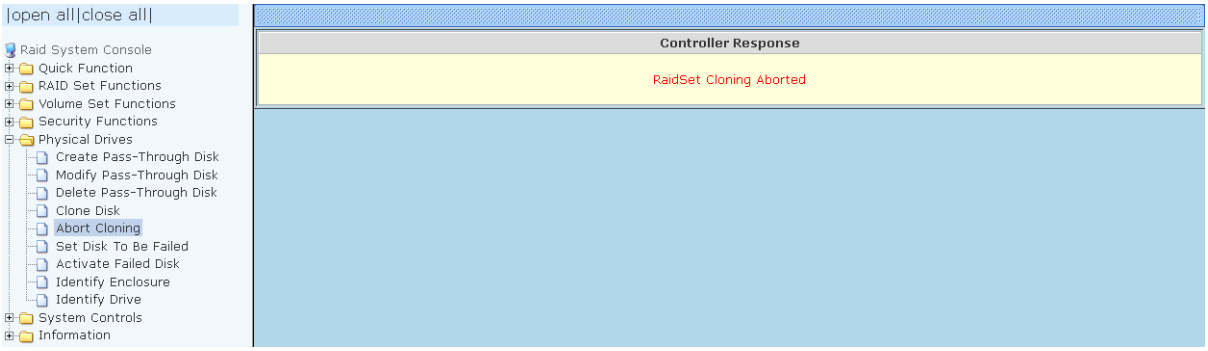
3.9.4.2 Clone Only

The stand-by disk will clone the logical drives without substituting it. The status of the stand-by drive will be marked as "Offlined" after the cloning process. The source drive will remain a member of the logical drive.

3.9.5 Abort Cloning

Use this function to stop the ongoing clone disk action.

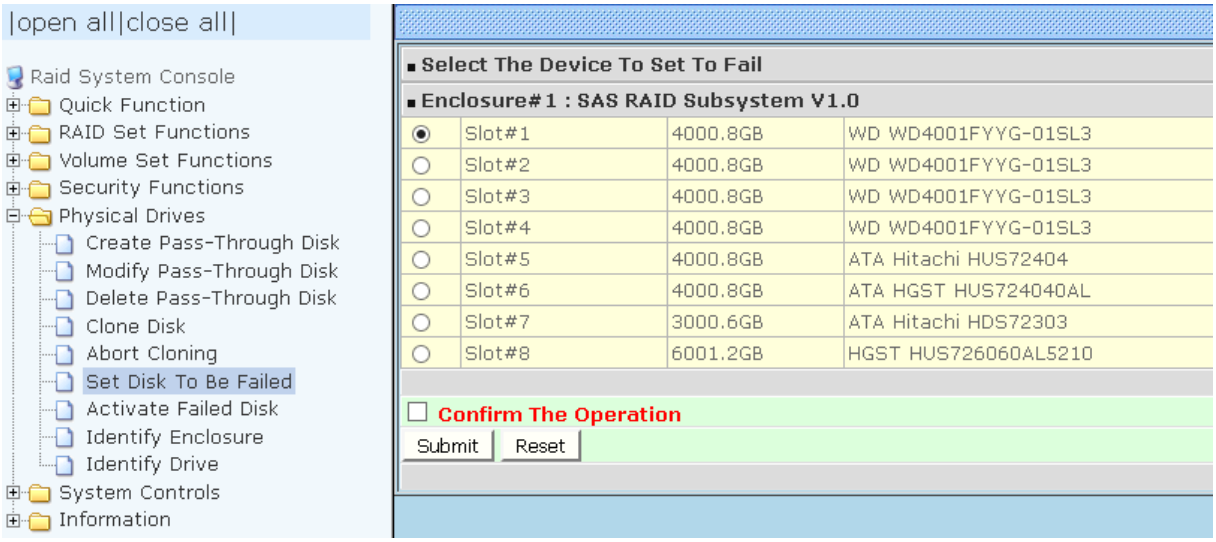




3.9.6 Set Disk To Be Failed

It sets a normal working disk as **failed** so that users can test some of the features and functions.

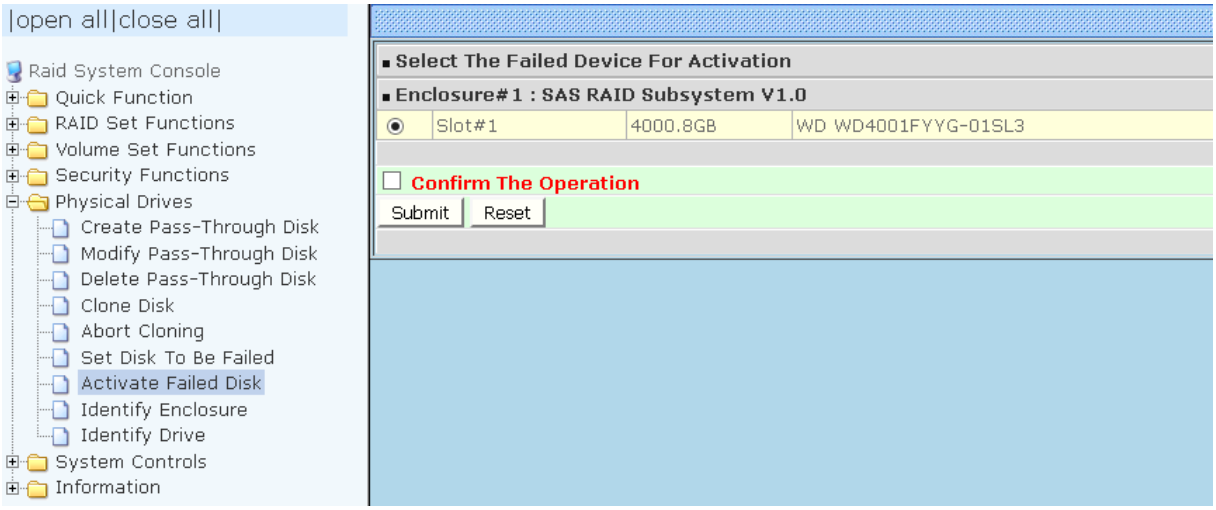
NOTE: When you want to set a disk as failed, please contact your vendor's support engineer for assistance.



3.9.7 Activate Failed Disk

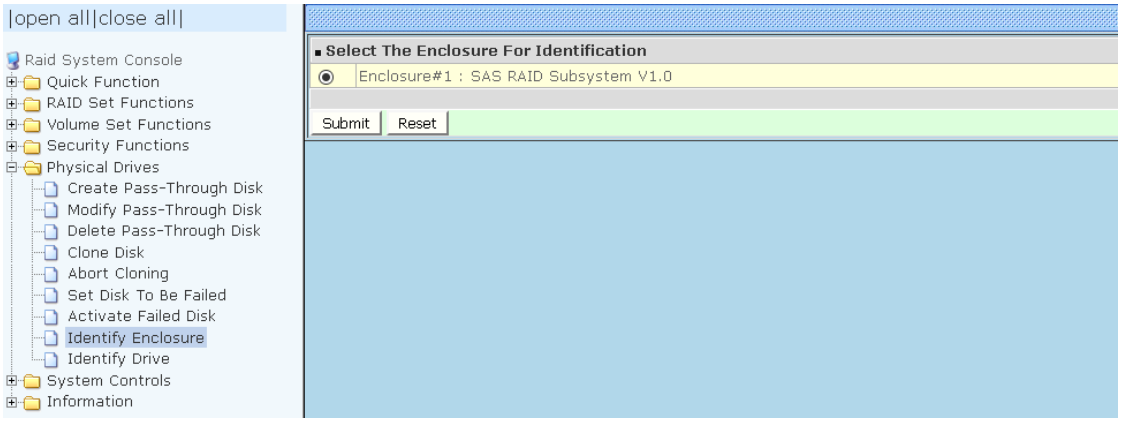
It forces the current **failed** disk in the system to be back online. **Activate Failed Disk** function has no effect on the removed disks, because a **removed** disk does not give the controller a chance to mark it as **failure**.

Followings are considered as **Removed-Disk**:
(1). Manually removed by user
(2). Losing PHY connection due to bad connector, cable, backplane
(3). Losing PHY connection due to disk fail
Basically, in the eyes of the controller, the disk suddenly disappears due to whatever reason.



3.9.8 Identify Enclosure

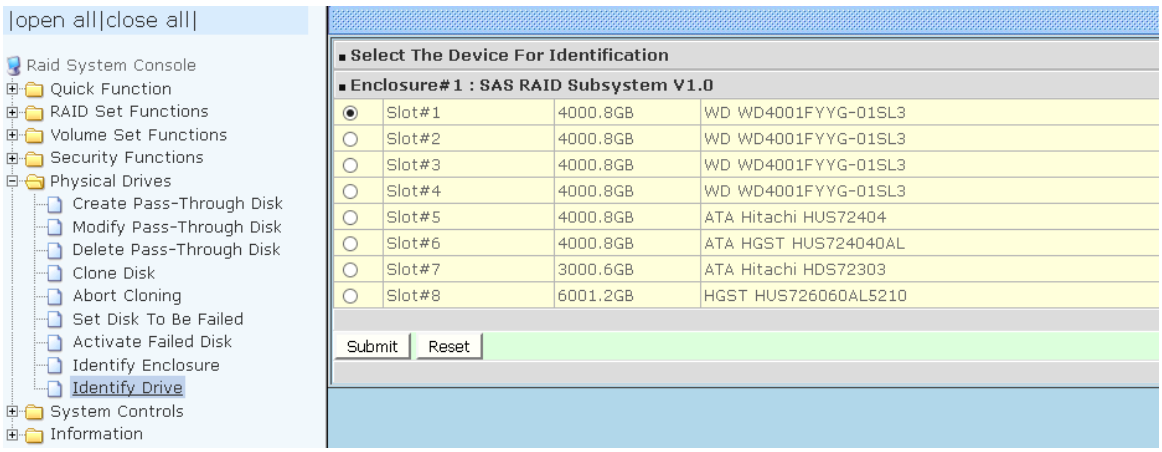
To identify an Enclosure, move the mouse cursor and click on **Identify Enclosure** link. The **Select The Enclosure For Identification** screen appears. Tick on the enclosure from the list of enclosures, then click on the **Submit** button to identify the selected enclosure. All disk drives' Status LEDs in an enclosure will be blinking when a particular enclosure is selected.



3.9.9 Identify Selected Drive

Use this option to physically locate a selected drive to prevent removing the wrong drive. When a disk drive is selected using the **Identify Drive** function, the Status LED of the selected disk drive will be blinking Red.

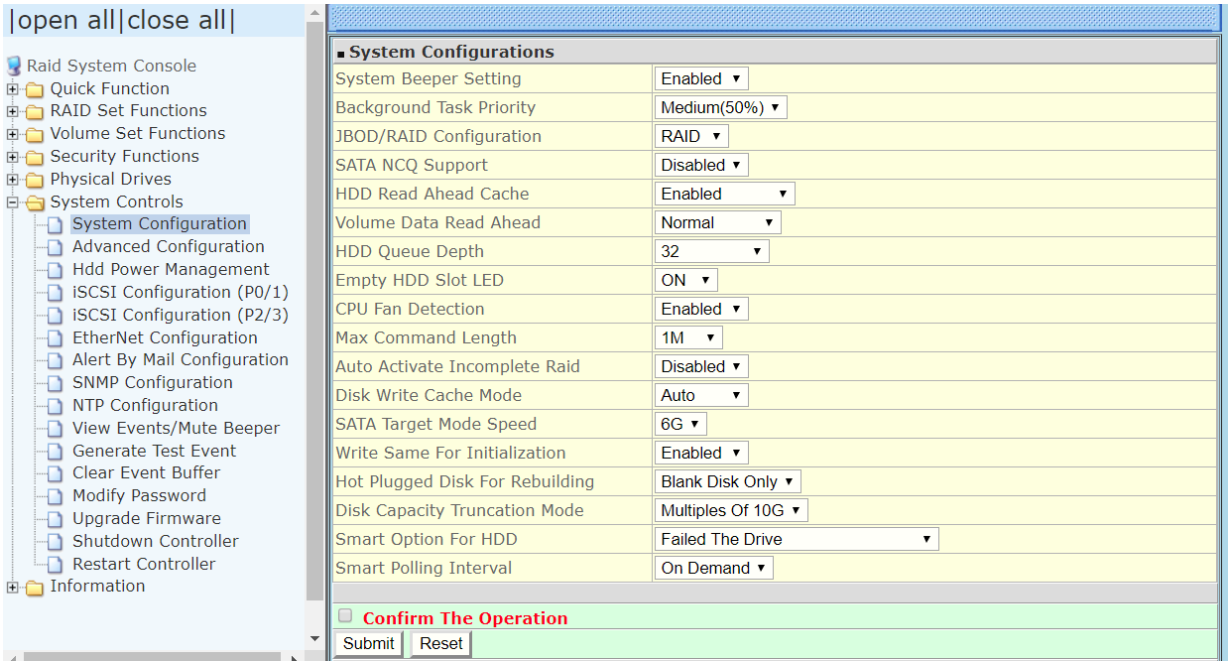
To identify a selected drive from the drives pool, click on the **Identify Drive** link. The "Select The IDE Device For identification" screen appears. Tick on the IDE device from the drives list. After completing the selection, click on the **Submit** button to identify selected drive.



3.10 System Controls

3.10.1 System Configuration

To set the RAID subsystem system configuration options, click the **System Config** link under the **System Controls** menu. The System Configuration screen will be shown. Set the system configuration option as needed.



System Beeper Setting:
This option is used to Disabled or Enable the subsystem's RAID controller alarm beeper.

Background Task Priority:
The Background Task Priority indicates how much time and system resource the RAID controller devotes to a background task, such as a rebuild operation. The RAID subsystem allows user to choose the background task priority (High 80%, Medium 50%, Low 25%, and Ultra Low 5%) to balance between background task process and Volume Set access. For high RAID subsystem performance, specify a low value.

JBOD/RAID Configuration:

The RAID subsystem supports JBOD and RAID configuration.

SATA NCQ Support:

NCQ is a command protocol in Serial ATA that can only be implemented on native Serial ATA hard drives. It allows multiple commands to be outstanding within a drive at the same time. Drives that support NCQ have an internal queue where outstanding commands can be dynamically rescheduled or re-ordered, along with the necessary tracking mechanisms for outstanding and completed portions of the workload. Disabled or Enable the SATA NCQ function.

HDD Read Ahead Cache:

This option allows the users to disable the cache of the HDDs on the RAID Subsystem. In some HDD models, disabling the cache in the HDD is necessary to prove the RAID Subsystem functions correctly. When Enabled, the drive's read ahead cache algorithm is used, providing maximum performance under most circumstances.

Volume Data Read Ahead:

This option allows the users to set the Volume Data Read Ahead function. Options are: Normal, Aggressive, Conservative, and Disabled.

HDD Queue Depth:

The queue depth is the number of I/O operations that can be run in parallel on a disk drive. This parameter is adjusted the queue depth capacity of NCQ (SATA HDD) or Tagged Command Queuing (SAS HDD) which transmits multiple commands to a single target without waiting for the initial command to complete. HDD Queue Depth options are 1, 2, 4, 8, 16, and 32.

Empty HDD Slot LED

The firmware has added the "Empty HDD Slot LED" option to setup the fault LED light "ON "or "OFF" when there is no HDD installed. When each slot has a power LED for the HDD installed identify, user can set this option to "OFF". Choose option "ON", the RAID controller will light the fault LED; if no HDD installed.

CPU Fan Detection

The "CPU Fan Detection" function is available in the firmware for detecting the cooling fan function on the ROC if you want to use the active cooling fan on the system. When using the passive heatsink only on the controller, disable the "CPU Fan Detection" function through this from Web Browser.

Max Command Length

Max Command Length is used to set a "best" IO size for the RAID controller.

Auto Activate Incomplete Raid

When some of the disk drives are removed in power off state or boot up stage, the RAID set state will change to "Incomplete State". But if a user wants to automatically continue to work while the RAID controller is powered on, the user can set the "Auto Activate Incomplete Raid" option to enable. The RAID state will change to "Degraded Mode" while it powers on.

Disk Write Cache Mode:

The RAID subsystem supports Disk Write Cache Mode options: Auto, Enabled, and Disabled. If the RAID subsystem has BBM (battery backup module), selecting the Auto option will automatically enable Disk Write Cache. On the other hand, if there is no BBM, the Auto option will disable Disk Write Cache.

SATA Target Mode Speed

The eSATA host interface appears to the host adapter as 6.0Gbps SATA target device. It can set as 3.0Gbps SATA target device in case any 3.0Gbps host adapter compatibility issue.

Write Same For Initialization

Drives that support the Write Same feature (SCT) can write to multiple drive sectors at once, improving initialization time. To take advantage of this feature, all the drives in the unit must support Write Same. User can set the "Enabled" or "Disabled" for the controller initialization.

Hot Plugged Disk For Rebuilding

It defines if the RAID array volume should start rebuilding or not when detects a disk is inserted/re-inserted during online.
The options are: Blank Disk Only, Always, and Disable. The default is **Blank Disk Only**.

Blank Disk Only: it will trigger the rebuilding if and only if the inserted disk has not been in the RAID array before, which has no RAID signature on it. So when a previously removed disk is self re-inserted, it won't trigger the degraded RAID array to rebuild, and so that the administrator has a chance to identify this misbehaving disk and replaces it.

Always: it is what it was before. Whenever a disk is inserted/ re-inserted whether new or previously existed, it always trigger a rebuilding for the Degraded RAID set/Volume.

Disable: it will not trigger rebuilding regardless what sort of disk plugging in. When **Disable** and/or **Blank Disk Only** is selected, the re-inserted/previously removed disk will be identified as a disk in a separate RAID set with duplicated RAIDset# and with all the rest of RAID members missing.

Disk Capacity Truncation Mode:

The RAID subsystem use drive truncation so that drives from different vendors are more likely to be able to be used as spares for each other. Drive truncation slightly decreases the usable capacity of a drive that is used in redundant units. Options are:

Multiples Of 10G: If you have several 120GB drives from different vendors, chances are that the capacity varies slightly. For example, one drive might be 121.1 GB, and the other 120.4 GB. This drive truncation mode makes the 121.1 GB and 120.4 GB drives same capacity as 120 GB so that one could replace the other.

Multiples Of 1G: If you have 120 GB drives from different vendors, chances are that the capacity varies slightly. For example, one drive might be 121.1 GB, and the other 121.4 GB. This drive truncation mode makes the 121.1 GB and 121.4 GB drives same capacity 121 GB so that one could replace the other.

No Truncation: The capacity of the disk drive is not truncated.

Smart Option For HDD

This option is used to increases the reliability of SSDs/HDDs by automatically copying data from a drive with potential to fail to a designated hot spare or newly inserted drive.
The options are: Failed The Drive, Failed The Drive If Hot Spare Exist, and Alert Only.
The default is **Alert Only**.

Failed The Drive- controllers kill off the SMART fail drive immediately.
Failed The Drive If Hot Spare Exist – controllers kill off the SMART fail disk if hot spare dive is existed.
Alert Only – it will trigger alert when there happens a SMART failed drive.

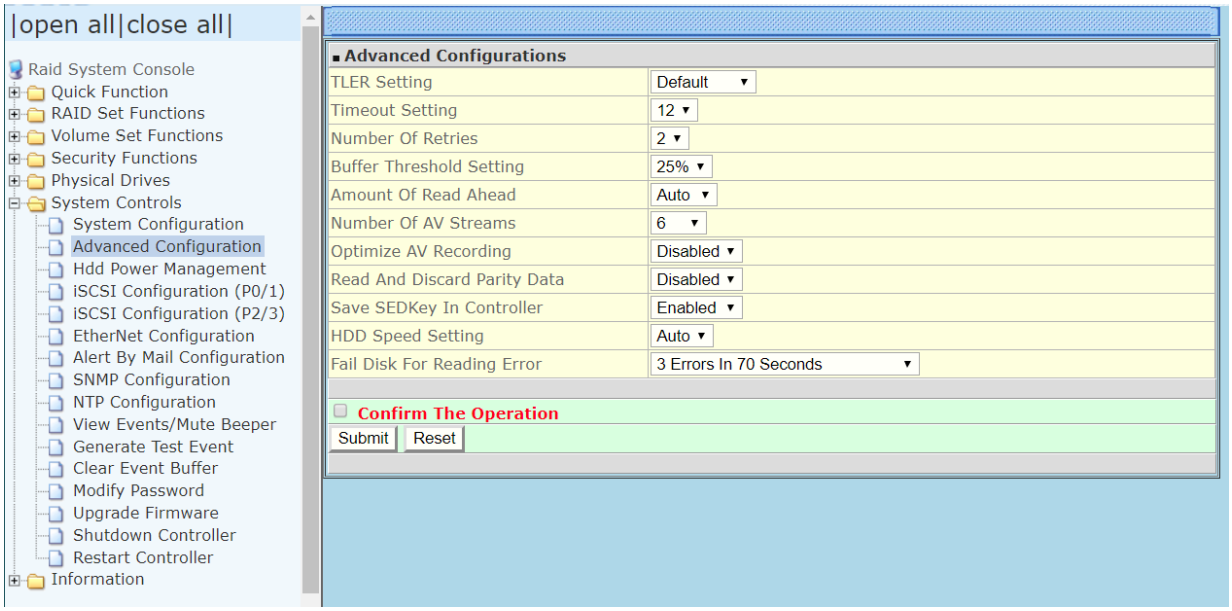
Smart Polling Interval

Besides the scheduled volume check, user can define the Smart Pulling Interval to pull the SMART status of each disk. The default is **on demand**. User can schedule every certain period of time interval to pull the SMART status of each disk.
When SMART pulling is executed, disk activity will be temporally halted until the SMART parameter reading is finished. That is why you don't want to set the Interval too frequent. What to use is up to the users to decide based on their applications and experiment results.

3.10.2 Advanced Configuration

To set the RAID system function, move the cursor to the main menu and click the **Advanced Configuration** link. The **Advanced Configuration** menu will show all items, then select the desired function.

NOTE: When you want to change the value on advance configuration screen, please contact your vendor's support engineer for assistance.



TLER Setting

TLER (time-limited error recovery) functions provide support for WD Caviar RE (RAID) series disks. This is a new option from WD to support RAID features that were traditionally missing from standard desktop drives. TLER is a method of signaling the system RAID controller in the event that an error recovery process is taking longer than time-out specifications allow. This prevents the RAID controller from dropping the drive from the array during this period. Default value is manufacture setting. You can select between 5, 6 and 7 second. This feature is to setup the HDD internal timeout value.

Timeout Setting

Disk time-out is a registry setting that defines the time that RAID controller will wait for a hard disk to respond to a command. You can modify the retry value by entering a new value in the edit box beside this button and then selecting the button. Normally you should not need to modify this value. Default value is 12 seconds: You can select between 8~32 second.

Number of Retries

This setting determines the number of access that will be attempted before the current command from the RAID controller to the disk drive is aborted. You can modify the retry value by entering a new value in the edit box beside this button and then selecting the button. Normally you should not need to modify this value. There are two selections, either 2 retry or 3 retry.

Buffer Threshold

This new feature there are 4 options; 5%, 25%, 50%, 75%. The percentage represents how much data should be kept in resident cache memory (how full cache should get) before controller starts to flush data onto the hard drives. If the buffer is set for 25%, then all 25% will be cached and is used for writing data. The remaining cache memory will be used for reading and other system overhead. Write buffer threshold for 5% is added for video recording. This option will push data to disk early.

This feature gives controller extra buffer time in case of slow response from the hard drives within a given time. Consequently, this can prevent a pause in data flow and there will be continues data access and stream. This feature is very useful for the video streaming applications where there is high demand for constant non-stop data flow with no interruption due to lower performance of specific hardware.

Amount of Read Ahead

Read-Ahead data is buffered in the RAID controller cache, however, thereby cutting down on the amount of I/O traffic to the disk. The Amount of Read Ahead defines how many data of reading at a time, making more efficient use of the RAID subsystem. This makes it possible to locate and re-issue the data without repetitive hard parsing activities.
The Amount of Read Ahead parameter is used to allocate an amount of memory in the cache memory the frequently executed queries and return the result set back to the host without real disk read execution. Default value is Auto: Controller will base on the HDD number to set the amount of Read Ahead value. You can select between 512KB ~ 32MB.

Number of AV Stream

RAID controllers are required to have not only the function of processing ordinary data but also the function of dealing with AV (audio/video) stream data needing real-time processing. Since the bus cycle used in RAID controller was designed to transfer the computer data exactly, it was unsuitable for the transfer of AV stream needing great band widths. They are required to do some setting for the handshaking during the processing of stream data. This setting is an object of transferring stream data efficiently on an existing RAID controller. Normally you should not need to modify this value. Default value is 6. You can select between 6~256.

To decide how to set AV stream playout parameter, you need to check the Number of Stream, Amount of Read Ahead, and Total Cache Memory during runtime. You can try to adjust the three numbers to get the best performance as your requirement. Number of Stream shows the number of stream added to the system, Amount of Read Ahead shows the amount of Read Ahead data taken from the cache without real disk execution, and total cache memory shows the total available memory being installed in the RAID controller.

Optimize AV Recording

AV recording option is for video recording (no time limit), but if used in normal operation, performance may be degraded. This new feature there are 4 options; Disabled, Mode1, Mode2 and Mode 3. Default value is Disabled. Our controller cache uses LRU method, there have no special memory capacity reserved for read or write. The Mode 1, 2 and 3 are used for define the command sorting method. The default sorting method is helpful for normal applications, but not useful for AV applications, so we have defined three different sorting methods for these special applications. To decide how to optimize AV stream recording parameter, you need to adjust the Optimize AV Recording, and Write Buffer Threshold during runtime.

Read And Discard Parity Data

This function is used to determine if parity data is to be read and discarded.

Save SED Key In Controller

<a> If enable → disable, clear SED Key saved in setup
<b> If disable → enable, if key exists, save to setup If enable→disable, the key will not remain in the flash. So that next time power up again, it will need to input the key from the CLI again.

HDD Speed Setting

This option is used to set HDD Speed. Default value is Auto. You can select 6G or 3G.

Fail Disk For Reading Error

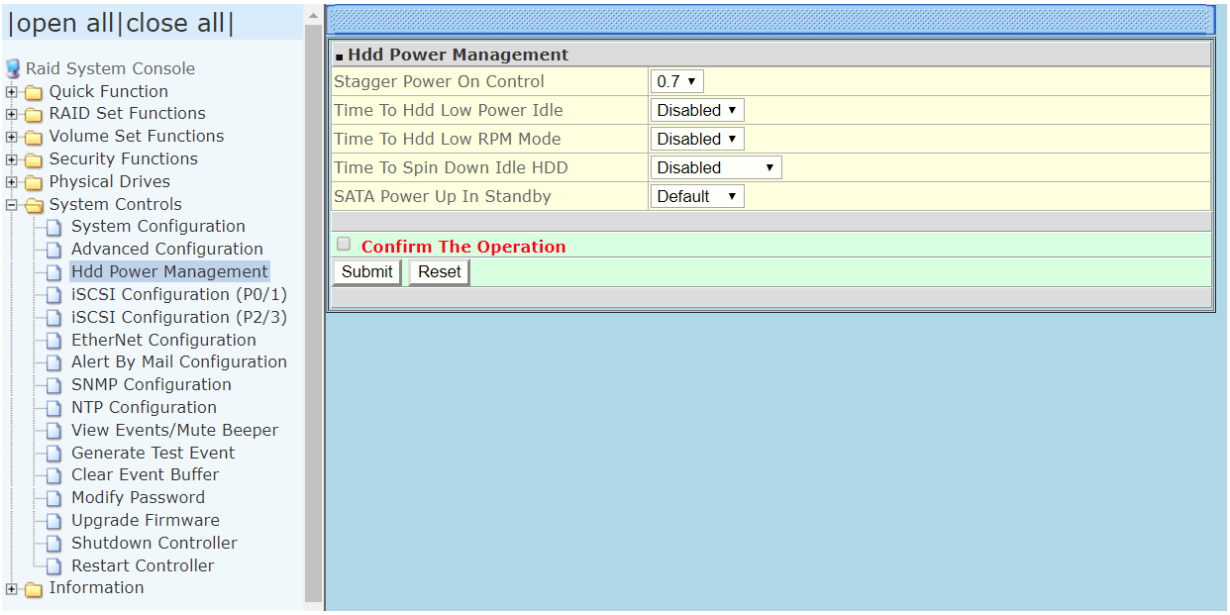
This option is available to improve the fail disk function if the disk has too many reading errors. This function is the option that RAID controller will kill off the HDD for reading error account setting value.

- 3 errors in 70 seconds: this option also includes 4 errors in 100 seconds, 5 errors in 120 seconds
- 6 errors in 2 minutes: this option also includes 8 errors in 180 seconds, 10 errors in 240 seconds
- 9 errors in 3 minutes: this option also includes 12 errors in 270 seconds, 15 errors in 360 seconds

3.10.3 HDD Power Management

MAID (**M**assive **A**rray of **I**dle **D**isks) is a storage technology that employs a large group of disk drives in which only those drives in active use are spinning at any given time. **This reduces power consumption and prolongs the lives of the drives.**
MAID is designed for Write Once, Read Occasionally (WORO) applications such as Data Backup, Document, Mail server, and so on.
MAID technology focuses on "Green Storage Concept" to save power consumption and enhance disk drives effective usage, i.e., "disk drives are spun down when there is no activity or I/O on the drives".

In the RAID subsystem, MAID is implemented in the **HDD Power Management** menu. Using the **Advanced Power Management (APM)** function of disk drives, HDD Power Management has three options (MAID Levels): (Level 1) Place idle drives in Lower Power Mode, where the drives' heads are unloaded; (Level 2) Place idle drives in Low RPM Mode, where drives' heads are unloaded and slows down to around 4000 RPM; and (Level 3) Spin down idle drives, where drives stops spinning and goes into sleep mode.



Stagger Power On Control:

This option allows the RAID subsystem's power supply to power up in succession each HDD in the RAID subsystem. In the past, all the HDDs on the RAID subsystem are powered up altogether at the same time. This function allows the power transfer time (lag time) from the last HDD to the next one be set within the range of 0.4 to 6.0 seconds. Default is 0.7 seconds.

Time to HDD Low Power Idle: (MAID Level 1)

This option enables the RAID subsystem to place idle HDDs of a RAID Set in Low Power Mode, where drives' heads are unloaded. The power consumption of the Idle HDD saving is around 15% to 20%. Recovery time is under a second.
Options are: Disabled, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, and 15 (Minutes).

Time to HDD Low RPM Mode: (MAID Level 2)

This option enables the RAID subsystem to place idle HDDs of a RAID Set in Low RPM Mode, where drives' heads are unloaded and drive platters speed is reduced to around 4000 RPM. The power consumption of the Idle HDD saving is from 35% to 45%. Recovery time is 15 seconds.
Options are: Disabled, 10, 20, 30, 40, 50, and 60 (Minutes).

Time to Spin Down Idle HDD: (MAID Level 3)

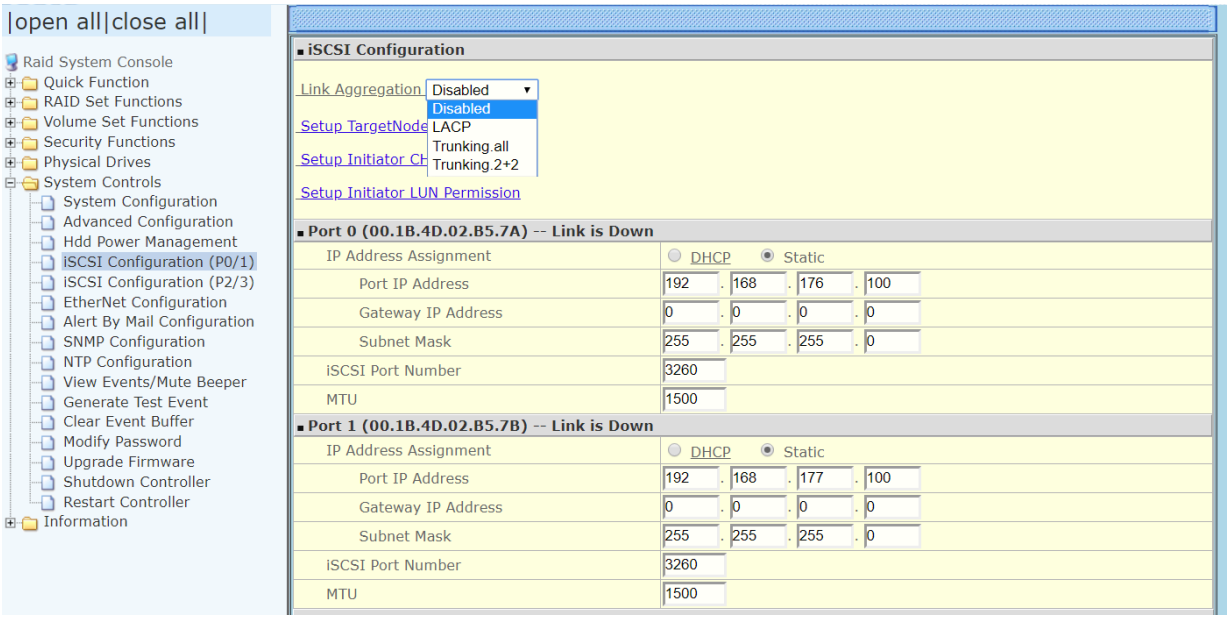
This option enables the RAID subsystem to spin down HDDs of a RAID Set after they become idle after a preset period of time. In this level, the drives stop spinning and go into sleep mode. The power consumption of the Idle HDD saving is from 60% to 70%. Recovery time is 30 to 45 seconds.
Options are: Disabled, 1 (For Test), 3, 5, 10, 15, 20, 30, 40, and 60 (Minutes).

SATA Power Up In Standby

SATA Power Up In Standby (power management 2 mode, PM2) is a SATA disk drive configuration which prevents the drive from automatic spinup when power is applied. **Enabled** option allows the drive to be powered-up into the Standby power management state to minimize inrush current at power-up and to allow the controller to sequence the spinup of devices. It is mainly for server/workstation environments operating in multiple-drive configurations.

3.10.4 iSCSI Configuration

To set the iSCSI Configuration options, click the **iSCSI Config** link under the **System Controls** menu. The iSCSI Configuration screen will be shown. Set the system configuration option as needed.



IP Address Assignment

- With DHCP (Dynamic Host Configuration Protocol), the IP address is assigned by the DHCP server. Click on the DHCP to show the DHCP lease information.
- With Static, the IP address must be entered manually for the iSCSI port. For a local environment, it's OK to leave Gateway IP Address as 0.0.0.0.

iSCSI Port Number: specify the port number to which the iSCSI port attempts to connect to the host adapter. Values within 1024 ~ 65535, excluding the registered ports, could be used. It's a good practice to keep this as 3260.

Maximum Transmission Unit (MTU): This parameter specifies the payload size of the GbE port, rather than the MTU of layer 3 packets. If Jumbo Frame is enabled by setting MTU to 1501 ~9000, make sure all the Ethernet switches and nodes are set to the same MTU. If unsure, set the MTU to 1500 for better compatibility.

Three types of access control can be applied.

1. Link Aggregation

Link Aggregation for Gigabit Interfaces feature allows you to bundle Gigabit Ethernet links to one logical link that functions as a single, higher-speed link providing dramatically increased bandwidth. All Gigabit Ethernet links must be point-to-point connections between the switch and the iSCSI port for link aggregation enable (LACP and Trunking). Two (P0&P1 or P2&P3) or four (P0&P1&P2&P3) Gigabit Ethernet connections are combined in order to increase the bandwidth capability and to create resilient and redundant links on the controller. The system offers these options for Link Aggregation that can be used within the switched environment;

Disabled: Indicates that the conventional connection is applicable.

LACP (IEEE 802.3ad): Use the switch-negotiated dynamic LACP.

Trunking (non-protocol): Provide manually configured, static-only Trunking.

The advantages of link aggregation enable in contrast with conventional connection are:

- higher potential transmission speed
- higher accessibility

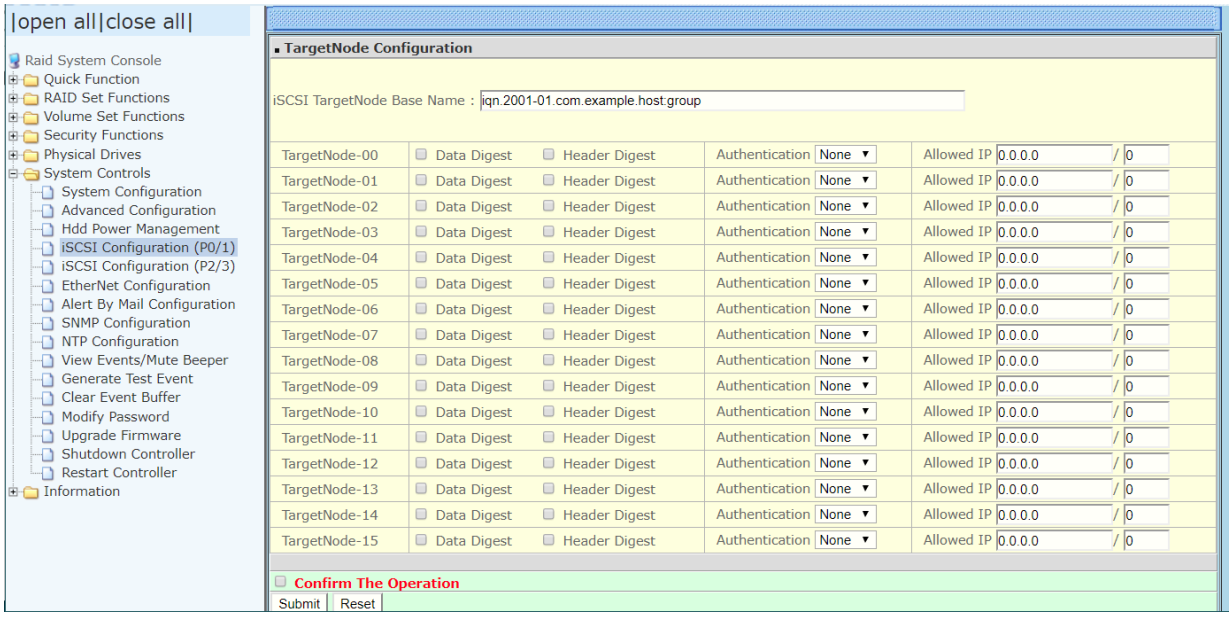
Disabled: Each of Gigabit Ethernet link is connected by itself and is not set to LACP and Trunking. The RAID controller supports four Gigabit Ethernet links to transmit data. Each of them must be assigned to individual port parameters in "Disabled" mode unless the link aggregation is enabled.

LACP (IEEE 802.3ad): LACP is part of the IEEE specification 802.3ad that allows you to bundle several Gigabit Ethernet links to form a single logical link. The RAID controller implements it as active mode which means that LACP port sends LACP protocol packets automatically. For this to work, both ends of the link must be dynamic LACP. If four ports are set in LACP mode, Port 0 parameters will be used for the Link Aggregated Group.

Trunking (Non-protocol): Trunking allows you to combine multiple Gigabit Interfaces in parallel to one logical link that functions as a single interface, higher-speed link providing dramatically increased bandwidth. If every two ports are set in Trunking mode (Trunking.2+2), Port 0&2 parameters will be used for the Link Aggregated Group. If four ports are set in Trunking mode (Trunking.All), Port 0 parameters will be used for the Link Aggregated Group.

2. Per TargetNode IP filtering

To setup volume TargetNode parameter, move the mouse to click on the "Setup TargetNode Parameter" function of the iSCSI Configuration. The"TargetNode Configuration" screen will be shown.



Data/Header Digest: The header/data digest fields are optional values in the iSCSI header to identify, reject and request retransmission of a corrupt PDU.

Authentication: The Challenge Handshake Authentication Protocol (CHAP) is a protocol that is used to authenticate the peer of a connection and is based upon the peers sharing a secret (a security key that is similar to a password).

The options are: "None", and "CHAP". The default is "None".

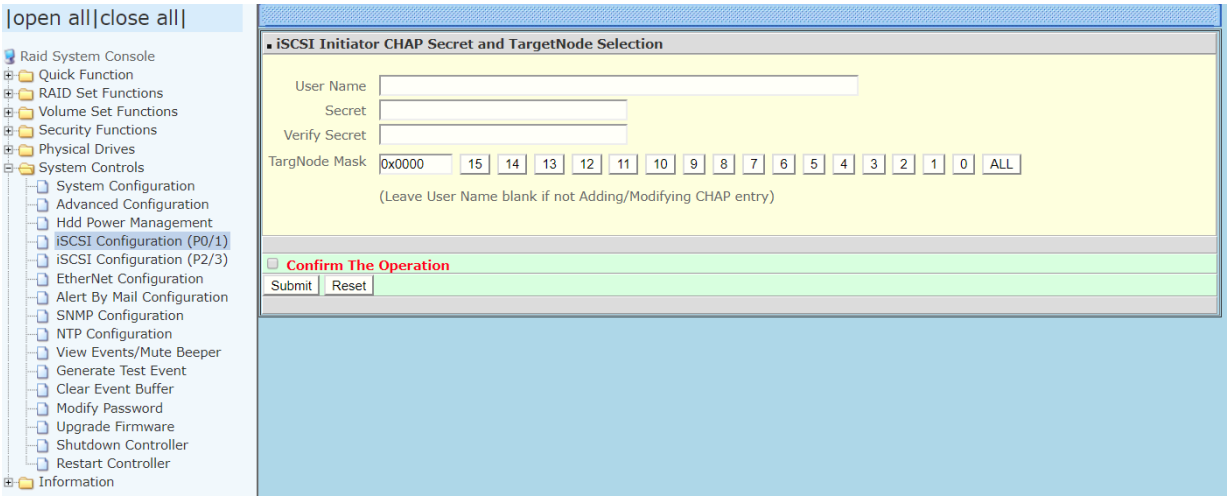
None: To disable CHAP function.

CHAP: Go to /iSCSI Configuration/Setup Initiator CHAP Secret page to create user Name, Secret and TargNode Mask.

Allowed IP: Applied with or without CHAP enabled. Only the specified subrange of IP address can access specific Target-Node. The IP subrange notation is similar to CIDR notation as xxx.xxx.xxx.xxx/mm (xxx.xxx.xxx.xxx is the base IP address and mm is # of mask bits). MaskBits is allowed to be 0~32 (instead of 0~30 in CIDR) and specifies bits to be matched from MSB. When mm is set to 0, all IP will match successfully (IP filtering is effectively disabled). When mm is set to 32, only single IP (host) can access the specified TargetNode.

3. Per Initiator TargetNode Mask

Setup an authentication for your iSCSI devices is optional. In a secure environment, authentication is not required because only trusted initiators can access the target devices. To setup the iSCSI initiator CHAP secret parameter, move the mouse to click on the "Setup iSCSI Initiator CHAP Secret" function of the iSCSI Configuration. The "iSCSI Initiator CHAP Secret and TargetNode Selection" screen will be shown.



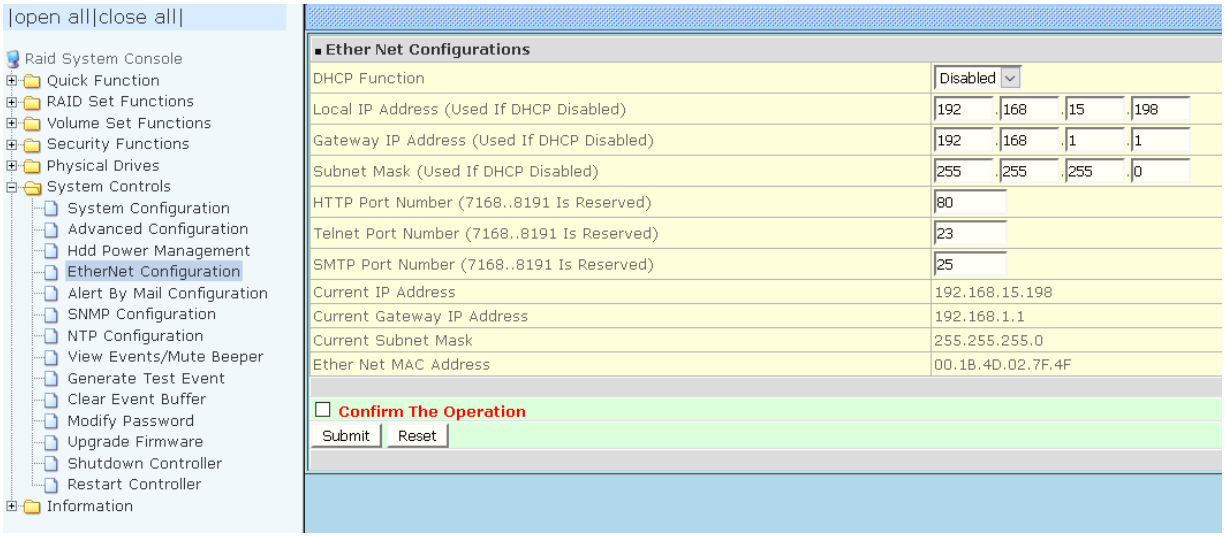
User Name: The initiator CHAP user name can be found using your iSCSI initiator software. The user name alphanumeric character length depends on the host adapter. Leave User Name blank if not Adding/Modifying CHAP entry.

Secret: It is the secret key that the initiator must know to participate in CHAP with the target similar to a password. The initiator CHAP secret alphanumeric character length depends on the host adapter.

TargNode Mask: Initiator accessibility can be limited to specific subset of TargetNodes with this. Click on the TargNode number (0 ~ 15) to exclude accessibility of that TargNode (corresponding mask bit is set to 1).

3.10.5 EtherNet Configuration

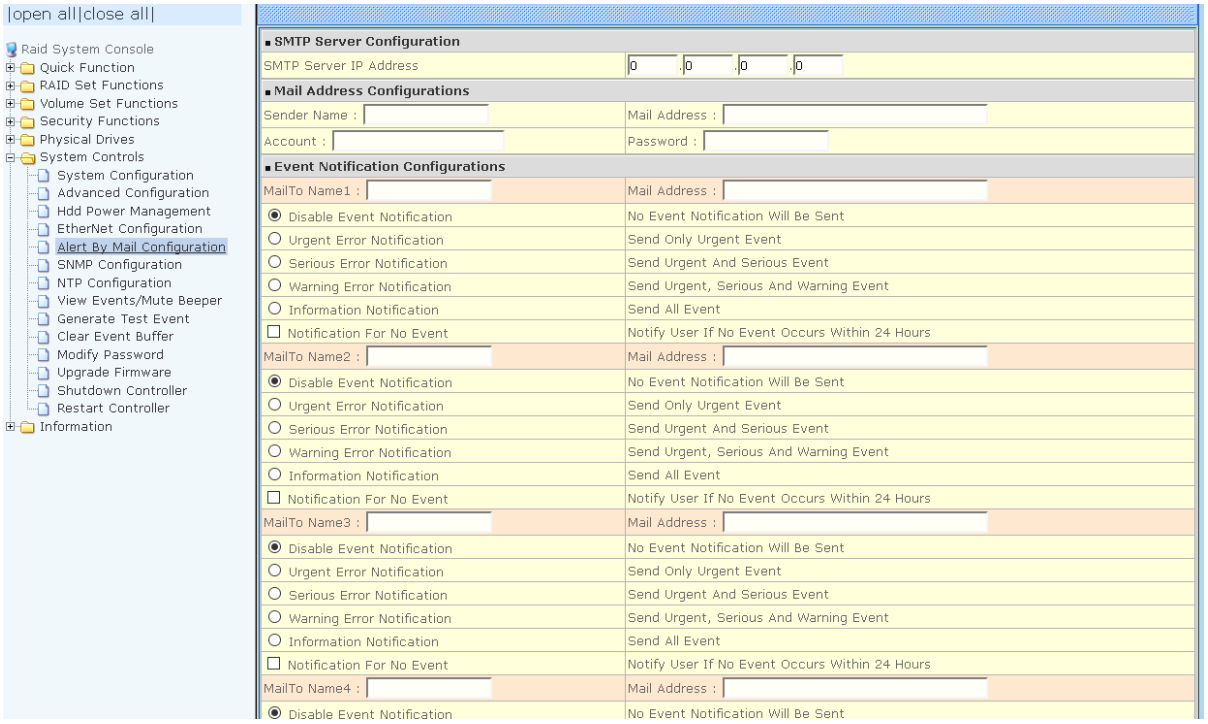
To set the Ethernet configuration, click the **EtherNet Configuration** link under the System Controls menu. The RAID subsystem EtherNet Configuration screen will be shown. Set the desired configuration. Once done, tick on the **Confirm The Operation** and click the **Submit** button to save the settings.



NOTE: If HTTP, Telnet and SMTP Port Number is set to "0", the service is disabled.

3.10.6 Alert By Mail Configuration

To set the Event Notification function, click on the **Alert By Mail Configuration** link under the System Controls menu. The Event Notification configuration screen will be shown. Set up the desired function and option. When an abnormal condition occurs, an error message will be emailed to the email recipient(s) that a problem has occurred. Events are classified into 4 levels (Urgent, Serious, Warning, and Information).



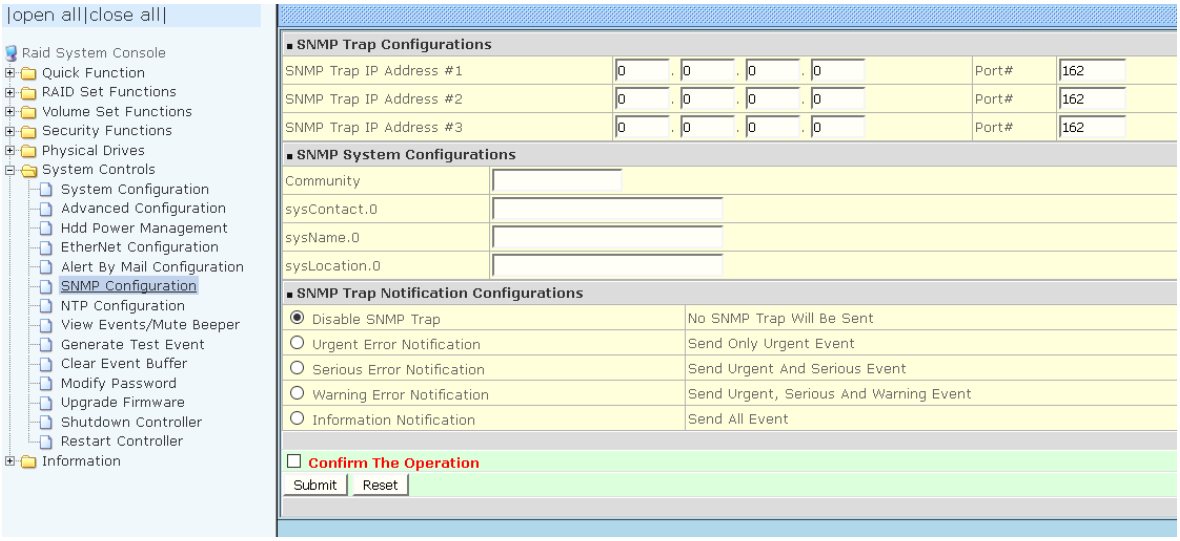
NOTE: If Event Notification by email is enabled, every 30 of event log will be sent to the email recipient(s) as one package log.

NOTE: If different email recipients are setup, the event notification levels for each email recipient can be configured differently. For example, first email recipient can be configured with "Urgent Error Notification" while second email recipient can be configured with "Serious Error Notification".

3.10.7 SNMP Configuration

The SNMP gives users independence from the proprietary network management schemes of some manufacturers and SNMP is supported by many WAN and LAN manufacturers enabling true LAN/ WAN management integration.

To set the SNMP function, move the cursor to the main menu and click on the **SNMP Configuration** link. The SNMP Configurations screen will be shown. Select the desired function and set the preferred option.



SNMP Trap Configurations: Type in the SNMP Trap IP Address box the IP address of the host system where SNMP traps will be sent. The SNMP Port is set to 162 by default.

SNMP System Configuration:

Community: Type the SNMP community. The default is public.
(1) **sysContact.0**, (2) **sysLocation.0**, and (3) **sysName.0**: SNMP parameter (31 bytes max). If these 3 categories are configured and when an event occurs, SNMP will send out a message that includes the 3 categories within the message. This allows user to easily define which RAID unit is having problem.

SNMP Trap Notification Configurations: Select the desired option.

After completing the settings, tick on the **Confirm The Operation** and click on the **Submit** button to save the configuration.

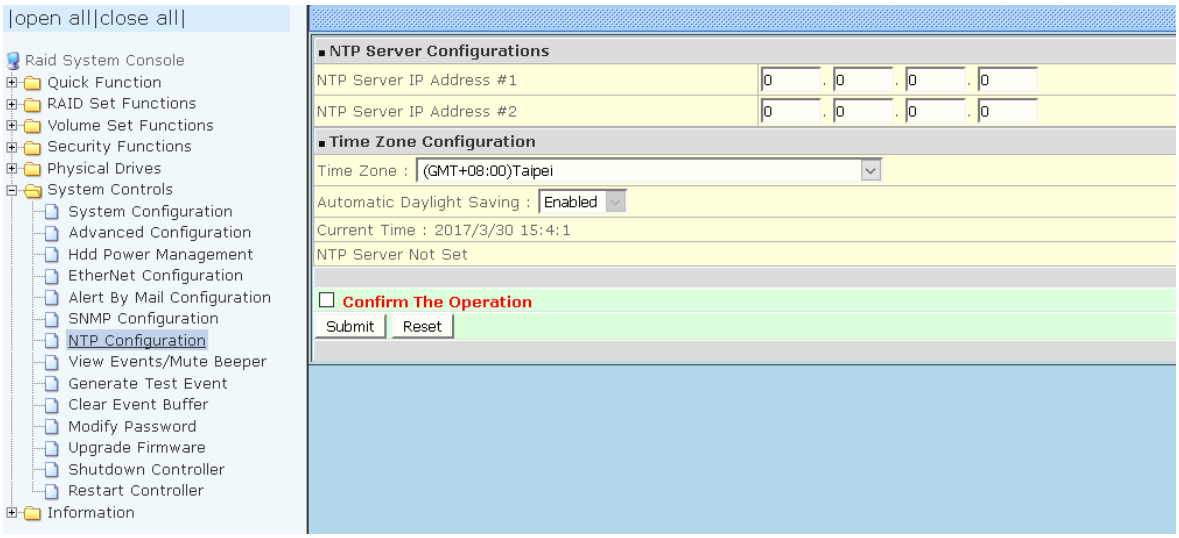
SNMP also works in the same as Alert By Mail when sending event notifications.

3.10.8 NTP Configuration

NTP stands for **Network Time Protocol**. It is an Internet protocol used to synchronize the clocks of computers to some time reference. Type the NTP Server IP Address to enable the RAID Subsystem to synchronize with it.

To set the NTP function, move the cursor to the main menu and click on the **NTP Configuration** link. The NTP Configuration screen will be displayed. Select the desired function and configure the necessary option.

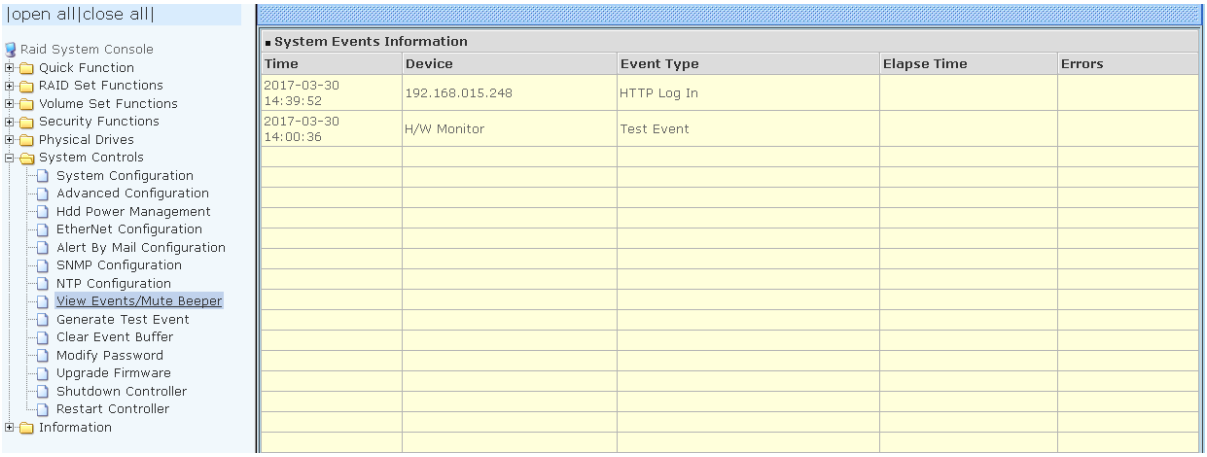
After completing the settings, tick on the **Confirm The Operation** and click on the **Submit** button to save the configuration.



3.10.9 View Events / Mute Beeper

To view the RAID Subsystem's event log information, move the mouse cursor to the System Controls menu and click on the **View Events/Mute Beeper** link. The System Events Information screen appears.

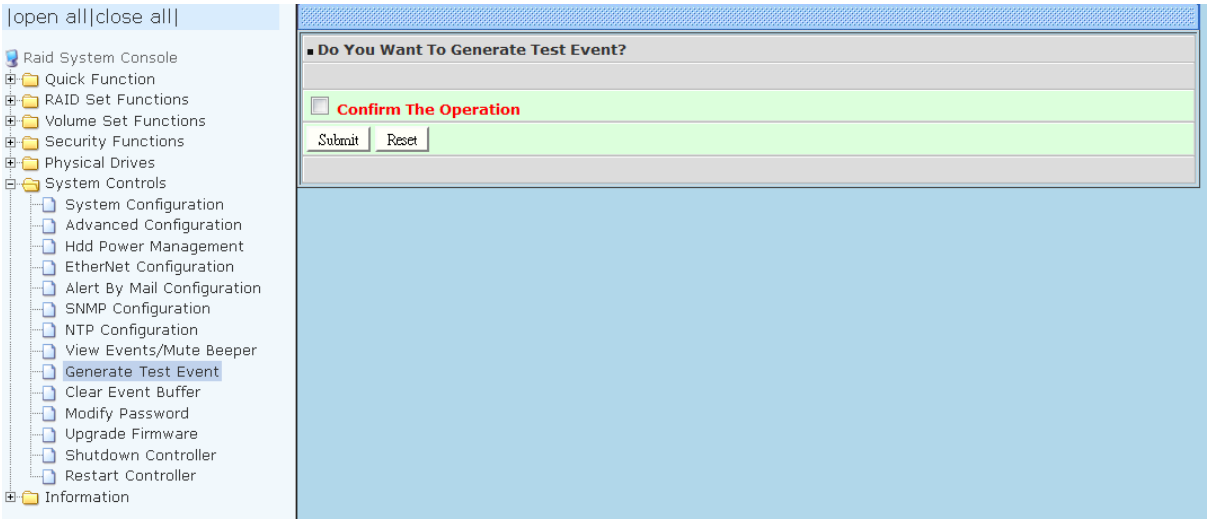
The System Events Information screen will show: Time, Device, Event type, Elapse Time and Errors.



This function is also used to silence the beeper alarm.

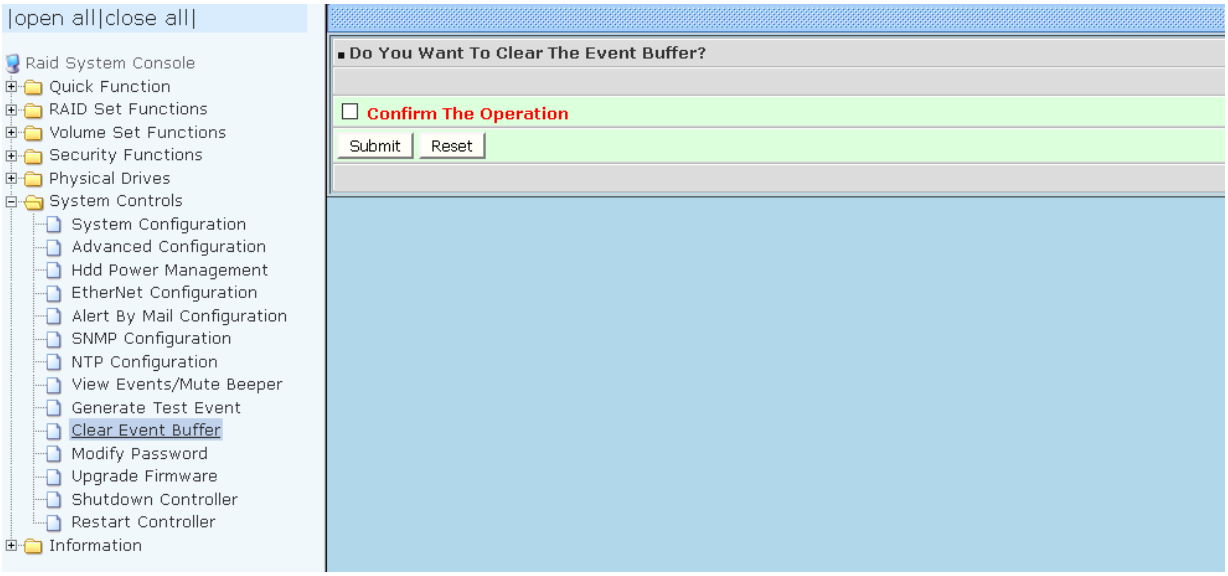
3.10.10 Generate Test Event

If you want to generate test events, move the cursor bar to the main menu and click on the **Generate Test Event** Link. Tick on the **Confirm The Operation** and click on the **Submit** button. Then click on the **View Events/Mute Beeper** to view the test event.



3.10.11 Clear Event Buffer

Use this feature to clear the RAID Subsystem's System Events Information buffer.



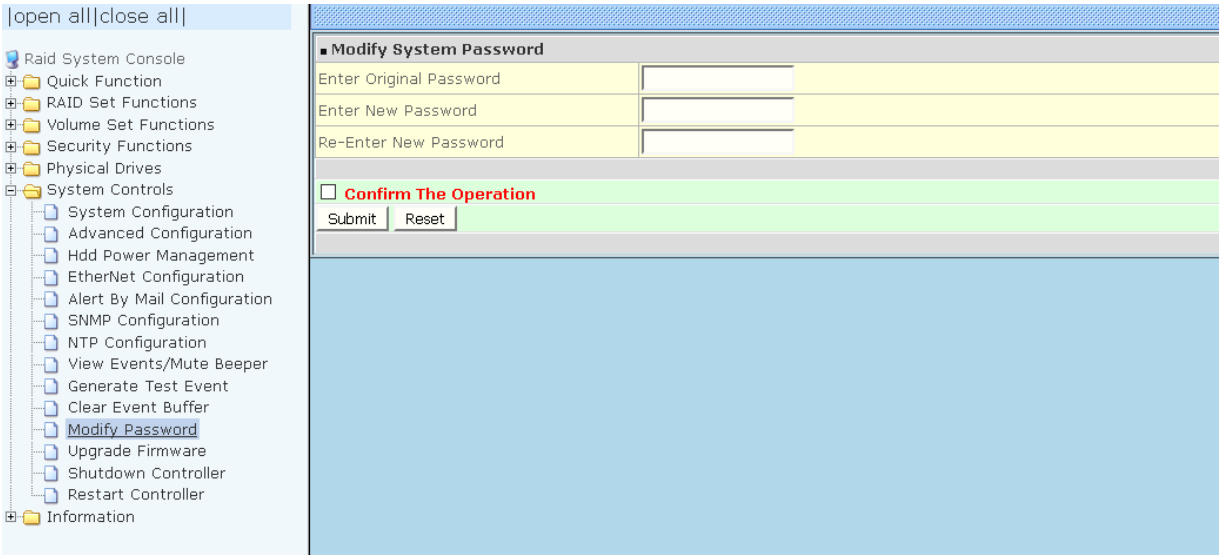
3.10.12 Modify Password

To change or disable the RAID Subsystem's admin password, click on the **Modify Password** link under the **System Controls** menu. The Modify System Password screen appears.

The factory-default admin password is set to **00000000**. Once the password has been set, the user or administrator can only monitor and configure the RAID Subsystem by providing the correct password.

The password is used to protect the RAID Subsystem's configuration from unauthorized access. The RAID controller will check the password only when entering the Main Menu from the initial screen. The RAID Subsystem will automatically go back to the initial screen when it does not receive any command after sometime.

To disable the password, enter only the original password in the **Enter Original Password** box, and leave both the **Enter New Password** and **Re-Enter New Password** boxes blank. After selecting the **Confirm The Operation** option and clicking the **Submit** button, the system password checking will be disabled. No password checking will occur when entering the main menu from the starting screen.



NOTE: The admin Password characters allowed are 'A' – 'Z', 'a' – 'z', and '0' – '9'. The minimum number of Password characters is null/empty (Password is disabled) and maximum number of Password characters is 15.

3.10.13 Upgrade Firmware

Please refer to Section 3.13 for more information.

3.10.14 Shutdown Controller

Use this function to shutdown the RAID Controller. This is used to flush the data from the cache memory, and is normally done before powering off the system power switch.

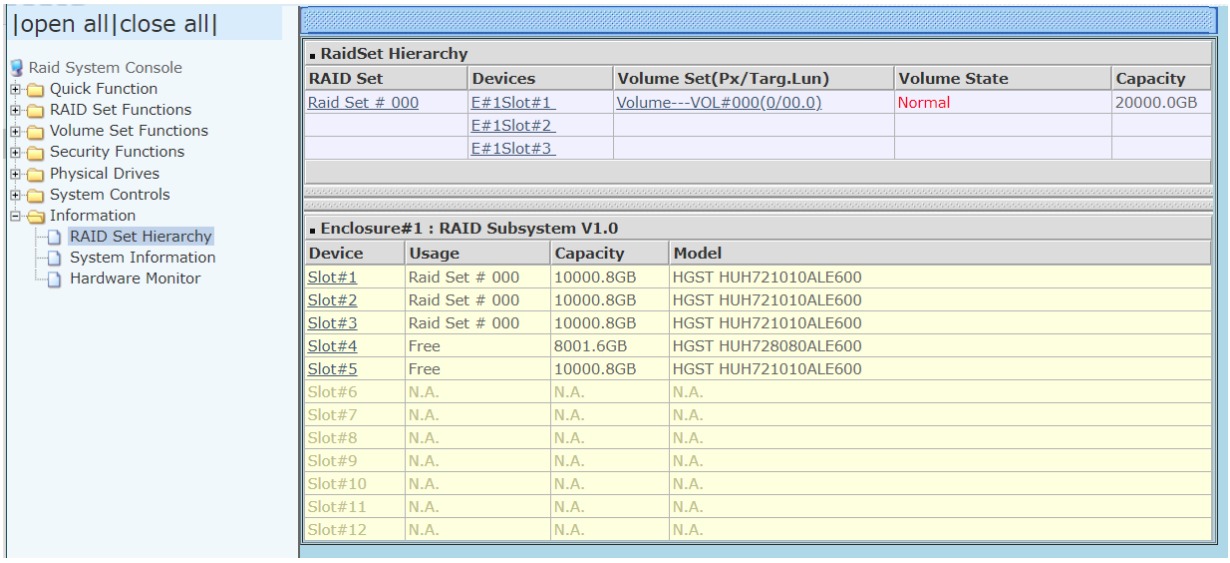
3.10.15 Restart Controller

Use this function to restart the RAID Controller.

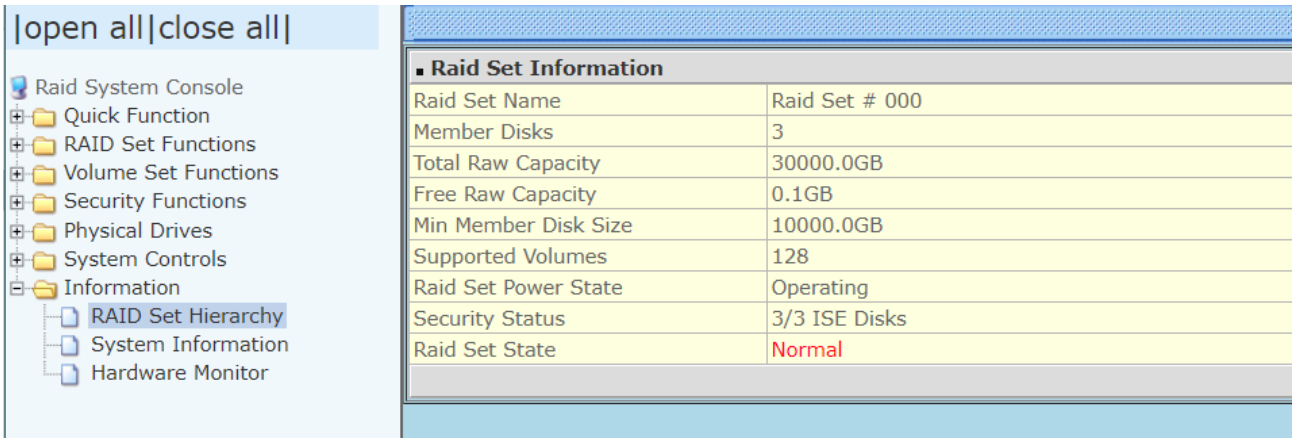
3.11 Information Menu

3.11.1 RaidSet Hierarchy

Use this feature to view the RAID subsystem's existing Raid Set(s), Volume Set(s) and physical disk(s) configuration and information. Select the **RaidSet Hierarchy** link from the **Information** menu to display the Raid Set Hierarchy screen..

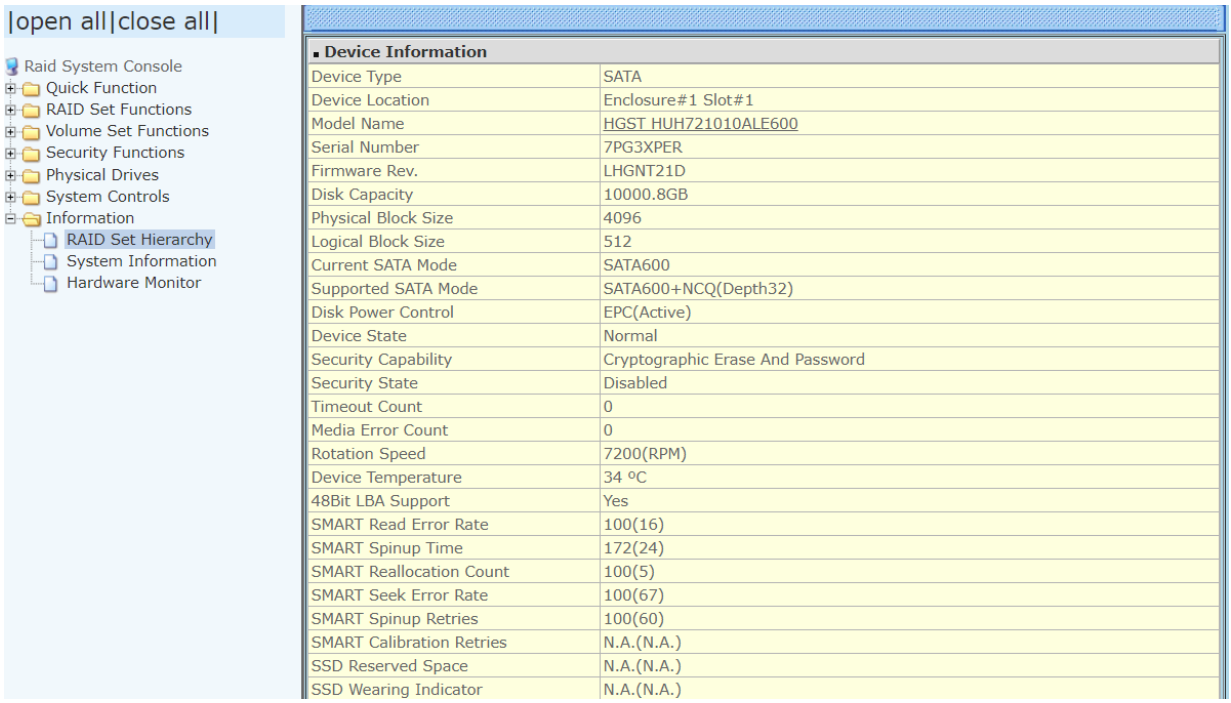


To view the Raid Set information, click the **Raid Set #** link from the Raid Set Hierarchy screen. The Raid Set Information screen appears.



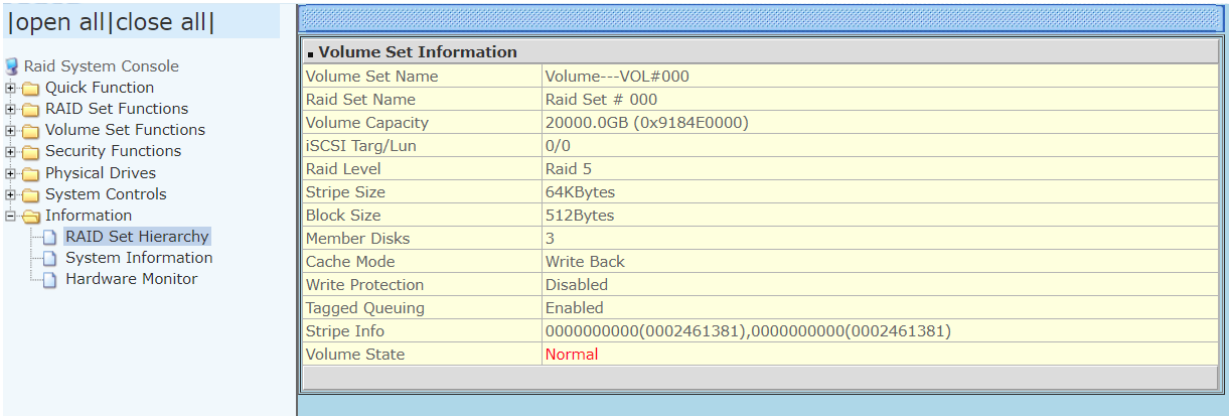
Raid Set Power State has Operation and Spin down.
Raid Set State has Normal mode, Degraded mode and Incomplete mode.

To view the disk drive information, click the **E# Slot#** link from the Raid Set Hierarchy screen. The Disk Information screen appears. This screen shows various information such as timeout count, media error count, and SMART information.



Device Information	
Device Type	SATA
Device Location	Enclosure#1 Slot#1
Model Name	HGST HUH721010ALE600
Serial Number	7PG3XPER
Firmware Rev.	LHGNT21D
Disk Capacity	10000.8GB
Physical Block Size	4096
Logical Block Size	512
Current SATA Mode	SATA600
Supported SATA Mode	SATA600+NCQ(Depth32)
Disk Power Control	EPC(Active)
Device State	Normal
Security Capability	Cryptographic Erase And Password
Security State	Disabled
Timeout Count	0
Media Error Count	0
Rotation Speed	7200(RPM)
Device Temperature	34 ºC
48Bit LBA Support	Yes
SMART Read Error Rate	100(16)
SMART Spinup Time	172(24)
SMART Reallocation Count	100(5)
SMART Seek Error Rate	100(67)
SMART Spinup Retries	100(60)
SMART Calibration Retries	N.A.(N.A.)
SSD Reserved Space	N.A.(N.A.)
SSD Wearing Indicator	N.A.(N.A.)

TTo view the Volume Set information, click the **Volume---VOL#** link from the Raid Set Hierarchy screen. The Volume Set Information screen appears.

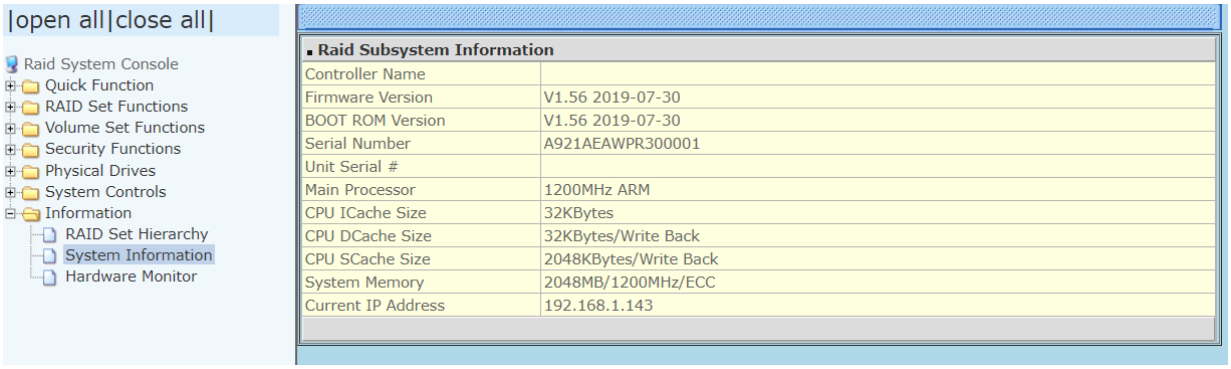


Volume Set Information	
Volume Set Name	Volume---VOL#000
Raid Set Name	Raid Set # 000
Volume Capacity	20000.0GB (0x9184E0000)
iSCSI Targ/Lun	0/0
Raid Level	Raid 5
Stripe Size	64KBytes
Block Size	512Bytes
Member Disks	3
Cache Mode	Write Back
Write Protection	Disabled
Tagged Queuing	Enabled
Stripe Info	0000000000(0002461381),0000000000(0002461381)
Volume State	Normal

Volume State has Normal mode, Degraded mode, Initializing mode (Foreground or Background), Rebuilding mode, Checking mode, Migrating mode, Cloning and Failed mode.

3.11.2 System Information

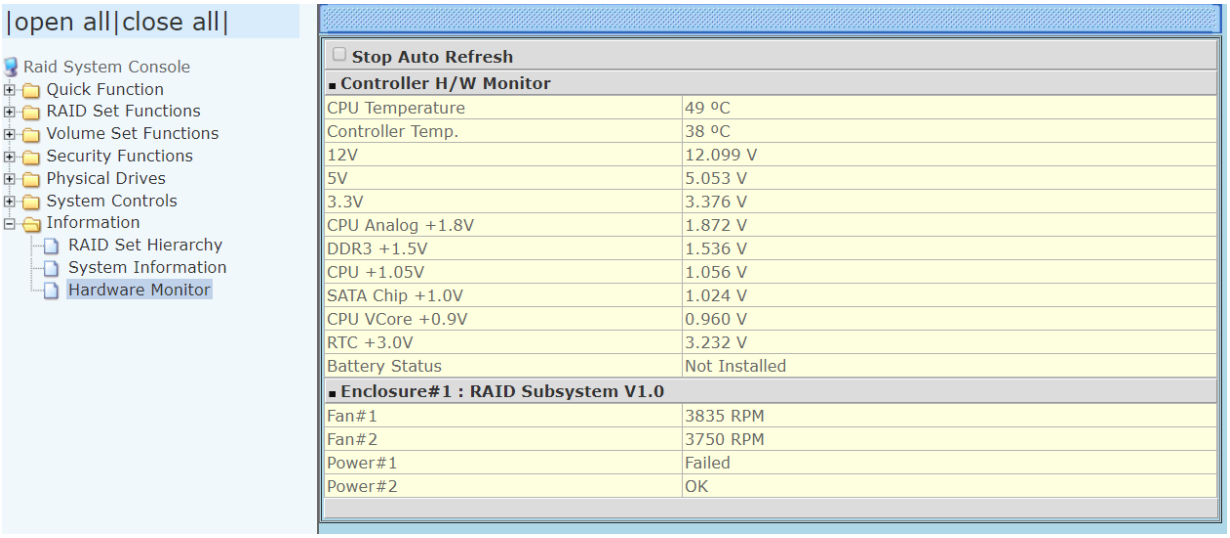
To view the RAID subsystem's controller information, click the **System Information** link from the **Information** menu. The Raid Subsystem Information screen appears.



The controller name, firmware version, BOOT ROM Version, serial number, main processor, CPU ICache size, CPU DCache size, CPU SCache Size, and system memory size/speed appear in this screen.

3.11.3 Hardware Monitor

To view the RAID subsystem's controller hardware information, click the **Hardware Monitor** link from the **Information** menu. The Hardware Monitor Information screen appears.



NOTE: To disable auto refresh of GUI, tick the "Stop Auto Refresh" option.

The following are the states of Battery Backup Module(BBM):

State	Description
Not Installed	BBM is not installed
xx%	The percentage of battery remaining
Charged(100%)	BBM is completely charged
Failed	BBM is Failed.

3.12 Upgrading the Firmware

Upgrading Firmware Using Flash Programming Utility

Since the RAID subsystem's controller features flash firmware, it is not necessary to change the hardware flash chip in order to upgrade the controller firmware. User can simply re-program the old firmware through the RS-232 port. New releases of the firmware are available in the form of binary file at vendor's FTP. The file available at the FTP site is usually a self-extracting file that contains the following:

XXXXVVV.BIN Firmware Binary (where "XXXX" refers to the model name and "VVV" refers to the firmware version)

README.TXT It contains the history information of the firmware change. Read this file first before upgrading the firmware.

These files must be extracted from the compressed file and copied to one directory in the host computer.

Establishing the Connection for the RS-232

The firmware can be downloaded to the RAID subsystem's controller using an ANSI/VT-100 compatible terminal emulation program or web browser-based RAID Manager remote management page.

With terminal emulation program, you must complete the appropriate installation and configuration procedure before proceeding with the firmware upgrade. Whichever terminal emulation program is used must support the ZMODEM file transfer protocol.

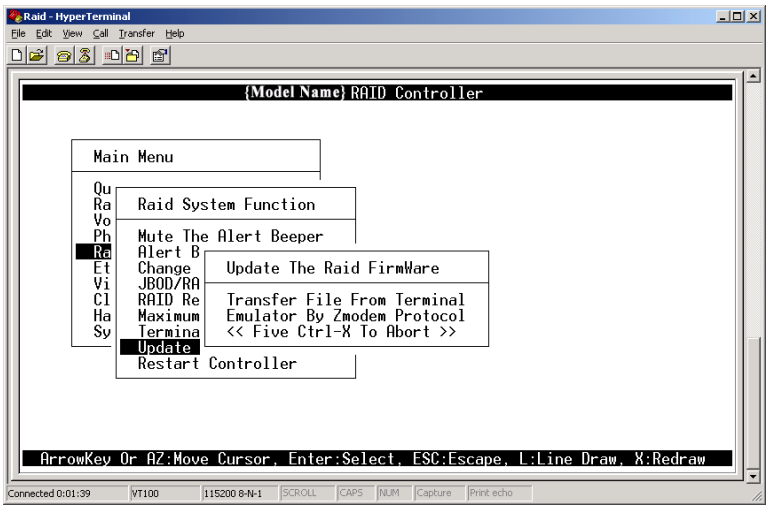
Web browser-based RAID Manager can be used to update the firmware. A web browser must have been installed and setup before proceeding with the firmware upgrade.

Upgrading Firmware Through ANSI/VT-100 Terminal Emulation

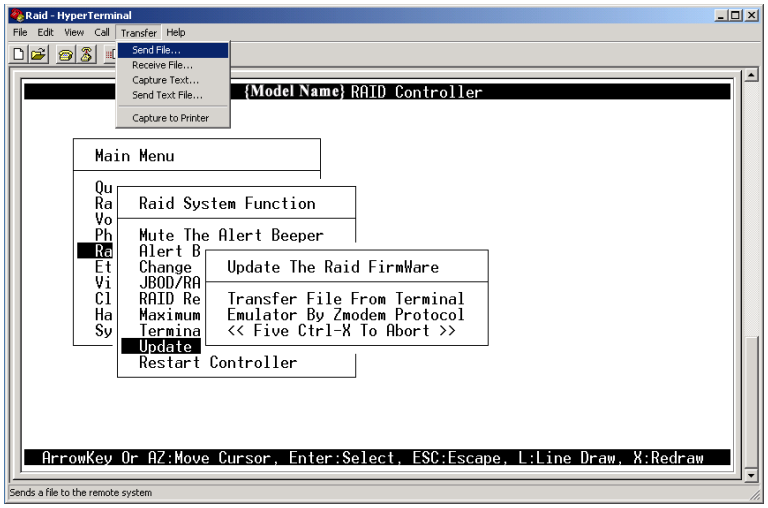
Get the new firmware version for your RAID subsystem controller. For Example, download the bin file from your vendor's web site into the local directory.

NOTE: When there is new boot ROM firmware that needs to be upgraded, upgrade first the boot ROM firmware. Then repeat the process (steps 1 to 9) to upgrade the firmware code after which a RAID controller restart will be necessary.

1. From the Main Menu, scroll down to "Raid System Function"
2. Choose the "Update Firmware". The **Update The Raid Firmware** dialog box appears.

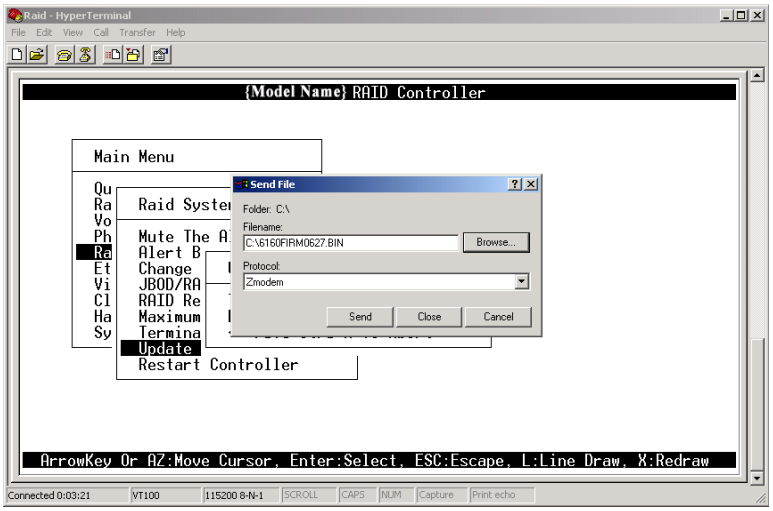


3. Go to the menu bar and click **Transfer**. Select **Send File**.

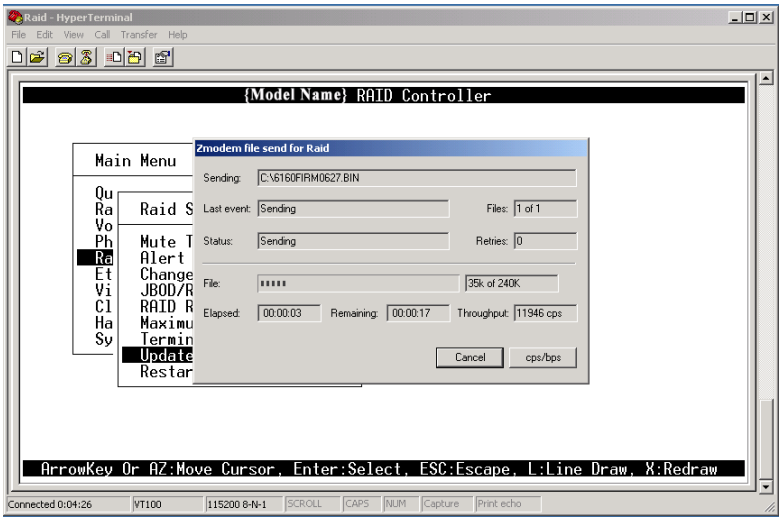


4. Select "ZMODEM modem" under Protocol to set ZMODEM as the file transfer protocol of your terminal emulation software.

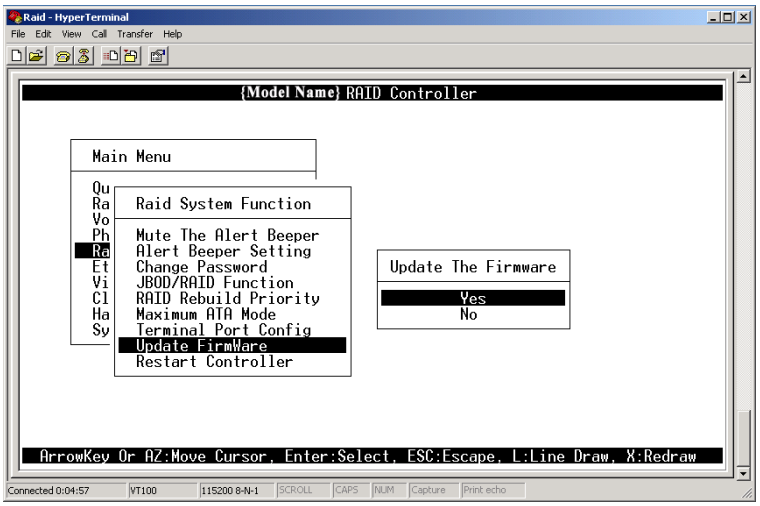
5. Click Browse. Look in the location where the firmware file was saved. Select the firmware file name "xxxxxxxx.BIN" and click Open.



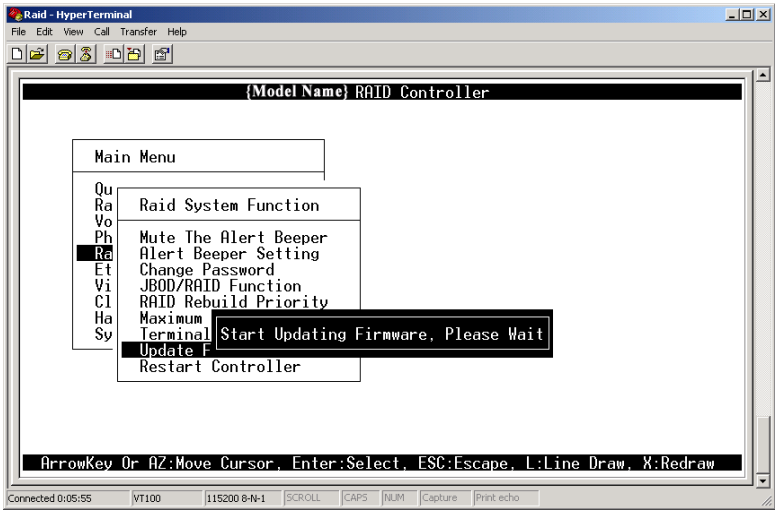
6. Click Send to send the firmware binary file to the RAID controller.



7. When the firmware downloading is completed, the confirmation screen appears. Select Yesto start programming the flash ROM.

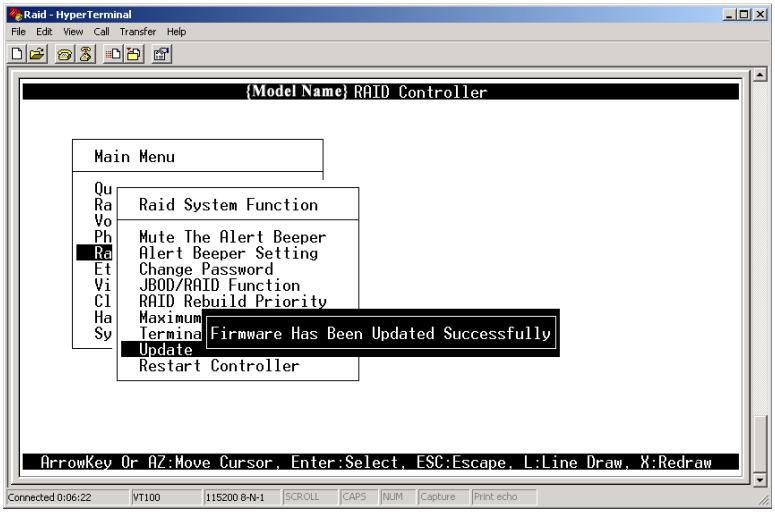


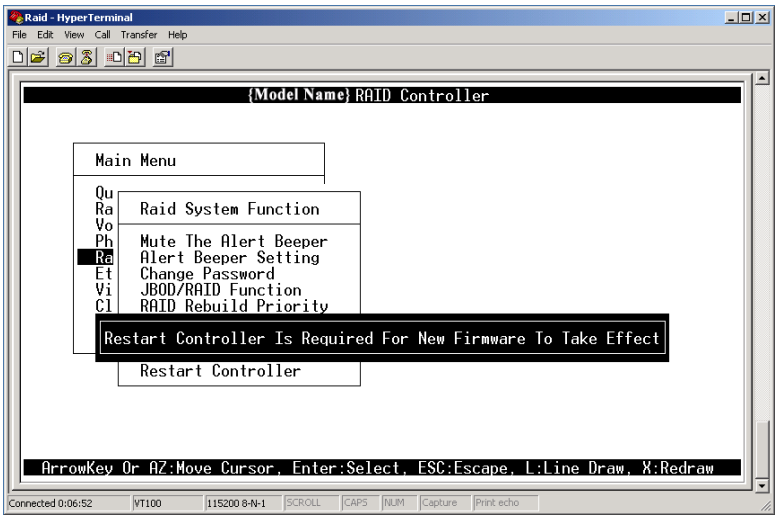
8. When the Flash programming starts, a message will show " Start Updating Firmware. Please Wait".



9. The firmware upgrade will take approximately thirty seconds to complete.

10. After the firmware upgrade is complete, a message will show "Firmware Has Been Updated Successfully". Restarting the RAID controller is required for the new firmware to take effect.





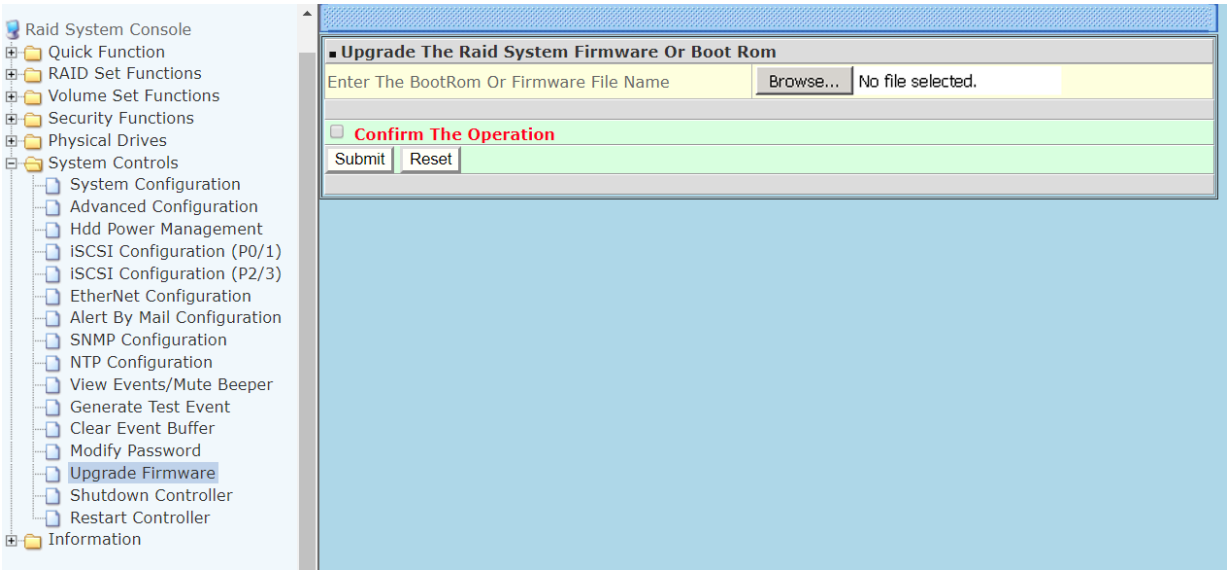
Upgrading Firmware Through Web Browser

Get the new version of firmware for your RAID subsystem controller.

NOTE: When there is new boot ROM firmware that needs to be upgraded, upgrade first the boot ROM firmware. Then repeat the process (steps 1 to 3) to upgrade the firmware code after which a RAID controller restart will be necessary.

1. To upgrade the RAID subsystem firmware, click the **Upgrade Firmware** link under **System Controls** menu. The Upgrade The Raid System Firmware Or Boot Rom screen appears.

2. Click **Browse**. Look in the location where the firmware file was saved. Select the firmware file name "xxxxxxxx.BIN" and click Open.



3. Select the **Confirm The Operation** option. Click the **Submit** button.

4. The Web Browser begins to download the firmware binary to the controller and start to update the flash ROM.

5. After the firmware upgrade is complete, a message will show "Firmware Has Been Updated Successfully". Restarting the RAID controller is required for the new firmware to take effect.