AMCC STORAGE

3ware®

SAS/SATA RAID Software User Guide

Supports the 9690SA Models

PN 720-0175-00
September 2007

User Guide

Copyright

Trademarks

Disclaimer

Table of Contents

About this User Guide

This document, *3ware SAS/SATA RAID Software User Guide, Version 9.5*, provides instructions for configuring and maintaining RAID units on 3ware 9690SA series RAID controllers.

This guide assumes that you have already installed your controller and drives in your system and any enclosures, if you have them. If you have not yet done so, see the installation guide that came with your controller. If you do not have the printed copy, a PDF of the installation guide is available on your 3ware CD, or you can download it from: http://www.3ware.com/support/userdocs.asp. (Note that there are different installation guides for different 3ware RAID controller models.)

There are often multiple ways to accomplish the same configuration and maintenance tasks for your 3ware RAID controller. This manual includes instructions for performing tasks using two tools:

- 3ware BIOS Manager (3BM), which runs at the BIOS level
- 3ware Disk Manager 2 (3DM 2), which runs in a browser

You can also perform many tasks at the command line, using 3ware's Command Line Interface (CLI). The CLI is described in a separate manual: *3ware SAS/SATA RAID Controller CLI Guide*. Information from both this Users Guide and the CLI Guide are also available in the *3ware HTML Bookshelf*, available in the 3ware Documentation folder and on your 3ware CD. (For more information, see "Using the 3ware HTML Bookshelf" on page ix.)

How this User Guide is Organized

Table 1: Chapters and Appendices in this Guide

Chapter/Appendix	Description
1. Introduction	Provides an overview of product features for the 3ware 9690SA controller models. Includes system requirements and an introduction to RAID concepts and levels.

Table 1: Chapters and Appendices in this Guide

Chapter/Appendix	Description
2. Getting Started	Provides a summary of the process you should follow to get started using your 3ware RAID controller.
3. First-Time RAID Configuration Using 3BM	Provides step-by-step instructions for configuring RAID units if you have just installed the controller.
4. Driver Installation	Describes how to install drivers for the 3ware controller if you have just installed and configured it.
5. 3ware BIOS Manager (3BM)	Describes the basics of using 3BM.
6. 3ware Disk Manager 2 (3DM 2)	Describes the basics of using 3DM. Also includes information about installing and uninstalling 3DM, and how to start the 3DM process manually, if required.
7. Configuring Your Controller	Describes how to view details about the controller, check its status, and change configuration settings that affect the controller and all associated drives.
8. Configuring Units	Describes how to configure new units and hot spares, change existing configurations, and set unit policies.
9. Maintaining Units	Describes how to check unit and drive status, review alarms and errors, schedule background maintenance tasks, and manually start them, when necessary or desirable. Includes explanations of initialization, verify, rebuild, and self-tests.
10. Maintaining Your Controller	Describes how to update the driver, and move a unit from one controller to another. Also includes information about checking battery status on a BBU (Battery Backup Unit).
11. Managing an Enclosure	Describes how to view details about an enclosure, check the status of enclosure components, and locate specific enclosure components by blinking an associated LED.
12. 3DM 2 Reference	Describes the features and functions on each of the pages in 3DM.
13. Troubleshooting	Provides common problems and solutions, and explains error messages.
A. Glossary	Includes definitions for terms used throughout this guide.
B. Software Installation	Provides instructions for installing software management tools (3DM 2, CLI, tw_update) and documentation.
C. Compliance and Conformity Statements	Provides compliance and conformity statement.
D. Warranty, Technical Support, and Service	Provides warranty information and tells you how to contact technical support.

Conventions

The following conventions are used throughout this guide:

- 3BM refers to the 3ware BIOS Manager.
- 3DM and 3DM 2 both refer to the 3ware Disk Manager, version 2.
- In the sections that describe using 3DM, *current controller* is used to refer to the controller which is currently selected in the drop-down list.
- *Unit* refers to one or more disks configured through 3ware to be treated by the operating system as a single drive. Also known as an array. Array and unit are used interchangeably throughout this manual.
- **Boldface** is used for buttons, fields, and settings that appear on the screen.
- `Monospace font` is used for code and to indicate things you type.

Screenshots

The screenshots in this documentation are examples only, and may not exactly reflect the operating system and browser you are using. 3ware software works on a number of different operating systems, including Microsoft Windows® and Linux®, and runs in a number of different browsers. In addition, the version numbers shown in screenshots for drivers, firmware, and software may not match your version. For the current released and tested version number, see the latest release notes.

In addition, the fields and columns in 3DM 2 vary for different models of 3ware RAID controllers. If you have multiple controllers of different models, you may notice some differences when switching between them in 3DM. For example, when displaying information about the 9690SA controllers, 3DM displays “VPorts” (for virtual port) on some screens while for earlier controllers the label is “port.”

Using the 3ware HTML Bookshelf

The 3ware HTML Bookshelf is an HTML version of this user guide and the CLI Guide, combined as one resource. It is available on your 3ware CD, in the /doc/3wareHTMLBookshelf folder. It can also be installed along with the software, as described in “Software Installation” on page 277.

To make use of the 3ware HTML Bookshelf

1 To launch the bookshelf at the opening page, do one of the following:
   - For Windows, from the Start menu, choose Programs > AMCC > Bookshelf shortcut.

- Navigate to the 3wareHTMLBookshelf folder on the 3ware CD and double click the file `index.html`.
- For Linux, open a browser window to the following location:
  `/opt/AMCC/Documentation/index.html`

When you use either of these methods, a navigation panel at the left automatically opens. It includes a Table of Contents, Index, and Search.

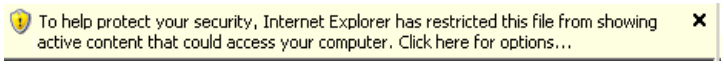
You can also open the bookshelf by double-clicking any other html file in the 3wareHTMLBookshelf folder. When you open an individual file, the navigation pane does not automatically open. In this case, you can display the navigation pane by clicking the **Show Navigation** button at the left.

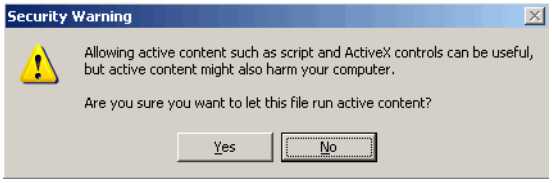
Figure 1. Navigation Button in the 3ware HTML Bookshelf Window

Click the **Show Navigation** button to display the Table of Contents

Note: The 3ware HTML Bookshelf is created as a set of HTML documents that are often displayed from a website. When installed on your personal computer, some browsers flag them as “active content,” and require your approval before displaying the content.

If you see messages similar to the following, you must confirm the display of active content in order to see the pages.





1

Introducing the 3ware® SAS/ SATA RAID Controller

AMCC 3ware RAID controllers deliver full-featured, true hardware RAID to servers and workstations. AMCC's RAID controllers offer Serial Attached SCSI (SAS) and Serial ATA (SATA) interfaces. Combined with an advanced RAID management feature-set that includes web-based, command-based, and API (application programming interface) software components, AMCC controllers provide compelling RAID solutions.

This section introduces the features and concepts of AMCC 3ware RAID controllers. It is organized into the following topics:

- What's New with 9690SA Models
- System Requirements
- Understanding RAID Concepts and Levels
- 3ware Tools for Configuration and Management
- Monitoring, Maintenance, and Troubleshooting Features

What's New with 9690SA Models

The 9690SA models in 3ware's 9000 series of RAID controllers have the following features and benefits:

- Dual-ported SAS drive support
- Ability to have SAS and/or SATA drives on the same controller
- Connectivity with up to 128 single-ported drives or 64 dual-ported drives
- Up to 32 drives in a unit
- Up to 32 active units
- Support for storage enclosures
- Simultaneous RAID 6 parity generation to maximize RAID 6 performance
- 8th-generation StorSwitch™ non-blocking switch fabric for maximum controller output

- StreamFusion™ optimizes RAID 5 and RAID 6 disk accesses to maximize application performance under heavy loads
- StorSave™ BBU with write journaling optimizes data protection and performance
- RAID levels 0, 1, 5, 6, 10, 50, and Single Disk
- PCI Express® x8 connectivity
- If you have a supported enclosure, the drive Locate feature allows you to easily identify a drive in the enclosure by blinking the LED associated with it. Depending on your enclosure, you may also be able to identify fans, power supplies, and temperature controls.

System Requirements

3ware 9690SA model RAID controllers have the following requirements:

Motherboard and Slot Requirements

A workstation-class or server-class motherboard, with an available PCI Express x8 or x16 slot that complies with PCI 1.1 or later.

A list of motherboards that have been tested is available at http://www.3ware.com/products/sys_compatibility.asp

Drive Requirements

The 3ware 9690SA RAID controller may be connected to up to 128 SAS and/or SATA drives. If all drives are SAS drives and connections are made to both ports of each SAS drive from the controller (for redundancy and performance), then a maximum of 64 drives may be used. A maximum of 32 drives are allowed per RAID unit and up to 32 active RAID units per controller. You cannot mix SAS and SATA drives in the same unit.

Drives and drive enclosures must meet SAS (3.0 Gbps) and SATA (1.5 or 3.0 Gbps) standards.

A list of drives that have been tested is available at http://www.3ware.com/products/sys_compatibility.asp

Drives may be of any capacity or physical form factor.

The length of internal unshielded interface cables may not exceed 1M (39”) and a maximum of 6M (234”) for external shielded cables.

Enclosure Requirements

Enclosure management features in 3ware software are available for supported enclosures with expanders that provide SCSI Enclosure Services 2 (SES-2).

Note: SAFTE (SCSI Accessed Fault Tolerant Enclosure) is not supported at this time.

A list of supported enclosures is available at http://www.3ware.com/products/sys_compatibility.asp

Cascading of enclosures is limited to 4 enclosures based on the same expander. Enclosures may contain cascaded expanders internally.

Operating System

3ware RAID controllers may be used with:

- Windows XP, Windows Server 2003, both 32-bit and 64-bit x86
- Red Hat Linux, 32-bit and 64-bit x86
- SuSE Linux, 32-bit and 64-bit x86
- Fedora Core, 32-bit and 64-bit x86
- Other versions of Linux, 32-bit and 64-bit x86, using the open source Linux 2.4 or 2.6 kernel driver

For the latest driver versions for all operating systems, see the current Release Notes at http://www.3ware.com/support/.

Other Requirements

- Adequate air flow and cooling
- Adequate power supply for drives
- 3DM 2 (3ware Disk Manager) displays information in a browser. It requires one of the following browsers:
  - Internet Explorer 5.5 and later
  - Mozilla Firefox 1.2 and later
  - Netscape 7 and later

  In addition:
  - JavaScript must be enabled
  - Cookies must be enabled
  - For best viewing, screen resolution should be 1024 x 768 or greater, with 16-bit color or greater.

For a complete listing of features and system requirements, refer to the 3ware SATA RAID Controller datasheets, available from the website at http://www.3ware.com/products.

Understanding RAID Concepts and Levels

3ware RAID controllers use RAID (Redundant Array of Inexpensive Disks) to increase your storage system's performance and provide fault tolerance (protection against data loss).

This section organizes information about RAID concepts and configuration levels into the following topics:

RAID Concepts

The following concepts are important to understand when working with a RAID controller:

- **Arrays and Units**. In the storage industry, the term "array" is used to describe two or more disk drives that appear to the operating system as a single unit. When working with a 3ware RAID controller, "unit" is the term used to refer to an array of disks that is configured and managed through the 3ware software. Single-disk units can also be configured in the 3ware software.
- **Mirroring**. Mirrored arrays (RAID 1) write data to paired drives simultaneously. If one drive fails, the data is preserved on the paired drive. Mirroring provides data protection through redundancy. In addition, mirroring using a 3ware RAID controller provides improved performance because 3ware's TwinStor technology reads from both drives simultaneously.
- **Striping**. Striping across disks allows data to be written and accessed on more than one drive, at the same time. Striping combines each drive's capacity into one large volume. Striped disk arrays (RAID 0) achieve highest transfer rates and performance at the expense of fault tolerance.
- **Distributed Parity**. Parity works in combination with striping on RAID 5, RAID 6, and RAID 50. Parity information is written to each of the striped drives, in rotation. Should a failure occur, the data on the failed drive can be reconstructed from the data on the other drives.
- **Hot Swap**. The process of exchanging a drive without having to shut down the system. This is useful when you need to exchange a defective drive in a redundant unit.

- **Array Roaming.** The process of removing a unit from a controller and putting it back later, either on the same controller, or a different one, and having it recognized as a unit. The disks may be attached to different ports than they were originally attached to, without harm to the data.

For definitions of other terms used throughout the documentation, see the "Glossary".

Available RAID Configurations

RAID is a method of combining several hard drives into one unit. It offers fault tolerance and higher throughput levels than a single hard drive or group of independent hard drives. RAID levels 0, 1, 10 and 5 are the most popular. AMCC's 3ware controllers support RAID 0, 1, 5, 6, 10, 50, and Single Disk. The information below provides a more in-depth explanation of the different RAID levels.

For how to configure RAID units, see "Configuring a New Unit" on page 85.

RAID 0

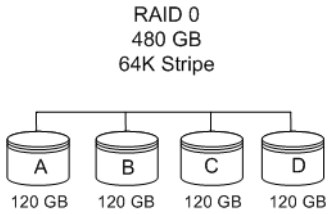
RAID 0 provides improved performance, but no fault tolerance. Since the data is striped across more than one disk, RAID 0 disk arrays achieve high transfer rates because they can read and write data on more than one drive simultaneously. The stripe size is configurable during unit creation. RAID 0 requires a minimum of two drives.

When drives are configured in a striped disk array (see Figure 2), large files are distributed across the multiple disks using RAID 0 techniques.

Striped disk arrays give exceptional performance, particularly for data intensive applications such as video editing, computer-aided design and geographical information systems.

RAID 0 arrays are not fault tolerant. The loss of any drive results in the loss of all the data in that array, and can even cause a system hang, depending on your operating system. RAID 0 arrays are not recommended for high availability systems unless additional precautions are taken to prevent system hangs and data loss.

Figure 2. RAID 0 Configuration Example



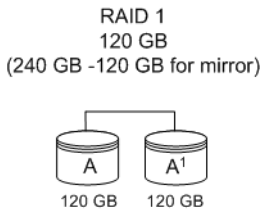
RAID 1

RAID 1 provides fault tolerance and a speed advantage over non-RAID disks. RAID 1 is also known as a mirrored array. Mirroring is done on pairs of drives. Mirrored disk arrays write the same data to two different drives using RAID 1 algorithms (see Figure 3). This gives your system fault tolerance by preserving the data on one drive if the other drive fails. Fault tolerance is a basic requirement for critical systems like web and database servers.

3ware uses a patented technology, TwinStor®, on RAID 1 arrays for improved performance during sequential read operations. With TwinStor technology, read performance is twice the speed of a single drive during sequential read operation.

The adaptive algorithms in TwinStor technology boost performance by distinguishing between random and sequential read requests. For the sequential requests generated when accessing large files, both drives are used, with the heads simultaneously reading alternating sections of the file. For the smaller random transactions, the data is read from a single optimal drive head.

Figure 3. RAID 1 Configuration Example



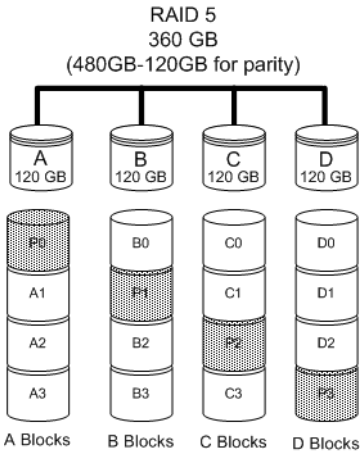
RAID 5

RAID 5 provides performance, fault tolerance, high capacity, and storage efficiency. It requires a minimum of three drives and combines striping data with parity (exclusive OR) to restore data in case of a drive failure. Performance and efficiency increase as the number of drives in a unit increases.

Parity information is distributed across all of the drives in a unit rather than being concentrated on a single disk (see Figure 4). This avoids throughput loss due to contention for the parity drive.

RAID 5 is able to tolerate 1 drive failure in the unit.

Figure 4. RAID 5 Configuration Example



RAID 6

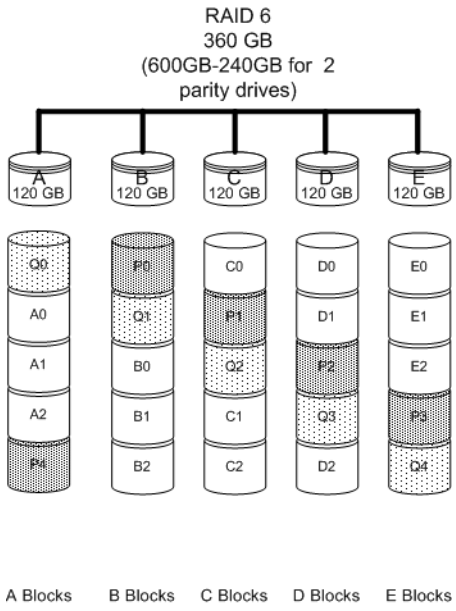
RAID 6 requires a 3ware 9650SE or 9690SA RAID controller.

RAID 6 provides greater redundancy and fault tolerance than RAID 5. It is similar to RAID 5, but has two blocks of parity information (P+Q) distributed across all the drives of a unit, instead of the single block of RAID 5.

Due to the two parities, a RAID 6 unit can tolerate two hard drives failing simultaneously. This also means that a RAID 6 unit may be in two different states at the same time. For example, one sub-unit can be degraded, while another may be rebuilding, or one sub-unit may be initializing, while another is verifying.

AMCC 3ware's implementation of RAID 6 requires a minimum of five drives. Performance and storage efficiency also increase as the number of drives increase.

Figure 5. RAID 6 Configuration Example



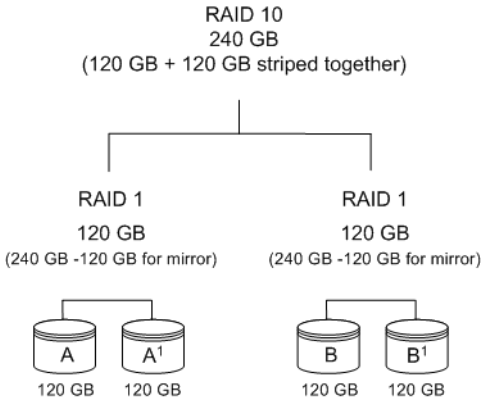
RAID 10

RAID 10 is a combination of striped and mirrored arrays for fault tolerance and high performance.

When drives are configured as a striped mirrored array, the disks are configured using both RAID 0 and RAID 1 techniques, thus the name RAID 10 (see Figure 6). A minimum of four drives are required to use this technique. The first two drives are mirrored as a fault tolerant array using RAID 1. The third and fourth drives are mirrored as a second fault tolerant array using RAID 1. The two mirrored arrays are then grouped as a striped RAID 0 array using a two tier structure. Higher data transfer rates are achieved by leveraging TwinStor and striping the arrays.

In addition, RAID 10 arrays offer a higher degree of fault tolerance than RAID 1 and RAID 5, since the array can sustain multiple drive failures without data loss. For example, in a twelve-drive RAID 10 array, up to six drives can fail (half of each mirrored pair) and the array will continue to function. Please note that if both halves of a mirrored pair in the RAID 10 array fail, then all of the data will be lost.

Figure 6. RAID 10 Configuration Example



RAID 50

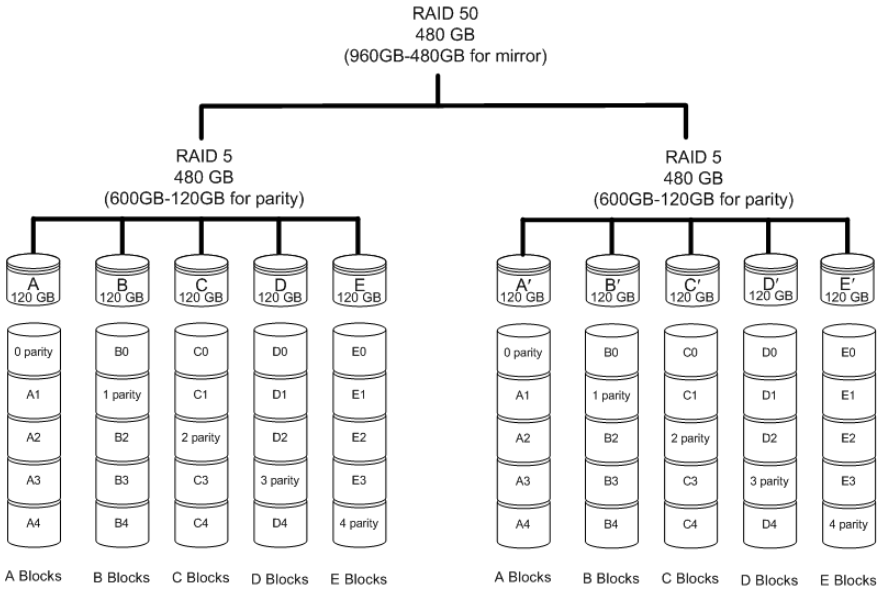
RAID 50 is a combination of RAID 5 with RAID 0. This array type provides fault tolerance and high performance. RAID 50 requires a minimum of six drives.

Several combinations are available with RAID 50. For example, on a 12-port controller, you can have a grouping of 3, 4, or 6 drives. A grouping of 3 means that the RAID 5 arrays used have 3 disks each; four of these 3-drive RAID 5 arrays are striped together to form the 12-drive RAID 50 array. On a 16-port controller, you can have a grouping of 4 or 8 drives.

No more than four RAID 5 subunits are allowed in a RAID 50 unit. For example, a 24-drive RAID 50 unit may have groups of 12, 8, or 6 drives, but not groups of 4 or 3.

In addition, RAID 50 arrays offer a higher degree of fault tolerance than RAID 1 and RAID 5, since the array can sustain multiple drive failures without data loss. For example, in a twelve-drive RAID 50 array, up to one drive in each RAID 5 set can fail and the array will continue to function. Please note that if two or more drives in a RAID 5 set fail, then all of the data will be lost.

Figure 7. RAID 50 Configuration Example



Single Disk

A single drive can be configured as a unit through 3ware software. (3BM, 3DM 2, or CLI). Like disks in other RAID configurations, single disks contain 3ware Disk Control Block (DCB) information and are seen by the OS as available units.

Single drives are not fault tolerant and therefore not recommended for high availability systems unless additional precautions are taken to prevent system hangs and data loss.

Hot Spare

A hot spare is a single drive, available online, so that a redundant unit can be automatically rebuilt in case of drive failure.

Determining What RAID Level to Use

Your choice of which type of RAID unit (array) to create will depend on your needs. You may wish to maximize speed of access, total amount of storage, or redundant protection of data. Each type of RAID unit offers a different blend of these characteristics.

The following table provides a brief summary of RAID type characteristics.

Table 2: RAID Configuration Types

RAID Type	Description
RAID 0	Provides performance, but no fault tolerance.
RAID 1	Provides fault tolerance and a read speed advantage over non-RAID disks.
RAID 5	This type of unit provides performance, fault tolerance, and high storage efficiency. RAID 5 units can tolerate one drive failing before losing data.
RAID 6	Provides very high fault tolerance with the ability to protect against two consecutive drive failures. Performance and efficiency increase with higher numbers of drives.
RAID 10	A combination of striped and mirrored units for fault tolerance and high performance.
RAID 50	A combination of RAID 5 and RAID 0. It provides high fault tolerance and performance.
Single Disk	Not a RAID type, but supported as a configuration. Provides for maximum disk capacity with no redundancy.

You can create one or more units, depending on the number of drives you have installed.

Table 3: Possible Configurations Based on Number of Drives

# Drives	Possible RAID Configurations
1	Single disk or hot spare
2	RAID 0 or RAID 1
3	RAID 0 RAID 1 with hot spare RAID 5
4	RAID 5 with hot spare RAID 10 Combination of RAID 0, RAID 1, single disk

Table 3: Possible Configurations Based on Number of Drives

# Drives	Possible RAID Configurations
5	RAID 6 RAID 5 with hot spare RAID 10 with hot spare Combination of RAID 0, RAID 1, hot spare, single disk
6 or more	RAID 6 RAID 6 with hot spare RAID 50 Combination of RAID 0, 1, 5, 6,10, hot spare, single disk

Using Drive Capacity Efficiently

To make the most efficient use of drive capacity, it is advisable to use drives of the same capacity in a unit. This is because the capacity of each drive is limited to the capacity of the smallest drive in the unit.

The total unit capacity is defined as follows:

Table 4: Drive Capacity

RAID Level	Capacity
Single Disk	Capacity of the drive
RAID 0	(number of drives) X (capacity of the smallest drive)
RAID 1	Capacity of the smallest drive
RAID 5	(number of drives - 1) X (capacity of the smallest drive) Storage efficiency increases with the number of disks: storage efficiency = (number of drives -1)/(number of drives)
RAID 6	(number of drives - 2) x (capacity of the smallest drive)
RAID 10	(number of drives / 2) X (capacity of smallest drive)
RAID 50	(number of drives - number of groups of drives) X (capacity of the smallest drive)

Through drive coercion, the capacity used for each drive is rounded down so that drives from differing manufacturers are more likely to be able to be used as spares for each other. The capacity used for each drive is rounded down to the nearest GB for drives under 45 GB (45,000,000,000 bytes), and rounded down to the nearest 5 GB for drives over 45 GB. For example, a 44.3 GB drive will be rounded down to 44 GB, and a 123 GB drive will be rounded

down to 120 GB. For more information, see the discussion of drive coercion under “Creating a Hot Spare” on page 97.

Note: All drives in a unit must be of the same type, either SAS or SATA.

Support for Over 2 Terabytes

Windows XP (32-bit), Windows 2003 (32-bit and 64-bit without SP1) and Linux 2.4 do not currently recognize unit capacity in excess of 2 TB.

If the combined capacity of the drives to be connected to a unit exceeds 2 Terabytes (TB), you can enable auto-carving when you configure your units.

Auto-carving divides the available unit capacity into multiple chunks of 2 TB or smaller that can be addressed by the operating systems as separate volumes. The carve size is adjustable from 1024 GB to 2048 GB (default) prior to unit creation.

If a unit over 2 TB was created prior to enabling the auto-carve option, its capacity visible to the operating system will still be 2TB; no additional capacity will be registered. To change this, the unit has to be recreated.

For more information, see “Using Auto-Carving for Multi LUN Support” on page 78.

You may also want to refer to Knowledgease article # 13431, at http://www.3ware.com/kb/article.aspx?id=13431.

3ware Tools for Configuration and Management

3ware software tools let you easily configure the drives attached to your 3ware RAID controller, specifying which drives should be used together as a RAID unit and the type of RAID configuration you want, and designating hot spares for use if a drive degrades.

3ware provides the following tools for use in configuring and managing units attached to the 3ware controller:

- **3BM (3ware BIOS Manager)**

  3BM is a BIOS level tool for creating, deleting, and maintaining disk arrays, rebuilding arrays, designating hot spares, and setting controller policies. 3BM is the tool most frequently used to configure units

immediately after installation of the controller, but can also be used after installation to maintain the controller and associated drives.

For general information about working with 3BM, see Chapter 5, “3ware BIOS Manager (3BM) Introduction.”

- **3DM 2 (3ware Disk Manager)**

  3DM is a daemon (under Linux) and a service (under Windows) which runs in the background on the controller’s host system, and can be accessed through a web browser to provide ongoing monitoring and administration of the controller and associated drives. It can be used locally (on the system that contains the 9690SA) or remotely (on a system connected via a network to the system containing the 9690SA).

  For details about working with 3DM, see “3DM 2 (3ware Disk Manager) Introduction” on page 58.

  3DM 2 is the current version of the 3ware Disk Manager. Throughout this documentation, it is referred to interchangeably as 3DM and 3DM 2.

- **3ware Alert Utility (WinAVAlarm)**

  The 3ware Alert Utility for Windows runs on the system in which the 3ware RAID controller is installed and provides direct notification by popup message and audio alarm when events occur. This utility can be configured to specify the type of events that should generate these notifications. For details, see “Using the Alert Utility Under Windows” on page 134.

- **3ware CLI (Command Line Interface)**

  The 3ware CLI provides the functionality available in 3DM through a Command Line Interface. You can view unit status and version information and perform maintenance functions such as adding or removing drives, and reconfiguring RAID units online. You can also use it to remotely administer controllers in a system.

  The 3ware CLI is described in *3ware SAS/SATA RAID Controller CLI Guide* and in the *3ware HTML Bookshelf*.

Monitoring, Maintenance, and Troubleshooting Features

Several 3ware RAID controller features aid in monitoring and troubleshooting your drives.

- **SMART Monitoring** (Self-Monitoring, Analysis and Reporting Technology) automatically checks a disk drive's health every 24 hours and reports potential problems. This allows you to take proactive steps to prevent impending disk crashes. SMART data is checked on all disk drives (array members, single disks, and hot spares). Monitoring of

SMART thresholds can be turned on and off in 3DM. See, “Selecting Self-tests to be Performed” on page 154 This feature does not apply to SAS drives. (For details, see “Viewing SMART Data About a Drive” on page 136.)

- **Staggered Spinup** allows drives that support this feature to be powered-up into the standby power management state to minimize in-rush current at power-up and to allow the controller to sequence the spin-up of drives. Both SATAII OOB and ATA spin-up methods are supported.The standby power management state is persistent after power-down and power-up. You can set the number of drives that will spin up at the same time, and the time between staggers in 3BM (the 3ware BIOS Management utility). This feature does not apply to drives that are attached to an expander. For details, see “Enabling and Setting Up Staggered Spin-up” on page 80.
- **Verification and Media Scans.** The verify task verifies all redundant units, and checks for media errors on single disks, spares and RAID 0 unit members. If the disk drive is part of a redundant unit, error locations that are found and are deemed repairable are rewritten with the redundant data. This forces the drive firmware to reallocate the error sectors accordingly. (For more information, see “About Verification” on page 141.)
- **Error Correction**. Bad sectors can be dynamically repaired through error correction (Dynamic Sector Repair). Reallocation of blocks is based intelligently on the location of the block in relation to the stripe.
- **Scheduled Background Tasks.** Initialize, rebuild, verify, and self-test tasks can all be run in the background, at scheduled times. This lets you choose a time for these tasks to be run when it will be least disruptive to your system. You can also define the rate at which background tasks are performed, specifying whether I/O tasks should be given more processing time, or background rebuild and verify tasks should be given more processing time. (For more information, see “Scheduling Background Tasks” on page 150.)
- **Write Cache**. Write cache can be enabled or disabled using 3BM, 3DM 2 and CLI. When write cache is enabled, data will be stored in 3ware controller cache and drive cache before the data is committed to disk. This allows the system to process multiple write commands at the same time, thus improving performance. However when data is stored in cache, it could be lost if a power failure occurs. With a Battery Backup Unit (BBU) installed, the data stored on the 3ware controller can be restored. (For more information, see “Enabling and Disabling the Unit Write Cache” on page 102.)
- **StorSave™ Profiles** allow you to set the level of protection versus performance that is desired for a unit when write cache is enabled. (For more information, see “Setting the StorSave Profile for a Unit” on page 106.)

- **Enclosure Services.** Drives, fans, temperature sensors, and power supplies in supported enclosures can be identified by flashing LEDs so that you can quickly identify which component needs to be checked or replaced. For more information, see “Managing an Enclosure” on page 179.
- **Auto Rebuild.** For times when you do not have a spare available, setting the Auto Rebuild policy allows rebuilds to occur with an available drive or with a failed drive. (For more information, see “Setting the Auto Rebuild Policy” on page 77.)

2

Getting Started with Your 3ware RAID Controller

Setting up your 3ware RAID controller involves these main steps:

- Physically Install the RAID Controller and Drives
- Configure a RAID Unit
- Install the Driver and Make the Operating System Aware of the New Drives
- Set Up Management and Maintenance Features

Once the controller and drives have been physically installed, the order in which you perform these steps depends in part on whether one of the units you configure will act as your boot drive.

Tip: When you are first setting up your system, you may want to review “System Requirements” on page 2.

Physically Install the RAID Controller and Drives

To install your controller, follow the instructions in the installation guide that came with your 3ware controller. If you do not have a hardcopy of the installation manual, it is available in the “doc” folder on your 3ware CD, or you can download it from the 3ware website at http://www.3ware.com/support/userdocs.asp.

For drive installation, see the instructions that came with your enclosure. If you are installing drives in a computer case, follow the manufacturer’s instructions.

Configure a RAID Unit

If you would like more information about what RAID level to choose for your situation, review the information under “Understanding RAID Concepts and Levels” on page 4. Then turn to “Configuring a New Unit” on page 85.

If you want to install the operating system on and boot from a drive managed through the new 3ware RAID controller, use the 3ware BIOS Manager (3BM) to define the configuration. You will find step-by-step instructions for initial

installation in. Chapter 3, “First-Time RAID Configuration Using 3BM.” Additional information about configuration is also included in the later chapters of this user guide.

If the operating system is already installed on another drive in your system, you can configure units through 3BM, through 3ware Disk Manager (3DM), or through the Command Line Interface (CLI). If you want to use 3DM or the CLI for configuration, go ahead and boot to the operating system, install the driver and the 3DM 2 software, and then configure your units. You may want to refer to the following information:

- Chapter 6, “3DM 2 (3ware Disk Manager) Introduction”
- Chapter 8, “Configuring Units”
- *3ware SAS/SATA RAID Controller CLI Guide*, available from the CD-ROM, the *3ware HTML Bookshelf* and from the website http://www.3ware.com/support/userdocs.asp

Install the Driver and Make the Operating System Aware of the New Drives

Instructions for installing drivers are available in “Driver Installation” on page 31.

You will also find instructions for updating the driver under “Downloading the Driver and Firmware” on page 158.

Set Up Management and Maintenance Features

3ware RAID controllers include a number of features to help you manage and maintain the controller and your configured units. The default settings for these features allow you to begin using your newly configured units right away. You can review and change these features as a final step in your initial setup, or you can make changes to them later, at your convenience. These features include:

- Controller and unit policies, such as Auto Rebuild, Auto Verify, use of write cache, use of queuing mode, and selection of a StorSave profile.
- Email notification of alarms and other events
- Schedules for when background tasks will be performed, to minimize the impact on day-to-day performance during peak usage times. (Background tasks include rebuild, verify, initialize, migrate, and self-test.)

Details about these features are described in this documentation. When you first set up your controller, you may want to review these sections in particular:

- “Configuring Your Controller” on page 72
- “Setting Unit Policies” on page 100
- “Setting Background Task Rate” on page 149

Initial Settings for Policies and Background Tasks

The table below lists the default settings for policies and background tasks. These settings are used if you do not explicitly change the policy settings.

Table 5: Default Settings for Policies and Background Tasks

Policy	Default Value	Where to Change
Controller-Level Settings (For details, see "Configuring Your Controller" on page 72		
Auto-Rebuild	Enabled	3BM, 3DM, CLI
Auto-Carving	Disabled	3BM, 3DM, CLI
Auto-Detect	Enabled	CLI
Carve Size or Factor	2048 GB	3BM, 3DM, CLI
Drives Per Spinup	1	3BM, CLI
Delay Between Spinup	6 seconds	3BM, CLI
Export Unconfigured (JBOD) Disks	Disabled	3BM, CLI
Staggered Method	ATA-6	3BM
Staggered Spinup	Enabled	3BM
Unit-Level Settings (For details, see "Setting Unit Policies" on page 100)		
Auto Verify	Disabled	3DM, CLI
Continue on Source Error During Rebuild	Disabled	3BM, 3DM, CLI
Boot Volume Size	Blank	3BM
Queuing (NCQ)	Enabled	3BM, 3DM, CLI
StorSave Profile	Protection	3BM, 3DM, CLI
Write Cache	Enabled	3BM, 3DM, CLI
Background Task Settings (For details, see "Scheduling Background Tasks" on page 150 and "Setting Background Task Rate" on page 149)		
Verify Task Schedules	Daily, starting at 12:00 am and running for 24 hours	3DM, CLI
Follow Verify Task Schedule	No	3DM, CLI
Rebuild Task Schedules	Daily, starting at 12:00 am and running for 24 hours	3DM, CLI

Table 5: Default Settings for Policies and Background Tasks

Policy	Default Value	Where to Change
Follow Rebuild Task Schedule	No	3DM, CLI
Self-test Task Schedules[a]	Daily, starting at 12:00 am and running for 24 hours	3DM, CLI
Follow Self-test Task Schedule	Yes	3DM, CLI

a. Although the default Self-test Task Schedule is for 24 hours, self-test tasks are run only at the beginning of that time period and take just a few minutes. For more information about task schedules, see “Scheduling Background Tasks” on page 150.

3

First-Time RAID Configuration Using 3BM

If you will install the operating system on and boot from a unit managed through the new 3ware RAID controller, follow the steps in this chapter to use the 3ware BIOS Manager (3BM) to configure the unit and install the driver.

If the operating system is already installed on another drive in your system, you can use the steps below or you can configure units through 3DM or the CLI.

You can create one or more units on a single controller, depending on the number of drives that the specific 3ware RAID controller supports and the number of drives attached. (For more information, see “Determining What RAID Level to Use” on page 11.)

Basic Steps for Creating a Unit

The process of configuring your RAID units includes these main steps, which are detailed in the step-by-step example:

- Launch 3BM (3ware BIOS Manager)
- Select the drives to be included and indicate that you want to create a unit
- Select the desired RAID configuration
- Set other parameters, depending on the type of RAID configuration
- Confirm the unit configuration
- Save your changes and finish up

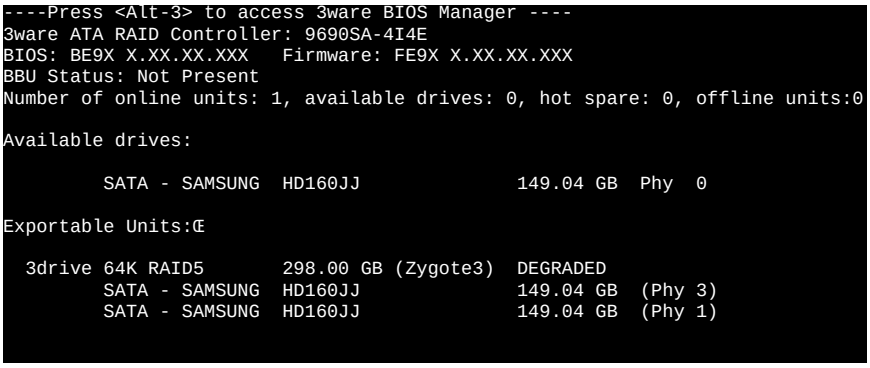
Note: If the capacity of the unit you create will exceed 2TB and you are using Windows XP (32-bit), Windows 2003 (32-bit and 64-bit without SP1) or Linux 2.4, you will need to enable auto-carving. Before creating your unit, follow the instructions under “Using Auto-Carving for Multi LUN Support” on page 78.

To launch 3BM

1 Power up or reboot your system.

While the system is starting, watch for a screen similar to Figure 8.

Figure 8. 3ware BIOS Screen

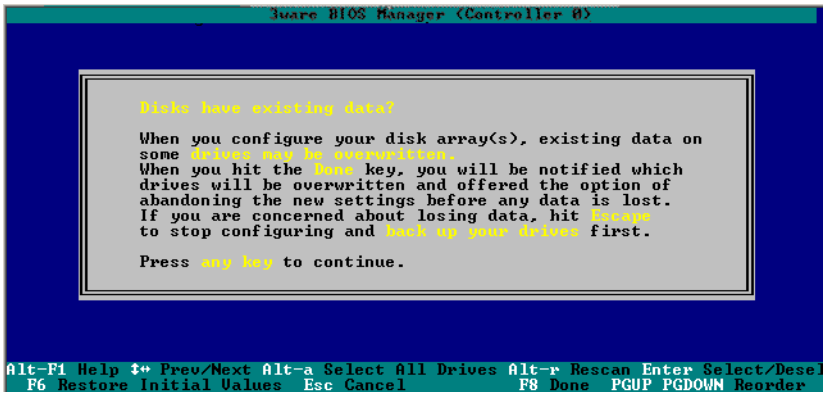


2 Press **Alt-3** immediately to bring up the **3ware BIOS Manager (3BM)**.

Normally your 3ware configuration remains on-screen for just a few seconds. However, if a unit has degraded, the screen indicates the problem and remains on your screen longer.

3 If you plan to make changes to your configuration and need to backup data before continuing, press **ESC** and do so now. Otherwise, press any key to continue.

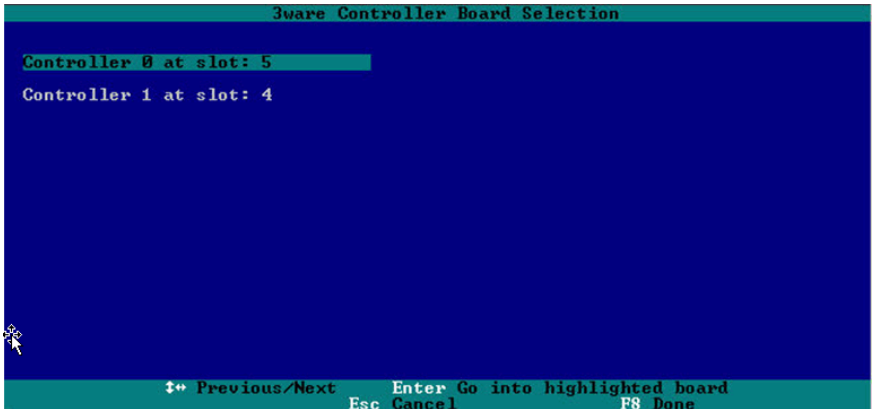
Figure 9. Warning Message When you Start 3BM



4 If you have more than one 9000-series controller in your system, a screen lists the available boards. (See Figure 10.) In this case, highlight the board with which you want to work and press **Enter**.

If you have more than 2 boards, you will only see two at first (only two can be processed at a time). After you exit from 3BM, you will have an opportunity to access the BIOS again, to access the next boards.

Figure 10. 3ware Controller Board Selection Screen



You will see a screen similar to Figure 9, warning you that changing your disk array configuration may overwrite data on the disks.

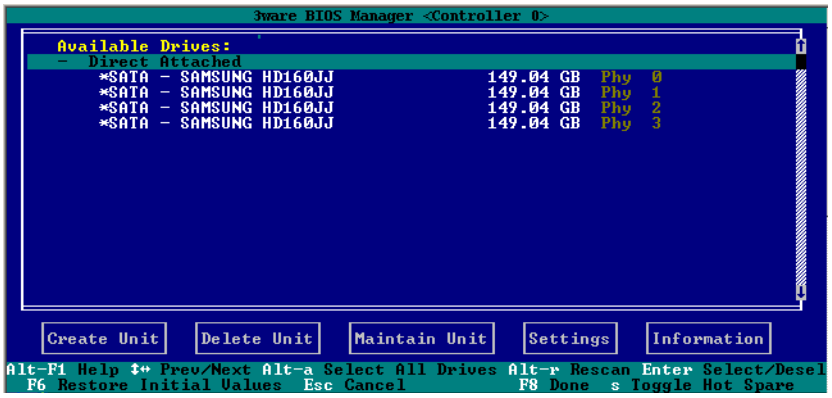
To select the drives and create a unit

1 Select the drives to be included by highlighting each one and pressing **Enter** to select it, or select all at once by selecting the heading above them.

When you select a drive, an asterisk appears next to it in the left-most column (see Figure 11).

You may include from one to thirty-two drives in the unit, depending on the number available.

Figure 11. Asterisks Next to Selected Drives

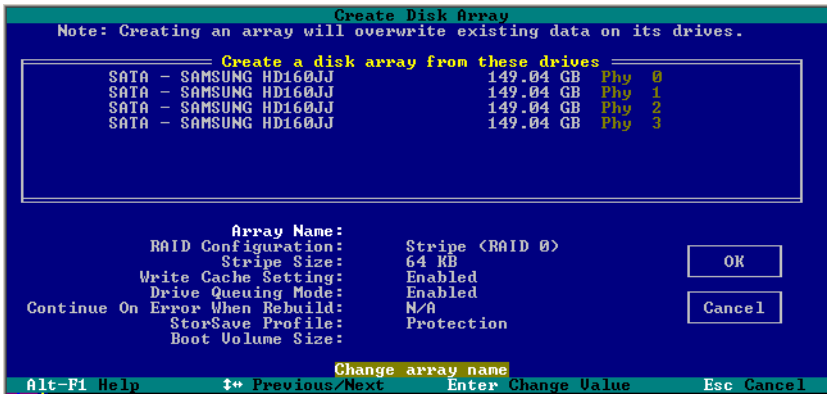


2 After all drives for the unit are selected, use the **Tab** to move to the **Create Unit** button and press **Enter**.

The **Create Disk Array** screen appears (see Figure 12).

3 Make sure that the proper drives are listed.

Figure 12. Create Disk Array Display



To name the unit and select the desired RAID configuration

1 (Optional) Press **Enter** in the **Array Name** field and type a name for the unit. Then press **Enter** again to accept the name.

2 Use the **arrow keys** or press **Tab** to move to the **RAID Configuration** field and press **Enter** to display the available RAID levels for the number of drives you selected.

Figure 13. List of Configuration Choices for Four Drives

3 Use the **arrow keys** to highlight the desired RAID configuration and press **Enter**.

For information about the different RAID levels and when to use each, see “Understanding RAID Concepts and Levels” on page 4.

4 Use the **arrow keys** or press **Tab** to move to the field **Stripe Size** and select the desired stripe size (16KB, 64KB, or 256KB).

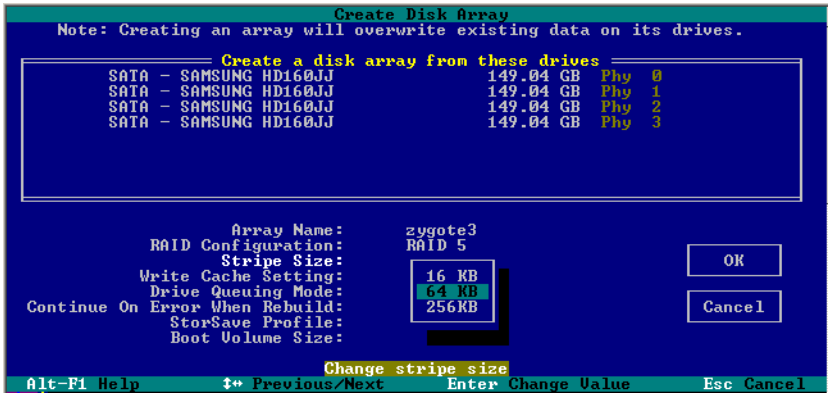
Notes:

Striping size is not applicable for RAID 1, because it is a mirrored unit without striping.

For RAID 6, only stripe size of 64KB is supported.

In general, use smaller stripe sizes for sequential access (such as video access) and larger stripe sizes for random access (such as a database).

Figure 14. Stripe Sizes for a RAID 5



To set other policies for the unit

While creating a unit through 3BM, you can set several policies that effect the unit (Write Cache, Drive Queuing Mode, and Continue on Error When Rebuild), and you can select a StorSave profile.

Each of these policies is already set to a default value, so you do not have to change them. In addition, you can change each of these policies later without affecting the configuration.

1 Use the arrow keys or press **Tab** to move to the field you want to change.

2 Press **Enter** to see the available options.

3 Use the **arrow keys** to select the option you want and press **Enter** to choose it.

For details about these parameters, see:

- “Enabling and Disabling the Unit Write Cache” on page 102
- “Enabling and Disabling Queuing for a Unit” on page 105
- “Setting the StorSave Profile for a Unit” on page 106
- “Setting Continue on Source Error During Rebuild” on page 104

To create a boot unit of a particular size

You can specify a portion of the unit you create to be used as a boot volume, if desired. This is useful if you will be installing your operating system onto the unit and want to have a designated volume for the OS. The remainder of the unit will be created as a separate volume.

Note: Setting a Boot Volume Size is optional. In addition, if you specify a boot volume, you do not have to install your operating system onto it. For more information about creating a boot volume, see “Boot volume size” on page 88. If the size of your array is 2TB or greater, you may also want to review the information about carving the unit into multiple volumes. For details, see “Using Auto-Carving for Multi LUN Support” on page 78.

1 Use the arrow keys or press **Tab** to move to the **Boot Volume Size** field.

2 Press **Enter** to display a text box.

3 Enter the size in Gigabytes that should be assigned to the boot volume.

4 Press **Enter** again to accept the size.

To confirm unit configuration

1 Press **Tab** to select the **OK** button and press **Enter** to confirm creation of the unit.

Or, if you want to cancel the creation of the unit, tab to **Cancel** and press **Enter**.

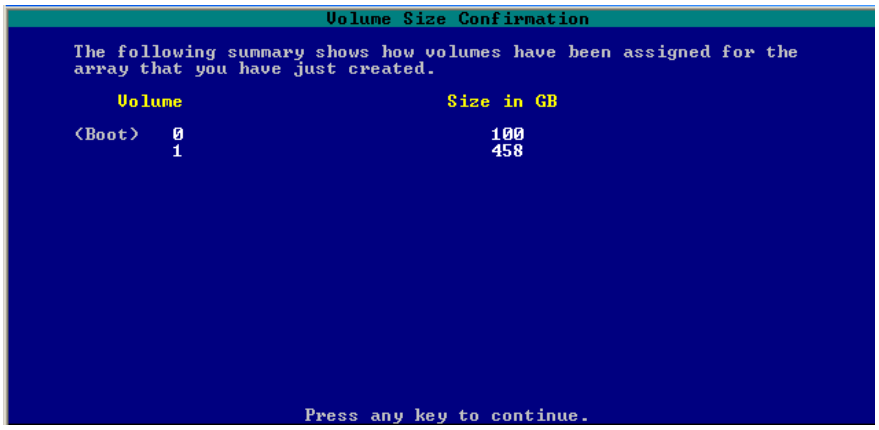
2 If you leave the **Unit Write Cache** field enabled and do not have a BBU installed, 3BM will ask you to confirm that you want to enable write cache.

The unit is not actually created and no data is overwritten until you have finished making all your changes and press **F8**.

3 If the volume summary screen appears, review the information and press any key to continue.

Multiple volumes will be created if you entered a Boot Volume Size of greater than zero (0), or if auto-carving is enabled and the combined size of the drives in your unit is large enough to divide it into multiple volumes. For more information about auto-carving, see “Using Auto-Carving for Multi LUN Support” on page 78.

Figure 15. Summary of Volumes to be Created



To finish up and save your changes

1 If you have additional drives, you can go ahead and configure an additional RAID unit or designate a hot spare. Then continue on with these steps. (For details about hot spares, see page 29.)

2 If you configured more than one unit, and you plan to install the operating system on one of them, make that unit be the first unit (Unit 0) in the list of Exportable Units.

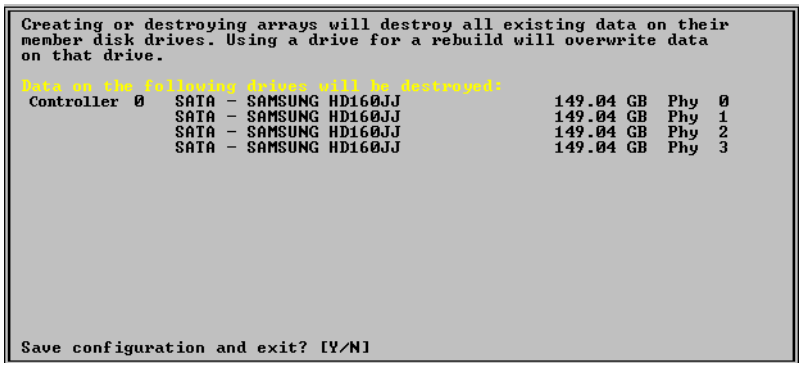
To move a unit up in the list, highlight it and press the **Page Up** key.

You will also want to make sure that the controller is the boot device for your computer. After finalizing the configuration below, be sure to follow the steps under “Checking the Motherboard Boot Sequence” on page 30.

3 When you are finished configuring units, press **F8** to save the changes and exit 3BM.

A warning message asks you to confirm that all existing data on the drives will be deleted.

Figure 16. Confirmation Message when Saving and Exiting



4 Type **Y** to continue, delete any existing data on the drives, and create the unit.

Depending on the RAID configuration you are creating, initialization of the unit may begin immediately. (RAID 6 units and some RAID 5 and RAID 50 units begin immediate initialization.) The initialization process can take several hours, depending on the size of your drives.

5 If you want to use a RAID configuration which has started initializing, you can press **Esc** to cancel the progress box. (Before doing this, be sure to read "Trade-offs to cancelling initialization," below.)

You can then exit 3BM and boot to the operating system before the process of writing zeroes to the drives is complete. Once you have booted to the operating system, background initialization of the unit will begin after a delay of up to ten minutes.

Trade-offs to cancelling initialization:

- Performance of these units will be lower until initialization is complete.
- When initializing is done after booting to the operating system, the process of initializing takes longer than it does if initialization is done by writing zeroes to the unit in the BIOS. Consequently, it will be a longer period of time until the performance of the unit is fully optimal. Data remains intact when initialization is done in the operating system.

For complete information about initialization of RAID units, see "About Initialization" on page 137.

6 If you are finished creating RAID units, be sure to check the boot sequence for your system, as described under "Checking the Motherboard Boot Sequence" on page 30.

Specifying a Hot Spare

You can designate one of the **Available Drives** as a hot spare in 3BM**.** If a hot spare is specified and a redundant unit degrades, an event notification will be generated. If the hot spare is of the same type (SAS or SATA) and of adequate size, it will automatically replace the failed drive without user intervention.

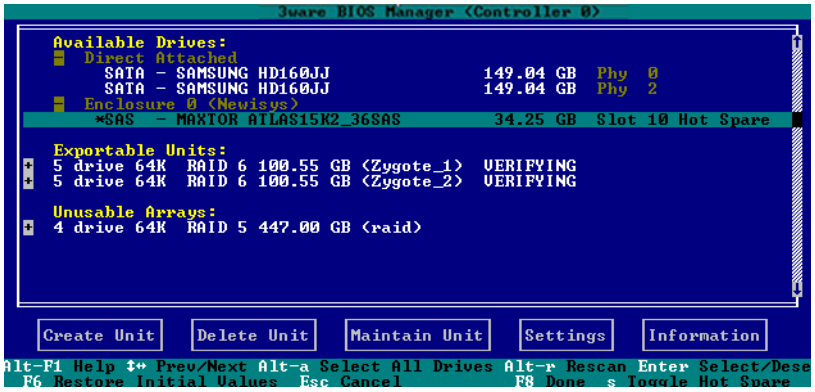
To specify a hot spare

1 In the list of **Available Drives**, highlight the drive to use**.**

2 Type **s** to specify that the selected drive will be the hot spare.

You'll see the words "Hot Spare" appear next to the drive in the Available Drives list.

Figure 17. Hot Spare Indicated



If a hot spare is already enabled, you can disable it by following the same process.

Note: In order to replace a failed drive in a degraded unit, a hot spare drive must have the same or larger storage capacity than the failed drive.

Making Drives Visible to the Operating System

By default, if you leave individual drives unconfigured, they will not be available to the operating system. If you want to be able to use individual drives, configure them as single-disk units.

Checking the Motherboard Boot Sequence

Using your computer's Setup utility, ensure that it shows the appropriate boot device.

After installing the 3ware controller in your system, go into the BIOS for your computer system to check and change the boot order. This is necessary because most systems automatically change the boot order when they detect a newly installed controller and device. Refer to the documentation for your system for information about starting the system BIOS.

- **If the OS is already installed on a unit connected to the system**, be sure that device precedes the 3ware RAID controller in the boot sequence. If you have other disks installed on the motherboard, the 3ware RAID controller should precede them in boot order.
- **If you will install your OS on a disk or unit attached to the 3ware RAID controller**, specify the controller as the boot device. (Note that if you configured more than one unit, the drive(s) specified as Unit 0 will be treated as the boot disk.)

What Next?

The final steps in setting up your RAID units are to load the 3ware driver and make the units available to your operating system. For details, turn to Chapter 4, "Driver Installation."

After installing the driver, in order to maintain your RAID units, you may also want to install 3ware's browser-based Disk Management tool, 3DM 2, or the 3ware Command Line Interface (CLI). For more information, see Appendix B, "Software Installation" on page 277.

4

Driver Installation

This chapter provides details about how to install the driver for your 3ware RAID controller and make the units available to your operating system.

- If the unit you have created will be your system's boot device, you install the driver for the controller as you install the operating system.
- If the operating system is already installed on a unit connected to another controller or to the motherboard, you start the operating system and then install the driver.

Details for both situations are described in this chapter. Driver information is organized by operating system:

- “Driver Installation Under Windows” on page 32
- “Driver Installation Under Linux” on page 38

Note: If you are working with a system that already has a 3ware RAID controller installed, and want to update the driver or firmware for your 3ware RAID controller to a newer version, see “Updating the Firmware and Driver” on page 157.

Driver Installation Under Windows

Note: Before installing the 3ware driver, you must have already physically installed your 3ware RAID controller in the system.

Consult the installation guide that came with your controller for how to do this. You can download that guide from: http://www.3ware.com/support/userdocs.asp.

The 3ware RAID controller can be used with Windows XP (SP1 or newer), and Windows Server 2003. Windows 2003 64-bit for AMD Opteron or Intel EM64T is also supported. It is recommended that you upgrade to the latest service pack available.

A drive or unit managed by the 3ware RAID controller may be configured to be your system's boot device. Or, you can use units managed by the 3ware controller for secondary storage and boot from another device, such as a disk attached to the motherboard, or other bootable media.

This section contains instructions for how to:

- Create a driver diskette for the 3ware RAID controller.
- Install the 3ware driver and Windows on a new drive or unit.
- Install the 3ware driver when Windows is already installed on a different device.

Note: You must have administrator privileges for your system to install the Windows operating system and the 3ware driver.

Materials Required

- 3ware software CD-ROM
- Microsoft Windows XP or Server 2003 installation CD-ROM. (Not required if Windows is already installed on another drive.).
- Floppy diskette, to create a driver diskette.

  If you are installing Windows onto the RAID unit you are creating, you must create a 3ware driver diskette. If Windows is already installed on another device, you may install the 3ware driver from either the 3ware software CD-ROM or from a diskette.

Creating a 3ware Driver Diskette

If you are installing Windows on a new unit or drive managed by the 3ware RAID controller, you must create a 3ware driver diskette.

To create a driver diskette

1 Insert the AMCC 3ware software CD into your Windows system.

Autorun should start the 3ware menu program. If it does not, open **My Computer**, select the CD, right-click and choose **AutoPlay**.

2 When the License screen appears, review and agree to the license in order to continue.

3 When the AMCC 3ware Menu appears, click **Driver Disk Images.**

4 In the AMCC 3ware Driver Disk Images menu, click the appropriate button to create the driver diskette that you need.

Note that there are both 32-bit and 64-bit drivers available for Windows. Be sure to select the correct one.

5 When the confirm message appears, insert a blank diskette into a floppy drive and click the **Yes** button to begin the process.

Installing the 3ware Driver and Windows on a New Unit

If you want to install Windows on a new drive configuration managed by the 3ware RAID controller, follow the instructions in this section.

If Windows is already installed on another drive, turn to “Installing the Driver on a System that Boots from a Different Device” on page 34.

To install Windows and the 3ware driver

1 Boot from the Windows XP, or Windows Server 2003 CD and press **F6** when you see the message: “Press F6 if you need to install a 3rd party SCSI or RAID driver” at the bottom of the display.

2 When you see the message: “Setup could not determine the type of one or more mass storage devices or you have chosen to manually specify an adapter…”

Type **S** to specify that you have an additional 3ware RAID controller.

3 Insert the 3ware driver diskette and press **Enter**.

4 When a box with **AMCC 3ware 9000 Series RAID Controller** appears, press **Enter** to select it.

5 Type **S** if you have additional devices to add. Otherwise, press **Enter**.

6 If the “Digital Signature Not Found” message appears, click **Yes** to continue the installation.

(If there are multiple controllers in the system, you will see this message once for each controller.)

7 Continue with the normal Windows installation at this point. There are no instructions after installing the driver that are specific to 3ware. If you need additional instructions, refer to the Windows XP, or Windows Server 2003 documentation supplied by Microsoft.

8 Follow the instructions under “Making Units Managed by a 3ware Controller Available to Windows” on page 37.

Installing the Driver on a System that Boots from a Different Device

If you are installing the 3ware RAID controller on a system that already has the operating system installed on another drive, follow the instructions in this section, depending on the version of Windows installed on your system:

To install the 3ware driver under Windows XP or 2003

When you start Windows after installing a 3ware RAID controller, Windows recognizes it as a Plug and Play device, and brings up the **Found New Hardware Wizard.** This wizard guides you in installing the 3ware driver (see Figure 18). Note that you will see screens for the installation of two drivers during this process.

Figure 18. Found New Hardware Wizard, Windows XP and 2003

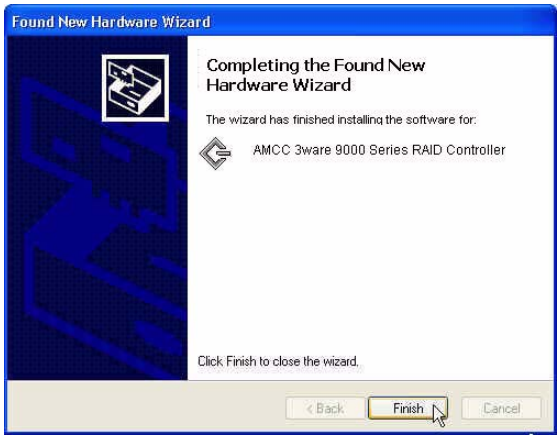
1 Click the **Next** button and respond to the questions the Wizard displays.

2 When the Wizard prompts you to select a device driver, click Have Disk, and then indicate that it is on the CD or floppy.

3 If the “Digital Signature Not Found” message appears, click **Yes** to continue the installation.

4 When the Completing the Found New Hardware Wizard screen appears (Figure 19), click **Finish**.

Figure 19. Completing Found New Hardware Wizard



5 If the “Completing” screen similar to the one above indicates that you should restart your computer, do so now.

6 When the Welcome to the Found New Hardware Wizard screen appears again (Figure 20), click **Next** and follow the prompts on the screen to install the second driver.

Figure 20. Welcome to the Found New Hardware Wizard

7 When the second Completing the Found New Hardware screen appears, click **Finish**.

Figure 21. Completing Found New Hardware Wizard

After the driver has been installed, continue with the instructions below under “Making Units Managed by a 3ware Controller Available to Windows” on page 37.

Making Units Managed by a 3ware Controller Available to Windows

After the 3ware driver has been installed, you need to partition and format the new units or disks.

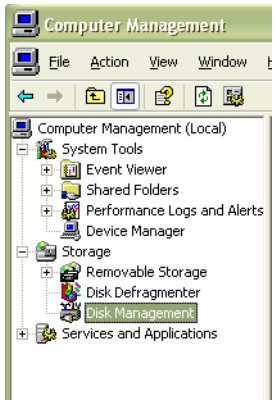
1 Remove the driver diskette or CD, reboot the system, and log in as the system administrator.

2 Use **Disk Administrator** to partition and format the new units or disks:

From the **Start** menu, choose **Programs>Administrative Tools** > **Computer Management**.

In the Computer Management window, under **Storage**, select **Disk Management.**

Figure 22. Computer Management Screen



3 Follow the steps that appear on the screen to write a signature to the drive.

4 Right-click on the drive and select **Create Volume**.

5 Follow the steps the appear on-screen to create a volume and to assign a drive letter.

Driver Installation Under Linux

Note: Before installing the 3ware driver, you must have already installed your 3ware RAID controller in the system. Consult the installation guide that came with your controller for how to do this. You can download that guide from: http://www.3ware.com/support/userdocs.asp

A drive or unit managed by the 3ware RAID controller may be configured to be your system's boot device. Or, you can use units managed by the 3ware controller for secondary storage and boot from another device, such as a disk attached to the motherboard, or other bootable media.

These steps assume that you do not have a 3ware 9000 Series card installed in the system already. If you already do and you wish to add a 9690SA to that same system, you will need to upgrade the 3ware driver, 3DM 2, and/or CLI with the current version.

The steps you follow to install the driver and make your RAID unit available depend on which version of Linux you are using, and whether it will be your boot device. This chapter provides step-by-step instructions for the following:

- Red Hat / Fedora Core Linux Installation
  - "Installing the 3ware Kernel Driver Module while Installing Red Hat Linux on a New Unit" on page 41
  - "Installing the 3ware Kernel Driver Module on a Red Hat or Fedora Core Linux System that Boots From a Different Device" on page 42
- SuSE Linux Installation
  - "Installing the 3ware Kernel Driver Module while Installing SuSE Linux on a New Unit" on page 46
  - "Installing the 3ware Kernel Driver Module on a SuSE Linux System that Boots from a Different Device" on page 46

The 9.4.1 code set from the 3ware website provides compiled drivers for these versions of Linux:

- Fedora Core 6 for AMD and Intel Platforms (32-bit & 64-bit)
- RedHat Workstation 5 for AMD and Intel Platforms (32-bit & 64-bit)
- openSuSE 10.2 for AMD and Intel Platforms (32-bit & 64-bit)
- SuSE Linux Enterprise Server 10.0 for AMD and Intel Platforms (32-bit & 64-bit)

If you are using an unsupported Linux distribution or kernel for which there is not a driver available from the 3ware download page, see the following article in the 3ware knowledgebase:
http://www.3ware.com/kb/article.aspx?id=14546. You can also contact

3ware Technical Support, or email your driver request to support1@amcc.com.

For information about how to compile a driver from the 3ware driver source, see the links appended to knowledgebase article 14546 (http://www.3ware.com/kb/article.aspx?id=14546).

Obtaining 3ware Linux Drivers

Obtain the 3ware driver for Linux from one of these two sources:

- **3ware software CD-ROM**. Compiled and tested drivers for Red Hat, SuSE, and Fedora Core Linux are included on this CD.
- **3ware web site.** You can download the latest compiled and tested driver for supported Linux distributions from the 3ware web site at http://www.3ware.com/support/index.asp. Included in these downloads is the Linux driver source, which you can use to compile the latest driver for RedHat, SuSE, and other similar distributions, running similar kernel strings.

Be Sure to Use the Correct Drivers

Warning: Be sure to use the correct driver for your processor. It is possible to load the wrong driver onto a system, however when you boot such systems, they will not work.

For Red Hat and SuSE, AMCC offers the following drivers:

- x86 32-bit for Intel x86 and AMD Athlon
- x86_64 64-bit for AMD Opteron and Intel Xeon (EM64T)

Determining the Current Version of your 3ware Driver

If you already have a 3ware controller installed, you can check the current driver version, using either 3DM 2 or the CLI. (For details, see "Viewing Information About a Controller" on page 72.)

You can also check it using the following method:

If you have a 2.4 kernel or earlier, type the following command:

```
cat /proc/scsi/3w-9xxx/*
```

where the asterisk (*) represents SCSI host ID and `9xxx` represents the family of the controller. For example:

```
cat /proc/scsi/3w-9xxx/0
```

If you have a 2.6 kernel with sysfs, type the following command:

```
cat /sys/class/scsi_host/<hostid>/stats
```

where <hostid> is usually host0, unless other SCSI devices are available, in which case it may be host1 or higher.

If you have a 2.6 kernel without sysfs, type the following command:

```
dmesg | grep 3w
```

Driver Installation Under Red Hat Linux or Fedora Core

Materials required

- 3ware software CD-ROM
- Floppy diskette, if you need to create a driver install diskette.
- Red Hat Linux installation DVD or CD-ROM. (Not required if Red Hat Linux is already installed on another drive.)

Creating a Red Hat Linux Driver Diskette

If you are installing Linux on the new drive or unit managed by the 3ware RAID controller, you must create a 3ware driver install diskette. If Linux is already installed on another device, you may install the 3ware kernel driver module from the 3ware software CD-ROM.

To create a Red Hat Linux driver install diskette

1 Insert the AMCC 3ware software CD into your Linux system. A GUI such as X windows is required to load the 3ware menu.

To manually mount the cd, type:

```
mount /dev/cdrom /mnt
```

To start autorun, type:
`/mnt/autorun`

When it starts, you will be asked to agree to the AMCC software license. To continue, click **Agree**.

2 When the AMCC 3ware Menu appears, click the **Driver Disk Images** button.

3 In the AMCC 3ware Driver Disk Images menu, click the button for the driver disk you want to create.

A confirmation window opens.

4 Insert a blank diskette into a drive and click the **Yes** button to begin creating the driver floppy diskette.

Note: If you need to create a Linux driver diskette for a Linux distribution other that what is available on the menu, see 3ware knowledgebase article 14546 http://www.3ware.com/kb/article.aspx?id=14546

Installing the 3ware Kernel Driver Module while Installing Red Hat Linux on a New Unit

Note: If Red Hat Linux is already installed and bootable on another drive, turn to “Installing the 3ware Kernel Driver Module on a Red Hat or Fedora Core Linux System that Boots From a Different Device” on page 42.

Note: We have tested some older systems where a drive connected to the motherboard interfered with using a drive or unit managed by the 3ware RAID controller as a boot device. Disconnecting the drive while installing Linux will eliminate this problem. After Linux is installed, the drive can be reconnected.

To install the 3ware kernel driver module while installing Red Hat or Fedora Core Linux on a new unit

1 Boot with the Red Hat or Fedora Core DVD or CD:

a Insert the Red Hat DVD or CD-ROM disk into your computer.

b Make sure the boot order in your motherboard’s BIOS is correct; then start or reboot your computer.

c When the Welcome to Red Hat display appears, type:
`linux dd`

A number of files will load and then a message will prompt you to insert your driver install disk.

4 Install the 3ware kernel driver module, using the driver install diskette:

Insert the driver install diskette containing the 3ware driver for Red Hat and press **Enter**.

The system automatically reports: `Loading 3w-9xxx`

5 When prompted, select the proper language and keyboard types for your locality.

6 If asked for what type of media, select Local CD-ROM since you are installing from the Red Hat CD-ROM.

7 After installation completes, remove media (CD and floppy disks).

8 Click reboot button to finish installation.

Installing the 3ware Kernel Driver Module on a Red Hat or Fedora Core Linux System that Boots From a Different Device

The steps for installing the 3ware kernel driver module vary slightly, depending on your specific installation requirements. Select the appropriate set of steps below, based on whether:

- You want to update the RAM disk
- You prefer to load the driver manually or from a script, instead of updating the RAM disk

About Variables In the Kernel Driver Module Installation Instructions

These conventions are used for variable text for kernel strings and module names in the instructions on the following pages.

Kernel String Conventions

<kernel string> refers to the kernel version.

The kernel string will have different endings, depending on the kernel you are using.

- For an SMP kernel (multi-processor), the kernel string will end in smp. For example: `2.6.16-smp`.
- For an Enterprise kernel, the kernel string will end in enterprise. For example: `2.6.16-enterprise`
- For a Bigmem kernel, the kernel string will end in bigmem. For example: `2.6.16-bigmem`

- For a Hugemem kernel, the kernel string will end in hugmem. For example: `2.6.16-hugmem`

Module Naming Conventions

3w-9xxx.* refers to the specific kernel driver module you will copy in the examples shown in steps 3 and 4. The name of the kernel driver module you will copy (`3w-9xxx.*`) varies, depending on the kernel; however you will always copy it to a file named `3w-9xxx.ko` for 2.6 kernels. Depending on the supported release, not all modules may be required or available.

The available kernel driver module files are:

- For UP kernels: `3w-9xxx.ko`
- For SMP kernels: `3w-9xxx.smp`
- For Enterprise kernels: `3w-9xxx.ent`
- For Bigmem kernels: `3w-9xxx.big`
- For Hugemem kernels: `3w-9xxx.hug`
- For IA32E kernels: `3w-9xxx.i32`

To install the 3ware driver and update the RAM disk

1 Log in as root and open a console window.

2 Mount the CD which contains the 3ware kernel driver module.

To mount the CD, type:

`mount /dev/cdrom /mnt` and press Enter.

3 Copy the kernel driver module:

For Redhat Linux Intel x86 and AMD, type:
`cp /mnt/packages/drivers/linux/redhat/`<version>`/x86/3w-9xxx.`<ko, smp, or hug>` /lib/modules/`<kernel string>`/kernel/drivers/scsi/3w-9xxx.ko`

For Fedora Core on Intel x86 and AMD, type**:**
`cp /mnt/packages/drivers/linux/fedora/`<version>`/x86/3w-9xxx.`<ko, smp, or hug>` /lib/modules/`<kernel string>`/kernel/drivers/scsi/3w-9xxx.ko`

If prompted to overwrite, type y.

For Redhat Linux on AMD Opteron and Intel EM64T, type:
`cp /mnt/cdrom/packages/drivers/linux/redhat/`<version>`/x86_64/3w-9xxx.`<ko or smp>` /lib/modules/`<kernel string>`/kernel/drivers/scsi/3w-9xxx.ko`

For Fedora Core on AMD Opteron and Intel EM64T, type:
`cp /mnt/packages/drivers/linux/fedora/`<version>`/x86_64/3w-9xxx.`<ko or smp>` /lib/modules/`<kernel string>`/kernel/drivers/scsi/3w-9xxx.ko`

If prompted to overwrite, type `y`.

4 **For 2.6 Kernels**, add the following line to `/etc/modprobe.conf`
```
alias scsi_hostadapter 3w-9xxx.ko
```

5 Update the `modules.dep` file, by issuing the following command:
```
/sbin/depmod -a
```

6 Run mkinitrd by entering the following:
```
/sbin/mkinitrd -v -f /boot/initrd-<kernel string>.img
<kernel string>
```

where <kernel string> is the /lib/modules directory from which to copy the 3w-9xxx driver. Example:
```
/sbin/mkinitrd -v -f /boot/initrd-2.6.18-14.img 2.6.18-14
```

7 If you are using the GRUB boot loader, skip to Step 8.

If you are using the LILO boot loader, run LILO to update the boot record on disk by typing the following:
```
/sbin/lilo
```

The output should be similar to:
```
Added linux *
```

8 Reboot.

The 3ware kernel driver module will be loaded from the ram disk automatically at boot time.

To install the 3ware kernel driver module and load the module manually instead of using a RAM disk

1 Log in as root and open a console window.

2 Mount the CD which contains the 3ware kernel driver module.

To mount the CD, type:
`mount /dev/cdrom /mnt` and press Enter.

3 Copy the kernel driver module.

For Redhat Linux on Intel x86 and AMD x86, type:
`cp /mnt/packages/drivers/linux/redhat/`<version>`/x86/3w-9xxx.<ko, smp, or hug> /lib/modules/`<kernel string>`/kernel/drivers/scsi/3w-9xxx.ko`

For Fedora Core on Intel x86 and AMD x86, type:
`cp /mnt/packages/drivers/linux/fedora/`<version>`/x86/3w-9xxx.<ko, smp, or hug> /lib/modules/`<kernel string>`/kernel/drivers/scsi/3w-9xxx.ko`

If prompted to overwrite, type `y`.

For Redhat Linux on AMD Opteron and EM64T, type:

```
cp /mnt/packages/drivers/linux/redhat/<version>/x86_64/
3w-9xxx.<ko or smp> /lib/modules/<kernel string>/kernel/
drivers/scsi/3w-9xxx.ko
```

For Fedora Core on AMD Opteron and EM64T, type:

```
cp /mnt/packages/drivers/linux/fedora/<version>/x86_64/
3w-9xxx.<ko or smp> /lib/modules/<kernel string>/kernel/
drivers/scsi/3w-9xxx.ko
```

If prompted to overwrite, type `y`.

4 Add the following line to `/etc/modprobe.conf`:

```
alias scsi_hostadapter 3w-9xxx
```

5 Update the `modules.dep` file, by issuing the following command:

```
/sbin/depmod -a
```

6 Load the kernel driver module manually. Type:

```
modprobe sd_mod
insmod /lib/modules/<kernel string>/kernel/drivers/scsi/3w-
9xxxx.ko
```

You can also incorporate the insmod command into a startup script.

Driver Installation Under SuSE Linux

Materials required

- 3ware software CD-ROM
- Floppy diskette, if you need to make a driver install diskette.
- SuSE Linux Installation CD-ROM/DVD (Not required if SuSE Linux is already installed on another drive.)

Creating a SuSE Linux Driver Diskette

If you are installing Linux on the new drive or unit managed by the 3ware RAID controller, you must create a 3ware driver install diskette. If Linux is already installed on another device, you may install the 3ware kernel driver module from the 3ware software CD-ROM.

To create a driver install diskette

1 Insert the 3ware software CD into your Linux system. A GUI such as X windows is required to load the 3ware menu..

To manually mount the cd, type:

```
mount /dev/cdrom /mnt
```

To start autorun, type:

```
/mnt/autorun
```

2 When the 3ware Menu appears, click **Driver Disk Images**.

3 In the 3ware Driver Disk Images menu, click the button for the driver disk you want to create.

A confirmation window opens.

4 Insert a blank diskette into a drive and click the **Yes** button to begin copying the driver to the floppy diskette.

Note: If you need to create a Linux driver diskette for a Linux distribution other that what is available on the menu, see 3ware knowledgebase article 14546 http://www.3ware.com/KB/article.aspx?id=14546

Installing the 3ware Kernel Driver Module while Installing SuSE Linux on a New Unit

Note: If SuSE Linux is already installed on another drive, turn to “Installing the 3ware Kernel Driver Module on a SuSE Linux System that Boots from a Different Device” on page 46.

1 Boot directly from the SuSE installation CD #1 or DVD.

2 When installing SuSE, press either the F6 key or the F3 key, depending on the version.

You will then be prompted to insert the driver install disk.

3 Insert the 3ware Linux driver installation diskette.

4 Click OK and continue with the installation.

Installing the 3ware Kernel Driver Module on a SuSE Linux System that Boots from a Different Device

1 Log in as root.

2 Edit `/etc/sysconfig/kernel` and make sure the file contains the following line:

```
INITRD_MODULES="reiserfs 3w-9xxx"
```

Note: Other modules may be listed before or after `3w-9xxx`, depending on the installation. You may see entries like `reiserfs`, `ext3` or `scsi_mod`. If present, leave them (ensuring there is a space between each module name), since the system needs them to boot properly.

Note about variables: In the instruction below, replace <kernel string> with the kernel version you are using (i.e. 2.6, etc.).

In addition, replace 3w-9xxx.* with the appropriate module file for your kernel. The available module files are:

For UP kernels: `3w-9xxx.ko`
For SMP kernels: `3w-9xxx.smp`
For BigSMP (high memory) kernels: `3w-9xxx.big`

3 If you are using SuSE 9.1 or earlier, after the existing 3w-xxx entry, add `3w-9xxx` to the file `/lib/modules/`<kernel string>`/modules.dep`

4 Mount the CD-ROM and copy and install the appropriate kernel driver module for your system.

Note: The AMD 64-bit driver is also used for 64-bit Intel Xeon.

```
mount /dev/cdrom /mnt
```

Copy the kernel driver module:

For openSuSE and SuSE Linux Enterprise Server 32-bit (x86), type:

```
cp /mnt/packages/drivers/linux/suse/<version>/x86/
3w-9xxx.<ko, smp, or big>
/lib/modules/<kernel string>/kernel/drivers/scsi/3w-9xxx.ko
```

For openSuSE and SuSE Linux Enterprise Server 64-bit (x86_64), type:

```
cp /mnt/packages/drivers/linux/suse/<version>/x86_64/
3w-9xxx.<ko, smp, or big>
/lib/modules/<kernel string>/kernel/drivers/scsi/3w-9xxx.ko
```

If prompted to overwrite, type `y`.

5 To load the kernel driver module, type:

```
modprobe sd_mod
```

```
insmod /lib/modules/<kernel string>/kernel/drivers/scsi/3w-
9xxxx.ko
```

Note: If the kernel driver module installation fails, confirm that the correct driver was installed from the CD-ROM. If a driver is not available for your system, you will need to compile your own driver. For more information, see 3ware knowledgebase article 14546 http://www.3ware.com/kb/article.aspx?id=14546.

6 Type:
```
/sbin/depmod -a
```

7 Type:
```
/sbin/mkinitrd
```

8 If you are using the GRUB boot loader, you are finished.

If you are using the LILO boot loader, run LILO to update the boot record on disk by typing the following:
```
/sbin/lilo
```

The output should be similar to:
```
Added linux *
```

Compiling a 3ware Driver for Linux

If you are using a Linux distribution for which there is not a compiled driver available from 3ware, you can copy the source from the 3ware software CD or download the source from the 3ware website and compile a new driver. For more information, see 3ware knowledgebase article 14546 http://www.3ware.com/KB/article.aspx?id=14546.

5

3ware BIOS Manager (3BM) Introduction

This section describes the basics of using 3ware BIOS Manager (3BM), one of the tools you can use to configure and maintain the units connected to your 3ware RAID controller. It is organized into the following topics:

- Starting 3BM
- Exiting the 3BM Configuration Utility
- Working in the 3BM Screens
- Adjusting BIOS Loading Settings
- Displaying Information About the Controller and Related Devices
- Getting Help While Using 3BM

For information about doing particular tasks in 3BM, refer to the later sections in this guide.

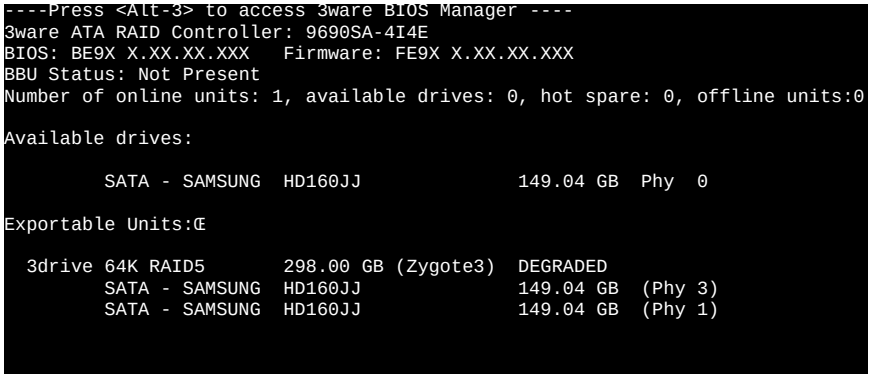
Starting 3BM

You access 3BM during the start-up process for your computer.

1 Power up or reboot your system.

2 While the system is starting, watch for a screen similar to the 3ware BIOS screen below.

Figure 23. 3ware BIOS Screen

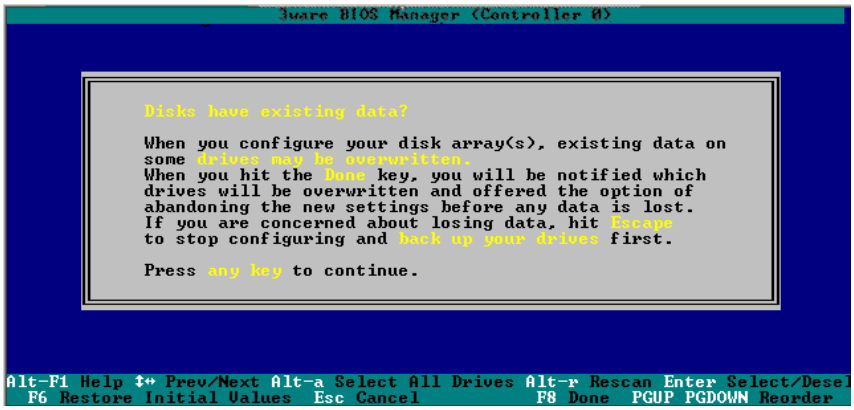


3 Press **Alt-3** immediately to bring up the **3ware BIOS Manager (3BM)**.

Normally your 3ware configuration remains on-screen for just a few seconds. However, if a unit has degraded, the screen indicates the problem and remains on your screen longer.

4 If you plan to make changes to your configuration and need to backup data before continuing, press **ESC** and do so now. Otherwise, press any key to continue.

Figure 24. Warning Message When you Start 3BM

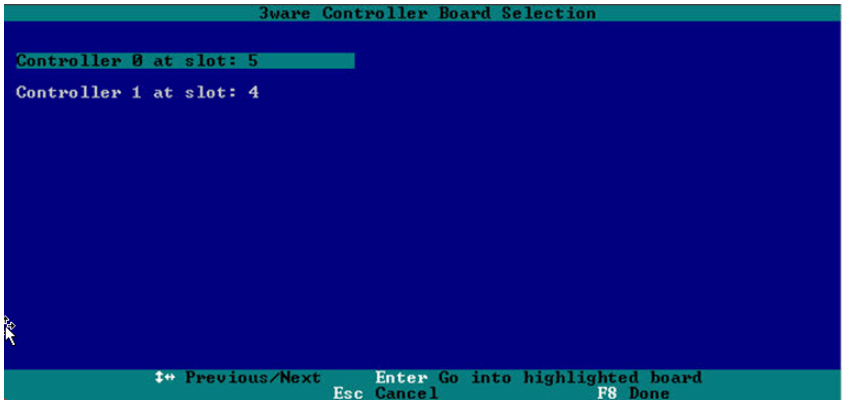


If 3BM detects a degraded array, a red message box appears, to alert you to the problem. For information about rebuilding a degraded array, see “About Degraded Units” on page 130.

5 If you have more than one 9000-series controller in your system, a screen lists the available boards (see Figure 25). In this case, highlight the board with which you want to work and press **Enter**.

If you have more than 2 boards, you will only see two at first (only two can be processed at a time). After you exit from 3BM, you will have an opportunity to access the BIOS again, to access the next boards.

Figure 25. AMCC Boards Selection Screen



You see a screen similar to the warning message below, warning you that changing your disk array configuration may overwrite data on the disks.

Exiting the 3BM Configuration Utility

When you are ready to exit the 3BM configuration utility, you have the option to save the configuration changes you have made, or to discard the changes.

To save your configuration modifications

1 Press the **F8** or **Esc** key.

A list of affected drives appears, and a messages ask you to confirm the configuration.

2 Type Y.

The booting process resumes.

To exit without saving changes

1 Press **Esc.**

2 If you have unsaved changes, 3BM will ask you whether you want to save the changes and exit, or exit without saving the changes.

If you want to exit without saving changes, type N.

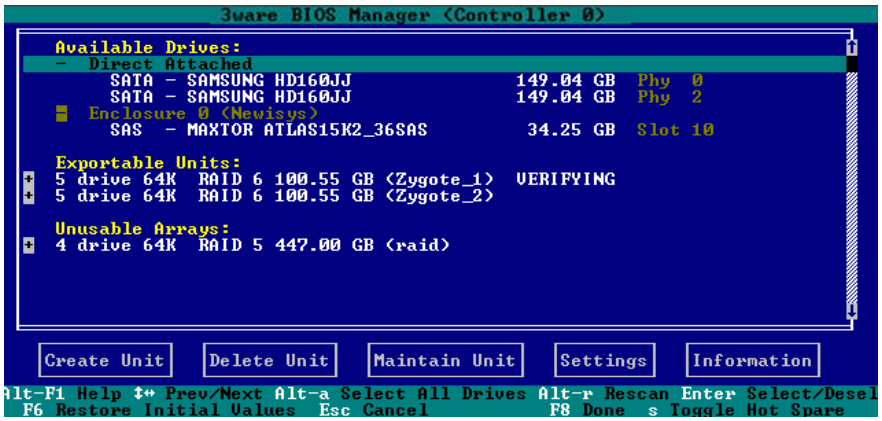
If you change your mind and want to save the changes, type Y.

Exception: Changes made to controller policies are saved when you leave the Policy screen. Pressing **F8** is not required to save those changes. For more about changing policies, see “Setting the Auto Rebuild Policy” on page 77.

Working in the 3BM Screens

The main **3BM** screen (Figure 26) shows the current configuration for the drives attached to your controller, and a list of any available drives. Unusable and incomplete drives are also shown.

Figure 26. 3BM Main Display



You will see one or more of the following sections in the main 3BM screen:

- **Available Drives** lists any unconfigured drives that are not associated with an array, and hot spares. If this section does not appear, there are no available drives.

  Direct Attached lists the drives directly attached to the controller.

  Enclosure lists the drives attached through an enclosure.

- **Exportable Units** lists the existing units and the drives contained in each unit. These are the units that will be available to the operating system when you boot your computer. If this section does not appear, no units have been configured.

  If you have more than one unit, the boot unit is the one at the top of the list. (You can change the order by highlighting a unit and pressing the **PgUp** or **PgDn** key.)

- **Unusable Arrays** lists any RAID configuration missing too many drives to construct the unit. For example, a RAID 5 unit with two or more drives missing would appear in this list.

- **Incomplete Drives and Others** lists drives that are remaining from a unit with missing or failed drives and drives that are not usable.

  When some of the drives are remaining from a unit, you can power down and add the missing drives to complete the unit. To use drives that are listed here in other units, you must first delete them. For more information, see “Deleting a Unit” on page 114.

If any of the sections are not shown, it means that there are no items of that type connected to the controller.

Table 6 lists how to move around and select information in the 3BM screens. When these commands are available in 3BM, they appear at the bottom of the 3BM screen.

Table 6: Working in 3BM

To do this	Use these keys
Move between units or drives in a list, between fields, and between buttons	Up and Down Arrow Keys OR Left and Right Arrow Keys OR Tab and Shift+Tab
Select (or unselect) what is currently highlighted. A selection may be a drive in a list of drives, a button at the bottom of the screen, or a field in the middle of the screen. In lists, an asterisk appears to the left of selected drives or units	Enter or the Spacebar
Display a drop-down list of available choices in a field	Enter
Move between choices in a field list	Up and Down Arrow Keys
Select all available drives	Alt+A
In the list of units, expand a selected unit to see any subunits and drives in the unit, or contract it to see only the heading again. In the list of available drives these keys also work to show or hide the drives in each enclosure.	Shift+ -
Highlight one of the primary buttons on the main screen: • Create Unit • Delete Unit • Maintain Unit • Settings • Information	 Alt+C Alt+D Alt+M Alt+S Alt+I

Table 6: Working in 3BM

To do this	Use these keys
Specify (or unspecify) a drive as a hot spare	S
Blink the LED associated with a drive	F4, from the Drive Information screen (requires use of a supported enclosure)
Return to starting values for this session in the 3ware BIOS Manager	F6 **Note:** F6 cannot bring back previous policy settings; they are saved when you exit the Policy screen.
Rescan the controller and update the status of units and drives	Alt+R
Return to the main 3ware BIOS Manager screen, from the Advanced Details screen	Any key
Move a highlighted unit up or down in the list of exportable units (The top-most unit will become the bootable unit, if you install the OS.)	Page Up Page Down (Available only when there are multiple units and a unit is highlighted.)
Display context sensitive help	F1 or Alt-F1
If you have multiple 3ware controllers in your system, return to the board selection screen.	Esc
Exit the utility and save or abandon all changes.	Esc
Exit the utility and save all changes	F8

Adjusting BIOS Loading Settings

3BM includes a few settings that let you customize the behavior of the BIOS for the selected controller. You can access these settings by selecting **Settings > BIOS Settings** from the main 3BM screen.

Power-On Self Test (POST) Display Options

Display Control. Specifies what level of detail to display on the start-up screen.

- **Full** displays all available information about the items attached to the controller, including available drives, hot spares, and configured units.
- **Unit Only** displays only configured units.
- **Summary** displays a one-sentence description of the items attached to the controller.

Array View. Specifies what level of information to show about configured units on the start-up screen.

- **Expanded** lists each unit and shows the specific drives that make up the unit.
- **Collapsed** lists only the configured units.

Pause Time. Sets the number of seconds that BIOS loading will pause to displaying the RAID configuration before continuing to boot the operating system. You can set a pause time of up to 10 seconds. The default is 6 seconds.

Full Screen Control. When you have many drives attached to a controller and choose to display the Full level of detail, the information can extend beyond a screens' worth. The Full Screen Control setting lets you specify whether to wait for a keystroke when the screen is full, before displaying additional information. This option can be either **No Key** or **Wait Key**.

BIOS Loading Options

Load Control. This setting is enabled by default. It allows you to boot from RAID units or drives managed by the controller. If this setting is disabled, you will only be able to boot from hard drives or peripheral devices (such as CD-ROM or floppy) that are not managed by the controller. You may wish to disable this setting if you have multiple controllers in a "headless" system with no monitor or keyboard.

Note: During the boot process, you can also bypass loading of the BIOS for all controllers for one time only by pressing **Alt-B**. This is useful to temporarily boot from a non-3ware device without having to change the system's boot order.

Changing BIOS Settings

You can change these BIOS settings from the one screen in 3BM.

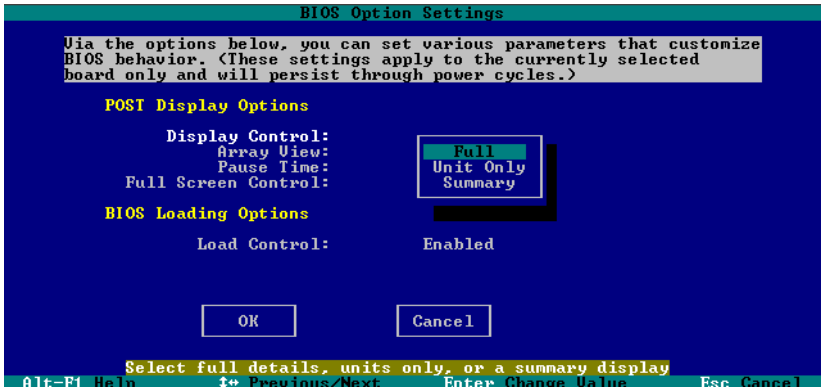
To change the BIOS Settings

1 On the main 3BM screen, **Tab** to **Settings** and press **Enter**.

2 On the pop-up menu, select **BIOS** and press **Enter**.

The BIOS Options Settings screen appears.

Figure 27. BIOS Option Settings Screen



3 **Tab** through the options and make the desired changes.

4 **Tab** to **OK** and press **Enter** to return to the main screen.

Displaying Information About the Controller and Related Devices

The 3BM Information menu gives you access to detailed information about the controller, BBU, drives, enclosures, and phys.

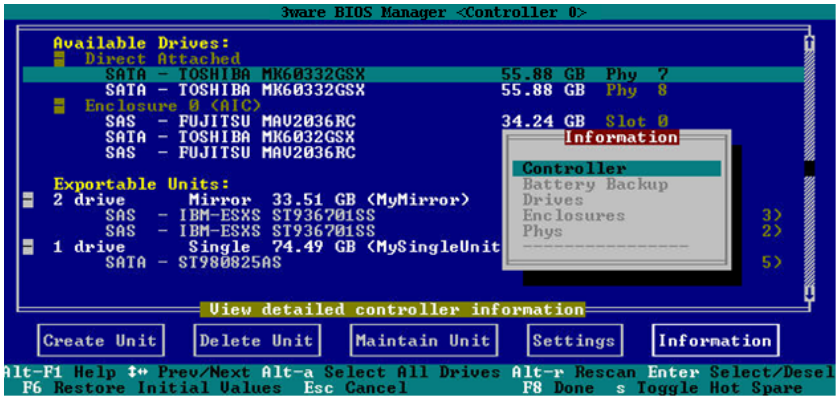
To see information about the controller or a related device

1 On the main 3BM screen, **Tab** to **Information** and press **Enter**.

A pop-up menu appears, listing the available information screens.

2 On the pop-up menu, select the item about which you want to see details and press **Enter**.

Figure 28. Controller Information Screen



A page appears showing details about selected item.

For more about how to use these pages, see the following topics:

- “Viewing Information About a Controller” on page 72
- “Viewing Battery Information” on page 175
- “Viewing a List of Drives” on page 127
- “Viewing a List of Enclosures” on page 180
- “Viewing Information About a Phy” on page 81

To return to the main screen

- Press **Enter**.

Getting Help While Using 3BM

You can get help with using 3BM while you are in the BIOS manager.

- Press **F1** or **Alt-F1** at any time.

  A description of the basic 3BM tasks appears.

  When you’re finished using help, press **Esc** to close the help window.

6

3DM 2 (3ware Disk Manager) Introduction

Note: 3DM 2 includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

3ware Disk Manager 2 (3DM 2) allows you to manage and view the status of your 3ware RAID controllers and associated drives.

There are two parts to 3DM: a process, that runs in the background on the computer where you have installed your 3ware controller, and a web application that can be used to access it. 3DM runs as a service under Microsoft Windows, and as a daemon under Linux. When the 3DM process is running, you can use your browser to go to 3DM application pages, where you can view status information about the controller and RAID units, create RAID units, and perform other administrative and maintenance tasks locally or remotely.

Two levels of access to 3DM are provided: user and administrator. Users have view-only access, and can check the status of drives and units. Administrators can view and make changes, using 3DM to configure RAID units and designate hot spares, and to perform maintenance tasks on RAID units.

In this section, information is organized into the following topics:

- Browser Requirements for 3DM
- Installing 3DM
- Starting 3DM and Logging In
- Working with the 3DM Screens
- Setting Up 3DM Preferences

For details about the settings and fields on each of the 3DM 2 screens, see “3DM 2 Reference” on page 186.

For additional information about managing and maintaining 3ware controllers using 3DM, see the remaining chapters in this guide.

Browser Requirements for 3DM

3DM runs in most current web browsers. Tested and supported browsers include:

- Internet Explorer 5.5 and above
- Mozilla Firefox
- Netscape 7 and above

Additional requirements:

- JavaScript must be enabled
- Cookies must be enabled
- For best viewing, use a screen resolution of 1024 X 768 or greater, and set colors to 16 bit color or greater.

Note: Because 3DM may be viewed in different browsers, the format and style of the 3DM browser windows illustrated in this documentation are examples only. The actual “look” of the windows will depend on the browser, 3DM version, and operating system you use.

Setting up Mozilla Firefox

Before setting up Mozilla Firefox, remember to download and install the latest available version of Mozilla Firefox. After installing the latest version, you may need to follow the instruction in the note below to have Mozilla Firefox working correctly with 3DM2.

Note: For security reasons, some web browsers do not allow connections to certain ports including port 1080 and 888. To override this on a per-port basis, the Mozilla release notes recommend adding a comma-separated list of ports to default/all.js (in your Mozilla installation directory). For example, to unblock port 888, add the following line:

```
pref(“network.security.ports.banned.override”, “888”)
```

This file is located at:

```
/usr/lib/mozilla/defaults/pref/all.js
```

Installing 3DM

3DM 2 can be installed from the 3ware CD that came with your 3ware RAID controller. You can also download the current version from the website at http://www.3ware.com/support/download.asp. Details about the installation are described in Appendix B, “Software Installation” on page 277.

3DM must be installed on the system in which the controller is installed. 3DM does not have to be installed on a remote system in order to remotely manage the 3ware controller; you simply enter the correct URL into a browser on the remote system. You will need to enable remote access first, however.

Starting 3DM and Logging In

3DM runs as a service under Windows, and as a daemon under Linux. Normally after installation, the 3DM process starts automatically when you start your system.

It is a good idea to leave the 3DM process running on the system that contains your 3ware RAID controller. That way email alerts can be sent by 3DM, and administrators can manage the controller remotely, if remote administration is enabled.

When 3DM is running in the background on your computer, you can access the 3DM web application through your browser to check status information and manage your 3ware RAID controller.

If you want to check the status of a controller from a different computer, see “Viewing 3DM Remotely Using a Web Browser” on page 62.

Logging In to the 3DM Web Application

When the 3DM process is running in the background, you can log into the 3DM application pages using a browser.

Two levels of access are provided:

- *Users* can check the status of the controller, units, and attached drives.
- *Administrators* can check status, configure, and maintain the units and drives on the 3ware controller.

Note: Administrator and User status in 3DM is not related to Administrator/User settings in the operating system.

To log in to the 3DM web application

1 Open your browser and enter the URL for your system.

The default URL is https://localhost:888/

If remote access is enabled, you can also replace “localhost” with the IP address of the computer that contains the 3ware controller. For example: https://<IP address>:888/

Note: If you receive a page not found message, make sure you entered the URL correctly by specifying https, not http. If you did, 3DM may not be running in the background. You can start it manually.

2 The first time you start 3DM, when the security certificate message displays, click **View Certificate** and accept the certificate so that you do not see the security message each time you start 3DM.

Figure 29. Security Certificate Message from Browser

(You can also click **Yes** or **Continue**, in which case you will see this message the next time you start 3DM.)

3 When the 3DM logon screen appears, select whether you are a **User** or **Administrator**.

4 Enter your password and click **Login**.

If you are logging in for the first time after installing 3DM, the default password for both User and Administrator is `3ware`.

Note: If you forget the passwords, uninstalling and reinstalling 3DM resets the passwords to `3ware`.

Note: If you close your browser, 3DM continues to run in the background on the system.

Starting the 3DM Daemon under Linux

3DM should start automatically after installation and upon bootup. If it does not, use the steps below to start it.

To start the 3DM daemon manually

1 Login as root on the machine on which 3DM is installed.

2 Afterwards, type:
`/etc/init.d/3dm2 start`

Starting the 3DM Process under Microsoft Windows

3DM should start automatically after installation and upon bootup. If it does not, use the steps below to start it.

To start the 3DM process manually

1 On the system on which 3DM is installed, login as Administrator.

2 Open **Control Panel>Administrative Tools>Services>3DM2** and select the **Start/Play** icon.

Viewing 3DM Remotely Using a Web Browser

When remote administration is enabled on the 3DM 2 Settings page, you can use 3DM to check status and administer your 3ware RAID controller from a browser on any computer, over an internet connection.

You do not need to install the 3DM software on the remote computer.

To connect to 3DM2 through your web browser

- In the address line of your browser, enter the URL or IP of the system containing the 3ware RAID controller.

  If you do not know the URL or IP for the system, you can contact your network administrator or from a Windows command prompt, type `ipconfig`. From a Linux command prompt, type `ifconfig`.

Note: When using 3DM to access a remote system, and auto logout is enabled, the time on the local system must match the time on the file server. If the time varies by more than 30 minutes, it will not be possible to remotely monitor the system (you will not be able to log in). If you are in a different time zone, you must first change the time of the local system to match the time of the remote system.

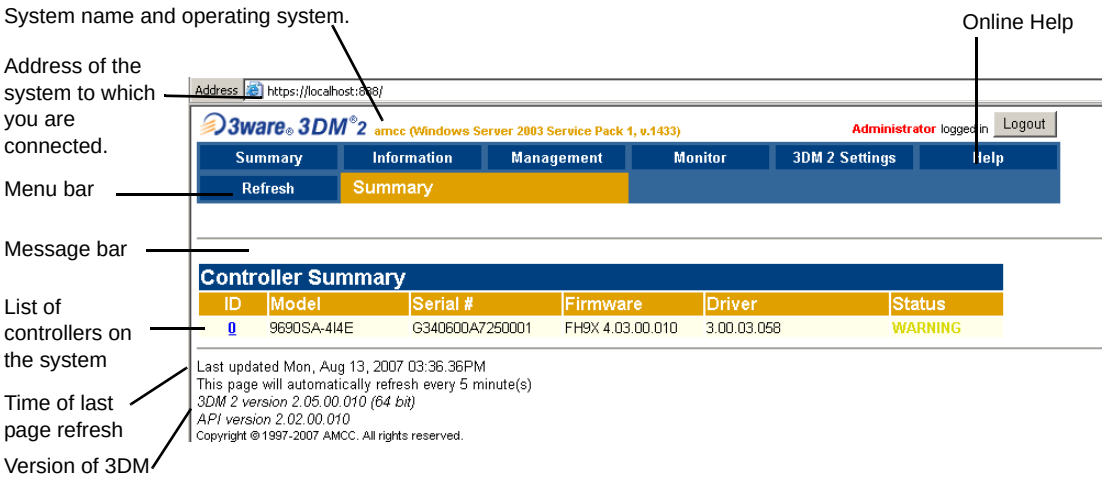
Working with the 3DM Screens

3DM's features are organized on a series of pages you view in your browser.

After you log in to 3DM, the Summary page shows a list of controllers installed in the computer at the URL you specified.

Note: If you expect to see a controller that is not listed, it may not be compatible with the driver that is loaded; a firmware flash upgrade may be required.

Figure 30. 3DM Main Screen



The menu bar across the top of the screen gives you access to other pages in 3DM. You can move between pages by using the menu bar, or by clicking a link on the page.

The main area of the page provides summary or detail information about your 3ware RAID controller and the resources connected to it.

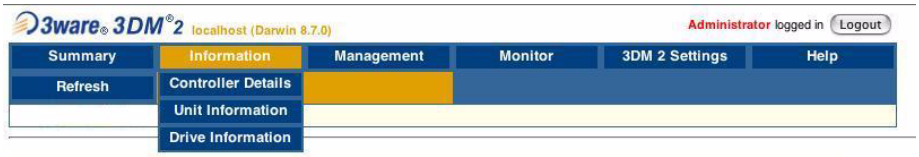
As you work in 3DM, the Messages area just below the menu bar displays information about the results of commands you have selected.

Tip: If you have a question about something you see on the screen, just click the Help button in the menu bar.

3DM Menus

The 3DM menu bar groups access to a number of 3DM pages on menus, and provides direct link access to others.

Figure 31. 3DM Menu Bar



Status information is available from the **Information menu**. You can view controller, unit, and drive information for a particular controller.

The **Management menu** gives you access to tasks used for managing controller-level settings (background task rate, unit polices such as enabling of unit write cache, and controller settings that affect all units managed by the controller), tasks that can be scheduled (rebuild, verify, and self-test), and maintenance of individual units. Unit configuration can also be done through the **Management > Maintenance** page.

The **Monitor menu** gives you access to the Alarms page, the BBU page, and the Enclosure Summary page. The **Alarms** page shows a list of alarms, including the specific alarm message, and the exact date and time it occurred. The **BBU** page shows the status of a Battery Backup Unit (BBU), if one is installed, and allows you to test the battery. The **Enclosure Summary** page provides lists the enclosures connected to the controller and lets you drill down for more detailed status information about each.

The **3DM 2 Settings** page lets you set preferences, including email notification for alarms, passwords, page refresh frequency, whether remote access is permitted, and the communication port which 3DM will use for listening.

Help lets you access information about using 3DM. The Help is context-sensitive, so you first see information about the page you now have in view. A Table of Contents and Index are available to help you find other information.

Viewing Information About Different Controllers

If you have more than one 3ware RAID controller in the system, you select the one you want to see details about from the drop-down list at the right of the menu bar.

This drop-down is available on all pages that provide controller-specific features.

Figure 32. 3DM Controller Selection Drop-down

Note: Throughout these instructions, the term *current controller* is used to refer to the controller which is currently selected in this drop-down list.

Note: The fields and columns in 3DM 2 vary for different models of 3ware RAID controllers. If you have multiple controllers of different models, you may notice some differences when switching between them in 3DM. For example, when displaying information about the 9690SA controllers, 3DM displays “VPort” (for virtual port) on some pages while for earlier controllers the label is “port.”

Refreshing the Screen

You can refresh the data on the screen at any time by clicking **Refresh Page** in the menu bar. This causes 3DM to update the information shown with current information from the controller and associated drives.

Automatic refreshes can also be set. For details, see “Setting the Frequency of Page Refreshes” on page 70.

Note: If you click Refresh on the browser window instead of on the 3DM menu bar, you will be taken back to the Summary page.

3DM Screens and What They're Used For

The table below shows a list of the pages you work with in 3DM and describes what they are used for. Details about each page and the fields and features on it are provided in Chapter 12, “3DM 2 Reference”. The page names in the table provide links to details about that page.

In addition, the step-by-step instructions provided in the chapters on configuring and maintaining your RAID controller and units explain how to do particular tasks in 3DM.

Table 7: List of 3DM Pages

3DM Page	Description
Controller Summary page	Provides basic information about each 3ware RAID controller in your system. To see this page, click **Summary** in the menu bar.
Controller Details page	Provides detailed information about the current controller. To see this page, choose **Information > Controller Details** from the menu bar.
Unit Information page	Shows a list of the units on the current controller and provides summary information about each unit. To see this page, choose **Information > Unit Information** from the menu bar or click an ID number on the Controller Summary.
Unit Details page	Shows details about a particular unit. To see this page, click an ID number on the Unit Information page.
Drive Information page	Shows a list of drives on the current controller and provides summary information about each drive. To see this page, choose **Information > Drive Information** from the menu bar.
Drive Details window	Shows the SMART data for a specific drive, and shows additional detail information for the drive. To see this page, click the Port # for a drive on the Drive Information page.
Controller Phy Summary page	Shows the properties of controller phys. There are two ways to access this page. If you have a direct-attached drive you can access this page from the **Information > Drive Information** page by clicking the phy ID for the drive. If all drives are connected via expanders, navigate to the **Management > Controller Settings** page. Under Other Controller Settings click the **#** link for Number of Controller Phys.

Table 7: List of 3DM Pages

3DM Page	Description
Controller Settings page	Lets you view settings that affect the units on the current controller and change some of those settings. Controller-level settings that can be changed include background task rate, Auto Rebuild, Auto-Carving, and Carve Size. Some additional policies are shown that can only be changed in the BIOS or CLI. Unit-level settings include specifying the StorSave Profile and enabling or disabling the Write Cache, Auto-Verify, Continue on Error During Rebuild, and Queuing. To see this page, choose **Management > Controller Settings** from the menu bar.
Scheduling page	Lets you view and change the schedule for tasks that affect all units on the current controller. To see this page, choose **Management > Scheduling** from the menu bar.
Maintenance page	Lets you configure new units and make changes to existing units. To view this page, choose **Management > Maintenance** from the menu bar.
Alarms page	Shows a list of alarms, including the specific alarm message, and the exact date and time it occurred. To view this page, choose **Monitor > Alarms** on the menu bar.
Battery Backup page	Shows the status of a Battery Backup Unit (BBU), if one is installed, and allows you to test the battery. To view this page, choose **Monitor > Battery Backup** on the menu bar.
Enclosure Summary page	Lists the enclosures attached to your 3ware controller. To view this page, choose **Monitor > Enclosure Support** on the menu bar.
Enclosure Details page	Shows details about a particular enclosure, including status information. You can also use this page to blink the LED for a particular drive. To view this page, click the ID number of the Enclosure on the Enclosure Summary page.
3DM 2 Settings page	Lets you set preferences, including email notification for alarms, passwords, page refresh frequency, whether remote access is permitted, and the incoming port which 3DM will use for listening. To view this page, click **3DM 2 Settings** on the menu bar.

Setting Up 3DM Preferences

The 3DM 2 Settings page lets you define preference settings that affect the overall operation of 3DM. Most of these settings are specified initially during installation of 3DM.

On the 3DM 2 Settings page you can perform the following tasks:

- Setting and Changing 3DM Passwords
- Managing E-mail Event Notification
- Enabling and Disabling Remote Access
- Setting the Listening Port #
- Setting the Frequency of Page Refreshes

Setting and Changing 3DM Passwords

3DM provides different access levels for users and administrators.

The Administrator access level allows the user to fully configure 3DM. The User access level allows the user to view pages within 3DM. These passwords work independently of each other.

The default password for both the User and Administrator is “3ware”.

Passwords are case sensitive.

You can only change passwords if you are logged in as Administrator. If you change the Administrator password, you will be automatically logged out, and must log back in with the new password.

To set or change the password

1 Click **3DM 2 Settings** on the 3DM menu bar.

2 On the 3DM 2 Settings page, in the **Password** section, select the type of password you want to change: **User** or **Administrator**.

3 Type the current password in the **Current Password** field.

If you are changing the password for the first time, the factory-set default password is `3ware`.

4 Enter the new password in the **New Password** field and again in the **Confirm New Password** field.

5 Click the **Change Password** button to enact the change.

Note: If you forget your password, you can uninstall 3DM and then reinstall it. This will reset the password to the default password, `3ware`.

Managing E-mail Event Notification

3DM can notify you when the 3ware RAID controller requires attention, such as when a disk unit becomes degraded and is no longer fault tolerant.

E-mail event notification can only occur while 3DM is running, so it is recommended that the 3DM process be left running in the background on the system that contains the 3ware RAID controller.

When events occur, notification can be e-mailed to one or more recipients. You can specify the type of events for which notifications will be sent by selecting the severity:

- **Information** will send e-mails for all events
- **Warning** will send e-mail for events with severity of Warning and Error.
- **Error** will send e-mail for events with severity of Error only.

Events are listed on the 3DM **Alarms** page.

Event notification can be set up during 3DM installation, and can be changed on the 3DM 2 Settings page.

To set up event notification

1 Click **3DM 2 Settings** on the menu bar.

2 In the **E-mail Notification** section of the 3DM 2 Settings page, enter or change the settings you want.
   - Enable or Disable all notifications.
   - Set the severity level of events for which e-mail notifications are sent.
   - Specify the email address of the sender. This will appear in the “From” field of the e-mail.
   - Enter the e-mail address(es) to which notifications are sent. (Separate multiple addresses with a comma (,) or a semicolon (;).
   - Enter the SMTP server name or IP of the mail server for the computer where the 3ware controller is installed.
   - If your email server requires authentication, enter the Mail Server Login and Password.

3 Click **Save E-mail Settings**.

To send a test message

You can send a test message to make sure you’ve entered the e-mail notification settings correctly.

- Click **Send Test Message**.

Enabling and Disabling Remote Access

When remote access is enabled, a user can connect to 3DM over the internet or an intranet, to check status or administer the controller and associated drives. (See “Viewing 3DM Remotely Using a Web Browser” on page 62.)

If remote access is disabled and a user attempts to connect to 3DM remotely, they will see the following error message: “Remote Access to 3DM has been disabled. Please connect using the local machine by entering “localhost” in the URL bar.”

Remote access can be enabled or disabled on the 3DM 2 Settings page.

To enable or disable remote access

1 Click **3DM 2 Settings** on the menu bar.

2 In the **Remote Access** section of the 3DM 2 Settings page, select either **Enabled** or **Disabled** in the **Allow Remote Connections** field.

The page refreshes, and a message at the top of the screen confirms that remote access has been enabled or disabled.

Setting the Listening Port

You can set the port which 3DM uses to listen for incoming messages. If you are not sure which port would be the best to use, leave this set to the default port of 888.

To set the listening port

1 Click **3DM 2 Settings** on the menu bar.

2 In the **Listening Port #** section of the 3DM 2 Settings page, enter the port number in the **Listening Port** field.

3 Click **Change Port**.

The page refreshes, and a message at the top of the screen confirms that the listening port has been changed.

Setting the Frequency of Page Refreshes

Since the status of the drives attached to your 3ware RAID controller can change while you are viewing information about them in 3DM, it is important to refresh the page information regularly. That way you can be assured that the information you see in 3DM is current.

You can manually refresh the information on a page by clicking **Refresh Page** in the menu bar. But you can also have 3DM refresh the information on a regular basis.

To set the frequency of page refreshes

1 Click **3DM 2 Settings** on the menu bar.

2 In the **Page Refresh** section of the 3DM 2 Settings page, select how often you want the page to be refreshed in the **Minutes Between Refresh** field.

Note: If you do not want 3DM to refresh the screen automatically, select **Never** in the **Minutes Between Refresh** field. You can then refresh manually by clicking Refresh on your web browser.

7

Configuring Your Controller

This section describes how to view details about the controller, check its status, and change configuration settings that affect the controller and all of the drives connected to it. It is organized into the following sections:

- Viewing Information About a Controller
- About Controller Policies
- Viewing Controller Policies
- Setting the Auto Rebuild Policy
- Using Auto-Carving for Multi LUN Support
- Setting the Size of Volumes Created with Auto-Carving
- Enabling and Setting Up Staggered Spin-up
- Viewing Information About a Phy
- Changing the Phy Link Speed

Note: Background task rate is also set for all units on a controller. For information about setting the task rate, see “Setting Background Task Rate” on page 149.

Viewing Information About a Controller

You can check the controller model, serial number, firmware and driver versions, and the status of the 3ware RAID controller in your computer.

If you have more than one controller in your system, you can easily view information about each one using 3DM. If you are working at the BIOS level, you access 3BM for each controller separately.

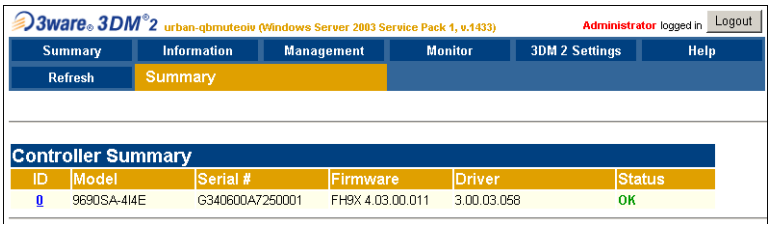
To see details about a controller in 3DM

1 Start 3DM and log in as an administrator.

The 3DM Unit Information page appears, listing all the 3ware controllers installed in your system.

The right-most column of the list shows the status of each controller.

Figure 33. Controller Summary Page



Tip: If you are managing controllers remotely, the list of controllers is for the machine with the IP or URL you entered in the browser address bar.

2 To see more details about a particular controller, click the ID link for that controller to display the Unit Information page.

To see information about a different controller in the 3DM pages

If you have more than one controller in the system, you can switch between them by selecting the one you want from the **Select Controller** drop-down list at the right of the menu bar. This drop-down is available on all pages that provide controller-specific features.

When you select a different controller from this list, the page in view changes, to reflect the details for the controller you selected.

Note: Throughout this documentation, the term *current controller* is used to refer to the controller currently selected in this drop-down list.

To see information about a controller in 3BM (BIOS)

1 Power up or reboot your system.

2 While the system is starting, watch for a screen showing information about the controller and units you want to work with.

When you have more than one controller installed, information about each one will be shown, sequentially.

3 Press **Alt-3** to bring up the **3ware BIOS Manager (3BM)**.

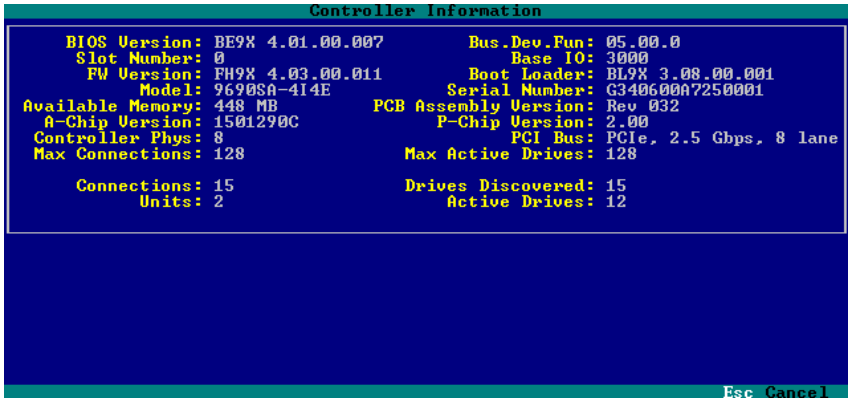
Note: If you accidentally bypass display of the controller you want to work with, press **Ctrl-Alt-Del** to restart your computer and try again

4 **Tab** to **Information** and press **Enter**.

5 On the pop-up menu, select **Controller** and press **Enter**.

The Controller Information page displays.

Figure 34. Controller Information page



About Controller Policies

The following policies affect all units and drives on a controller and can be adjusted as appropriate for your equipment. Controller policies are shown at the bottom of the Controller Settings page in 3DM (Figure 35) and on the Policy Control screen in 3BM (Figure 36).

- **Auto Rebuild.** Determines whether the Auto Rebuild policy is enabled or disabled. When disabled, degraded units can only be rebuilt with designated spares. When enabled, the controller firmware will automatically attempt to rebuild a degraded unit if there is no spare, using either an available drive or a failed drive.
- **Auto-Carving.** Determines whether the auto-carving policy is enabled or disabled. When it is enabled, any unit larger than a specified size (known as the *carve size*) is broken into multiple volumes that can be addressed by the operating system as separate volumes. The default carve size is 2 TB.

  This auto-carving feature is sometimes referred to as multi-LUN, where each volume that is created is referred to as a "LUN."
- **Carve Size.** (Referred to as *Carving Factor* in 3BM) Sets the size for dividing up units into volumes when Auto-Carving is enabled. This setting can be between 1024 GB and 2048 GB.
- **Staggered spin-up.** Spin-up allows drives to be powered-up into the Standby power management state to minimize in-rush current at power-up and to allow the controller to sequence the spin-up of drives. Compatible drives are sent a spin up command based on the settings specified with the policies **Number of drives per spin-up** and **Delay between spin-up**

settings. This policy does not apply to drives attached to an expander. These policies can only be set using 3BM or the CLI.

- **Number of drives per spin-up.** Number of drives that will spin up at the same time when the controller is powered up, if staggered spin-up is enabled. From 1 to x, depending on the number of ports on the controller.
- **Delay between spin-up.** The delay time (in seconds) between drive groups that spin up at one time on this particular controller, if staggered spin-up is enabled.

It is possible to enable or disable automatic detection of drives on the controller's ports for staggered spinup during hot swapping of drives. This feature is only available in the CLI using the **autodetect=on|off** command. For more information, see*3ware SAS/SATA RAID Controller CLI Guide*.

- **Export unconfigured disks (JBOD).** This setting is disabled by default.

Some additional policies can be set at the unit level. For more information, see "Setting Unit Policies" on page 100.

Viewing Controller Policies

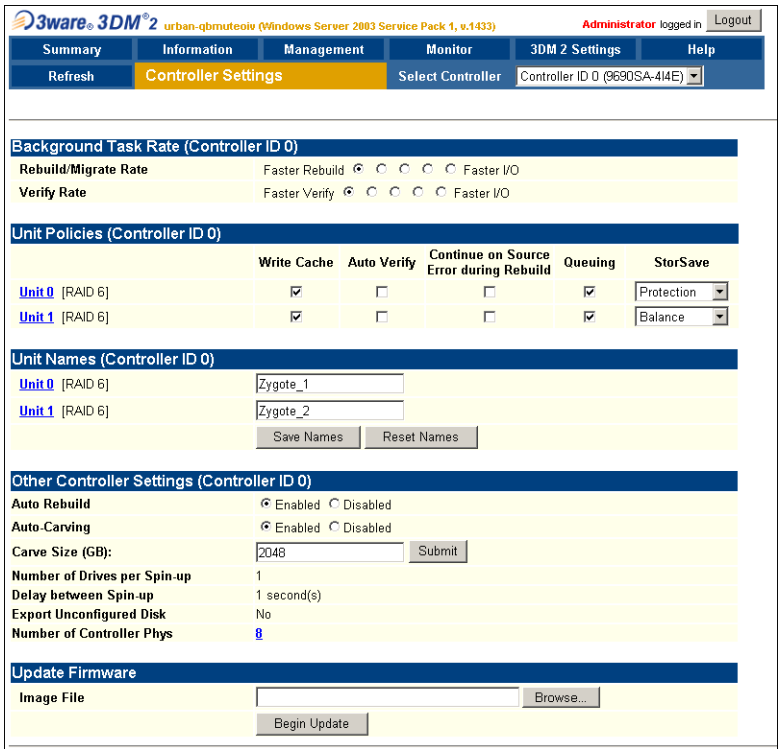
You can view the current state of controller policies in 3DM, in the **Other Controller Settings** section at the bottom of the Controller Settings page (See Figure 35). Only the Auto Rebuild, Auto-Carving, and Carve Size policies can be changed on this page. The other policies can be changed in 3BM or through the CLI. For a summary of the initial default settings, see Table 5, "Default Settings for Policies and Background Tasks," on page 19.

To view controller policies in 3DM

- Choose **Management > Controller Settings** from the menu bar.

  The policies that appear under Other Controller Settings vary, depending on the controller model you are using.

Figure 35. 3DM Controller Settings Page



To view controller polices in 3BM

You can also view and change these controller polices in 3BM, as shown in Figure 36.

1 On the main 3BM screen, **Tab** to **Settings** and press **Enter**.

2 On the pop-up menu, select **Controller Policies** and press **Enter**.

The Policy Control screen displays.

Figure 36. 3BM Policy Control Screen

Setting the Auto Rebuild Policy

The Auto Rebuild policy determines how the controller firmware will attempt to rebuild degraded units.

When Auto Rebuild is disabled, only spares will be automatically used to rebuild degraded units. When Auto Rebuild is enabled, the firmware will select drives to use for automatically rebuilding a degraded unit using the following priority order.

- Smallest usable spare.
- Smallest usable unconfigured (available) drive.
- Smallest usable failed drive.

Enabling Auto Rebuild allows you to add a drive to the controller and have it be available for a rebuild, without having to specify it as a spare.

With Auto Rebuild enabled, if you accidentally disconnect a drive (causing the controller to see it as a failed drive) and then reconnect it, the controller will automatically try to use it again.

You can enable or disable the Auto-Rebuild policy through 3DM or 3BM.

To enable Auto Rebuild through 3DM

1 Choose **Management > Controller Settings** from the menu bar in 3DM.

2 In the Other Controller Settings section at the bottom of the screen, select the **Enabled** option for **Auto Rebuild**.

The page refreshes, and a message at the top confirms the change you have made.

To enable Auto-Rebuild through 3BM

1 On the main 3BM screen, **Tab** to **Settings** and press **Enter**.

2 On the pop-up menu, select **Controller Policies** and press **Enter**.

3 On the Policy Settings page, **Tab** to the **Auto-Rebuild** field, press **Enter** to display the options, select **Enable** and press **Enter** again to select it.

4 **Tab** to **OK** and press **Enter** to select it.

The policy is enabled immediately.

Using Auto-Carving for Multi LUN Support

When the Auto-Carving policy is on, any unit larger than a specified size (known as the *carve size*) is created as multiple volumes that can be addressed by the operating system as separate volumes. These chunks are sometimes known as multiple LUNs (logical units). However, throughout the 3ware documentation, they are referred to as *volumes*.

For example, using the default carve size of 2 TB, if the unit is 2.5 TB then it will contain two volumes, with the first volume containing 2TB and the second volume containing 0.5 TB. If the unit is 5.0 TB then it will contain 3 volumes, with the first two volumes containing 2 TB each and the last volume containing 1 TB. (**Note:** If a specific Boot Volume was also specified in 3BM or CLI, the first volume will be the size specified for the Boot Volume, and then the carve size will be applied to the remainder of the unit. For more information, see “Boot volume size” on page 88.)

Each volume can be treated as an individual disk with its own file system. The default carve size is 2 TB; you can change this to a setting in the range of 1 TB to 2 TB (1024 GB to 2048 GB). 3ware firmware supports a maximum of 8 volumes per controller, up to a total of 16 TB.

If you are migrating a unit to a size that is larger than the carve size and auto-carving is on, multiple volumes will be created.

Note: Carving a unit into mutliple volumes can have an impact on performance.

The main use of auto-carving is to gain use of the full capacity in units greater than 2 TB. This is because Windows 2003 (32-bit and 64-bit without SP1) and Windows XP (32-bit), do not currently recognize unit capacity in excess of 2 TB. For more information see, http://www.3ware.com/kb/article.aspx?id=13431.

Note: Operating systems without this limitation include Linux 2.6, Windows XP (64bit), and Windows 2003 (32-bit and 64-bit with SP1 or newer).

Even though the Linux 2.6 kernel supports partitions larger than 2 TB, the installers for SuSE and Redhat do not. Turn auto-carving on to prevent the installation from failing.

You must turn on the Auto-Carving policy before creating the unit. Units created with this policy turned off will not be affected by a change to the policy. If the policy is turned off later, units that have been carved into volumes will retain their individual volumes; existing data is not affected.

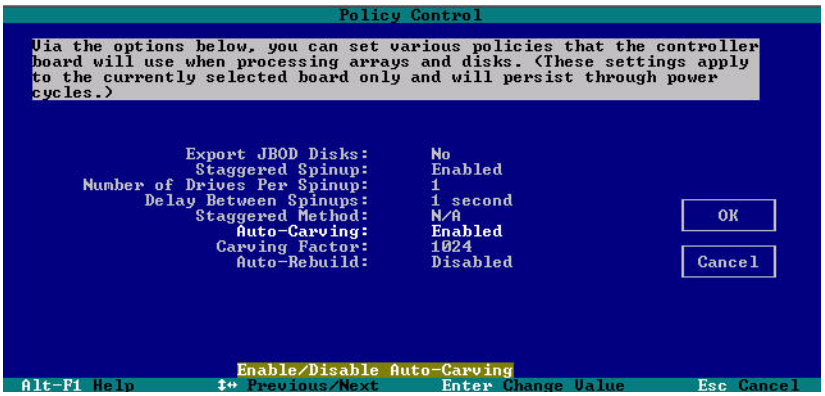
To use auto-carving

1 Enable the auto-carving feature. You can do so using 3DM or 3BM.

In 3DM, enable Auto-Carving at the bottom of the **Management > Controller Settings** page.

In 3BM, you enable Auto-Carving on the **Settings > Controller Policies** page.

Figure 37. Auto-Carve policy in 3BM



2 Create a new unit or migrate an existing unit to include the drives you want to use.

If the combined capacity of the drives exceeds the carve size, a number of volumes will be created.

3 Verify the creation of the volumes.

In 3DM 2, the number of volumes is shown on the Unit Details page.

4 Verify that the volumes appear in the operating system. They will appear as additional drives.

Notes:

- If you are configuring a unit for primary storage and it will be greater than 2 TB, be sure to enable the auto-carve policy before creating the unit.
- When volumes have been created through auto-carving, they cannot be deleted except by deleting the unit.
- If you create a bootable unit that has multiple volumes, the first volume can be used as the boot device.
- Changing the auto-carve policy does not affect existing units.

Setting the Size of Volumes Created with Auto-Carving

If you create units over 2 TB in size and use auto-carving to divide them into multiple volumes, you can control the size of the volumes to be created by setting the carve size (referred to as *carving factor* in 3BM) to use. The carve size can be between 1 TB (1024 GB) and 2 TB (2048 GB); the default is 2 TB.

When you change this policy, it applies to units you create in the future. Existing units will not be affected.

To set the carve size in 3DM

1 Choose **Management > Controller Settings** from the menu bar in 3DM.

2 In the Other Controller Settings section at the bottom of the screen, in the **Carve Size** field, enter the size you want (between 1024 GB and 2048 GB) to use and click **Submit**.

The page refreshes, and a message at the top confirms the change you have made.

To set the carve size (carving factor) in 3BM

1 On the main 3BM screen, **Tab** to **Settings** and press **Enter**.

2 On the pop-up menu, select **Controller Policies** and press **Enter**.

3 On the Policy Settings page, **Tab** to the **Carving Factor** field, press **Enter** to display the text entry box, enter the size you want (between 1024 GB and 2048 GB) and press **Enter** again to accept it.

4 **Tab** to **OK** and press **Enter** to select it.

The policy is enabled immediately.

Enabling and Setting Up Staggered Spin-up

You can set the number of SAS and SATA drives that will spin up at the same time and the delay time between drive group spinups. This does not apply to SAS or SATA drives that are attached to an expander.

Three policy settings let you set the number of drives that will spin up at the same time and set the delay between drive groups that spin up at one time. Not all SATA drives support staggered spinup. If you enable staggered spinup and have drives that do not support it, the setting will be ignored. You can change these settings in 3BM or using the CLI.

It is possible to enable or disable automatic detection of drives on the controller's ports for staggered spinup during hot swapping of drives. This feature is only available in the CLI using the **autodetect=on|off** command. For more information, see /cx set autodetect=on|off disk=<p:-p>|all *3ware SAS/SATA RAID Controller CLI Guide*.

Note: Some hard drives require that the power management jumper (PM2) be set to enable staggered spinup, in order for the SATA OOB option to be used. For more information, see the knowledgebase article 14889, at **http://www.3ware.com/KB/article.aspx?id=14889**

To enable or disable spinup and set the delay between spinups

1 At the main 3BM screen, **Tab** to **Policy** and press **Enter**.

2 On the Policy **Control** screen, **Tab** through these fields, making the choices you want to use:

- **Staggered Spinup:** Choose enabled or disabled.
- **Number of Drives Per Spinup:** Select the number of drives, depending on the number of ports on the controller.
- **Delay between spinup:** Select the number of seconds—from 1 to 6.

3 **Tab** to the **OK** button and press **Enter**.

You will notice a short delay as 3BM makes the policy changes.

Viewing Information About a Phy

The 3ware 9690SA RAID controller has 8 phy transceivers (phys) that receive and transmit the serial data stream between the controller and drives and other devices in the SAS domain.

Phys are associated with the SAS ports on the controller. Multiple phys can be associated with one SAS port, which is then called a "wide port." In the 9690SA, there are two wide ports and each wide port has 4 phys.

You can check the phy properties on the Controller Phy Summary page.

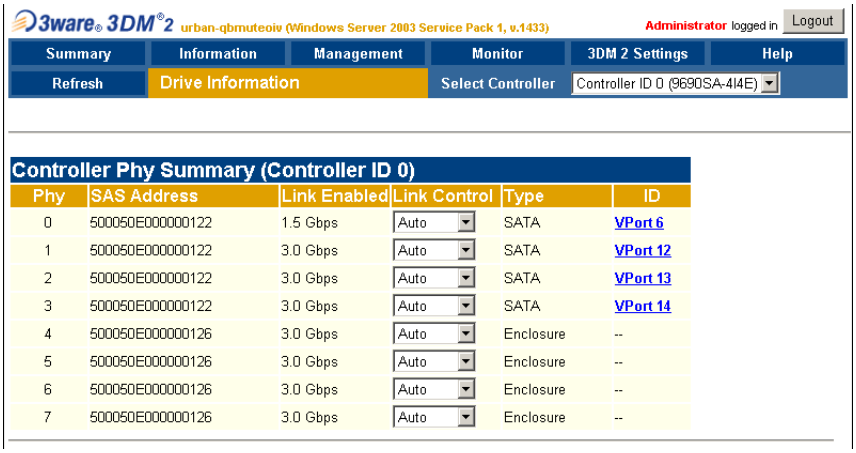
To see information for a phy in 3DM

1 Select the controller for which you wish to view phy information from the drop-down list on the menu bar.

2 If you have a direct-attached drive you can access the Controller Phy Summary page from the **Information > Drive Information** page by clicking the phy ID for the drive. Otherwise, navigate to the **Management > Controller Settings** page.

3 Under **Other Controller Settings** click the # link for **Number of Controller Phys**.

Figure 38. Phy Summary Page



For details about the columns on this page, see “Controller Phy Summary page” on page 197.

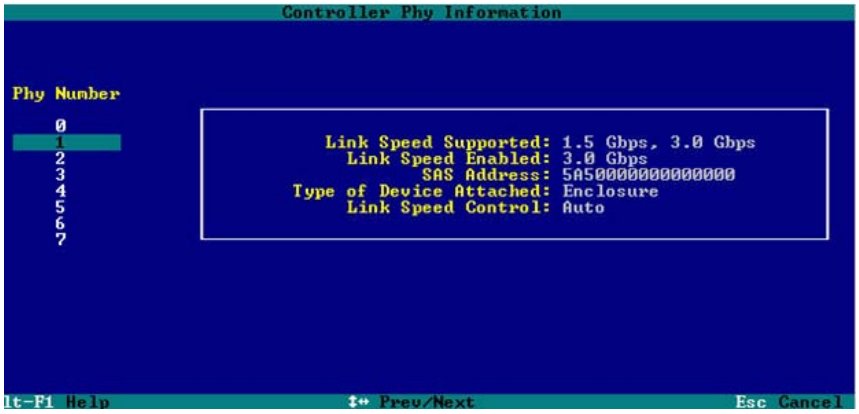
To see information for a phy in 3BM

1 On the main 3BM screen, **Tab** to **Information** and press **Enter**.

2 On the pop-up menu, select **Phys** and press **Enter**.

3 On the Controller Phy Information page, use the arrow keys to select the Phy you want to see details about. The information displays on the right.

Figure 39. Controller Phy Information page



Changing the Phy Link Speed

You can change the link speed between the controller and an expander or between the controller and a drive that is directly connected to the controller. Typically, the phy link speed is set to Auto. If desired for compatibility, troubleshooting or performance analysis, you can specify a specific link speed (1.5 or 3.0 Gbps).

To change the phy link speed in 3DM

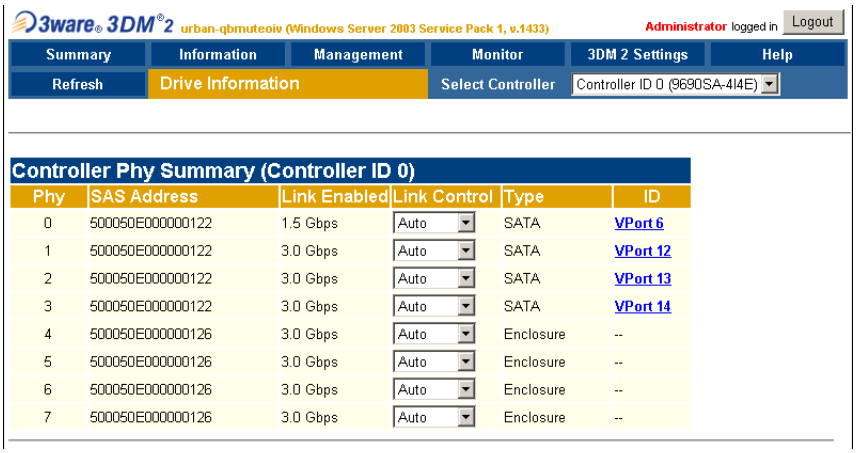
1 On the Controller Phy Summary page, identify the phy device for which you wish to change the link speed. Direct-attached drives are identified by their VPort ID.

2 In the **Link Control** drop-down menu, select the desired speed: 3 Gbps, 1.5 Gbps, or Auto.

The link speed is now reset.

For details about the information displayed on this screen, see “Controller Phy Summary page” on page 197.

Figure 40. Controller Phy Summary page



To change the phy link speed in 3BM

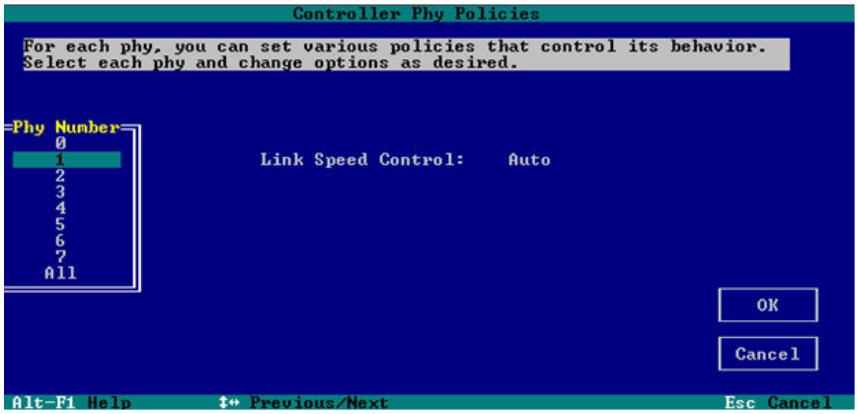
1 On the main 3BM screen, **Tab** to **Settings** and press **Enter**.

2 On the pop-up menu, select **Phy Policies** and press **Enter**.

3 On the Controller Phy Policies page, use the arrow keys to select the Phy for which you want to set the link speed.

4 Press **Enter** to display a popup of the possible settings, select the one you want, and press **Enter** again.

Figure 41. Controller Phy Policies page



8

Configuring Units

This section includes information and procedures on configuring units attached to your 3ware RAID controller. It is organized into the following topics:

- Configuring a New Unit
- Creating a Hot Spare
- Naming a Unit
- Setting Unit Policies
- Changing An Existing Configuration by Migrating (RAID Level Migration or Online Capacity Expansion)
- Deleting a Unit
- Removing a Unit
- Moving a Unit from One Controller to Another
- Adding a Drive
- Removing a Drive
- Rescanning the Controller

Configuring a New Unit

When you configure a new unit, you specify some details related to the type of RAID configuration that you want, and others that enable or disable features.

This section first provides an overview of the different settings you can specify during configuration and then provides step-by-step instructions for creating a unit through both 3DM and 3BM.

Configuration Options When Creating a Unit

This section provides an overview of the choices you have when configuring a new unit. For step-by-step instructions, see “Creating a Unit through 3DM” on page 89 and “Creating a Unit through 3BM” on page 91.

When you configure a new unit, you specify the following:

- Drives to be included in the unit
- Type of configuration (RAID Level)
- Name of the unit (optional)
- Stripe size, if appropriate for the RAID level
- Unit policies that affect how the unit will be handled
- Boot volume size (optional; can only be specified in 3BM or CLI)

You can make some types of changes to the RAID configuration later, and you can change the unit name and the unit policies. For details, see “Changing An Existing Configuration by Migrating” on page 109 and “Setting Unit Policies” on page 100.

Note: If you will install the operating system on and boot from a unit managed through the new 3ware RAID controller, see Chapter 3, “First-Time RAID Configuration Using 3BM.”

Drives to be included in the unit

You may include from one to thirty-two drives in the unit, depending on the number of drives available and the model of the controller you have. (For information about how many drives to select for a given RAID level, see “Determining What RAID Level to Use” on page 11.)

When creating units on the 9690SA controller, you cannot mix SAS and SATA drives in the same unit.

Available drives are those that are not currently part of a unit. If you want to use drives that are currently part of a different unit, you must first delete that unit to make the drives available. (For details, see “Deleting a Unit” on page 114.) If drives are listed under “Incomplete Drives and Others,” they must be deleted before they can be used.

If you want to add drives to be used in the unit, see “Adding a Drive” on page 122.

Type of configuration (RAID Level)

Available configuration types include RAID 0, RAID 1, RAID 5, RAID 6, RAID 10, RAID 50, and Single Disk. For information about the different RAID levels, see “Understanding RAID Concepts and Levels” on page 4.

Warning: Creating a unit erases all data on all drives.

Name of the unit (optional)

Units can be given names. These names will be visible in 3DM and 3BM.

Stripe size, if appropriate for the RAID level

In general, smaller stripe sizes are better for sequential I/O, such as video, and larger stripe sizes are better for random I/O (such as databases).

Striping size is not applicable for RAID 1, because it is a mirrored array without striping.

Using the default stripe size of 64KB usually gives you the best performance for mixed I/Os. If your application has some specific I/O pattern (purely sequential or purely random), you might want to experiment with a smaller or larger stripe size.

Unit policies

Several unit policies are set when you create a new unit:

- Write Cache (enabled, by default)
- Unit Queuing (enabled, by default)
- Auto Verify (disabled, by default)
- Continue on Source Error During Rebuild (disabled, by default)
- StorSave Profile (Protection, by default)

The particular policies that you can adjust when you create the unit vary, depending on which program you are using: 3DM, 3BM, or the CLI.

- In 3DM and the CLI, you can enable/disable all unit policies.
- In 3BM, you can specify all policies except Auto-Verify

You can change all of these policies after the unit has been created.

For a summary of what these policies do, see the discussion under “Setting Unit Policies” on page 100. For how to adjust each one, see the procedures later in this chapter.

Boot volume size

When you create a unit through 3BM (or through the CLI), you can create a special volume to function as the boot volume. You specify the size you want this volume to be. This is useful if you will be installing an operating system onto the unit, and want it to be installed in one volume and have a separate volume for data.

This is an optional feature. You do not have to create a boot volume if you plan to install the operating system on the unit.

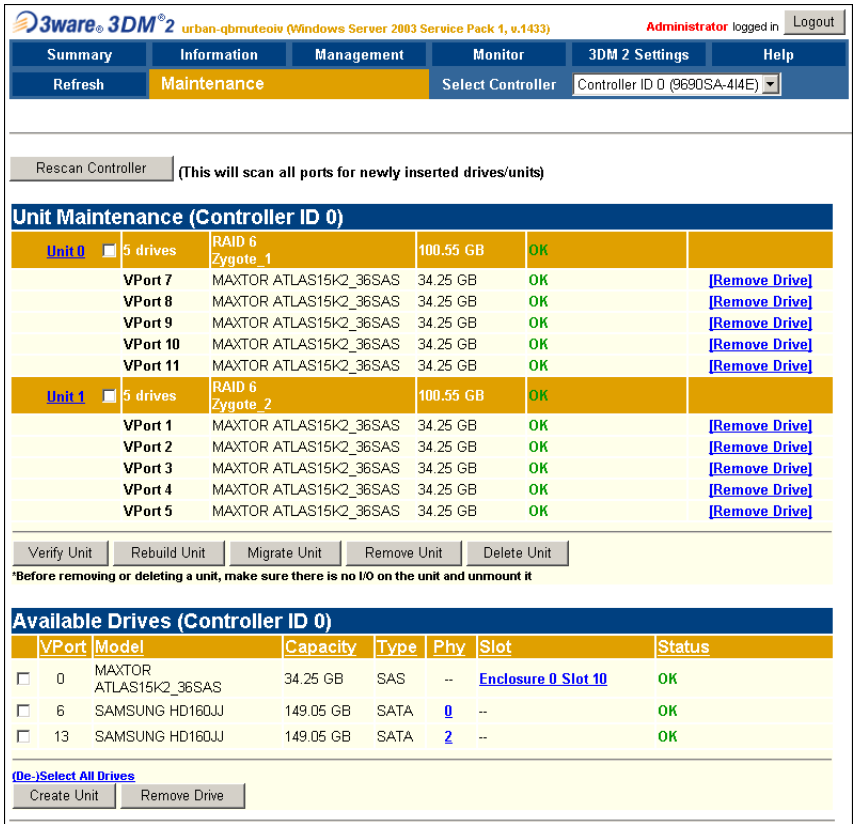
If you are creating a very large unit (2 TB or greater) and have enabled the Auto-Carving policy, the boot volume will be created in addition to any volumes created through auto-carving. For more information about auto-carving, see “Using Auto-Carving for Multi LUN Support” on page 78.

This feature can only be specified in 3BM and CLI.

Creating a Unit through 3DM

In 3DM, creating a unit starts from the **Management > Maintenance** page (Figure 42).

Figure 42. 3DM Maintenance Page



To create a unit

1 In 3DM, choose **Management > Maintenance.**

2 In the Available Drives list, select the drives you want to include in the unit by marking the checkbox in front of the VPort number for each one. (This will be a port number if you are using a controller other than the 9690SA)

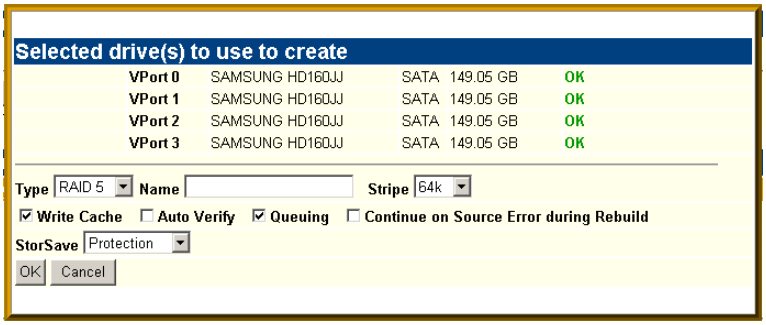
All drives in a unit must be of the same type—either SAS or SATA.

Although the best practice is to create a unit from drives in the same enclosure, you can create a unit with drives from different enclosures.

3 Click **Create Unit**.

A window similar to the one below shows the drives you selected, and lets you specify configuration settings.

Figure 43. Configuring a Unit in 3DM



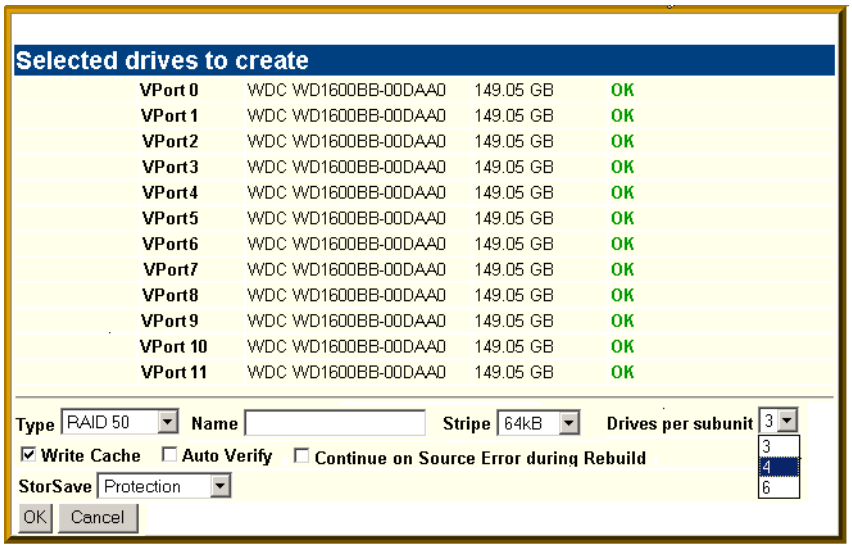
4 In the **Type** field, select the RAID configuration you want.

5 If stripe size applies to the RAID type you select, select a **Stripe Size**. (Stripe size does not apply to RAID 1.)

6 Optional: In the **Name** box, enter a name for the unit (up to 21 characters, including dashes and underscores).

7 If you have 12 drives attached to the controller and selected RAID 50 as the configuration in step 3, select whether you want 3, 4, or 6 Drives Per Subunit, as shown here.

Figure 44. Configuring a RAID 50 with 12 Drives



8 Make changes to the unit policies, as desired. You can enable or disable the **Write Cache**, **Auto Verify**, and **Continue on Source Error During Rebuild**. You can also set the **StorSave** policy.

For details about these settings, see “Setting Unit Policies” on page 100.

9 Click **OK**.

The new unit appears in the Unit Maintenance list at the top of the page and the operating system is notified of the new unit.

If you have auto-carving enabled and the size of your unit exceeds the carve size, you may see multiple unit volumes in your operating system. For details, see “Using Auto-Carving for Multi LUN Support” on page 78.

In Linux, a device node will now be associated with each unit created. In Windows, the device manager will reflect the changes under the disk drives icon.

10 Partition, format, and mount the unit. The required steps will vary depending on the operating system. For details, see “Partitioning, Formatting, and Mounting Units” on page 95.

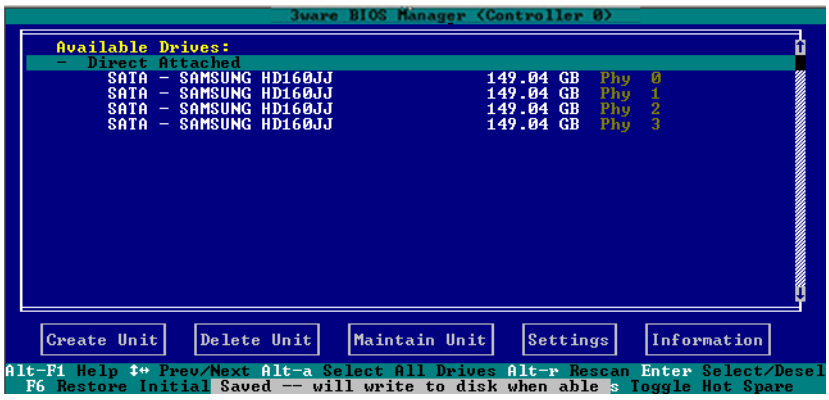
Note: For RAID 5 and RAID 6 units with 5 or more disks, and RAID 50 units with subunits of 5 drives or more, initialization (synchronization) of the unit begins immediately.

The unit can be used while it is initializing and is fault-tolerant.

Creating a Unit through 3BM

In 3BM, configuration tasks start from the main 3ware BIOS Manager screen shown in Figure 45.

Figure 45. 3BM Main Display



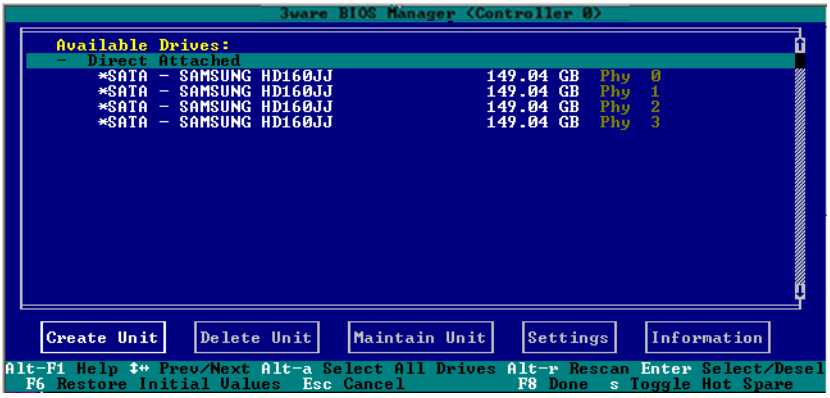
To create a unit through 3BM

1 At the main 3BM screen, select the drives to be included by highlighting each one and pressing **Enter** or **Space** to select it.

When you select a drive, an asterisk appears next to it in the left most column (see Figure 46).

Tip: If you want to use all available drives, press **Alt-A** to select them all.

Figure 46. Asterisks Next to Selected Drives

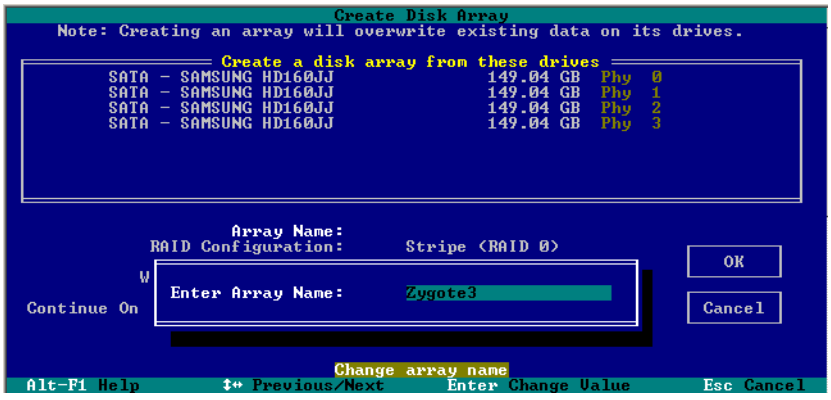


2 After all drives for the unit are selected, **Tab** to the **Create Unit** button and press **Enter**.

Tip: You can also press **Alt-C** to choose Create Unit.

3 On the **3ware Disk Array** screen, make sure that the proper drives are listed.

Figure 47. Create Disk Array Display



4 (Optional) Press **Enter** and type a name for the unit; then press **Enter** again to set the name.

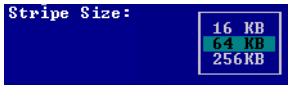
5 **Tab** to the **RAID Configuration** field and press **Enter** to display a list of available configurations for the number of drives you selected.

Figure 48. Configuration Choices for Four Drives

6 Use the **arrow keys** to select the configuration you want and press **Enter**.

7 **Tab** to the field **Stripe Size** and select the desired striping size (16, 64, or 256 KB).

Figure 49. Stripe Sizes for a RAID 5



8 (Optional) **Tab** through the policy fields and make any appropriate changes to the settings for:

- **Write Cache Setting**
- **Drive Queuing Mode**
- **Continue on Error During Rebuild**
- **StorSave Policy**

For details about these settings, see “Configuration Options When Creating a Unit” on page 86.

9 (Optional) **Tab** to the field **Boot Volume Size**, press **Enter** and type the size for the boot volume (volume 0) in gigabytes; then press **Enter** again to set the size.

10 **Tab** to the **OK** button and press **Enter** to confirm creation of the unit.

11 If the volume summary screen appears, review the information and press any key to continue.

Multiple volumes will be created if you entered a Boot Volume Size of greater than zero (0), or if auto-carving is enabled and the combined size of the drives in your unit is large enough to divide it into multiple volumes.

If you are not satisfied with how the volumes will be split up in the unit, delete the unit from the main 3BM screen and recreate it using a different Boot Volume Size. If desired, you can change the auto-carving policy or the carve size on the Policies page. For more information, see “Using Auto-Carving for Multi LUN Support” on page 78.

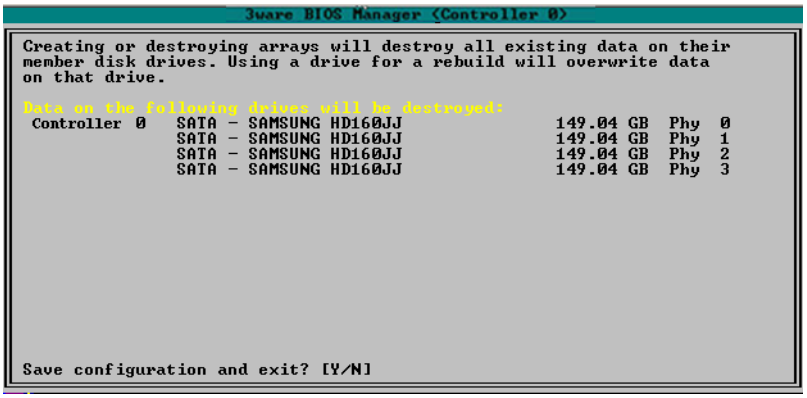
You are returned to the main 3BM screen.

Note: The unit is not actually created and no data is overwritten until you have finished making all your changes and press **F8**.

12 When you are finished making configuration changes, press **F8** to save the changes and exit 3BM.

A warning message tells you that all existing data on the drives will be deleted, and asks you to confirm that you want to proceed.

Figure 50. Confirmation Message when Saving and Exiting



If you made changes to units on more than one controller, the details about changes about to be made may extend beyond one screen. In this case, you use the **PgUp** and **PgDn** keys to bring more information into view.

13 Type Y to continue, delete any existing data on the drives, and create the unit.

14 Partition and format the units, as described under “Partitioning, Formatting, and Mounting Units” on page 95.

Note: For RAID 5 and RAID 6units with 5 or more disks, and RAID 50 units with a subunit of 5 or more disks, initialization of the unit begins immediately. You can postpone initialization if you want to begin using the units right away, however initialization from the BIOS is faster than it is under the operating system, so it will be a longer period of time until the unit has optimal performance. For more information, see “About Initialization” on page 137.

Ordering Units in 3BM

If you configure multiple units in 3BM and you want to install the OS on one of them so that you can boot from that unit, that unit must be the first unit.

You can change the order of the units in 3BM.

To change the order of units in 3BM

1 At the main 3BM screen, in the list of exportable units, highlight the unit you want to move.

2 Press the **Page Up** key to move the unit up the list; press the **Page Down** key to move the unit down the list.

Position the unit you want to be bootable at the top of the list of exportable units.

3 When you are finished working in 3BM, press **F8** to save your changes and exit.

Partitioning, Formatting, and Mounting Units

After you create a unit, whether through 3BM or 3DM, it needs to be formatted, partitioned, and mounted by the operating system before it can be used.

The steps vary, depending on whether your operating system is Windows, or Linux.

To partition, format, and mount under Windows

1 Boot the system and log in as a system administrator.

2 Partition and format the new arrays or disks using the **Administrative Tools** from the **Start** menu:

a Choose **Computer Management** from the **Administrative Tools** menu.

b Select **Storage.**

c Select **Disk Management**.

4 Follow the steps that appear on-screen to write a signature to the drive.

5 Right-click on the drive and select **Create Volume**.

Note: If you plan on migrating your unit to a larger array or another RAID type in the future remember to select the dynamic disk option. Only dynamic disks can be resized into larger partitions. Older Windows systems cannot convert basic disks into dynamic disks after the file system has been created.

6 Follow the steps that appear on-screen to create a volume and to assign a drive letter.

The volume is automatically mounted after formatting completes.

To partition, format, and mount under Linux

1 Boot the system and log in as root.

2 Open a terminal window.

3 Partition the unit:

Depending on the version of Linux you are using, some of the following parted command outputs will be slightly different.

```
fdisk /dev/sda
```

If the unit is over 2 TB, use:

```
parted /dev/sda

(parted) mklabel
New disk label type? gpt
(parted) p

Disk geometry for /dev/sda: 0kB - 1074GB
Disk label type: gpt
Number Start End Size File system Name Flags
parted /dev/sda

(parted) mkpart

Partition type? [primary]?
File system type? [ext2]?
Start? 0
End? 1074gb

(parted) p
Disk geometry for /dev/sda: 0kB - 1074GB
Disk label type: gpt
Number Start End Size File system Name Flags1 17kB 1074MB
1074MB
```

4 Create or make the file system:

```
mkfs /dev/sda1
```

Use of the -j option to turn on journaling is recommended for large partitions.

For example:
```
mkfs -j /dev/sda1
```

If the partition is over 2TB, use `parted` to also make the file system:
```
parted /dev/sda1

(parted) mkfs
Partition number? 1
File system? [ext2]?
writing per-group metadata (begins)...0% to 100% is
displayed)

(parted) quit (when completed)
```

5 Mount the volume:
```
mount /dev/sda1 /mnt
```

Creating a Hot Spare

You can designate an available drive as a hot spare**.** If a redundant unit degrades and a hot spare the size of the degraded disk (or larger) is available, the hot spare will automatically replace the failed drive in the unit without user intervention.

Note: When a hot spare replaces a failed drive, an event notification is generated and appears in the list of alarms in 3DM. You can also have 3DM send you an email about this. See “Managing E-mail Event Notification” on page 69.

It is a good idea to create a hot spare after you create a redundant unit.

In order to replace a failed drive, a hot spare must have the same or larger storage capacity than the drive it is replacing, and must be of the same type (SAS or SATA).

The Auto Rebuild policy allows automatic rebuilding to occur with available drives that are not designated as spares. For more information, see “Setting the Auto Rebuild Policy” on page 77.

Note: 3ware's 9000 series RAID controllers use drive coercion so that drives from differing manufacturers and with slightly different capacities are more likely to be able to be used as spares for each other. Drive coercion slightly decreases the usable capacity of a drive that is used in redundant units.

The capacity used for each drive is rounded down to the nearest GB for drives under 45 GB (45,000,000,000 bytes), and rounded down to the nearest 5 GBytes for drives over 45 GB. For example, a 44.3 GB drive will be rounded down to 44 GBytes, and a 123 GB drive will be rounded down to 120 GBytes.

If you have 120 GB drives from different manufacturers, chances are that the capacity varies slightly. For example, one drive might be 122 GB, and the other 123 GB, even though both are sold and marketed as "120 GB drives." 3ware drive coercion uses the same capacity for both of these drives so that one could replace the other.

Specifying a Hot Spare through 3DM

If you need to add a drive to be used as the hot spare, follow the instructions under "Adding a Drive" on page 122.

To specify a hot spare after the system is booted

1 In 3DM, choose **Management > Maintenance.**

2 In the Available Drives list, select the drive you want as a hot spare by marking the checkbox in front of it's Port number.

3 Click **Create Unit**.

4 In the dialog box that appears, select the configuration type **Spare**.

5 Click **Ok**.

You will see the spare appear at the top of the page, under **Unit Maintenance**.

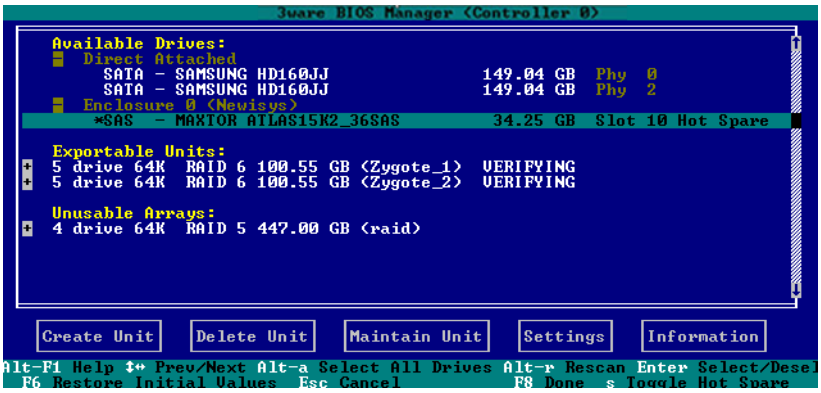
Specifying a Hot Spare through 3BM

1 On the main 3BM screen, in the list of **Available Drives**, highlight the drive you want to use**.**

2 Type **s** to specify that the selected drive will be the hot spare.

You'll see the words "Hot Spare" appear next to the drive in the Available Drives list.

Figure 51. Hot Spare Indicated



If a hot spare is already enabled, you can disable it by pressing **s** again.

3 If you are finished making changes in 3BM, press **F8** to save the changes and exit.

Note: If the drive you designated as a spare is not large enough to replace a failed drive in a fault-tolerant unit, or if there is not a fault-tolerant unit for the spare to support, 3BM will notify you.

Naming a Unit

Units can be given unique names to more easily identify them. A unit can be assigned a name when it is created. It can also be named or renamed at a later time.

To name or rename a unit through 3DM

1 Make sure the appropriate controller is selected in the drop-down list at the right of the menu bar.

2 Choose **Management > Controller Settings** from the menu bar in 3DM.

3 In the **Unit Names** section of the Controller Settings page, locate the unit for which you want to change the name.

4 In the text box, enter or type over the name shown. A name can be up to 21 characters, and can include dashes and underscores.

5 Click the **Save Names** button.

Note: If you want to cancel your change before saving it, click the **Reset Names** button.

To name or rename a unit through 3BM

1 At the main 3BM screen, select the unit by highlighting it and pressing **Enter**.

An asterisk appears in the left-most column to indicate that it is selected.

2 **Tab** to the **Maintain Unit** button and press **Enter**.

3 On the pop-up menu, select **Configure** and press **Enter**.

On the Configure Disk Array screen, the **Array Name** field is already selected.

4 Press **Enter** to open a text box.

5 Type a name for the unit and press **Enter**.

6 **Tab** to the **OK** button and press **Enter** to select it. You return to the main 3BM screen.

7 When you are finished making changes, press **F8** to save them and exit 3BM.

Setting Unit Policies

The following polices are set when you create a unit, and can be adjusted later through settings on the **Management > Controller Settings** pages of 3DM and 3BM. Details about adjusting each policy are described on the following pages.

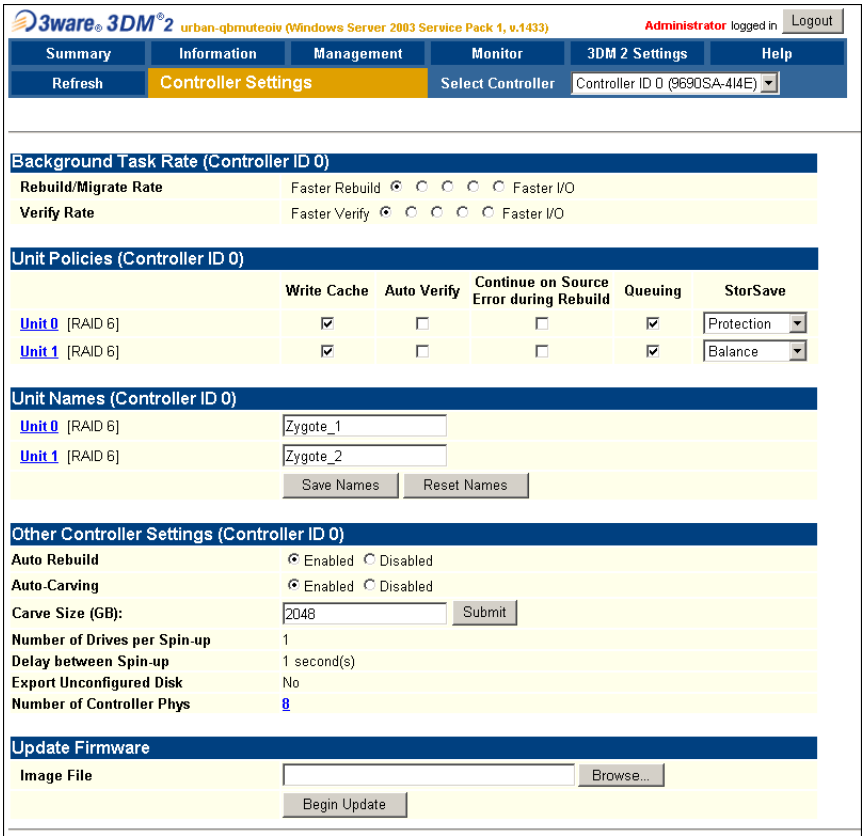
- **Unit Write Cache.** Determines whether write cache is enabled for the unit. When the write cache is enabled, data is stored locally on the controller before it is written to disk, allowing the computer to continue with its next task. This provides the most efficient access times for your computer system. When disabled, the computer will wait for the controller to write all the data to disk before going on to its next task. For details, see “Enabling and Disabling the Unit Write Cache” on page 102.

  This feature interacts with functionality of the BBU, if you have one, and with the unit’s StorSave profile. For details, see “Enabling and Disabling the Unit Write Cache” on page 102.

- **Auto Verify.** Determines whether Auto Verify is enabled for the unit. When enabled, the Auto Verify policy causes a verify task to be performed automatically once every 24 hours. This feature is designed to make it easier to insure regular verification of units. If verify schedules have been enabled, then Auto Verify will run only in the scheduled verify time slots. When Auto Verify is disabled, you must manually specify when you want to verify a unit, even if you have set a verify schedule. For details, see “Setting Auto Verify for a Unit” on page 103.

- **Continue on Source Error During Rebuild.** Determines whether ECC errors are ignored when they are encountered during a rebuild. (ECC errors are an indication of errors that have occurred on a particular drive since it was last read.) When not enabled, a rebuild will abort upon encountering an ECC error and the unit will be set to Degraded. For details, see “Setting Continue on Source Error During Rebuild” on page 104.
- **Queuing.** Determines whether command queuing is enabled for the unit. When enabled for drives that support it, this policy can improve performance. For details, see “Enabling and Disabling Queuing for a Unit” on page 105.
- **StorSave Profile.** Determines what StorSave profile is used for the unit. Three profiles are available: Protection, Balanced, and Performance. For details, see “Setting the StorSave Profile for a Unit” on page 106.

Figure 52. Unit Policies on Controller Settings Page in 3DM



Enabling and Disabling the Unit Write Cache

Write cache is used to store data locally in memory on the controller before it is written to the disk drive media, allowing the computer to continue with its next task. This improves performance. However, there may be instances when you want the computer to wait for the drive to write all the data to disk before going on to its next task. In this case, you must disable the write cache.

Note: If write cache is enabled, in the event of a power failure, the data in the controller cache will be lost if you do not have a Battery Backup Unit (BBU).To avoid a sudden power failure if you do not have a BBU, it is advisable to have an Uninterruptible Power Supply (UPS).

Write cache can be turned on or off for individual units in both 3DM, CLI, and 3BM without changing the configuration or losing data from the drives.

If you have a BBU (Battery Backup Unit) installed on the controller, the battery preserves the contents of the controller cache memory for a limited period of time (up to 72 hours) in the event of a system power loss. When a BBU is installed, if the battery is not “Ready,” write cache is disabled and cannot be enabled.

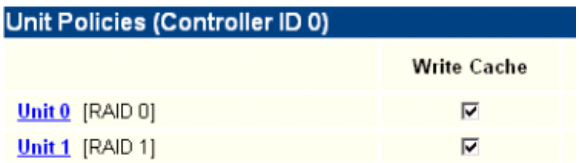
The unit's StorSave profile can also determine whether the write cache can be enabled or disabled. A warning message will be given if the change is not permitted due to the StorSave setting and the state of the unit.

Note: If the **Write Cache** checkbox is disabled (not selectable), check to see if the unit has degraded. If a unit has a StorSave policy of “Protect” and the unit degrades, the policy prevents write cache from being re-enabled until the unit has been rebuilt.

To enable or disable unit write cache through 3DM

1 Choose **Management > Controller Settings** from the menu bar in 3DM.

2 In the **Unit Policies** section of the Controller Settings page, check the Write Cache box to enable it for the designated unit.



The page refreshes, and a message at the top confirms the change you have made.

If your system has no BBU, a message will caution you about enabling write cache.

To enable or disable unit write cache through 3BM

1 At the main 3BM screen, select the unit by highlighting it and pressing **Enter**.

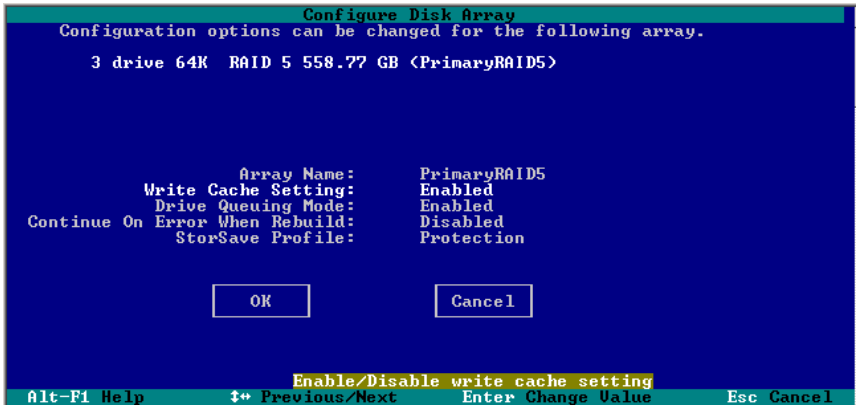
An asterisk appears in the left-most column to indicate that it is selected.

2 **Tab** to the **Maintain Unit** button and press **Enter.**

3 On the pop-up menu, select **Configure** and press **Enter**.

4 In the Configure Disk Array screen, **Tab** to the field **Write Cache Settings**.

Figure 53. Unit Write Cache State in 3BM



The current setting—Enabled or Disabled—is shown. (The initial default setting is for write cache to be enabled.)

5 Press **Enter** to display the choices, use the **arrow keys** to select the setting you want, and press **Enter** again to choose it.

6 Tab to the **OK** button and press **Enter** to select it.

You return to the main 3BM screen.

7 When you are finished making changes, press **F8** to save them and exit 3BM.

Setting Auto Verify for a Unit

The Auto Verify policy causes verify tasks to be performed automatically. This feature is designed to make verification of units easier.

If Auto Verify is set and there is no schedule set up for verify tasks, then the controller firmware can initiate a verify task once every 24 hours. If verify time windows are scheduled, then the controller will only start an automatic verify task during the scheduled time windows. (For information about schedules, see “Scheduling Background Tasks” on page 150.)

If Auto Verify is not set, you must manually specify when you want to run a verify, on the 3DM **Controller Settings** page. If a schedule is set for verify, then the verify that you manually start will only run during the scheduled time.

You can set the Auto Verify policy while creating a unit through 3DM or you can change the setting later using the following method.

To set the Auto Verify policy for an existing unit

1 Choose **Management > Controller Settings** from the menu bar in 3DM.

2 In the **Unit Policies** section of the Controller Settings page, check the **Auto Verify** box for the appropriate unit. (To disable this policy, uncheck the box.)

The page refreshes, and a message at the top confirms the change you have made.

Setting Continue on Source Error During Rebuild

The **Continue on Source Error During Rebuild** policy is available for units which are redundant. (For units which are not redundant, this option is not shown on the screen.) When this policy is set, ECC (Error Correcting Code) errors are ignored when they are encountered during a rebuild. (ECC errors are typically defects that have been detected in the drive since initialization.) When this policy is not set, if a unit is rebuilding, the rebuild will abort when it encounters an ECC error and the unit will be set back to Degraded.

Since enabling this policy could result in the loss of some source data in the event of source errors, the default is to not enable this policy. Select this option only if you want to ensure that a rebuild will complete successfully without manual intervention. If the rebuild fails and **Continue on Source Error During Rebuild** is not selected, then you have the option to start another rebuild manually. After completing a rebuild with this policy enabled, it is recommended that you execute a file system check when the rebuild completes. Under Windows, you can do this by right-clicking on the Drive and choosing Properties; then on the Tools tab, click Check Now. Under Linux use `fsck /dev/sda1`.

To set the Continue on Source Error During Rebuild policy in 3DM

1 Choose **Management > Controller Settings** from the menu bar in 3DM.

2 In the **Unit Policies** section of the Controller Settings page, check the boxes to select the policies you want to be in effect for each unit

The page refreshes, and a message at the top confirms the change you have made.

To set the Continue on Source Error During Rebuild policy in 3BM

1 At the main 3BM screen, select the unit by highlighting it and pressing **Enter**.

An asterisk appears in the left-most column to indicate that it is selected.

2 Tab to the **Maintain Unit** button and press **Enter**.

3 On the pop-up menu, select **Configure** and press **Enter**.

4 In the **Configure Disk Array** screen, **Tab** to the field **Continue on Source Error During Rebuild**.

5 Press **Enter** to display the choices, use the **arrow keys** to select the setting you want (Enabled or Disabled), and press **Enter** again to choose it.

6 **Tab** to the **OK** button and press **Enter** to select it.

You return to the main 3BM screen.

7 When you are finished making changes, press **F8** to save them and exit 3BM.

Enabling and Disabling Queuing for a Unit

Some drives support command queuing, a feature that can result in increased performance for applications that require a lot of random access of data (usually server-type applications). This is accomplished by causing command reordering to be done on the drive.

In order to make use of command queuing, the feature must be enabled at both the drive and the controller. You can enable support for command queuing on a per-unit basis, as described below.

You can see whether command queuing is supported and enabled for a particular drive in the Drive Details window. For details, see “Drive Details window” on page 195.

Note: Not all drives support command queuing. If a drive does not support command queuing, the policy setting for the controller is ignored. Queuing information for SAS is not available.

To enable or disable queuing for a unit through 3DM

1 Choose **Management > Controller Settings** from the menu bar in 3DM.

2 In the **Unit Policies** section of the Controller Settings page, enable queuing by checking the box under “Queuing” for the designated unit; disable it by unchecking the box.

The page refreshes, and a message at the top confirms the change that you have made.

To enable or disable queuing for a unit through 3BM

1 At the main 3BM screen, select the unit by highlighting it and pressing **Enter**.

An asterisk appears in the left-most column to indicate that it is selected.

2 Tab to the **Maintain Unit** button and press **Enter**.

3 On the pop-up menu, select **Configure** and press **Enter**.

4 In the **Configure Disk Array** screen, **Tab** to the field **Drive Queuing Mode**.

5 Press **Enter** to display the choices, use the **arrow keys** to select the setting you want (Enabled or Disabled), and press **Enter** again to choose it.

6 **Tab** to the **OK** button and press **Enter** to select it.

You return to the main 3BM screen.

7 When you are finished making changes, press **F8** to save them and exit 3BM.

Setting the StorSave Profile for a Unit

You can set the desired level of data protection versus performance for a unit by selecting the StorSave Profile. Three profiles are provided: *Protection* (maximum data protection), *Performance* (maximum performance, less data protection), and *Balanced* (a middle ground).The default is Protection.

About StorSave Profile Levels

The three profiles automatically adjust several different factors that affect protection and performance on a per unit basis. These are summarized in the table below and further explained after the table.

Table 8: StorSave Profile Definitions

	Protection (Default)	Balanced	Performance
Definition	Maximum data protection, but slower performance.	More data protection than *Performance* but less data protection than *Protection*.	Maximum performance for the unit, but less data protection.
FUA (Force Unit Access)	Honor FUA (If no BBU is present) Ignore FUA (If BBU is present)	Honor FUA (If no BBU is present) Ignore FUA (If BBU is present)	Ignore FUA
Write Journaling	Enabled	Disabled, if no BBU present. (Enabled, if BBU is present.)	Disabled (If BBU is present, this essentially disables the BBU for this unit.)
Disable Cache on Degrade	Enabled	Disabled	Disabled

- **FUA (Force Unit Access)**. The FUA bit is a way that the RAID controller or a program (such as a database program) can ensure that data is actually written to the disk drive media, and is not stored in cache. When a write command has the FUA bit set, then the disk drive will only issue “command complete” to the controller once the data is written to media. When performance is considered more important than protection, it may be desirable to ignore the FUA bit.

  The Protection and Balanced profiles honor FUA commands if no BBU is present; the Performance profile ignores them regardless of whether a BBU is present.

  If you use a battery backup unit (BBU), FUA is ignored, because the BBU preserves the contents of the controller cache memory for a limited period of time (up to 72 hours), in the event of a power failure.

- **Write Journaling**. Write journaling tracks the writing of data to disk and preserves a copy of data that has not yet been written to the disk media. Following a power failure or in the event of accidental drive removal and reinsertion, the firmware can recover the unit without data loss. All pending writes sitting in the controller cache are replayed after power is restored or the drive is reinserted and are flushed from the controller to the drive.

  Using write journaling helps protect your data, however it can have an impact on performance.

The Protection profile enables write journaling; the Performance and Balanced Profile disables it. The Balanced profile disables it only if no BBU is present.

If write journaling is disabled and a BBU is present, then it is as if the BBU was disabled for that unit.

- **Write cache disabled on degrade**. In the event that a unit degrades, the use of write cache can be disabled until the unit is rebuilt. Once the unit is rebuilt, you must enable the write cache manually. The write cache will not automatically reenable when the unit is rebuilt.

  The Protection profile enables this feature, so that write cache is disabled in the event a unit degrades; the Performance and Balanced profiles disable this feature, so that write cache continues to be enabled.

Setting the StorSave Profile through 3DM

In 3DM, the StorSave Profile is a unit policy that can be set on the **Controller Settings** page.

To set the StorSave profile through 3DM

1 Choose **Management > Controller Settings** from the menu bar in 3DM.

2 In the **Unit Policies** section of the Controller Settings page, select the profile you want to use from the drop-down list in the StorSave column.

  The page refreshes, and a message at the top confirms the change you have made.

Setting the StorSave Profile through 3BM

In 3BM, the StorSave Profile is set on the **Configure Disk Array** screen.

To set the StorSave Profile through 3BM

1 At the main 3BM screen, select the unit by highlighting it and pressing **Enter**.

  An asterisk appears in the left-most column to indicate that it is selected.

2 Tab to the **Maintain Unit** button and press **Enter**.

3 On the pop-up menu, select **Configure** and press **Enter**.

4 In the **Configure Disk Array** screen, **Tab** to the field StorSave Profile.

  The current setting—Protection, Balanced, or Performance—is shown. (The default setting is Protection.)

5 Press **Enter** to display the choices, use the **arrow keys** to select the setting you want, and press **Enter** again to choose it.

6 **Tab** to the **OK** button and press **Enter** to select it.

You return to the main 3BM screen.

7 When you are finished making changes, press **F8** to save them and exit 3BM.

Changing An Existing Configuration by Migrating

You can convert one RAID configuration into another while the unit is online. This process is known as RAID Level Migration (RLM).You can use RAID Level Migration to make two main types of configuration changes:

- RAID Level (for example, a RAID 1 to a RAID 5)
- Unit Capacity Expansion (for example, adding a 4th drive to a 3-drive RAID 5)

You can also use RLM to change the stripe size of a unit.

Note: A unit being migrated can still be used (I/O still continues), however the performance will be affected while the migrating task is active. You can control how much effect this has on performance by setting the background task rate. For more information, see “Setting Background Task Rate” on page 112.

This section includes the following topics about changing existing configurations:

- RAID Level Migration (RLM) Overview
- Changing RAID Level
- Expanding Unit Capacity
- Informing the Operating System of Changed Configuration

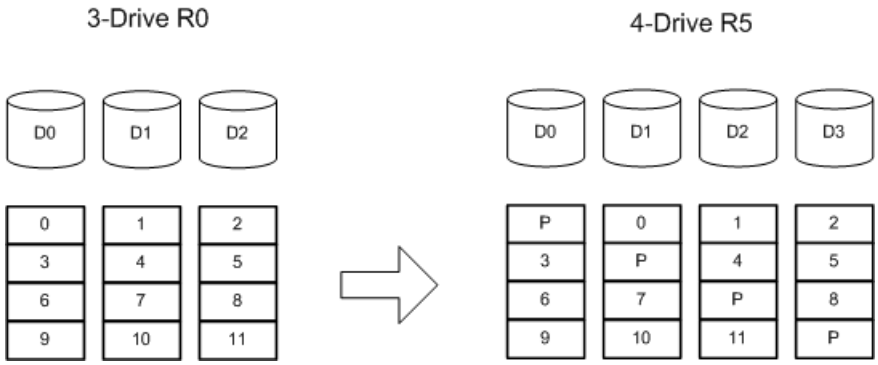
If you want to change the policy settings for an existing unit, there is no need to change the configuration. See “Setting Unit Policies” on page 100.

RAID Level Migration (RLM) Overview

RAID level migration is the process of converting one RAID configuration to another. When you migrate a unit to a different configuration, the user data on it is redistributed to the format of the new configuration. This data redistribution process is a background task, similar to the rebuild or verify processes.

Figure 54 shows an example of how data is reconfigured during a migration. In this example, the migration is from a 3-drive RAID 0 to a 4-drive RAID 5, with both having the same stripe size. As can be seen, every piece of user data is moved from its original physical location.

Figure 54. RAID Level Migration Example



Typically, a unit is reconfigured with the same or more storage capacity. Sometimes additional drives are added. The following table shows valid reconfigurations, some of which will require the addition of more drives.

Table 9: Valid Migration Paths

	Destination							
Source	**R0**	**R1**	**R5**	**R6**	**R10**	**R50**	**Single**	**Spare**
R0	Yes	No	Yes	Yes	Yes	Yes	No	No
R1	Yes	No	Yes	Yes	Yes	Yes	Yes	No
R5	Yes	No	Yes	Yes	Yes	Yes	No	No
R6	Yes	No	Yes	Yes	Yes	Yes	No	No
R10	Yes	No	Yes	Yes	Yes	Yes	No	No
R50	Yes	No	Yes	Yes	Yes	Yes	No	No

Table 9: Valid Migration Paths

	Destination							
Source	**R0**	**R1**	**R5**	**R6**	**R10**	**R50**	**Single**	**Spare**
Single	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Spare	No	No	No	No	No	No	No	No

Warning: If you are booted from a mirror (RAID 1 unit), never split it into 2 single (identical) drives. Once the unit is split, any pending writes cannot be written to the second drive. In addition, the file system on the drive will not be clean. Instead, shut down the system, replace one of the drives, and start the rebuild from 3BM.

Note: You can only migrate a unit to a RAID level that has the same or more capacity as the existing one. A four-drive RAID 5 unit can migrate to a four-drive RAID 0, but a three-drive RAID 0 unit cannot migrate to a three-drive RAID 5, without adding another drive, due to the need for additional storage capacity for parity bits.

Changing RAID Level

You can use migrate to change the RAID level of an existing unit while the unit is online, without experiencing any data loss. When you change a RAID level, you may also add one or more drives to the unit. You can also migrate to change the unit's stripe size. For example, a four-drive RAID 5 with a 64KB stripe size can be migrated to a four-drive RAID 5 with 256KB stripe size. The steps below describe how to change a RAID level in 3DM2.

Note: Once migration starts, the unit stays in the migrating state until the migration process is complete. The migration process cannot be aborted, and must be allowed to finish before a rebuild or verify to the unit is permitted.

Warning: It is important that you allow migration to complete before removing any drives that are involved in the migration. Removing drives from the unit during migration may cause the migration process to stop, and can jeopardize the safety of your data.

To change the RAID level of a unit

1 In 3DM 2, choose **Management > Maintenance**.

2 In the Unit Maintenance table on the Maintenance Page, select the unit for which you wish to change the RAID level, by checking the box next to the Unit ID.

The unit to be migrated must be in a normal state (not degraded, initializing, or rebuilding) before starting the migration.

3 Click the **Migrate Unit** button.

The Migrate dialog box appears.

4 Select any drives to be added to the unit.

5 Select the new RAID level.

6 Optionally, select a new Stripe size.

7 Click **OK**.

The Maintenance page updates to show the new unit and the Migration progress.

8 Inform the operating system of the change, as described below under “Informing the Operating System of Changed Configuration”.

Expanding Unit Capacity

You can expand a unit's capacity by adding one or more drives to it without changing the RAID level, except for singles and RAID 1 units. (Since a single can only have one drive, and a RAID 1 can only have two drives, if you add a drive to either, the RAID level must be changed.)

For example, for a RAID 5 with 3 drives, you can change the capacity by adding a forth drive.

Expanding unit capacity can be accomplished while the unit is online, without experiencing any data loss. This process is also referred to as Online Capacity Expansion (OCE).

To expand a unit’s capacity

1 In 3DM 2, choose **Management > Maintenance.**

2 In the Unit Maintenance table on the Maintenance Page, select the unit you wish to expand by checking the box next to the Unit ID.

3 Click the **Migrate Unit** button.

The Migrate dialog box appears, listing the drives which can be added to the unit.

4 Select the drives(s) you wish to add to the unit by checking the Port ID box next to each one.

5 If desired or necessary, select the appropriate RAID level.

6 Click **OK**.

The Maintenance page updates to show the newly reconfigured unit. The Status column title indicates that Migration is in progress.

7 If you booted from the unit that is being migrated, when migration is complete, reboot your system. Then turn to Step 4 under "Informing the Operating System of Changed Configuration" on page 113.

8 After the migration is complete, inform the operating system of the change, as described below.

You can check the status of the migration on the Maintenance page.

Informing the Operating System of Changed Configuration

After you change the configuration of a unit, you must inform the operating system of the change, and you may need to re-partition the unit.

In addition, in order to use the new capacity, you need to either resize the existing partition or add a new partition.

To inform the operating system that a unit has been changed

1 If the unit you reconfigured is the boot unit, restart the system and skip to Step 3.

If the unit you reconfigured is secondary storage, unmount the file system from the unit.

Under Windows, go to **Start > Administrative Tools > Computer Management**, and select **Disk Management.** Remove the logical drive letter for the unit.

Under Linux from a command prompt, type `sync` <enter>, `sync` <enter>, `sync` <enter>.

You can then unmount the unit with this command: `umount <mount location>`

2 In the software, remove and rescan the controller, in order to update unit information.

   a In 3DM2 choose **Management > Maintenance** and select the appropriate unit.

   a Click the **Remove Unit** button.

   b After the unit has been removed, click the **Rescan** button. The new unit capacity displays.

3 Resize the partition and file system or create a new partition.

   In Windows, use the disk management utility to determine whether the disk is a basic disk or a dynamic disk.

   - Go to Administrative Tools > Computer Management, and then select Disk Management in the list on the left.

     Only dynamic disks can be expanded with Windows Disk Management. If the unit is shown as a basic disk, right-click on the disk icon and change it to a dynamic disk.

     Older Windows systems cannot convert basic disks into dynamic disks after the file system has been created.

   - If the unit is shown as a dynamic disk, right-click on it and choose Extend Volume to launch the Extend Volume wizard.

   In Linux, the tools to expand the partition and file system can vary, depending on the kernel version and file system that you are using. Please consult your Linux documentation and the 3ware Knowledgebase for more information.

Deleting a Unit

You delete a unit—either an array of disks, or a Single Disk—when you want to reconfigure the unit or use the drives for other purposes.

After you delete a unit, the drives appear in the list of Available Drives.

Warning: When a unit is deleted, all of the data on that unit will be lost. The drives cannot be reassembled into the same unit because the data on it is erased. If you want to reassemble the drives into the same unit on another controller, use the **Remove Unit** button in 3DM instead of the **Delete Unit** button. Or, if you're at the BIOS level already, you can shut down the computer and physically move the drives to another 3ware 9000 series RAID controller. When you restart your system, the controller will recognize the unit. For more information see "Moving a Unit from One Controller to Another" on page 119.

If you have incomplete drives, or drives that appear with a message such as "Unsupported DCB," indicating that they were previously part of a unit on a

3ware 7000/8000 series controller, they must be deleted before you use them. (If you want to move a unit from a 7/8000 controller to a 9000 series controller, you must convert the drives first. For more information, see “Moving a Unit from One Controller to Another” on page 119.)

Deleting a Unit through 3DM

In 3DM, the command for deleting a unit is on the **Maintenance** page. Be sure to follow steps 1 through 3 in the instructions before using the Delete command.

To delete a unit through 3DM

1 Make sure the operating system is not accessing the unit you want to delete.

For example, make sure you are not copying files to the unit, and make sure that there are no applications with open files on that unit.

2 Backup any data you want to keep.

3 Unmount the unit.

This step is very important. If a unit is not unmounted and you delete it, it is the equivalent of physically yanking a hard drive out from under the operating system. You could lose data, the system could hang, or the controller could reset.

Under Windows, go to **Start > Administrative Tools > Computer Management**, and select **Disk Management.** Remove the logical drive letter for the unit.

Under Linux, you can unmount the unit with this command:
`umount <mount location>`

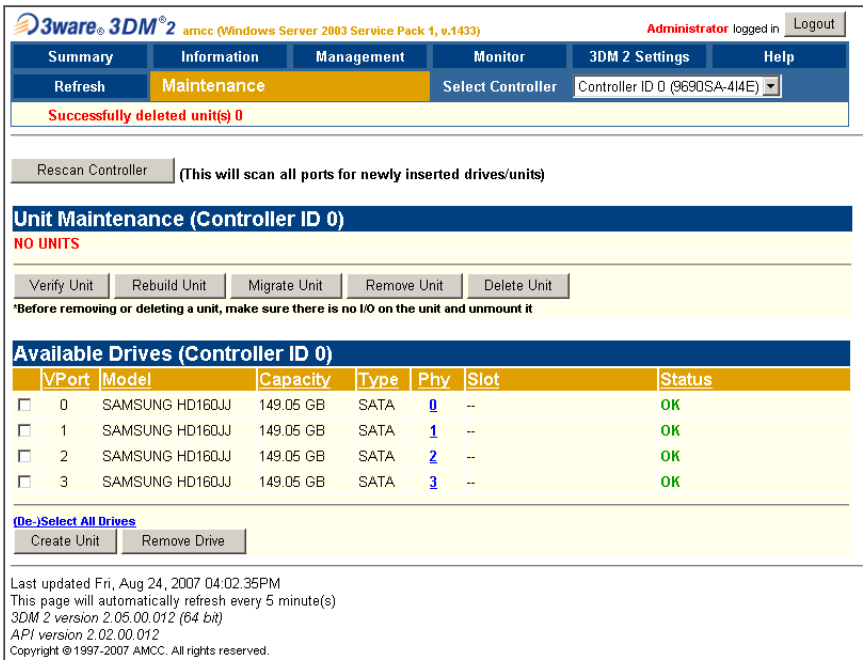
4 In 3DM, choose **Management > Maintenance**.

5 In the Unit Maintenance section of the Maintenance page, select the unit you want to remove and click **Delete Unit**.

6 When a message asks you to confirm, click **OK.**

Configuration information associating the drives with the unit is deleted, and the individual drives appear in the Available Drives list (Figure 55). You can now use them as part of another unit, or designate them as Spares, for use in a rebuild.

Figure 55. Unit Successfully Deleted through 3DM



Deleting a Unit through 3BM

In 3BM, the command for deleting a unit is on the main 3BM screen.

To delete a unit through 3BM

1 At the main 3BM screen, select the unit in the list of Exportable Units by highlighting it and pressing **Enter** or **Space**.

An asterisk appears in the left-most column to indicate that it is selected.

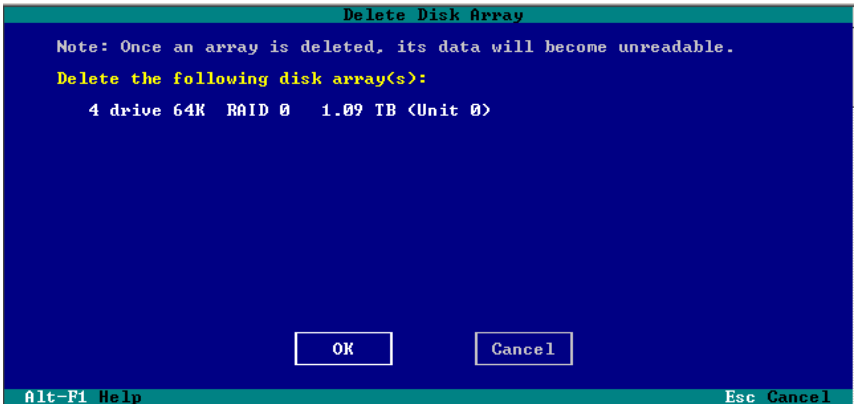
2 **Tab** to the **Delete Unit** button and press **Enter.**

Note: If you want to delete an incomplete drive or unusable unit, or a drive that appears with a message such as “Unsupported DCB,” select it in a similar manner and then select **Delete Unit**, even though it appears in the list **Incomplete Drives and Others**.

Warning: Any data on the unit will be lost once the unit is deleted. Backup any data that you want to keep.

3 On the **Delete Disk Array** screen, review the information about the unit to make sure it is the one you want to delete.

Figure 56. Deleting a Unit in 3BM



4 **Tab** to the **OK** button and press **Enter.**

You return to the main 3BM screen, and the drives associated with the unit now appear in the list of Available Drives.

Remember: The unit is not actually deleted and no data is overwritten until you press the **F8** key to save your changes, or press **Esc** and select **Yes** when asked if you want to save.

5 **Press F8** to save your changes, or press **Esc** and then **Yes**.

Removing a Unit

Removing a unit through software (also known as 'array roaming') keeps the data intact on the unit. It allows you to move the unit to another controller or to store the drives for safekeeping purposes.

Removing a unit is different than deleting a unit. Deleting a unit will destroy the data on the unit.

Warning: It is important to remove the unit through software, before removing it physically. Failure to do so could result in a system crash or hang and may even corrupt the data and the unit configuration from being reassembled later.

Power-down your system before physically removing any drive that is not in a hot swap bay.

Note: You can also remove a drive, if you want to force a degrade on a redundant unit, or if you want to remove a drive from the “Available Drives” list so that you can then remove it from the system. For more information, see “Removing a Drive” on page 123.

Removing a Unit Through 3DM

In 3DM, the command for deleting a unit is on the **Maintenance** page. Be sure to follow steps 1 and 2 in the instructions before using the Remove command.

To remove a unit through 3DM

Note: If your drives are not in hot swap bays, you do not need to remove a unit via 3DM. Simply power down the system and remove the applicable drives. Refer to your system's user guide for details on removing fixed disks. If your drives are in hot swap bays, follow the steps below.

1 Make sure the operating system is not accessing the unit you want to remove.

For example, make sure you are not copying files to the unit, and make sure that there are no applications with open files on that unit.

2 Unmount the unit.

This step is very important. If a unit is not unmounted and you remove it, it is the equivalent of physically yanking a hard drive out from under the operating system. You could lose data, the system could hang, or the controller could reset.

Under Windows, go to **Start > Administrative Tools > Computer Management**, and select **Disk Management.** Remove the logical drive letter for the unit.

Under Linux, you can unmount the unit with this command:
`umount <mount location>`

3 In 3DM, choose **Management > Maintenance**.

4 In the **Unit Maintenance** table on the Maintenance page, select the unit you want to remove and click **Remove Unit**.

5 When a message asks you to confirm, click **OK.**

The unit number and information is removed from the **Maintenance** page in 3DM.

The operating system is notified that the unit was removed. In Linux the device node associated with this unit is removed. In Windows the Device Manager will reflect the changes under the disk drives icon.

You can now physically remove the drives and move them to another controller. If the drive is in a hot swap bay, you can do this without shutting down the system. If the drive is not in a hot swap bay, power-

down the system and ground yourself before making changes to the hardware.

If you change your mind before physically removing the drives and want to reuse the drives and unit on the current controller, just click **Rescan Controller.**

Removing a Unit Through 3BM

Note: Even though removing a unit is supported in 3BM, you can also simply power down to remove the applicable drives since you are not booted yet.

To remove a unit through 3BM

1 If your drives are not in hot swap bays, you do not need to remove a unit via 3BM. Simply power down and remove the applicable drives. Refer to your system's user guide for details on removing fixed disks.

Warning: Physically removing drives which are not in hot swap bays can result in a system hang or may even damage the system and the drive.

2 At the main 3BM screen, highlight the unit you want to remove and press **Enter** to select it.

An asterisk appears in the left-most column to indicate that the unit is selected.

3 Tab to the **Maintain Unit** button and press **Enter**.

4 In the pop-up menu, select **Remove** and press **Enter**.

You can now physically remove the drives and move them to another controller. If your drives are in hot swap bays, you can do this without shutting down the system.

Moving a Unit from One Controller to Another

After you have configured a unit on a 3ware 9000 series controller, you can move it to a different 3ware 9000 series controller, and retain the configuration on the new controller. This is referred to as “array roaming.”

When connecting the unit to the new controller, you do not have to physically connect the drives to the same physical slots to which they were connected on

the previous controller. The firmware will still recognize the unit. This feature is referred to as “disk roaming.”

3DM includes two features that help you move a unit without powering down the system, allowing you to hot swap the unit. The Remove Unit feature lets you prepare a unit to be disconnected from the controller, and the Rescan feature checks the controller for drives that are now connected, and updates the 3DM screens with current information. For details, see “Removing a Unit” on page 117 and “Rescanning the Controller” on page 124.

Note: Moving a unit to another controller while the unit is in the migration state is supported with one restriction. If the unit was in the middle of the migration process and the controller was shutdown uncleanly, the unit cannot be moved to another controller until the unit has recovered from the unclean shutdown. This may require initializing, verifying, or rebuilding the unit.

Caution: If you have a configured RAID unit on an older controller, such as an 8506, and you move the drives to a new controller, such as a 9690SA, you must first convert the units from 7xxx/8xxx format to 9xxx format using a 3ware utility available from 3ware Technical Support.

You cannot move drives back from a 9690SA controller to an older controller and maintain the data. If you want to swap drives back and forth between controller cards, be sure to have a backup of your data.

Moving Units from an Earlier 9000 Series to a 9690SA Controller

If you are moving units from a 9500S controller to a 9690SA controller, the process is a little different. The steps you follow depend on whether you are booting from the drives attached to the 9500S, or whether they are being used for secondary storage.

To move a bootable unit from an earlier 9000 series controller to a 9690SA controller

1 If you are working with a Linux system, skip to step 2.

  If you are working with a Windows system:

  a Power down the computer.

  b Install the 9690SA controller in the computer, leaving the original controller installed and its drives attached.

  c Boot to the operating system.

2 Update the driver for the 9690SA RAID controller.

   If you are using Linux, you will also need to update the initial RAM disk with the `mkinitrd` command.

3 Power down the computer.

4 Remove the original controller.

5 If you are working with a Linux system, install the 9690SA controller.

6 Attach the drives that were on the original controller to the 9690SA controller.

7 Power up the computer and verify that the upgrade is complete. (The existing units should be available for use.)

8 Remove old 3DM and CLI files and install new versions.

To move a secondary storage unit from an earlier 9000 series controller to a 9690SA controller

1 Power down the computer.

2 Remove the 9500S, 9550SX, 9550SXU or 9650SE controller.

3 Install the 9690SA controller in the computer.

4 Attach the drives that were on the original controller to the 9690SA.

5 Boot to the operating system.

6 Update the driver for the 9690SA.

   If you are using Linux, you may also need to update the initial RAM disk with the `mkinitrd` command.

7 Reboot if you are prompted to do so by the operating system.

   Some operating systems (for example, Windows 2003) will allow the unit(s) attached to the controller to be used at this point without an additional reboot.

8 Remove old 3DM and CLI files and install new versions.

Adding a Drive

If you have a hot swap bay or an enclosure with removable trays, you can add a drive to your system and make it available through 3DM without powering down the system.

Without hot swap bays, you should not add a drive via 3DM. Instead, power down the system and add the applicable drives.

Warning: Physically adding a drive without using a hot swap bay and without powering down your system can result in a system hang or may even damage the system and the drive.

Note: When you add a drive to your system and connect it to the controller, it is automatically detected and listed in 3DM. If it does not immediately display, or if it is part of a unit, you can use the rescan feature, as described below.

To add a drive

1 Insert the drive into the hot swap bay or into your enclosure.

2 In 3DM, choose **Management > Maintenance**.

3 On the Maintenance page, click **Rescan Controller.**

The drive will appear in the list of available drives. You can now use it in a new RAID configuration, as part of an existing configuration, or as a replacement drive in the event that another drive degrades.

If you want to use this drive as a spare, see “Creating a Hot Spare” on page 97.

Removing a Drive

If you have hot swappable drives in a carrier or an enclosure and you want to physically remove a drive from your system without powering it down, you should first remove it through the 3ware software.

Follow this procedure if you know that a drive is developing a problem and you want to replace it, or to replace a drive which has already failed.

Warnings:

Physically removing a drive that is not in a hot swap bay or that is part of a non-redundant unit, can result in a system hang or may even damage the system and the drive.

The steps below will destroy any information that identifies this drive as part of a RAID unit. **Existing data on this drive will no longer be available.**

Notes:

If you want to remove a unit from your system and reassemble it in another system, do not follow these steps. Instead, turn to “Removing a Unit” on page 117.

If you physically remove a drive on a controller without first removing it in 3DM, it will be listed as removed, however it will not be completely removed unless you Rescan the controller.

Drives that are part of a non-redundant or degraded unit cannot be removed.

To remove a drive

1 In 3DM, choose **Management > Maintenance**.

On the Maintenance page, **Remove Drive** links appear next to all drives that can be removed from units, and next to drives in the Available Drives list.

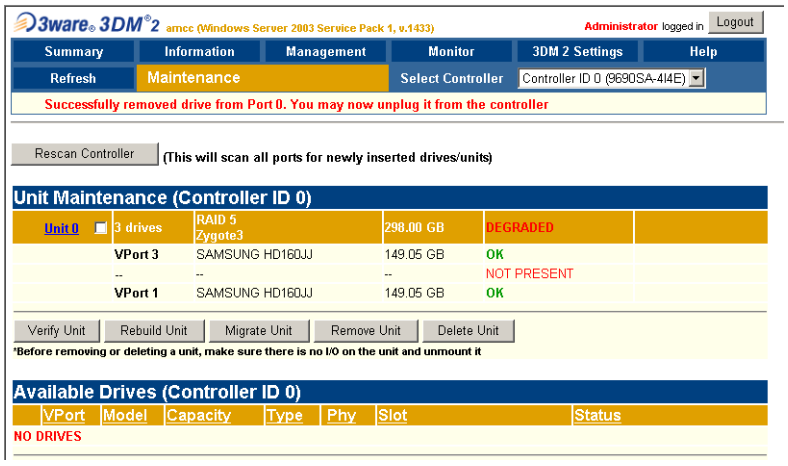
2 Locate the drive you want to remove and click the **Remove Drive** link (Figure).

3 When 3DM asks you to confirm that you want to remove the drive, click **OK**.

You can now remove the drive from your system.

If you removed a drive that was part of a unit, the unit will become degraded, as shown in (Figure 57).

Figure 57. Result of Removing Drive from Unit in 3DM



Rescanning the Controller

When you make a change by physically adding or removing drives or units, you can have 3DM rescan the controller to update the list of units and available drives shown on the **Maintenance** page.

This is useful in a variety of circumstances. For example, if you add new drives to the controller, you can make them available by rescanning the controller. Or if you turn on an enclosure after turning on your computer, you can use rescan to make the controller see the drives.

Rescanning checks all ports on the controller. It then updates the status of all attached disks, so if error conditions have been fixed, the status is updated to reflect that. For more details about how the Rescan feature works, see the information in the 3DM Reference section, under “Maintenance page” on page 204.

To rescan the controller through 3DM

1 In 3DM, choose **Management > Maintenance**.

2 On the Maintenance page, click **Rescan Controller.**

3DM scans the controller for information about units and drives, and updates the information shown on the **Maintenance** page.

To rescan the controller through 3BM

1 From the main 3BM screen, press Alt-r.

You are warned that any configuration changes you have made in 3BM will be lost.

2 Type Y for Yes to rescan the controller.

9

Maintaining Units

3ware RAID controllers include a number of features in the firmware that help maintain the integrity of your drives, check for errors, repair bad sectors, and rebuild units when drives degrade. In addition, 3ware BIOS Manager (3BM) and 3ware Disk Manager (3DM) provide tools to let you check unit and drive status, and manually start background maintenance tasks. 3DM also lets you review alarms and errors and schedule background maintenance tasks. On Windows systems, the WinAVAlarm utility monitors the controller and will display a message window and give an audible alarm when events occur at or above the threshold you select for it.

Details about these features are described in this section, which is organized into the following topics:

- Checking Unit and Drive Status through 3DM
  - Viewing a List of Drives
  - Enclosure Drive LED Status Indicators
  - Unit Statuses
  - Drive Statuses
- About Degraded Units
- About Inoperable Units
- Locating a Drive by Blinking Its LED
- Alarms, Errors, and Other Events
- Background Tasks
- Scheduling Background Tasks

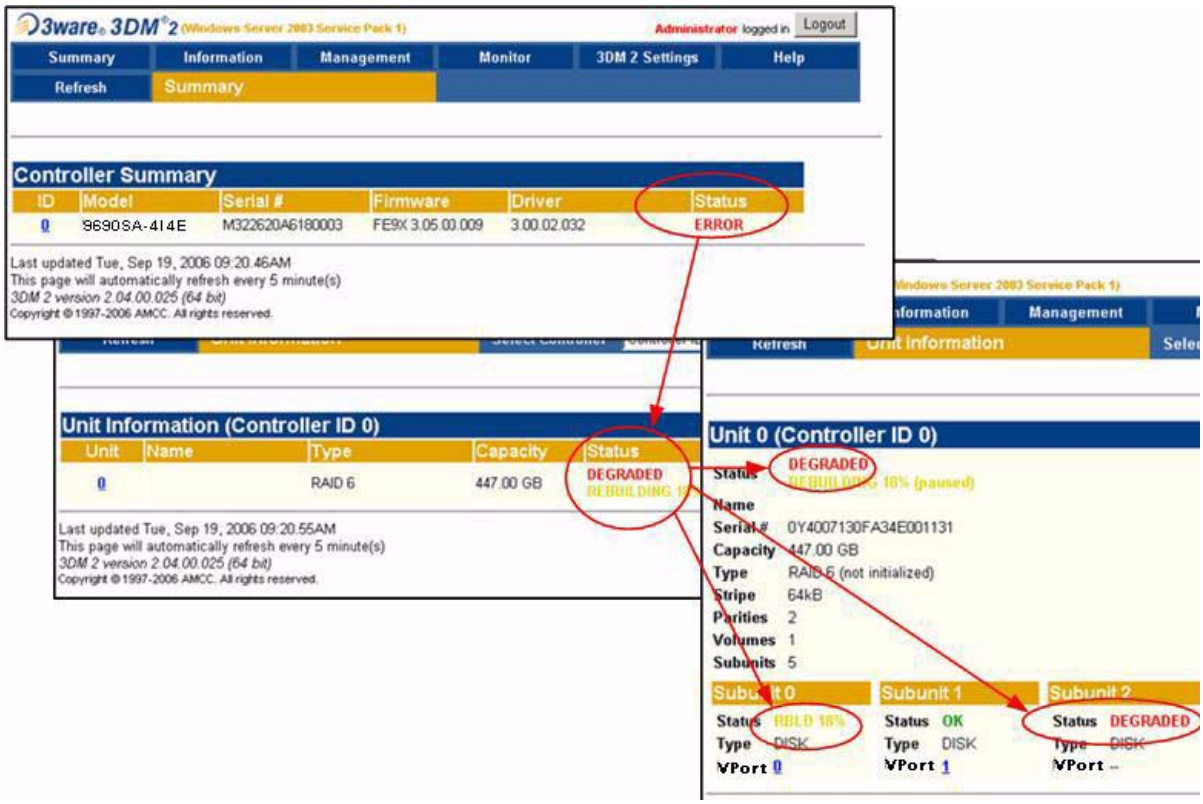
Checking Unit and Drive Status through 3DM

The information screens in 3DM let you see both summary and detailed information about your 3ware RAID controller, configured units, and available drives. You can quickly see the status of your controller and drives, and drill down to find details about any units or drives that have problems.

A status column on the controller, unit, and drive information pages lets you quickly see whether everything is working (OK), performing a task (such as initializing, verifying, or rebuilding), or has a problem (error, degraded, warning).

The next figure illustrates how you can drill down to get additional detail about units and drives in your system.

Figure 58. Drilling Down to Check Status Information



For some RAID levels (RAID 6, RAID 10, and RAID 50), a single RAID unit may have more than one status. For example, part of the unit could be rebuilding, while another part is degraded or initializing. When this is the case, you will see both statuses listed at the top unit level. When you drill in to see details, you will be able to see which the specific subunits or drives to which the status applies.

For an explanation of unit and drive status, see:

- “Unit Statuses” on page 129
- “Drive Statuses” on page 130

If you use a supported enclosure with enclosure services, the LEDs on your enclosure may also provide some status information. For details, see “Enclosure Drive LED Status Indicators” on page 128.

Viewing a List of Drives

You can see a list of drives connected to your 3ware RAID controller, and see additional detail about each of those drives.

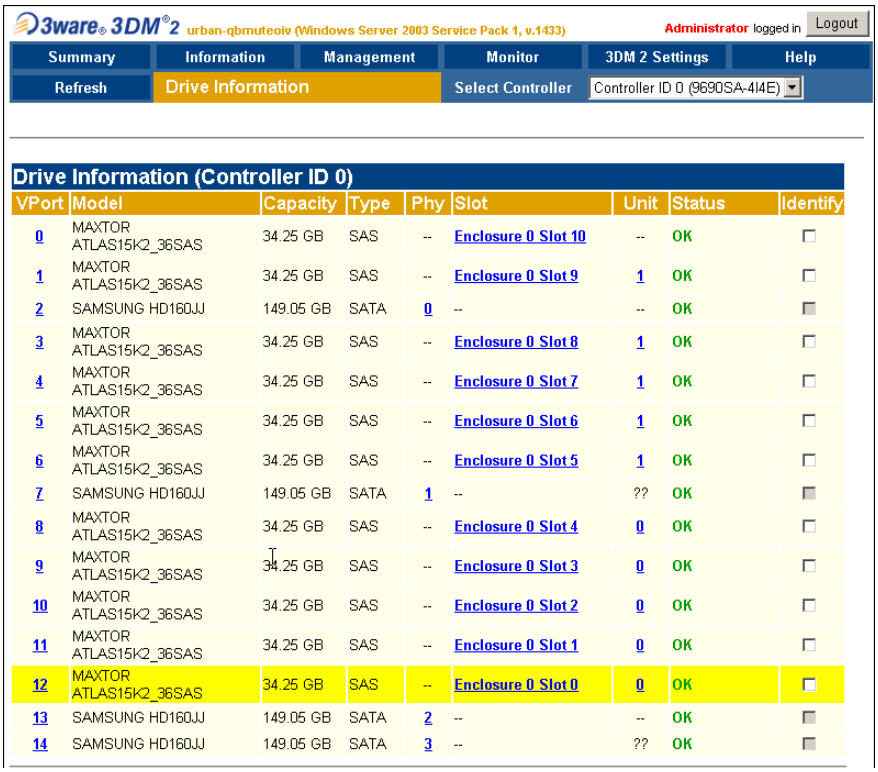
To view a list of drives in 3DM

- Choose **Information > Drive Information** from the main menu in 3DM.

  On the Drive Information page, you can access details about any of the drives listed by clicking the link for that drive in the **VPort** column.

  For more information about the Drive Information page, see page 193.

Figure 59. Drive Information Page



To view a list of drives in 3BM

1 On the main 3BM screen, **Tab** to **Information** and press **Enter**.

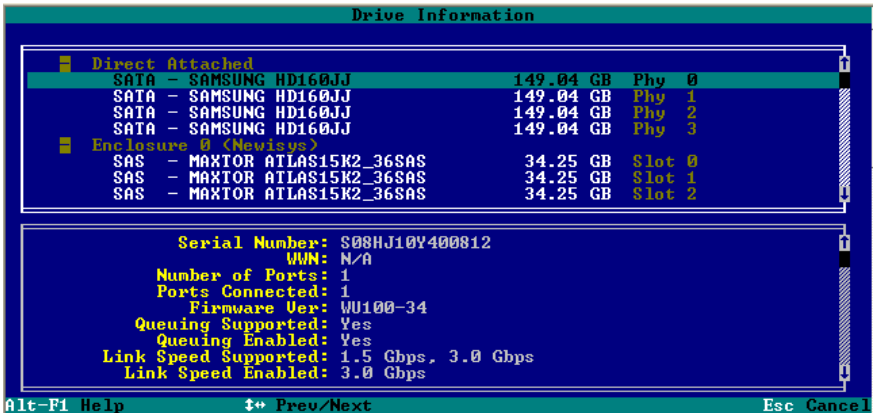
2 On the pop-up menu, select **Drives** and press **Enter**.

3 On the Drive Information page, use the arrow keys to move from one drive to another.

  Details about the selected drive are displayed in the bottom of the page.

Tip: You can scroll both sections of the Drive Information page to bring additional drive information or drives into view. Press **Tab** to move between the two sections.

Figure 60. Drive Information page (3BM)



Enclosure Drive LED Status Indicators

If you have a supported enclosure, the LEDs on your enclosure may be able to provide some status information about your drives and units.

Note: The following table is an example of how LEDs may be used. Check with your chassis or enclosure documentation for more details. Not all features may be supported or implemented in the same way on all chassis.list of supported enclosures is available at http://www.3ware.com/products/sys_compatibility.asp

Table 10: Meaning of LED Colors and Behavior

Color	Drive Status
Solid green	OK
Blinking green	Identify This occurs when you have used the Identify command in 3DM to locate a particular drive or unit. (See “Locating a Drive by Blinking Its LED” on page 131.)
Black	No drive
Solid Amber	Hot spare
Blinking amber	Rebuilding The drive in this slot is part of a RAID unit that is currently rebuilding. You can continue to use the unit. For more information, see “Rebuilding Units” on page 144.

Table 10: Meaning of LED Colors and Behavior

Color	Drive Status
Solid red	Drive fault This drive has failed. You should replace it and rebuild the unit.
Blinking red	Predicted drive fault 3ware software predicts that this drive will fail soon. You may want to replace it.

Unit Statuses

The following is a list of unit statuses you may see in 3DM:

- **OK.** The unit is optimal and is functioning normally.
- **Rebuilding.** The unit is in the process of writing data to a newly added disk in a redundant unit, in order to restore the unit to an optimal state. The unit is not fully fault tolerant until the rebuilding is complete. For more information, see “To verify a unit through 3BM” on page 143.
- **Rebuild-Paused.** The unit is set to rebuild, however scheduling is enabled, and the present time is not during a scheduled timeslot. Rebuilding will start at the next scheduled time slot. Rebuilds are also paused for up to ten minutes after a reboot, even during a scheduled timeslot.
- **Initializing.** The unit is in the process of writing to all of the disks in the unit in order to make the array fault tolerant. For more information, see “About Initialization” on page 137.
- **Initializing-Paused.** The unit is set to initialize, however scheduling is enabled and the present time is not during a scheduled timeslot. Initializing will start at the next scheduled time slot. Initialization is also paused for up to ten minutes after a reboot, even during a scheduled timeslot.
- **Verifying.** The unit is in the process of ensuring that the parity data of a redundant unit is valid. For more information, see “About Verification” on page 141.
- **Verify-Paused.** The unit is set to verify, however, scheduling is enabled, and the present time is not during a scheduled timeslot. Verification will start at the next scheduled time slot.
- **Migrating.** The unit is in the process of being reconfigured while it is online. Migration can be used to change the RAID level, to expand the capacity by adding additional drives, or to change the stripe size. For more information, see “Changing An Existing Configuration by Migrating” on page 109.

- **Migrate-Paused.** The unit is in the process of migrating, however scheduling is enabled, and the present time is not during a scheduled timeslot. Migrating will start at the next scheduled time slot. Migration is also paused for up to ten minutes after a reboot, even during a scheduled timeslot.
- **Degraded.** One or more drives in the redundant unit is no longer being used by the controller. For more information, see "About Degraded Units" on page 130.
- **Inoperable.** This is a condition where one or more drives are missing from a unit, causing the unit to no longer be available to the operating system. Data on an inoperable unit cannot be accessed. For more information, see "About Inoperable Units" on page 131.

Drive Statuses

The following is a list of drive statuses you may see in 3DM:

- **OK.** The drive is fine and is functioning normally.
- **Not Present.** No drive is present in this slot.
- **Drive Removed.** The drive has been removed.
- **Other.** A number of other drive statuses may appear in the event of a problem. If you have a question about a status shown, contact AMCC customer support. knowing the exact drive status can help trouble-shoot the problem.

About Degraded Units

Fault tolerant RAID units provide data redundancy by duplicating information on multiple drives. These RAID units make it possible to continue use even if one of the drives in the unit has failed.

- RAID 1 and RAID 10 units each use mirroring to achieve fault tolerance. Identical data is stored on two or more drives to protect against drive failure.
- RAID 5, RAID 6, and RAID 50 units achieve fault tolerance by using a simple (exclusive OR) function to generate the parity data that is distributed on all drives.
- RAID 6 adds an extra level of protection over RAID 5 by generating a second parity when data is written. This allows two drives to fail without compromising data integrity, especially on larger units.

When one of the drives in a fault-tolerant unit fails or is removed or unplugged, the unit is said to be *degraded*.

You can still read and write data from a degraded unit, but the unit will not be fault tolerant until it is rebuilt using the Rebuild feature.

When a RAID unit becomes degraded, it is marked as such, and the drive(s) that failed are marked as **Not In Use** in the 3BM screens and **Degraded** in the 3DM pages. If supported by your enclosure, the LED for failed drives may turn red.

You should replace the failed drive and rebuild the unit as soon as it is convenient to do so. The unit will not be fault tolerant until it has been rebuilt. Rebuilding can occur automatically, depending on your settings. For more information, see “Rebuilding Units” on page 144.

About Inoperable Units

Units become inoperable when there are no longer enough drives in the unit for it to function. For example, a RAID 5 unit created from four drives becomes degraded if one drive fails or is removed, but becomes inoperable if two drives fail or are removed. A RAID 6 unit created from five drives becomes degraded if one or two drives is removed, but becomes inoperable if three drives fail or are removed.

Data on an inoperable unit cannot be accessed unless the missing drives are reconnected.

If you have data on a unit that is currently “inoperable,” contact technical support.

Locating a Drive by Blinking Its LED

If you use a supported enclosure with enclosure services, you may be able to easily identify the drives in a unit, or locate an individual drive, by causing the LEDs associated with the drives to blink.

You can issue the command to blink the LED through 3DM or 3BM.

(For details about what the different LED patterns on the enclosure may mean, see “Enclosure Drive LED Status Indicators” on page 128.)

To blink the LED for a drive through 3DM

1 Do one of the following:

- Choose **Information > Drive Information** from the main menu in 3DM. On the Drive Information page, identify the drive you want to physically locate.

- Choose **Monitor > Enclosure** from the main menu in 3DM. On the list of enclosures, click the ID number of the enclosure. On the Enclosure Detail page, identify the drive you want to physically locate.

2 Check the box in the **Identify** column.

The LED on the enclosure begins blinking.

3 When you are finished working with the drive and no longer need to see the LED, return to this page and uncheck the **Identify** box.

To blink the LED for a drive through 3BM

1 On the main 3BM screen, **Tab** to **Information** and press **Enter**.

2 On the pop-up menu, select **Drives** and press **Enter**.

3 On the Drive Information page, use the arrow keys to select the drive you want to identify.

4 Press **F4**.

The LED on the enclosure begins blinking. (Note that this feature is only available for drives in enclosures.)

5 When you are finished working with the drive and no longer need to see the LED, return to this page and press **F4** again to halt the blinking.

To blink the LEDs for all drives in a unit

1 Choose **Information > Unit Information** from the main menu in 3DM.

2 On the Unit Information page, identify the unit you are interested in.

3 Check the box in the **Identify** column.

The LEDs for the drives in the selected unit begin blinking.

4 When you no longer need to see the LEDs, return to this page and uncheck the **Identify** box.

Alarms, Errors, and Other Events

3ware provides several levels of detail about alarms, errors, and other events. This information is available through the 3DM web application and the CLI. On Windows systems, the WinAVAlarm alert utility can also be used to notify you of events.

The next few pages describe these capabilities.

- "Viewing Alarms, Errors, and Other Events" on page 133
- "Using the Alert Utility Under Windows" on page 134
- "Downloading an Error Log" on page 136
- "Viewing SMART Data About a Drive" on page 136

CLI capabilities are described in the *3ware SAS/SATA RAID Controller CLI Guide*.

Tip: If you have a supported enclosure, the LEDs on your enclosure may also provide you with status information about drives. For more information, see "Enclosure LED Status Indicators" on page 150.

Viewing Alarms, Errors, and Other Events

The **Alarms** page in 3DM shows a log of all events (also called Asynchronous Event Notifications, or AENs) that have occurred on units. These events include alarms that occur when the 3ware RAID controller requires attention, such as when a disk unit becomes degraded and is no longer fault tolerant. They also include SMART notifications and informational notification, such as when sectors have been repaired during verification.

Event messages are categorized into the following levels of severity:

- **Errors** (high severity events), shown next to a red box
- **Warnings**, shown next to a yellow box
- **Information,** shown next to a blue box

Examples of event messages:

- **Error**: Unclean shutdown
- **Warning:** Degraded unit
- **Information:** Start and completion of rebuilding, verifying, initializing, migrating, and so forth.

3DM can e-mail notifications of these events to one or more recipients. For more information, see "Managing E-mail Event Notification" on page 69.

If your 3ware RAID controller is installed in a Windows system, the WinAVAlarm alert utility can notify you of events immediately with an audible alarm and a popup message. For details, see “Using the Alert Utility Under Windows” on page 134.

A list of the possible error and other event messages is provided under “Error and Notification Messages” on page 228.

To view alarms, errors and other events in 3DM

1 Choose **Monitor > Alarms**.

The Alarms page displays, listing all event notifications.

2 For details about a particular alarm, click it.

A Help window opens with additional information about the alarm.

To see an explanation of a specific item in 3DM

- Click on the message you are interested in, on the 3DM Alarms page.

  A help topic opens with additional information.

Using the Alert Utility Under Windows

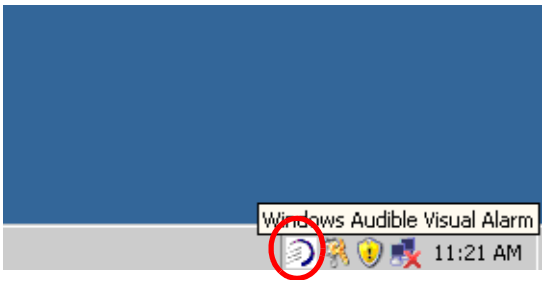
An alert utility, WinAVAlarm, is automatically installed on Windows systems when 3DM is installed. It can provide immediate notification of events, through a popup message and an audible alert. By default it is set to notify you whenever an error (high-severity event) occurs, through both a popup message and an audible alert. You can configure the alert settings to specify types of events you want to be notified of: Errors, Warnings, or Information.

WinAVAlarm is a stand-alone utility and does not require 3DM to be running, unlike e-mail notification. After it is installed, an icon for it appears in your System tray.

To change the alert utility settings

1 Double-click on the WinAVAlarm icon in the system tray.

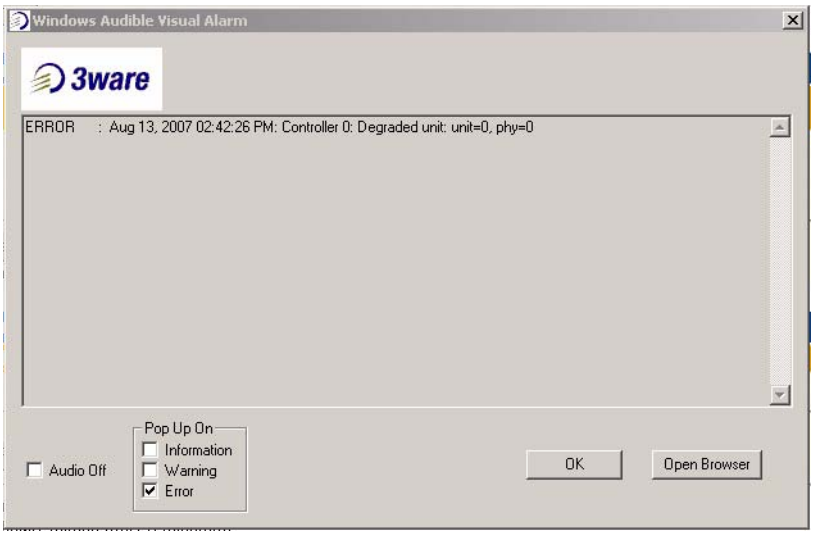
Figure 61. WinAVAlarm in the Windows System Tray



2 In the Windows Audible Visual Alarm window, select the types of alerts you want to be notified of.

If you want to turn off the sound alarm and only have a pop-up message appear, check the **Audio Off** button.

Figure 62. WinAVAlarm Popup Window



If you wish, you can open 3DM from this window by clicking **Open Browser**. This can be useful when you receive a message, because the 3DM Alarms page allows you to easily access online help associated with the events.

3 Click **OK** to close the window and accept any changes you have made.

Downloading an Error Log

You can download an error log containing information from the firmware log. This can be useful when troubleshooting certain types of problems. For example, you might want to send the saved file to 3ware Customer Support for assistance when troubleshooting.

To download the error log

1 In 3DM, choose **Information > Controller Details** from the menu bar.

2 Make sure the correct controller is displayed in the **Select Controller** field in the menu bar.

3 On the Controller Details page, click the **Download Error Log** link.

4 When the Save or Open dialog box appears, navigate to where you want to save the log and click **OK**.

Viewing SMART Data About a Drive

You can view SMART (Self-Monitoring, Analysis, and Reporting Technology) data about a SATA drive to help troubleshoot problems that occur. SMART data is available on all SATA disk drives (unit members, Single Disks, and Hot Spares). Although SAS drives are monitored, the data for them is not displayed.

You can also set self-tests that will check the SMART attributes and post messages to the Alarms page when they are exceeded. For more information, see “Selecting Self-tests to be Performed” on page 154.

To view SMART data

1 Choose **Information > Drive Information** from the menu bar.

2 On the Drive Information page, click the port number for the drive you are interested in.

A window showing details of the SMART data opens. The data is shown as hex values.

Background Tasks

Background tasks are maintenance tasks that help maintain the integrity of your drives and data. These tasks include

- Initialization of units
- Verification of units
- Rebuilds when units have become degraded
- Migration of an on-line RAID from one RAID configuration to another
- Self-tests

You can set up your system so that these tasks occur as they are needed, or you can create schedules so that they occur during non-peak times. Background tasks can have an effect on performance, so using a schedule can minimize the impact.

This section includes the following topics related to background tasks:

- About Initialization
- About Verification
- Starting a Verify Manually
- Rebuilding Units
- Cancelling a Rebuild and Restarting It with a Different Drive
- Setting Background Task Rate
- Background Task Prioritization
- Scheduling Background Tasks
- Viewing Current Task Schedules
- Turning On or Off Use of a Task Schedule
- Removing a Task Schedule
- Adding a New Task Schedule Slot
- Selecting Self-tests to be Performed

Although the migration of a unit is handled as a background task, initiating it is similar to creating a new unit. For details, see “Changing An Existing Configuration by Migrating” on page 109.

About Initialization

For 3ware SATA RAID controllers, *initialize* means to put the redundant data on the drives of redundant units into a known state so that data can be recovered in the event of a disk drive failure. This is sometimes referred to as *background initialization* or *resynching*, and does not erase user data.

Some RAID levels must be initialized for best performance. (For specifics, see “Initialization of Different RAID Types” on page 139.) When these units are created in the BIOS (through 3BM), initialization begins immediately. This type of initialization is referred to as *foreground initialization*, because it is the primary task being performed on the system, before the operating system has loaded. **This process erases existing data**, by writing zeroes to all of the drives in the unit. You can elect to cancel foreground initialization, put the units into service, and have initialization run in the background, instead.

Foreground Versus Background Initialization

Initialization makes parity information valid. Foreground initialization does this by simply writing zeroes to all the drives so that they all have the same values, overwriting any existing data in the process. In contrast, background initialization uses an algorithm to resynch the parity information on the drives and does not rewrite existing data.

A foreground initialization is run from the BIOS using 3BM. It clears all existing data from the drives. Foreground initialization can take several hours, depending upon the size of the unit. After foreground initialization completes, you can start the operating system and units will perform at peak efficiency.

If immediate access to the unit is important, you can stop foreground initialization by pressing **Esc** and booting to the operating system. Background initialization will then start automatically within about 10 minutes. Background initialization (resynching) does not write zeroes to the drives or harm your data. You can partition, format, and use the unit safely while it is initializing. The unit is fully fault-tolerant while the initialization takes place. That is, if the unit degrades before the initialization is complete, the data will remain intact.

When initializing is done after booting to the operating system, the process of initializing takes longer than it does if initialization is done by writing zeroes to the unit in the BIOS. Consequently, it will be a longer period of time until the performance of the unit is fully optimal.

Although you can use the unit while it is being initialized in the background, initialization does slow I/O performance until completed. You can adjust how much initialization will slow performance by setting the rate at which it occurs. (See “Setting Background Task Rate” on page 149.) You can also postpone initialization until a scheduled time. (See “Scheduling Background Tasks” on page 150).

Note: Units that do not need to be immediately initialized for full performance will be automatically initialized using background initialization when they are verified for the first time. (Verification requires that the units have been previously initialized.) This will not affect the data on the drives, and the units will perform normally, although performance will be slowed until the initialization and verification are completed.

Initialization of Different RAID Types

Information about initialization for each of the different RAID types is described below and summarized in Table 11 on page 140.

Initialization of RAID 0 Units

RAID 0 units do not need to be initialized and cannot be initialized. RAID 0 units are immediately available for use with full performance when created.

Initialization of RAID 5, RAID 6, and RAID 50 Units

RAID 5 units with three or four drives will be automatically initialized the first time they are verified.

Regardless of the size, all 9000-series RAID 5, RAID 6, and RAID 50 units are fully fault tolerant upon creation. These configurations use a specialized scheme for writing to the unit, which does not have to be valid to provide fault tolerance.

Performance of RAID 6, RAID 5 units with 5 or more disks, and RAID 50 units with 2 subunits of 5 or 6 disks will improve after the unit has been initialized. For these configurations, initialization begins automatically after you create them. If you create them in the 3BM utility, zeroes are written to all unit members. If you create them through 3DM, RAID 5 parity is calculated and written to disk, keeping any data in the unit intact.

RAID 5 units with 3 or 4 disks do not need to be initialized to have full performance upon creation. It is okay that 3 or 4 disk RAID 5 units are not initialized. These RAID types are fully redundant, regardless of whether or not they are initialized. Similarly, RAID 50 units with a grouping of 3 or 4 disks in a subunit do not need to be initialized. However, RAID 50 with a grouping of 5 or more disks in a subunit do need to be initialized for full performance.

Notes:

For RAID 5 with more 5 or more drives, it is strongly recommended that you initialize the unit before using it. Initializing such a unit is critical to insuring data integrity on the unit.

For RAID 5 with 3 or 4 drives, initialization before use is not required. However, initialization is required before a unit can be verified. Consequently, if you attempt to verify a RAID 5 with 3 or 4 drives that has not yet been initialized, you will see a message that the array has not been initialized, and initialization will begin. This is considered part of normal operation of the unit.

Initialization of RAID 1 and RAID 10 Units

RAID 1 and RAID 10 units do not need to be initialized when they are created to be fault tolerant and are immediately available for use with full performance when created.

Initialization of RAID 1 or RAID 10 units will take place automatically the first time the unit is verified.

Initialization of a RAID 1 unit results in data from one disk (the disk on the lower port number) being copied to the other disk. In RAID 10 units, data from one half of the unit is copied to the other half.

After the initialization, subsequent verifies to a RAID 1 or RAID 10 unit check for data consistency by comparing the data from one drive (or set of drives) to the other drive (or set of drives).

Table 11: Initialization Requirements for Different RAID Configurations

Initialization Required for Highest Performance?	RAID Configurations
No	Single drive
No	RAID 0
No	RAID 1 RAID 10
No	RAID 5 with 3 or 4 disks RAID 50 with 6, 8, or 9 disks RAID 50 with 12 disks in 3 subunits of 4 RAID 50 with 12 disks in 4 subunits of 3 RAID 50 with 16 disks in 4 subunits of 4
Yes	RAID 5 with 5 or more disks RAID 6 RAID 50 with subunits of 5 or more disks

Background Initialization After Power Failure

The 3ware controller detects and handles power failures, using a mechanism that ensures that redundant units have consistent data and parity. When a redundant unit is unexpectedly shutdown, there is a possibility some data and parity may be inconsistent. If a unit or sub-unit of a redundant unit is detected to have been shutdown uncleanly, the unit or sub-unit will change its mode to either ‘Initializing’ or ‘Verifying.’

When the initialization is complete, the unit is guaranteed to be redundant again. The initialization does not erase user data.

About Verification

The verify feature combines verification of redundant units (confirming the validity of the redundant data) and media scans for non-redundant units.

Verification can provide early warning of a disk drive problem or failure. This allows you to replace drives before they fail.

You can manually request a verify, or you can enable the Auto Verify policy, and the controller will automatically start verification once every 24 hours. (See “Starting a Verify Manually” on page 143 and “Setting Auto Verify for a Unit” on page 103.)

During verification, I/O continues normally, but with a slight performance loss, depending on your verify rate setting. You can adjust how much verification will slow performance by setting a rate at which it occurs. (See “Setting Background Task Rate” on page 149.) You can also postpone verification until a scheduled time. (See “Scheduling Background Tasks” on page 150.)

Note: Not verifying the unit periodically can lead to an unstable array unit and may cause data loss.

It is strongly recommended that you schedule a verify at least 1 time per week.

What Verification Does

For a RAID 1 or RAID 10 unit, a verify compares the data of one mirror with the other. For RAID 5, RAID 6, and RAID 50, a verify calculates parity and compares it to what is written on the disk drive.

Verification checks each sector on a drive. This is important, because day-to-day use of the media may leave many sectors on a drive unused or unchecked for long periods of time. This can result in errors occurring during user operation. Periodic verification of the media allows the disk drive firmware to take corrective actions on problem areas on the disk, minimizing the occurrence of uncorrectable read and write errors.

Verifies can be performed through either 3BM (BIOS) or through 3DM. In addition, they can be scheduled to run at preferred times, through 3DM or through the CLI, or can be run automatically during the Verify schedule window, if scheduling and the Auto Verify feature are enabled.

Verification of Non-Redundant Units

Verification of non-redundant units (single disks, spares, and RAID 0 units) read each sector of a drive, sequentially. If a sector can’t be read, it is flagged as unreadable, and the next time the controller writes to that location, the drive reallocates the data to a different sector.

Verification of Redundant Units

Verification of redundant units also reads each sector, working from lowest block to highest block. If verification cannot read data in a sector, dynamic sector repair is used to recover the lost data from the redundant drive or drives; this recovered data is written to the problem sector. This forces the drive to reallocate the defective sector with a good spare sector.

If the verify unit process determines that the mirrored drives are not identical or the parity is not correct, the error is corrected. For RAID 1 and 10, this involves copying the miscompared data from the lower port(s) to the higher port(s) of the mirror. For RAID 5, RAID 6, and RAID 50, this involves recalculating and rewriting the parity that was incorrect. AEN 36 ("Verify detected and fixed data/parity mismatch") is posted to the Alarms page.

For RAID 1 and 10, verification involves copying the data from the lower port(s) to the higher port(s) of the mirror. For RAID 5 and RAID 50, this involves recalculating and rewriting the parity for the entire unit. If the unit is not redundant, a file-system check is recommended to correct the issue. If the errors persist and cannot be overwritten from a backup copy, perform a final incremental backup. You will need to replace the defective drive, recreate the unit, and reinstall the data.

How Errors Are Handled

Verification makes use of the same error checking and error repair techniques used during ordinary use of drives configured through 3ware RAID controllers.

When verification encounters an error, the controller typically retries the command. If there are cable CRC errors, there may be multiple retries including downgrade of the UDMA mode. If the error persists and is unrepairable (e.g., ECC errors), an error notification is issued to indicate the problem. (See AEN "0026 Drive ECC error reported" on page 243.)

If the disk drive is part of a redundant unit that is in a redundant state (not degraded or rebuilding), then Dynamic Sector Repair automatically rewrites the redundant data to the error location to force the drive to reallocate the error location. A notification of repair is posted to the alarms list. The result is a restoration of drive and data integrity; the primary and redundant data are again both valid.

If the unit is not redundant, it is recommended that you perform a file-system check to correct the issue. Under Windows, you can do this by right-clicking on the Drive and choosing Properties; then on the Tools tab, click Check Now. If the errors persist and cannot be overwritten from a backup copy, perform a final backup of files that have changed since your last backup. You will need to replace the defective drive, recreate the array, and reinstall the data.

Starting a Verify Manually

Verification of units can be done automatically, on a schedule, or can be started manually, as described below. (See “Setting Auto Verify for a Unit” on page 103 and “Scheduling Background Tasks” on page 150.)

Note: If the unit has not previously been initialized and you manually select **Verify Unit** in either 3BM or 3DM, the initialization process starts.

You can manually start a verify through either 3DM or 3BM.

To verify a unit through 3DM

1 In 3DM, choose **Management > Maintenance**.

2 In the **Unit Maintenance** section of the Maintenance page, select the unit you want to verify and click **Verify Unit**.

3DM puts the selected unit in verifying mode. If verify scheduling is not enabled on the Scheduling page, the verification process begins almost immediately. If verify scheduling is enabled, the unit will not start actively verifying until the next scheduled time.

A **Stop Verify** link appears next to the unit on the Maintenance page. If you need to stop the verify process, use this link. (If initialization starts because the unit had not previously been initialized, it cannot be halted, so no **Stop Verify** link appears.)

To verify a unit through 3BM

1 At the main 3BM screen, select the unit by highlighting it and pressing **Enter**.

An asterisk appears in the left-most column to indicate that it is selected.

2 **Tab** to the **Maintain Unit** button and press **Enter**.

3 On the pop-up menu, select **Verify** and press **Enter**.

Verification of the selected unit starts immediately.

Figure 63. Verifying a Unit

Notes:

If a unit that requires initialization has not previously been initialized, selecting Verify Unit starts initialization. This is because fault-tolerant units cannot be verified until after they are initialized.

If the unit is already in a state of rebuild, initialization, or verification, the unit cannot be verified in 3BM. You must boot the system and let the task finish in the background.

Rebuilding Units

Rebuilding is the process of generating data on a new drive after it is put into service to replace a failed drive in a fault tolerant unit.

If a hot spare of the appropriate drive type (SAS or SATA) is specified and a redundant unit degrades, it will be used to automatically replace the failed drive in the redundant unit without intervention on your part. The rebuild process will automatically be launched as a background process at the next scheduled time. If scheduling is turned off, the rebuild process will start almost immediately (within a couple of minutes). If 3DM is running and E-mail notification is enabled, an event notification will be sent to specified users when the unit degrades and again when the rebuild process is complete.

If the Auto Rebuild policy is enabled (see “Setting the Auto Rebuild Policy” on page 77), the firmware will attempt to rebuild a degraded unit with an available drive or a failed drive.

If desired, you can manually replace the drive, rescan the controller, and start the rebuild process. Manual rebuilds can be started from either 3BM or 3DM, although the rebuild itself only happens when the operating system is running.

Rebuilds on multiple units can take place simultaneously.

If multiple drives are faulted in a RAID 10 configuration, the drives are rebuilt simultaneously. In a 4-drive RAID 10 configuration, up to two drives can be rebuilt. In a 6-drive configuration, up to three drives can be rebuilt. In an 8-drive configuration, up to four drives can be rebuilt. In a 12-drive configuration, up to six drives can be rebuilt.

Note: If both drives in a RAID 10 mirrored set are faulted, the data is not recoverable. Up to half of the drives in a RAID 10 unit can become defective and still have the user data retained, as long as the failed drives are only half of each mirrored pair.

A RAID 5 unit can have one drive fail before becoming inoperable.

A RAID 50 unit can sustain multiple drive failures, as long there is only one failed drive in each RAID 5 set.

A RAID 6 unit can have two simultaneous drive failures, before becoming inoperable.

When a RAID 5 or RAID 6 is running in Degraded mode and you rebuild it, the missing data is reconstructed from all functioning drives.

Note: If a rebuild fails, check the Alarms page for the reason. If there was an ECC error on the source disk, you can force the rebuild to continue by checking the Overwrite ECC Error policy on the Controller Settings page in 3DM and then running Rebuild again. This will cause uncorrectable blocks to be rewritten, but the data may be incorrect. It is recommended that you execute a file system check when the rebuild completes. Under Windows, you can do this by right-clicking on the Drive and choosing **Properties**; then on the **Tools** tab, click **Check Now**. Under Linux use `fsck /dev/sda1`.

Rebuilding a Unit Through 3DM

When a drive on a unit becomes defective, you replace it with an available drive and then rebuild the unit. If Auto Rebuild is enabled and a drive is available, starting the rebuild is optional as it will start automatically.

To rebuild a unit through 3DM

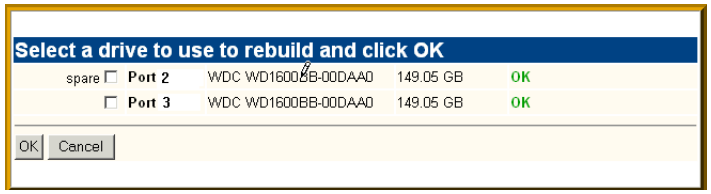
1 If necessary, add a new drive to replace the failed drive. (For details, see “Adding a Drive” on page 122.)

2 In 3DM, choose **Management > Maintenance**.

3 In the **Unit Maintenance** section of the Maintenance page, select the degraded unit and click the **Rebuild Unit** button.

4 When a dialog box displays available drives, select the drive you want to replace the failed drive and click **OK.**

Figure 64. Selecting a Drive when Rebuilding



5 If the degraded unit has more than one failed drive (for example, a RAID 10 where both mirrored pairs each have a failed drive), repeat step 3 and step 4 to select another drive.

If rebuild scheduling is not enabled on the **Scheduling** page, the rebuild process begins almost immediately in the background. If rebuild scheduling is enabled, the unit will not start actively rebuilding until the next scheduled time.

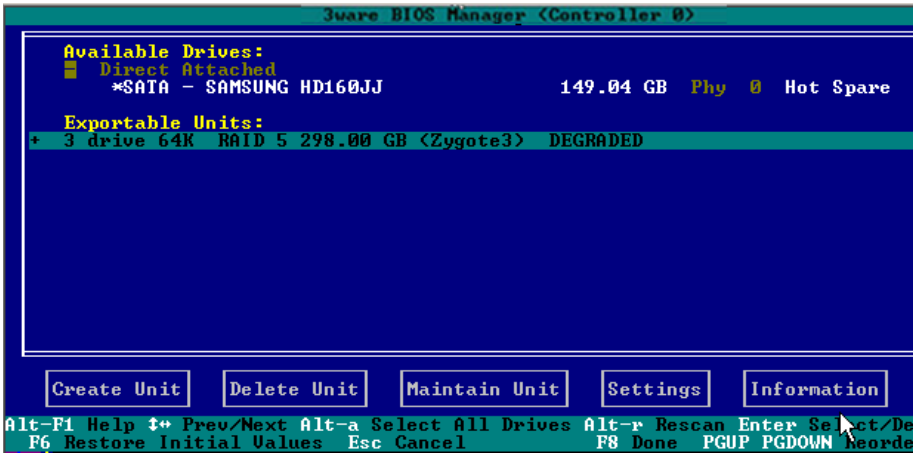
Note: If you need to cancel a rebuild, you can do so by using the **Remove Drive** link on the Maintenance page to remove the drive from the unit.

Rebuilding Units through 3BM

When a RAID unit becomes degraded, it is marked as such, and the drive(s) that failed are marked as **Not In Use** in the 3BM screens.

Figure 65 shows an example of how a degraded RAID 5 unit appears in 3BM.

Figure 65. Degraded RAID 5 Array to be Rebuilt



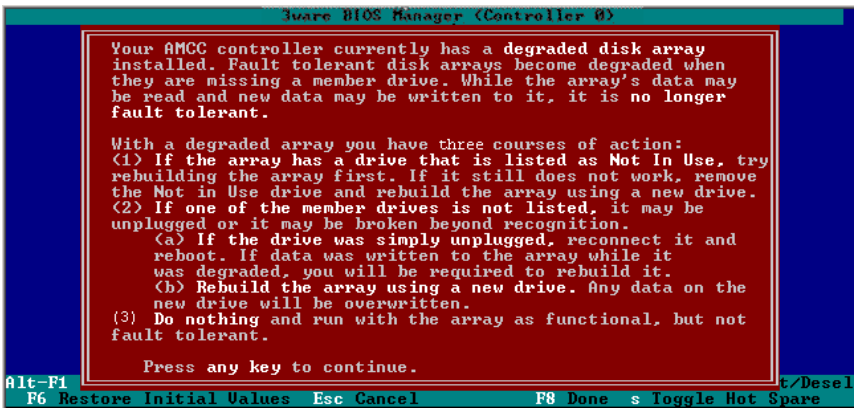
You can start the rebuild of a degraded unit manually in 3BM, or you can let the system boot and allow the rebuild to take place automatically.

To start the rebuild of a unit through 3BM

1 Reboot the system and start 3BM.

A red message box informs you that the unit is degraded, and suggests some possible approaches. Figure 66 shows an example of a degraded-array message.

Figure 66. Degraded Disk Array Warning Message



2 Press a key to continue.

3 If your degraded unit has a drive indicated as **Not in Use**, the drive may still be usable. Try rebuilding with the **Not in Use** drive intact. Simply select the unit (highlight it and press **Enter**) and then select the **Rebuild Unit** button.

4 When the **Rebuild** confirmation screen appears, confirm that you selected the correct unit by selecting **OK**.

5 Press **F8** to save your changes and exit 3BM**.** The unit will begin rebuilding after the operating system finishes loading.

If the rebuild fails and you have no available drives, do one of the following:

- If your system has hot swap bays, you can replace the failed or **Not In Use** drive and rescan (Alt-R) the unit.
- If your system does not have hot swap bays, power down the system and replace the failed or **Not In Use** drive. Then power on the system and restart 3BM.

Then follow these steps:

1 At the main 3BM screen, highlight an available drive to replace the faulted drive and press **Enter** to select it.

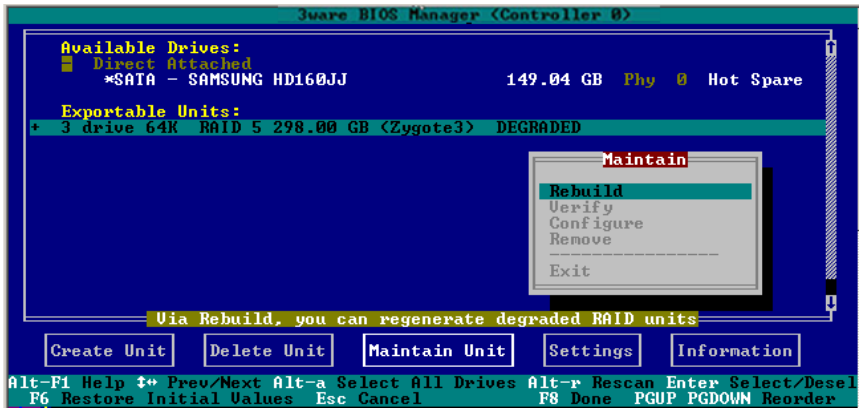
An asterisk appears in the left most column to indicate the drive is selected.

2 Press **Tab** to select the degraded unit and press **Enter** to select it.

3 **Tab** to the **Maintain Unit** button and press **Enter**.

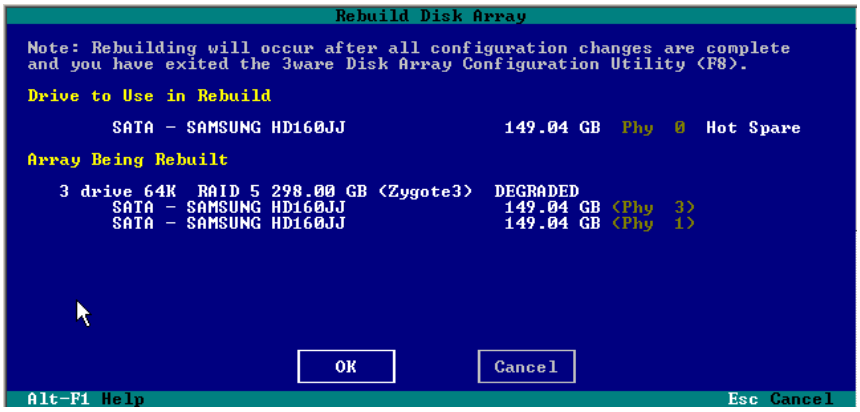
4 Select **Rebuild** from the pop-up menu and press **Enter**.

Figure 67. Rebuild Option on the Maintain Menu



The Rebuild Disk Array screen displays.

Figure 68. Rebuild Disk Array Screen



5 Press **Enter** to select the **OK** button to continue.

You are returned to the main screen; “Rebuilding” appears next to the unit you selected.

6 Press **F8** to save your changes and exit 3BM**.**

The unit will begin rebuilding about ten minutes after the operating system finishes loading and the 3ware driver has loaded.

Cancelling a Rebuild and Restarting It with a Different Drive

When you start a rebuild from 3BM, you cannot cancel from within the 3BM interface. However, if you have drives in hot swap bays, you can remove and replace the drive, rescan the controller (Alt-R), and then select a new drive to be used in the rebuild. You can also boot the operating system, launch 3DM, and cancel a rebuild by using the **Remove Drive** link on the Maintenance page.

If your drives are not in hot swap bays and you do not want to boot the operating system and launch 3DM, you can also cancel a rebuild by powering down the system, physically removing a drive, and installing another one that you want to use. Then when you start 3BM, the unit will appear as degraded and you can rebuild it, using the steps described under “Rebuilding Units through 3BM” on page 146.

Note: If you want to pause the rebuild process through 3DM, you can do so by setting or changing the rebuild schedule on the Scheduling page. If you set a schedule for rebuilds that does not include the current time, the rebuild process will pause.

Setting Background Task Rate

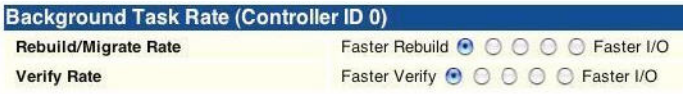
In 3DM, you can set the relative performance of background tasks (initializing, rebuilding/migrating, and verifying) in relation to normal I/O activity (reading and writing to disk).

Controllers can have separate settings for Rebuild/Migrate Rate and Verify Rate. (Initialization occurs at the Rebuild rate.)

To change the background task rate

1 Choose **Management > Controller Settings** from the menu bar.

2 In the **Background Task Rate** section of the Controller Settings page, select one of the five radio buttons to indicate the relative task rate for Rebuild and Verify Tasks.



The furthest left buttons set the firmware to the fastest rebuild and verify settings. This means that maximum processing time will be given to rebuilds or verifies rather than I/O. The furthest right buttons set the firmware to the slowest rebuild and verify settings, giving maximum processing time to I/O.

After you select one of the radio buttons, the page refreshes, and a message at the top confirms the change you have made.

Background Task Prioritization

Although migration tasks follow the same schedule as rebuild and initialization tasks, they are always given the highest priority because of the controller and disk resources required during migration.

Once a unit is put into the migration state, it must be allowed to complete the process. While migrating, rebuilds or verifies to the unit are not permitted.

Rebuilding preempts verify operations. If a unit requires rebuilding, that process will take place before the unit is verified.

Controllers can work on multiple units at the same time. This means that if you have both a redundant unit and a non-redundant unit, the verification of the redundant unit and the media scan of the non-redundant unit will occur at the same time.

Scheduling Background Tasks

You can set up scheduling windows for when background tasks occur so that routine maintenance of storage media occurs when it will be least likely to interfere with day-to-day work on the system (peak I/O times). By creating and using schedules, you can specify when active rebuilding, migrating, verifying, and testing of units should occur. For example, you might these tasks to occur at 2AM each day, or on weekends.

The initial schedule setting is to “Ignore Schedule.” This allows the controller firmware to automatically initiate background tasks.

Note: Initialization follows the rebuild/migrate schedule.

Rebuild/migrate, verify, and self-test tasks are scheduled separately, but in a very similar way. You can perform the following scheduling tasks:

- Viewing Current Task Schedules
- Turning On or Off Use of a Task Schedule
- Removing a Task Schedule
- Adding a New Task Schedule Slot
- Selecting Self-tests to be Performed

Tip: If you want to change a task schedule window, you first remove the schedule item and then add it back with the desired day, time, and duration.

Note: Setting up the scheduling window does not actually request background tasks. It simply specifies when they can run. For more information about the background tasks themselves, see “Background Tasks” on page 137.

You can also set the rate at which background tasks are performed compared to I/O tasks. For more information, see “Setting Background Task Rate” on page 149.

Scheduled Task Duration

If a rebuild completes within a scheduling window, it will not start over at the next scheduled time block, unless another rebuild is required.

If a rebuild does not complete in the scheduled time block, it will continue where it left off at the next scheduled time block.

Similarly, if a verify operation does not complete in the scheduled time block, it will continue where it left off at the next scheduled time block.

Viewing Current Task Schedules

You can see the current schedules for background tasks on the **Scheduling** page.

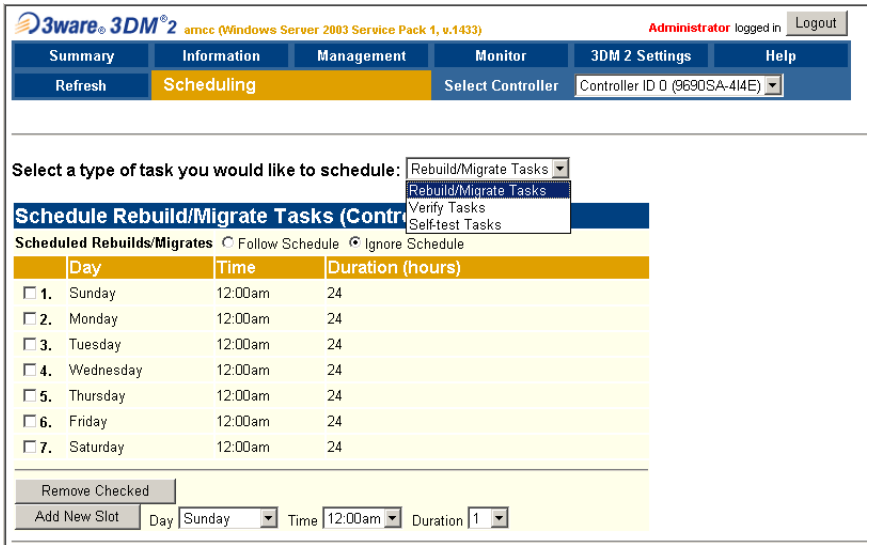
To view the current task schedule

1 Choose **Management > Schedule** from the menu bar.

The Scheduling page appears, showing the schedule for Rebuild Tasks. (Migration and initialization tasks follow the Rebuild Task schedule.)

2 To view Verify Tasks or Self-test Tasks, select it from the drop-down list at the top of the page.

Figure 69. Selecting Task Schedules to View



Turning On or Off Use of a Task Schedule

Turning on the schedule for Rebuild/Migrate and Verify tasks forces rebuilds, migrates, and verifies to be performed only during the time specified by the schedule. If the schedule is not turned on, rebuilds, migration, initialization, and verify can happen whenever they are required or are manually started.

There may be times when you want to disable scheduled rebuild/migrate or verify tasks, so that you can rebuild, migrate, or verify a unit right away, without waiting for the next scheduled time. In this case, you can disable the schedule, as described below.

Note: When you first use 3DM, daily schedules exist with 24 hour duration—that is, the schedule is for “all the time.” Until you change these 24-hour daily schedule, enabling the schedule will not have any direct effect.

You can easily disable a current Verify or Rebuild/Migrate schedule without deleting the schedule itself.

To turn on or off use of the current Verify or Rebuild task schedule

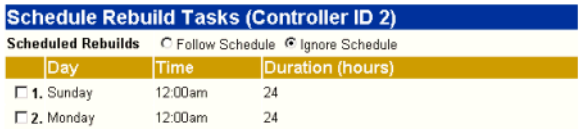
1 Choose **Management > Schedule** from the menu bar.

The Scheduling page appears, showing the schedule for Rebuild/Migrate Tasks.

2 To view Verify Tasks, select it from the drop-down list at the top of the page.

3 In the Schedule Rebuild Tasks section, select the appropriate setting: **Follow Schedule** or **Ignore Schedule**.

The illustration below shows this setting for the rebuild task schedule.



Note: Self-test schedules cannot be turned off in this way. To disable self-tests you must either remove all schedule times, or uncheck the tests listed in the **Tasks** column. For more information, see “Selecting Self-tests to be Performed” on page 154.

Removing a Task Schedule

By default, daily task schedules are defined, each starting at 12:00 am and running for 24 hours.

A maximum of seven schedules can be defined. When seven schedules are shown for any of the tasks, you must remove a schedule before you can add another.

To remove a task schedule

1 Choose **Management > Schedule** from the menu bar.

The Scheduling page appears, showing the schedule for Rebuild/Migrate Tasks.

2 To view Verify Tasks or Self-test Tasks, select it from the drop-down list at the top of the page.

3 Select the checkbox next to the schedule(s) you want to remove.

4 Click the **Remove Checked** button.

The page refreshes, and the selected schedule(s) are removed. You can now add another schedule.

Adding a New Task Schedule Slot

When you add a rebuild/migrate or verify task schedule, you specify the day of the week, time, and duration for the task. For self-test schedules, you specify day and time, but not duration. (Duration is not required for self-tests.)

Depending on the schedule and system workload, background tasks may require more than one scheduled duration to complete.

To add a task schedule slot

1 Choose **Management > Schedule** from the menu bar.

The Scheduling page appears, showing the schedule for Rebuild/Migrate Tasks.

2 To view Verify Tasks or Self-test Tasks, select it from the drop-down list at the top of the page.

3 Scroll to the section of the Scheduling page that shows the task you want to add.

4 In the fields at the bottom of the section, select the Day, Time, and Duration for the task.

5 Click the **Add New Slot** button.

The page refreshes and the new schedule is added to the list.

Note: The scheduled tasks can be added in any order. For example a new task scheduled for Tuesday (slot-2) will preempt the task originally scheduled for Wednesday (slot-1).

Selecting Self-tests to be Performed

For 3ware RAID controllers older than the 9690SA, two self-tests can be set: one to check whether UDMA Mode can be upgraded, and another to check whether SMART thresholds have been exceeded. For the 9690SA, you can only check the SMART thresholds for drives. (For more information about these self-tests, see the 3DM Reference section, “Scheduling page” on page 202.)

Initially, these tests are set to run every 24 hours. You can change the schedule for when they are run, and you can disable the tests, if you prefer not have to have them performed.

Note: These tasks will only be run during scheduled times if they are checked in the **Schedule Self-tests** section of the Scheduling page. If neither of the tasks is checked, self-tests will never run, even if you have scheduled time slots set.

To select self-tests to be performed

1 Choose **Management > Schedule** from the menu bar.

The Scheduling page appears, showing the schedule for Rebuild Tasks.

2 Select Self-test Tasks from the drop-down list at the top of the page.

3 Check the boxes next to the self-tests you want to be performed.

To disable self-tests

Unlike scheduling of rebuilds and verifies, scheduling of self-tests is always enabled.

To disable self-tests you must either remove all schedule times, or uncheck the tests listed in the **Tasks** column.

10

Maintaining Your Controller

This section contains instructions for how to perform tasks that help you maintain your controller, including:

- Determining the Current Version of Your 3ware Driver
- Updating the Firmware and Driver
- Downloading the Driver and Firmware
- Updating the Firmware Through 3DM 2
- Viewing Battery Information
- Testing Battery Capacity

Determining the Current Version of Your 3ware Driver

You can view controller and driver information in several different ways:

- Using 3DM 2 you can see both the driver and firmware versions (see the “Controller Summary page” on page 187)
- Using 3BM you can see the firmware version (see “Displaying Information About the Controller and Related Devices” on page 56)
- Using the CLI you can see both the driver and firmware versions (see *3ware SAS/SATA RAID Controller CLI Guide*)
- Under Linux, you can type the following command if you have a 2.4 kernel or earlier:

  ```
  cat /proc/modules/scsi/3w-9xxx/*
  ```

  where the asterisk (*) represents controller number and “9xxx” represents the type of the controller.

  If you have a 2.6 kernels with sysfs, type the following command:

  ```
  cat /sys/class/scsi_host/<hostid>/stats
  ```

  where <hostid> is usually host0, unless other SCSI devices are available, in which case it may be host1 or higher.

If you have a 2.6 kernel without sysfs, type the following command:

```
dmesg | grep 3w
(dmesg can also be used with earlier kernel versions.)
```

- Under Windows, you can follow the first 5 steps under “Updating the 3ware Driver Under Windows XP” on page 165.

Updating the Firmware and Driver

Important: Updating the firmware can render the device driver and/or management tools incompatible. Before you update the firmware on your controller, please follow these recommendations:

1) Back up your data.

2) Make sure you have a copy of the current firmware image so that you can roll back to it, if necessary.

3) Close all applications.

This chapter details several ways to update the firmware and driver for the 3ware RAID controller, depending upon operating system.

Before starting the update of either driver or firmware, you will want to make sure you have the latest files. For details, see “Downloading the Driver and Firmware” on page 158.

To update the firmware

- All operating systems can do so through 3DM. For details, see “Updating the Firmware Through 3DM 2” on page 159.
- All operating systems can do so through CLI. For details, see *3ware SAS/SATA RAID Controller CLI Guide*.
- Windows users can update the firmware along with the driver by using the Update Utility. For more information, see “Updating the 3ware Driver and Firmware Under Windows” on page 160.
- Linux users can use a command-line utility. For details, see “Updating the Firmware Under Linux” on page 174.

To update the driver

- Windows users can update the driver along with the firmware by using the 3ware Update Utility. For more information, see “Updating the 3ware Driver and Firmware Under Windows” on page 160.
- Windows users can also update only the driver through Windows Device Manager. For details, see “Updating the 3ware Driver Under Windows XP” on page 165.

- Linux users can update the driver at the command line. For details see:
  - Updating the 3ware Driver Under Red Hat or Fedora Core
  - Updating the 3ware Driver Under SuSE
  - Updating the Firmware Under Linux

Downloading the Driver and Firmware

You can download the latest drivers and firmware from the 3ware website, at http://www.3ware.com/support.

Note: Information in this section applies to updating drivers and firmware for the 9690SA controllers. The 3ware website also allows you to download drivers for other 3ware controller models and associated release notes.

For Windows, the firmware and driver can be installed from the Windows driver download, which contains 3wUpdate.exe. When you run the update utility, you can choose to update both the driver and the firmware, or only the driver.

For Linux, updating the driver and updating the firmware are done separately. You can download them individually from the website.

Note: For Linux, do not use the driver from the external Linux distribution as it is older than the currently supported driver. Instead, use the driver from the 3ware CD or from the 3ware web site.

To download the driver or firmware

1 On the 3ware website (www.3ware.com), navigate to **Service and Support** > **Software Downloads**.

2 Click **Download Released Software**.

3 Select your product series and then the model of your controller.

4 Select Driver or Firmware as the item to download.

5 Select the Operating System you are using.

6 Click **Next**.

7 When details about the download you requested appear, click the link for the item you want to download.

Depending on the item you selected, you may see either .zip (for Windows) or .tgz (for Linux) files to download.

Note: If using Winzip or another Windows utility to extract the Linux file, use the.zip version instead of the .tgz version. Otherwise the files will not be compatible with Linux.

8 Read and agree to the license agreement that appears.

9 Click **Save** to save the file to disk.

10 Uncompress the file to extract the driver or firmware files to a local directory. (Note that the firmware will not fit on a floppy diskette.)

(Make note of the absolute path to the local directory.)

11 Turn to the driver section for your operating system:

- For Windows, turn to page 165
- For RedHat Linux, turn to page 171
- For SuSE Linux, turn to page 172

Or, to update the firmware, turn to

- "Updating the Firmware Through 3DM 2" on page 159 (for any operating system with a Windowing user interface)
- "Updating the Firmware Under Linux" on page 174 (for command line instructions)

Updating the Firmware Through 3DM 2

You can use 3DM 2 to update the 3ware RAID controller firmware for any operating system that has a graphical user interface such as Windows or X Windows.

To update the firmware through 3DM

1 Download the firmware update from the 3ware website. For details, see "To download the driver or firmware" on page 158.

2 In 3DM 2, navigate to **Management > Controller Settings**.

3 In the **Update Firmware** section of Controller Settings page, browse to the location where you have saved the downloaded firmware update. The update name will be something like `prom`*`xxx`*`.img`.

4 Click **Begin Update**.

The Compatibility Information window appears.

5 Click **Proceed Update**.

The 3ware RAID controller firmware is updated.

Updating the 3ware Driver and Firmware Under Windows

You can update both the driver and the firmware under Windows, using the utility 3wUpdate.exe. This utility is included with the driver and firmware files when you download them.

If you only need to update the driver, you can either use the update utility as described below, or you can update it through the Windows Device Manager, as described under “Updating the 3ware Driver Under Windows XP” on page 165.

When you use the update utility, you bypass the device driver screens that you see when you update just the driver through Windows Device Manager.

Note: At the end of this process, you may need to restart the system. Restarting is always required if you update the firmware. In addition, if you boot from a unit on a 3ware RAID controller, updating the driver will require that you restart the system.

To update the 3ware driver and firmware using the update utility

1 Download and extract the driver files, as described under “Downloading the Driver and Firmware” on page 158.

2 Backup any critical data prior to updating the 3ware driver.

3 Log in to your system as system administrator.

4 Locate the folder that contains the driver files you extracted in step 1.

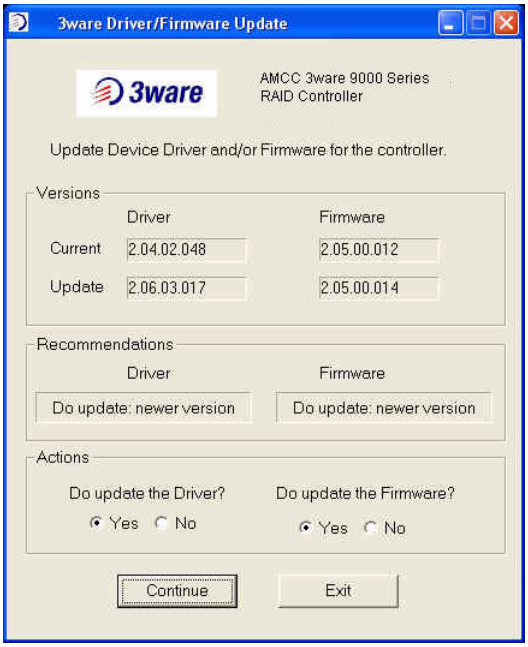
5 Double-click on the file `3wUpdate.exe`.

You see a progress dialog box while the update utility checks your system for the driver and firmware versions presently installed.

Figure 70. Update Utility Progress Dialog (System Check)

When the 3ware Driver/Firmware Update dialog box appears, it shows available updates for the device driver and for the firmware.

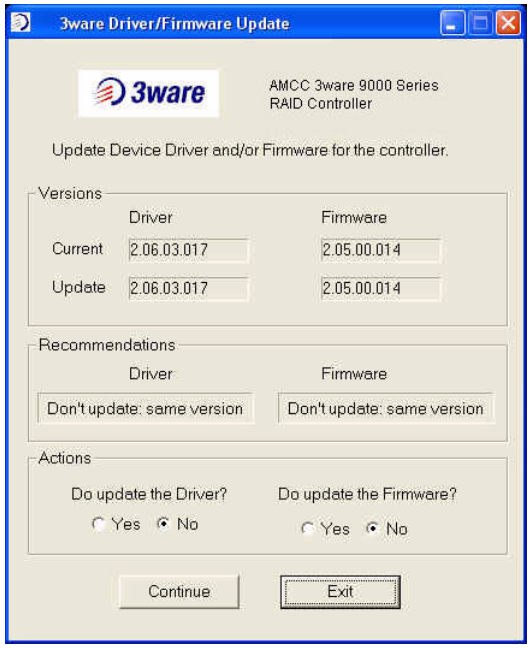
Figure 71. Update Utility Showing Available Drivers



The updater tells you whether newer updates are available, and makes recommendations for whether you should update.

If either your driver or firmware is current, the screen reflects that.

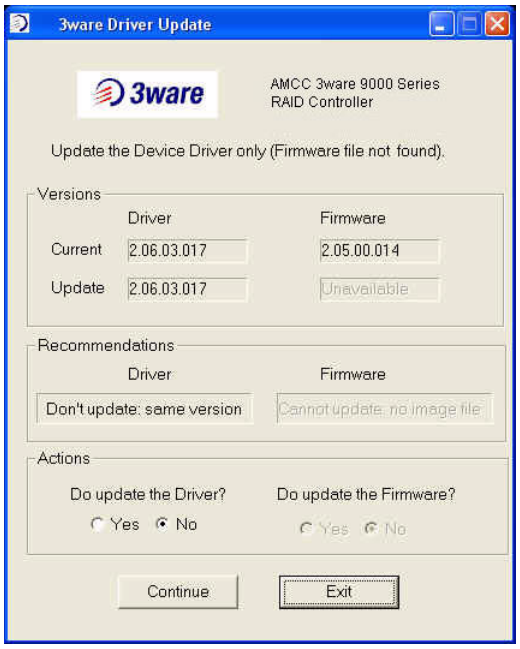
Figure 72. Update Utility Showing Drivers Already Current



In this example, both the driver and firmware are already current on the system, so the recommendation is not to update either one.

If the firmware image is not found with the driver files, the 3ware Driver/ Firmware Update dialog box will show only the driver as available.

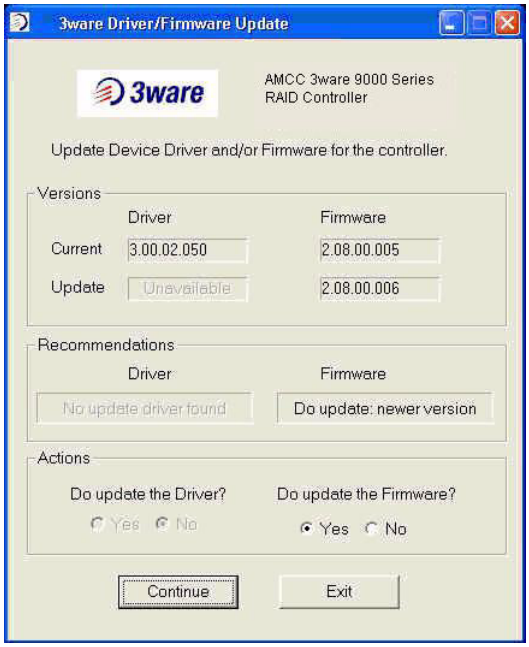
Figure 73. Update Utility Showing Only Driver Available



Only the driver is available, because the firmware image was not found.

If the driver is not found, the 3ware Driver/Firmware Update dialog box will show only the firmware as available.

Figure 74. Update Utility Showing Only Firmware Available



Only the firmware is available, because the driver image was not found.

Note: If you have multiple controllers in your system, your screen will look slightly different, so that you can update the firmware for one or all controllers. For details, see “Using the Update Utility With Multiple Controllers” on page 164

6 In the Action section of the dialog, make any changes to what will be updated and click **Continue** to install your selections.

During the update, the driver installs on your local drive. The firmware will first download and then will flash a new image to the controller.

You will see either one or two progress dialog boxes, depending on what is being installed. Progress is shown during:

- Driver installation
- Firmware download and flashing of the controller

Warning: Do not power off the system while the firmware is being flashed. Doing so will render the controller unusable.

7 If a dialog box prompts you to restart or power-cycle your computer, click **Yes** to do so.

(If you were working from a driver diskette, be sure to remove the floppy diskette before Windows starts again.)

Figure 75. Dialog Prompting for Restart

8 If the driver you are installing is unsigned, you will receive a message to that effect.

To complete the installation with an unsigned driver, click **OK**.

9 If a final message box confirms that the process is complete, click **OK**.

(This message appears if you do not need to restart your computer.)

Figure 76. Dialog Indicating Update Complete

Using the Update Utility With Multiple Controllers

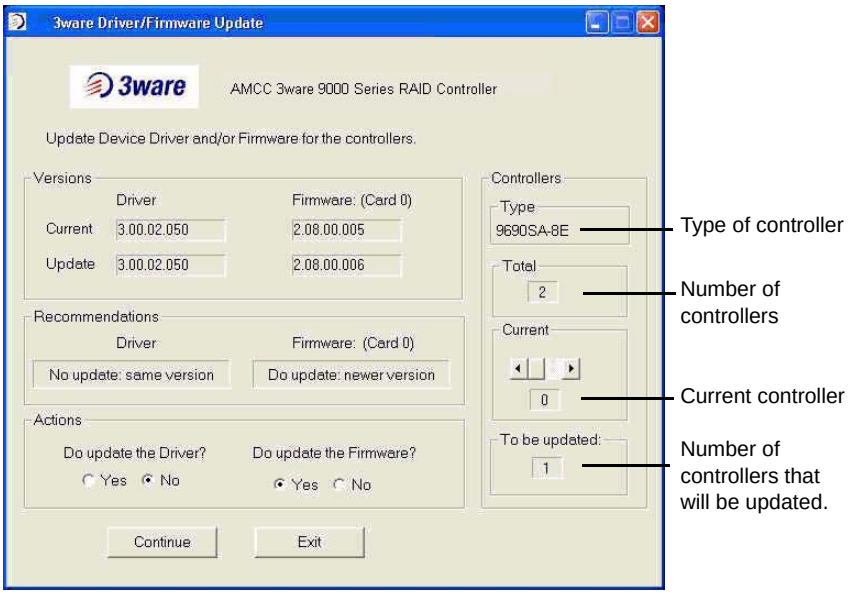
When your system has multiple 3ware RAID controllers installed, the update utility lets you update the firmware on any or all of the installed controllers.

To update the firmware on multiple controllers

1 Follow steps 1 through 5 above, under "Updating the 3ware Driver and Firmware Under Windows" on page 160.

When the 3ware Driver/Firmware Update dialog box appears, it lists the number of controllers in your system, shows available updates for the device driver, and available firmware updates for the first controller.

Figure 77. Show Update Utility Showing Available Drivers



2 Use the scroll arrows under "Current" Controller to see firmware recommendations for each controller on your system.

3 For each controller, review the option for whether the firmware should be updated, and change it if appropriate.

4 Continue with step 6 above, in the procedure “Updating the 3ware Driver and Firmware Under Windows.”

Updating the 3ware Driver Under Windows XP

If you prefer, you can update the 3ware driver through the Windows Device Driver Manager, instead of using the Update Utility described above.

To update the 3ware driver under Windows XP

(Note that during this process, you will step through driver installation wizards twice.)

1 Download and extract the driver files, as described under “Downloading the Driver and Firmware” on page 158.

2 Backup any critical data prior to updating the 3ware driver.

3 Log in to your system as system administrator.

4 From the **Start** menu, open the **Control Panel** window.

5 In the **Control Panel** window, double-click on the **System** icon.

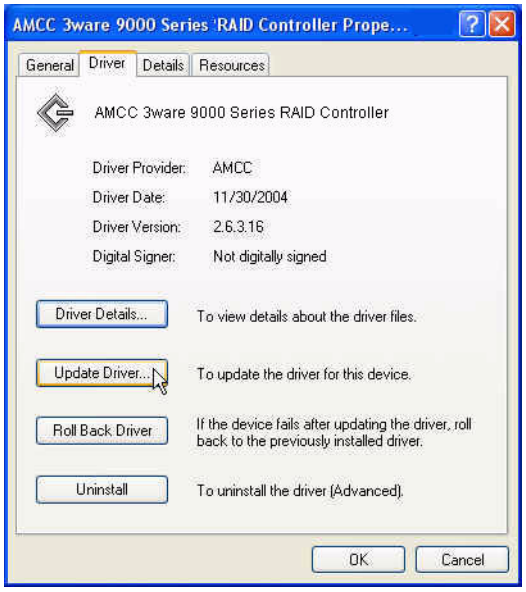
6 Click on the **Hardware** tab and then click on the **Device Manager** tab.

7 Open the **SCSI and RAID Controllers** selection.

8 Locate and double-click on the applicable **3ware Serial ATA RAID Controller**. The **3ware 9000 Series ATA RAID Controller Properties** dialog box appears.

9 Click the **Driver** tab (Figure 78).

Figure 78. 3ware Serial ATA RAID Controller Properties Dialog



10 Click the **Update Driver…** button.

11 If your system has Windows XP Service Pack 2, the first screen asks whether you want to connect to Windows Update.

Select “No, not this time” and click **Next**.

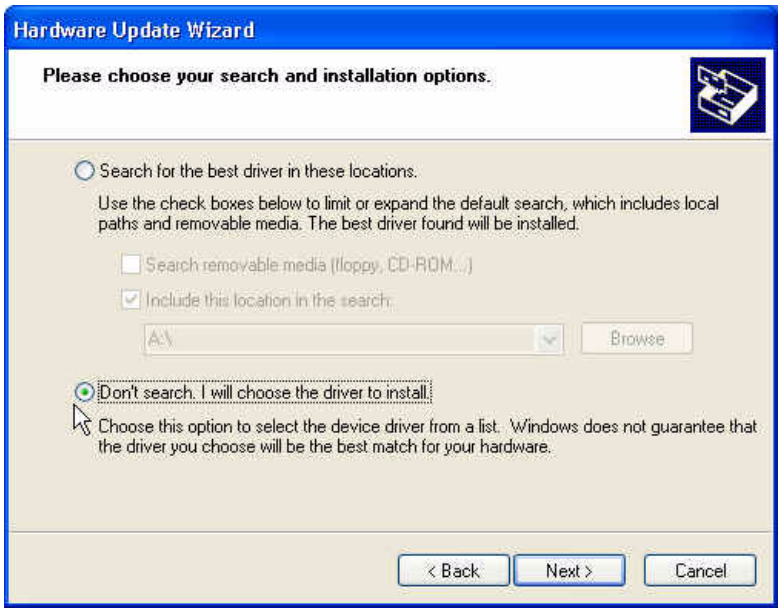
Figure 79. Windows XP Service Pack 2 Windows Update Query

12 When you reach the **Hardware Update Wizard** screen shown below, select “Install from a list or specific location (Advanced)” and then click **Next**.

Figure 80. Upgrade/Install Device Driver Wizard

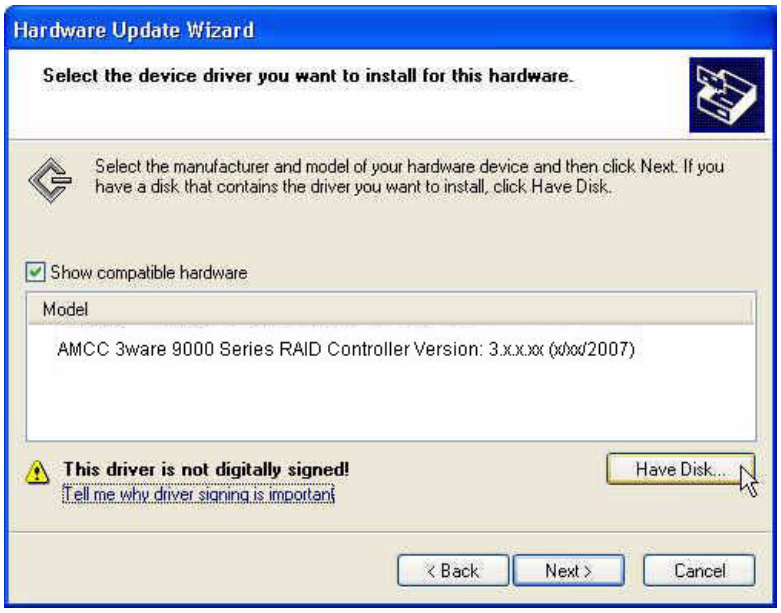
13 At the next screen (Figure 81) choose “Don’t search. I will choose the driver to install” and click **Next**.

Figure 81. Search for Driver Screen



14 When the **Select the Device Driver** screen appears (Figure 82), click the **Have Disk…** button.

Figure 82. Select the Device Driver Screen



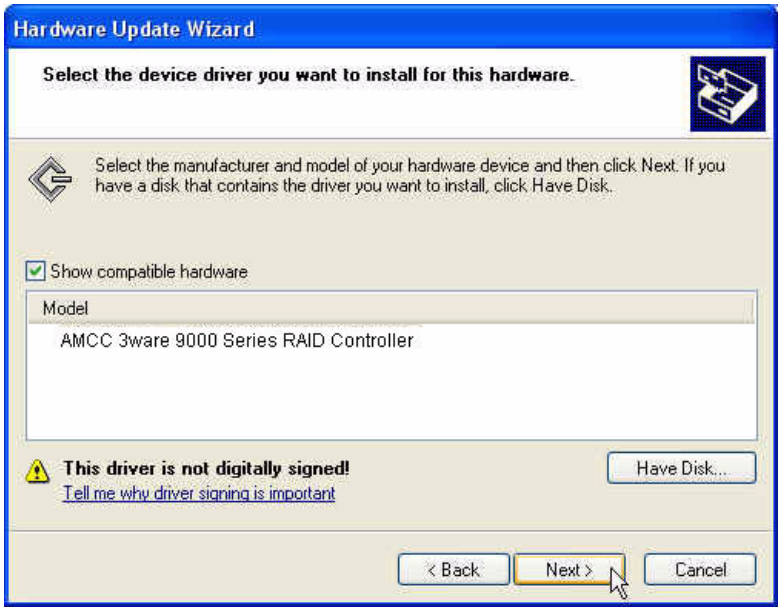
15 When the **Install from Disk** dialog box appears (Figure 83), enter the correct path name to the driver. If you created a driver diskette, insert it now. (The path will be A: if you are using a diskette in the A drive.)

Figure 83. Install From Disk Dialog Box

16 When the **Select the Device Driver** dialog box reappears, select the appropriate driver (Figure 84) and click **Next**.

Be sure to select the correct driver name, otherwise the driver upgrade will not be successful.

Figure 84. Select a Device Driver



The wizard begins installing the driver. You will see a progress box during installation.

17 If the **Digital Signature Not Found** screen appears, click **Yes** to continue and follow the instructions to complete the driver installation.

18 When the **Completing the Hardware Update Wizard** screen appears, click **Finish**.

19 If you are prompted to restart the system, do so.

Shortly after clicking **Finish**, or after the machine reboots, the first screen of the Hardware Update Wizard appears again, informing you that Windows has found new hardware.

If you are using Windows XP Service Pack 2, the screen asks whether you want to connect to Windows Update (Figure 85).

Figure 85. Found New Hardware Screen

20 Choose “No, not this time” and click **Next**.

At the next screen, leave the selection as “Install the software automatically.” Click **Next** and follow the prompts on the screen.

21 When the second **Completing the Found New Hardware** screen appears, click **Finish**.

Figure 86. Completing Found New Hardware Wizard

Updating the 3ware Driver Under Red Hat or Fedora Core

The following steps describe how to update the 3ware driver under Red Hat.

Note: Pre-compiled, tested, and supported drivers are no longer available for older RedHat or Fedora Core releases using the 2.4 kernel. The source code is still available (for a limited time) if a newer driver is still needed. Check the release notes for more details regarding supported operating systems

Backup your original driver before updating in case you need to revert back to it. However, you will not be able to revert back to the original driver if you are booting from that unit.

To update the 3ware driver under Red Hat

1 Download and extract the driver, as described under “Downloading the Driver and Firmware” on page 158.

2 Backup any critical data prior to updating the 3ware driver.

3 Change the directory to the location with the extracted driver.

4 Copy the files to the appropriate directory.

(In the commands below, replace <version> with the applicable Red Hat or Fedora Core version, such as ws4_u4 or fc5, and replace <kernel string> with the applicable kernel, for example 2.6.15-x)

Note: The name of the module you will copy (`3w-9xxx.*`) varies, depending on the kernel; however you will always copy it to a file named 3w-9xxx.ko for 2.6 kernels

For Red Hat or Fedora Core Uniprocessor

```
cp <version>/3w-9xxx.ko /lib/modules/
<kernel string>/kernel/drivers/scsi/3w-9xxx.ko
```

For Red Hat SMP

```
cp <version>/3w-9xxx.smp /lib/modules/
<kernel string>/kernel/drivers/scsi/3w-9xxx.ko
```

For Red Hat Bigmem

```
cp <version>/3w-9xxx.big /lib/modules/
<kernel string>/kernel/drivers/scsi/3w-9xxx.ko
```

For Red Hat Hugemem

```
cp <version>/3w-9xxx.hug /lib/modules/
<kernel string>/kernel/drivers/scsi/3w-9xxx.ko
```

5 **For 2.4 Kernels**, add the following line to `/etc/modules.conf`:

```
alias scsi_hostadapter 3w-9xxx.ko
```

For 2.6 Kernels, add the following line to `/etc/modprobe.conf`.

```
alias scsi_hostadapter 3w-9xxx
```

6 Complete the upgrade by upgrading the initial ramdisk.

Change the directory to the boot directory:

```
cd /boot
```

Run mkinitrd by entering the following:

(In the commands below, replace <kernel string> with the applicable kernel, for example 2.4.20-8)

For Red Hat or Fedora Core Uniprocessor

```
mkinitrd –v –f initrd-<kernel string>.img <kernel string>
```

For Red Hat SMP

```
mkinitrd –v –f initrd-<kernel string>smp.img <kernel string>smp
```

For Red Hat Bigmem

```
mkinitrd –v –f initrd-<kernel string>bigmem.img <kernel string>bigmem
```

For Red Hat Hugemem

```
mkinitrd –v –f initrd-<kernel string>hugmem.img <kernel string>hugmem
```

7 If you are using lilo, run lilo to update to the boot loader.

You should see a printout of kernels that are able to boot on this system after running lilo.

Updating the 3ware Driver Under SuSE

The following steps describe how to update the 3ware driver under SuSE.

Note: Pre-compiled, tested, and supported drivers are no longer available for older SuSE releases using the 2.4 kernel. The source code is still available (for a limited time) if a newer driver is still needed. Check the release notes for more details regarding supported operating systems.

Backup your original driver before updating in case you need to revert back to it. However, you will not be able to revert back to the original driver if you are booted from that unit.

To update the 3ware driver under SuSE

1 Download and extract the driver, as described under “Downloading the Driver and Firmware” on page 158.

2 Backup any critical data prior to updating the 3ware driver.

3 Change the directory to the location with the extracted driver.

4 Copy the files to the appropriate directory.

(In the commands below, replace <version> with applicable SuSE version, such as su10)

Replace <kernel string> with applicable kernel (i.e.: 2.6.16.x)

For SuSE Uniprocessor (2.6 kernels)
`cp <version>/3w-9xxx.ko /lib/modules/<kernel string>/kernel/drivers/scsi/3w-9xxx.ko`

For SuSE SMP (2.6 kernels)
`cp <version>/3w-9xxx.smp /lib/modules/<kernel string>/kernel/drivers/scsi/3w-9xxx.ko`

For SuSE high memory systems (2.6 kernels)
`cp <version>/3w-9xxx.big /lib/modules/<kernel string>/kernel/drivers/scsi/3w-9xxx.ko`

5 Run `/sbin/depmod -a`

6 Make sure the `file /lib/modules/<kernel string>/modules.dep` contains an entry for 3w-9xxx. If not, add it after the `3w-xxxx` entry.

7 Complete the upgrade by upgrading the initial ramdisk. (Skip to step 10 if you prefer to use insmod 3w-9xxx.ko, instead.)

Make sure the file /`etc/sysconfig/kernel`
contains the following line:
`INITRD_MODULES=”3w-9xxx”`

Note: Other modules may be listed before or after 3w-9xxx depending on the installation. You may see entries likes reiserfs, ext3 or scsi_mod. Leave these entries alone, if present, as the system may need them to boot properly.

8 Run mkinitrd.

9 If you are using lilo, use lilo to update to the boot loader.

You should see a printout of kernels that are able to boot on this system after running lilo.

10 Reboot, if booted from the 3ware controller. Otherwise, continue with step 11.

The driver is now updated.

11 Stop the current driver module, if loaded:

```
rmmod 3w-9xxx
```

12 Load the new driver module:

```
modprobe 3w-9xxx
```

If the new driver fails to load properly, confirm that you used correct driver. If your kernel or SuSE version is not supported, you will need to compile your own driver. For more information, see knowledgebase article 14546 (http://www.3ware.com/KB/article.aspx?id=14546).

Updating the Firmware Under Linux

The following steps describe how to update the firmware under Linux using the utility tw_update. (You can also update the firmware through 3DM. For details, see “Updating the Firmware Through 3DM 2” on page 159.) The PROM images that are installed when you update the firmware include any 3BM and BBU firmware updates.

Note: The tw_update utility will only be available for a limited time because tw_update is being replaced by the firmware update feature in 3DM and CLI.

To update the firmware under Linux

1 Download and extract the firmware, as described under “Downloading the Driver and Firmware” on page 158.

2 Backup any critical data prior to updating the 3ware firmware.

3 Change the directory to the location with the extracted files, which include tw_update.

Run the tw_update utility:

4 `./tw_update fw=/mnt/fw/9xxxSA/prom0008.img`

The utility shows the version of the driver and firmware included in the utility, the versions currently installed on your controller, and recommends whether to upgrade the firmware or not.

```
Warning: We strongly recommend backing up your data before updating
the firmware. Updating the firmware can render the device driver
and/or management tools incompatible. It is recommended to have
a copy of current firmware image for rollbacks.

Examining compatibility data from firmware image and /c0 ...

New-Firmware        Current-Firmware    Current-Driver    Current-API
-------------------------------------------------------------------------
FE9X 3.0x.xx.xxx    FE9X 3.0x.xx.xxx     2.xx.xx.xxx      2.xx.xx.xxx
```

```
Both API and Driver are compatible with the new firmware.
Recommendation: proceed to update.

Given the above recommendation...
Do you want to continue? Y|N [N]: y
```

5 If the firmware is newer and the recommendation is to proceed, type `Y` and press Enter.

```
Downloading the firmware from file /mnt/fw/9xxxSA/
prom0008.img ... Done.
The new image will take effect after reboot.
```

Viewing Battery Information

The Battery Backup Unit (BBU) is an add-on card that can be attached to most 3ware 9000 RAID controllers to supply power from a battery pack in the event of a system power loss. This allows the controller to use write-caching for optimal performance and to preserve data in the event of a system power failure. When fully charged, the battery preserves the contents of the cache memory for up to 72 hours. When power is restored, the cached write data is written to the disks.

You can see information about a battery backup unit attached to your controller in both 3DM 2 and 3BM.

Note: When the BBU status is not “Ready,” write caching is automatically disabled on all units attached to the controller

To view information about a BBU in 3DM 2

- On the menu bar, choose **Monitor** > **Battery Backup**.

  The Battery Backup page appears, on which you can see details and status about the unit. This page is refreshed every 30 seconds.

  For details about the fields on this page, see “Battery Backup page” on page 213.

To view information about a BBU in 3BM

- At the main 3BM screen, tab to the **Information** button and press **Enter**.

  On the pop-up menu, select **Battery Backup** and press **Enter**.

  The Battery Backup Unit screen appears.

  The fields on this screen are the same as those available through 3DM. For details about the fields, see “Battery Backup page” on page 213.

Testing Battery Capacity

Batteries in the BBU need to be replaced periodically. A battery test should be run every four weeks in order to get a reliable estimate of battery capacity, and to determine when it needs to be replaced.

The battery test is used to measure the battery's capacity to back up write data. In order to make a reliable estimate of battery capacity, the BBU pre-charges the battery before it proceeds with a full discharge cycle. The battery is automatically charged again after the test completes. The whole process usually takes between 8 and 12 hours.

While running the battery test and until charging is completed, write cache is temporarily disabled.

- For how to replace the battery, see the installation guide that came with your controller. Documentation is available online at:

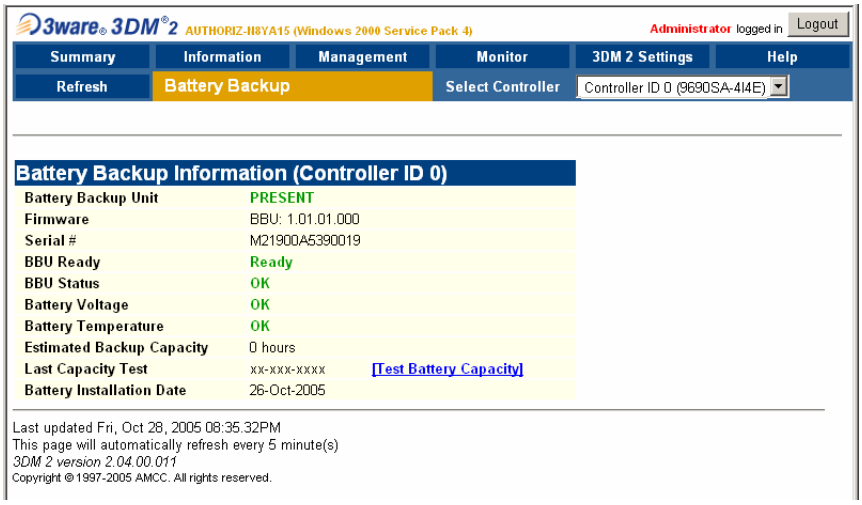
  http://www.3ware.com/support/userdocs.asp

To test the battery in a BBU in 3DM 2

1 On the menu bar, choose **Monitor** > **Battery Backup**.

2 On the Battery Backup page, click the **Test Battery Capacity** link.

Figure 87. Battery Backup Information Screen in 3DM

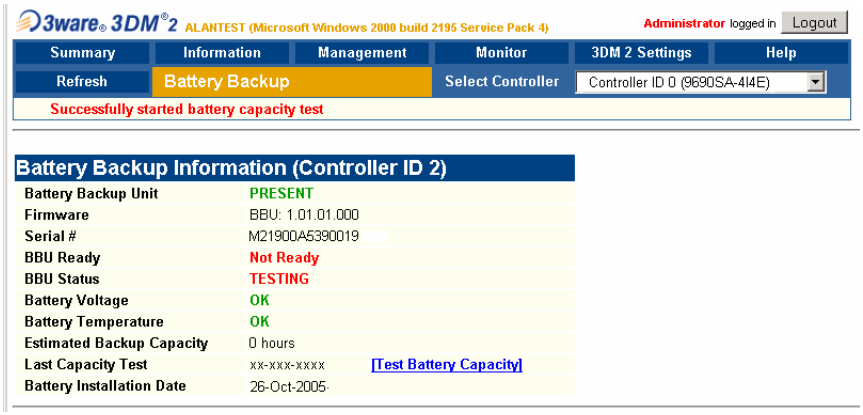


3 When a message cautions you that testing the battery will disable the BBU for up to 24 hours, click **OK** to continue.

After the battery test starts, you will see the voltage start dropping; eventually the battery voltage will say "LOW". This is part of the battery test. After the voltage drops to a point, it will start charging again, and the

status will change to “Charging.” Eventually, the battery voltage will say “OK” again.

Figure 88. BBU Information Screen While Battery is Testing

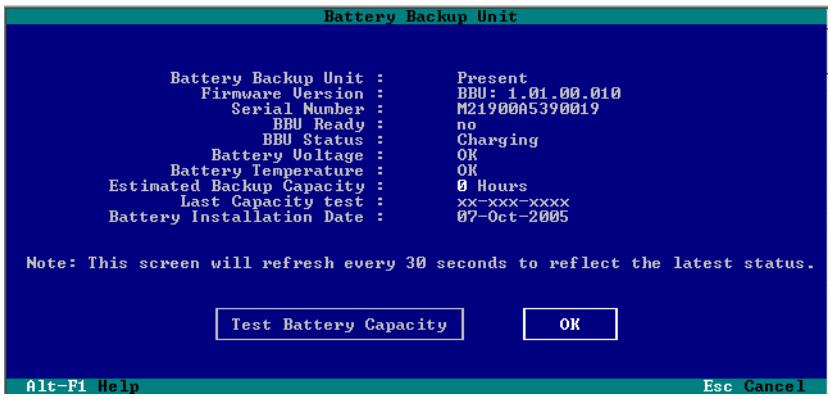


To test the battery in a BBU in 3BM

1 At the main 3BM screen, tab to the **BBU** button and press **Enter**.

2 Tab to **Test Battery Capacity** and press **Enter**.

Figure 89. Battery Backup Information Screen in 3BM



11

Managing an Enclosure

3ware enclosure management features let you view the status of enclosure hardware, such as fans, power supplies, and temperature sensors through 3DM, and locate individual hardware components by blinking LEDs associated with them.

Enclosure management features in 3ware software are available for enclosures with expanders that support SCSI Enclosure Services 2 (SES-2).

Note: The SAFTE (SCSI Accessed Fault Tolerant Enclosure) specification is not supported at this time.

A list of supported enclosures is available at http://www.3ware.com/products/sys_compatibility.asp

Depending on the manufacturer of your enclosure, you may see variations in the features supported by your enclosure from the ones described in this chapter. For details about what features are supported, refer to the documentation for your enclosure.

This chapter describes how to view and locate enclosure-specific hardware. For information about identifying drives in an enclosure, see “Locating a Drive by Blinking Its LED” on page 131.

Details about enclosure management are organized into the following topics:

- Viewing a List of Enclosures
- Checking Enclosure Component Status
- Locating a Specific Enclosure Component
- Downloading an Enclosure Diagnostic Log

Viewing a List of Enclosures

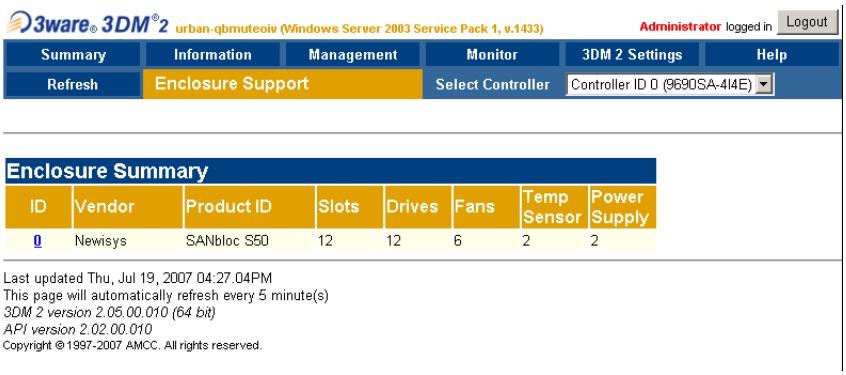
If you have multiple enclosures attached to your 3ware RAID controller, you can see a list of them.

To see a list of enclosures in 3DM

- Choose **Monitor > Enclosure Support** from the menu.

  The Enclosure Summary screen appears.

Figure 90. Enclosure Summary page



  To see details about a particular enclosure, click the link in the ID column. (See “Checking Enclosure Component Status” on page 181)

To see a list of enclosures in 3BM

1 On the main 3BM screen, **Tab** to **Information** and press **Enter**.

2 On the pop-up menu, select **Enclosures** and press **Enter**.

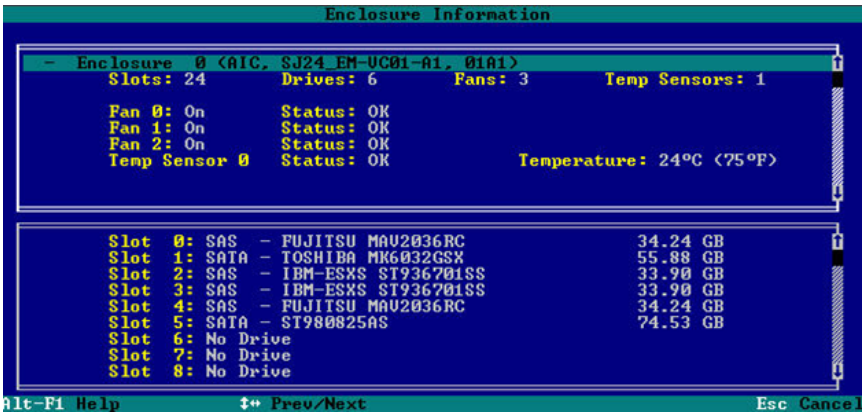
  The Enclosure Information page appears, with information about enclosure components displayed in the top section, and details about the slots in the selected enclosure displayed in the bottom section.

  For an explanation of statuses for the different components, see the status topics starting under “Fan Status” on page 183.

3 On the Enclosure Information page, use the arrow keys to move from one enclosure to another. You can use the - and Shift+ keys to hide or show details about an enclosure, if desired.

  Tip: You can scroll both sections of the Enclosure Information page to bring additional enclosure information or enclosures into view. Press **Tab** to move between the two sections.

Figure 91. Enclosure Information page (3BM)



Checking Enclosure Component Status

If your enclosure supports enclosure services, you may be able to check the status of enclosure components such as power supplies, fans, slots, drives, and temperature sensors.

To check the status of components in your enclosure in 3DM

1 Choose **Monitor > Enclosure Support** from the menu.

2 On the Enclosure Summary page, click the blue Enclosure ID link for the enclosure for which you want to see details.

The Enclosure Details page appears.

Explanations of the statuses for the various enclosure components are provided on the next few pages.

Figure 92. Enclosure Details page

To check the status of components in your enclosure in 3BM

When you view the list of enclosures in 3BM, the status information is available on the same screen. For details, see “To see a list of enclosures in 3BM” on page 180.

Fan Status

The following is a list of possible fan statuses:

- **OK.** The fan is optimal and is functioning normally.
- **Off.** The fan is off.
- **Failure.** The fan is present, but is malfunctioning.
- **Not Installed.** There is no fan installed.
- **Unknown.** The status of the fan is not reportable.

Temp Sensor Status

Below is a list of possible temperature sensor statuses.

Note that the temp sensor status indicates the temperature of the enclosure or backplane. Drive temperature, if supported, is available on the Drive Details page.

- **OK.** The temperature sensor is functioning normally.
- **Failure.** The temperature sensor is present, but is malfunctioning.
- **Not Installed.** There is no temperature sensor installed.
- **Unknown.** The status of the temperature sensor is not reportable.
- **Over Temp Warning.** Temperature is higher than normal operating temperature.
- **Over Temp Fail.** Temperature is higher than safe operating temperature.
- **Under Temp Warning.** Temperature is colder than normal operating temperature.
- **Under Temp Fail.** Temperature is lower than safe operating temperature.

Power Supply Status

The following is a list of possible power supply statuses.

- **OK.** The power supply is functioning normally.
- **Failure.** The power supply is present, but is malfunctioning.
- **Off.** The power supply is off.
- **Not Installed.** There is no power supply.
- **Unknown.** The status of the power supply is not reportable.

Slot Summary

The following is a list of possible slot statuses:

- **OK.** The slot is functioning normally.
- **Inserted.** A drive has been inserted in the slot.
- **Ready to Insert.** The slot is ready to accept a drive.
- **Ready to Remove.** The drive in the slot can be removed.

Locating a Specific Enclosure Component

If you have a supported enclosure and the identify feature is supported by your enclosure manufacturer, you can locate power supplies, fans, and temperature sensors by blinking the leds associated with them. This can help you quickly identify which component needs to be checked or replaced. The specific components that can be located in this way will depend on your enclosure.

For details about how to locate a drive by blinking an LED, see “Locating a Drive by Blinking Its LED” on page 131.

To locate a fan, power supply, or temperature sensor

1 Choose **Monitor > Enclosure Support** from the 3DM menu.

2 On the Enclosure Summary page, click the blue Enclosure ID link for the enclosure you are interested in.

3 Check the **Identify** box next to the component you want to locate.

4 Examine the enclosure for the blinking LED.

Downloading an Enclosure Diagnostic Log

The enclosure diagnostic log may be requested by 3ware Customer Support to help troubleshoot problems on your controller. You can download this diagnostic log from the Enclosure Details page.

To download the diagnostic log

1 In 3DM, choose **Monitor > Enclosure Summary** from the menu bar.

2 Make sure the correct controller is displayed in the **Select Controller** field in the menu bar.

3 On the Enclosure Summary page, click the **ID** link of the desired enclosure.

The Enclosure Details page for the selected controller appears.

4 Click on the **Diagnostic Text** link.

5 When the Save or Open dialog box appears, navigate to where you want to save the log and click **OK**.

12

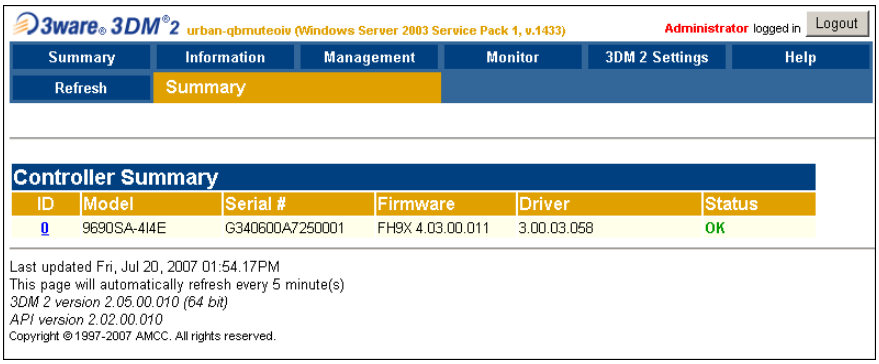
3DM 2 Reference

This section includes details about the fields and features available on the pages you work with throughout 3DM 2. It is organized by 3DM page, as the pages are organized on the 3DM menu bar.

- Controller Summary page
- Controller Details page
- Unit Information page
- Unit Details page
- Drive Information page
- Drive Details window
- Controller Phy Summary page
- Controller Settings page
- Scheduling page
- Maintenance page
- Alarms page
- Battery Backup page
- Enclosure Summary page
- Enclosure Details page
- 3DM 2 Settings page

Controller Summary page

Figure 93. Controller Summary Page



The Summary page appears after you first logon to 3DM, or when you click the Summary link in the menu bar.

This page provides basic information about each 3ware RAID controller in your system. To see details about the units in a controller, click the link in the ID column.

ID. The ID that the operating system assigns to the controller.

Model. The model name of the controller. (The model number is also printed on a sticker on the outside bracket of the controller.)

Serial #. The serial number of the controller. (The serial number is also printed on a sticker on the outside bracket of the controller.)

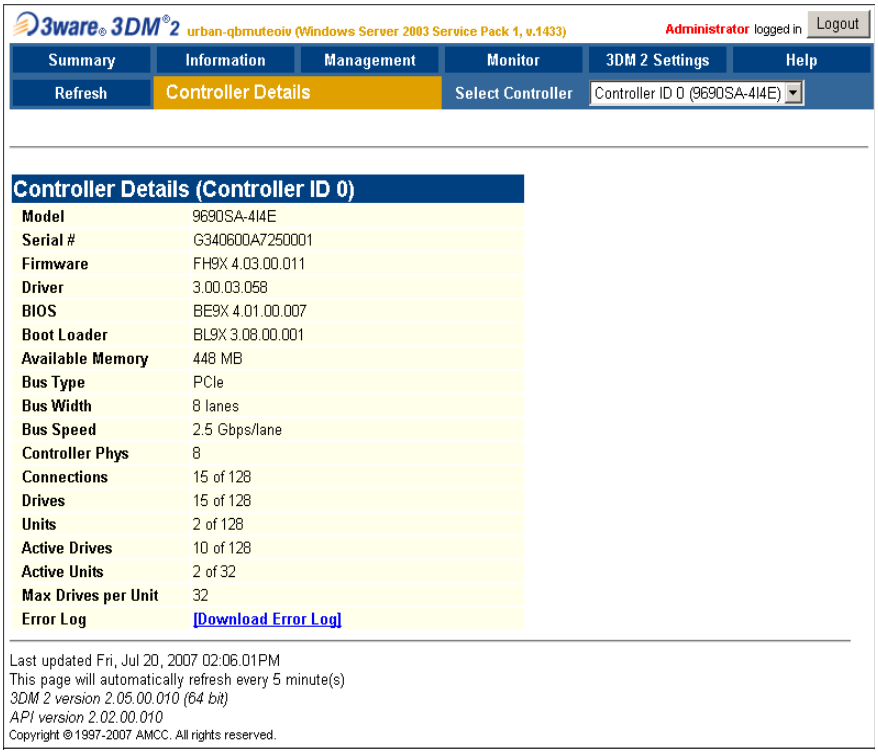
Firmware. The firmware version running on the controller.

Driver. The driver version being used to interact with the controller.

Status. The overall status of the controller. Possible statuses include OK, Warning, Error, and No Units. **Warning** indicates that a background task is currently being performed (rebuilding, migrating, or initializing). **Error** indicates that a unit is degraded or inoperable. If both Error and Warning conditions exist, the status will appear as Error. For more information, see “Checking Unit and Drive Status through 3DM” on page 125.

Controller Details page

Figure 94. Controller Details Page



The Controller Details page appears when you choose **Information > Controller Details** from the menu bar.

This page provides detailed information about the controller specified in the drop-down list on the menu bar.

You can also open or download an error log from this screen.

Model. The model name of the controller.

Serial #. The serial number of the controller.

Firmware. The firmware version running on the controller.

Driver. The driver version being used to interact with the controller.

BIOS. The BIOS version on the controller.

Boot Loader. Boot Loader version on the controller.

Available Memory. The amount of available memory on the controller. In the example above, 448MB is available out of the 512MB installed.

Bus Type. The bus type used on the controller: PCIE.

Bus Width. The bus width used on the controller. This is 8 lanes for the 9690SA controller.

Bus Speed. The speed of the bus used on the controller.

Controller Phys. The number of phys on the controller, regardless of whether each currently has a device connected. The 9690SA controller has 8 phys.

Connections. The number of connections that are presently being used out of the total number possible on the controller.

Drives. The number of drives that are connected to the controller out of the total number of devices possible on the controller.

Active Drives. The number of drives connected to the controller that are in an active unit out of the total number possible on the controller.

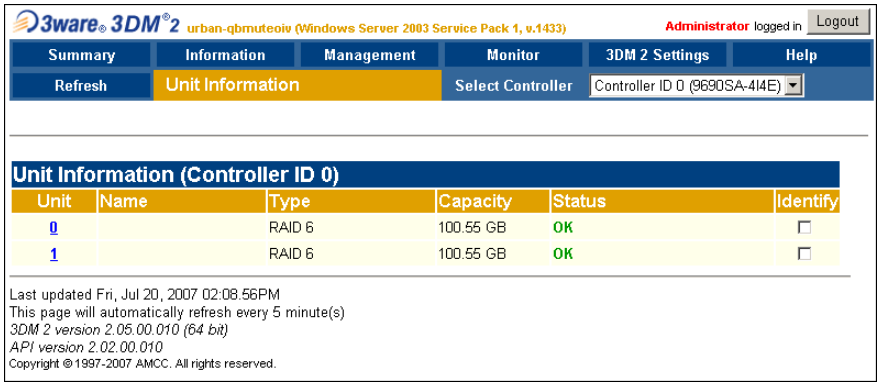
Active Units. The number of units on the controller that are active out of the total number possible on the controller.

Max Drives per Unit. The maximum number of drives that can be in a unit with the present firmware.

Error Log. Provides access to the firmware error log. Click on the **Download Error Log** link to download the firmware error log to your computer. This feature is important when contacting AMCC for support with your controller. It will help AMCC identify the problem you encountered.

Unit Information page

Figure 95. Unit Information Page



The Unit Information page appears when you choose **Information > Unit Information** from the menu bar, or when you click an ID number on the Controller Summary page.

This page shows a list of the units on the current controller and provides summary information about each unit.

To see details about a particular unit, click the link in the Unit # column.

Unit #. The unit number assigned to the unit by the firmware.

Name. If a name has been given to this unit, it shows here. If it is empty, no name has been assigned. You can name your unit in the **Unit Names** section of the **Management > Controller Settings** page.

Type. The type of unit, specified during configuration: RAID 0, RAID 1, RAID 5, RAID 6, RAID 10, RAID 50, Single Disk, or Spare. For details about each of the RAID levels, see “Available RAID Configurations” on page 5.

Capacity. The logical capacity (size) of the unit. (1KB defined as 1024 bytes)

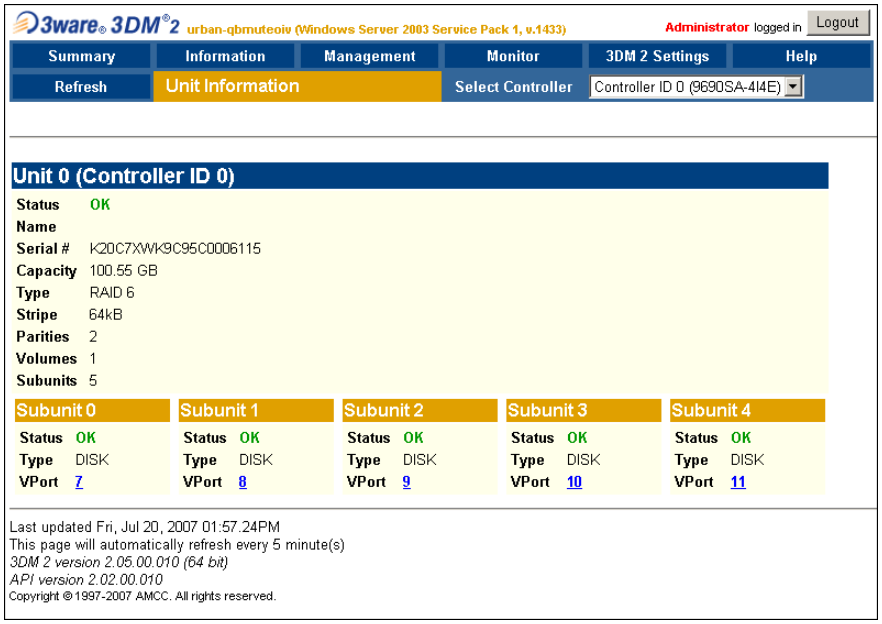
Status. The operational status of the unit: OK, Rebuilding, Initializing, Migrating, Verifying, Degraded, or Inoperable (missing drives). When a unit is Rebuilding, Initializing, Migrating, or Verifying, the percentage (%) complete is also shown. For an explanation of the statuses, see “Unit Statuses” on page 129.

Note: If an asterisk (*) appears next to the status of a unit, there is an error on one of the drives in the unit. This feature provides a diagnostic capability for potential problem drives. The error may not be a repeated error, and may be caused by an ECC error, SMART failure, or a device error. To see if this error condition still exists, rescan the controller; rescanning will clear the drive error status if the condition no longer exists.

Identify. Check this box to cause the LED for the drives associated with this unit to blink in the enclosure. If the box is grayed, identify is not supported.

Unit Details page

Figure 96. Unit Details Page



The Unit Details page appears when you click an ID number on the Unit Information page. Because it is a sub-page of Unit Information, the page title in the menu bar continues to display “Unit Information” even when you view details of a unit.

The Unit Details page shows details about a particular unit. The specific information shown depends on what type of unit it is. For example, details about a RAID 5 unit made up of three subunits, each of which contains one drive, will include details about the unit and each subunit, as shown in Figure 96. However, if the unit is a Single Disk, only information about one disk will be shown.

Details on this page may include all or some of the following information described below.

To see details about a particular drive, click the VPort # (virtual port number). You’ll see a list of all drives, with the drive you selected highlighted.

Status. The operational status of the unit or subunit: OK, Rebuilding, Migrating, Initializing, Verifying, Degraded, or Inoperable (missing drives). When a unit is Rebuilding, Initializing, or Verifying, the percentage (%) complete is also shown. For status definitions, see “Unit Statuses” on page 129.

Name. The name assigned to the unit by an administrator.

Serial #. The serial number of the unit. This number is assigned by the firmware when the unit is created.

Capacity. The total capacity of the unit (capacities of subunits are not shown).

Type. The type of unit or subunit. RAID 0, RAID 1, RAID 5, RAID 6, RAID 10, RAID 50, Single Disk, Spare, or Disk.

Stripe. The stripe size of the unit, if applicable.

Parities. The number of parity drives in the RAID unit.

Volumes. Displays the number of volumes in a unit. This is usually 1. If you created a boot volume on this unit, or if you have a unit on which you have enabled the auto-carving policy, you will see the number of volumes into which the unit has been divided. For more information, see “Using Auto-Carving for Multi LUN Support” on page 78.

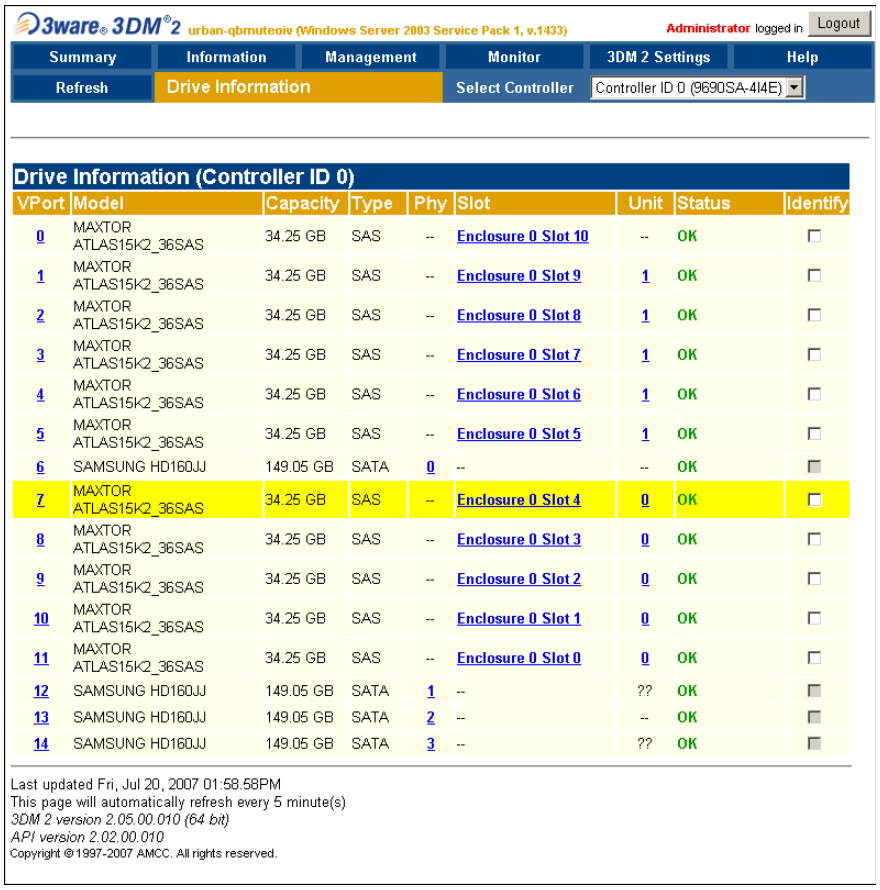
Subunits. If the unit has subunits, details of the subunits are shown.

Note: If an asterisk (*) appears next to the status of a subunit, there is an error on one of the drives in the subunit. This feature provides a diagnostic capability for potential problem drives. The error may not be a repeated error, and may be caused by an ECC error, SMART failure, or a device error. Rescanning the controller will clear the drive error status if the condition no longer exists.

VPort #. If the unit Type is Disk, Single Disk, or Spare, the VPort (Virtual Port) to which the drive is connected is shown. For multiple-drive units, the VPort numbers are shown in the subunits section. The VPort number is a link to the Drive Information page.

Drive Information page

Figure 97. Drive Information Page



The Drive Information page appears when you choose **Information > Drive Information** from the menu bar, or when you click a VPort # on the Unit Details page. If you arrive at this page from the VPort # hyperlink on the Unit Information page, the line showing the VPort # you clicked on is highlighted.

This page shows a list of drives on the current controller and a summary of each one.

To see additional detail about a particular drive in the Drive Details window, including the SMART data, whether command queuing is supported and enabled, and the SATA Link speed, click the link in the VPort # column.

VPort #. The virtual port to which the drive is assigned.

Model. The model of the drive.

Capacity. The physical capacity of the drive. (Note that the capacity as shown on 3DM screen is calculated as 1KB = 1024. This amount may differ from the capacity that is printed on the disk drive, where it typically has been

calculated as 1KB = 1000. Consequently, the capacity of the drive may appear smaller in the 3DM screens. No storage capacity is actually lost; the size has simply been calculated differently for consistency.)

Type. The type of drive: SATA or SAS.

Phy. The number of the controller phy to which the drive is connected. Click the link to go to the Controller Phy Summary page. (For details, see “Controller Phy Summary page” on page 197.)

Slot. The number of the enclosure slot in which the drive is located. Click the link to go to the Enclosure Details page.

Unit. The unit the drive belongs to, if applicable.

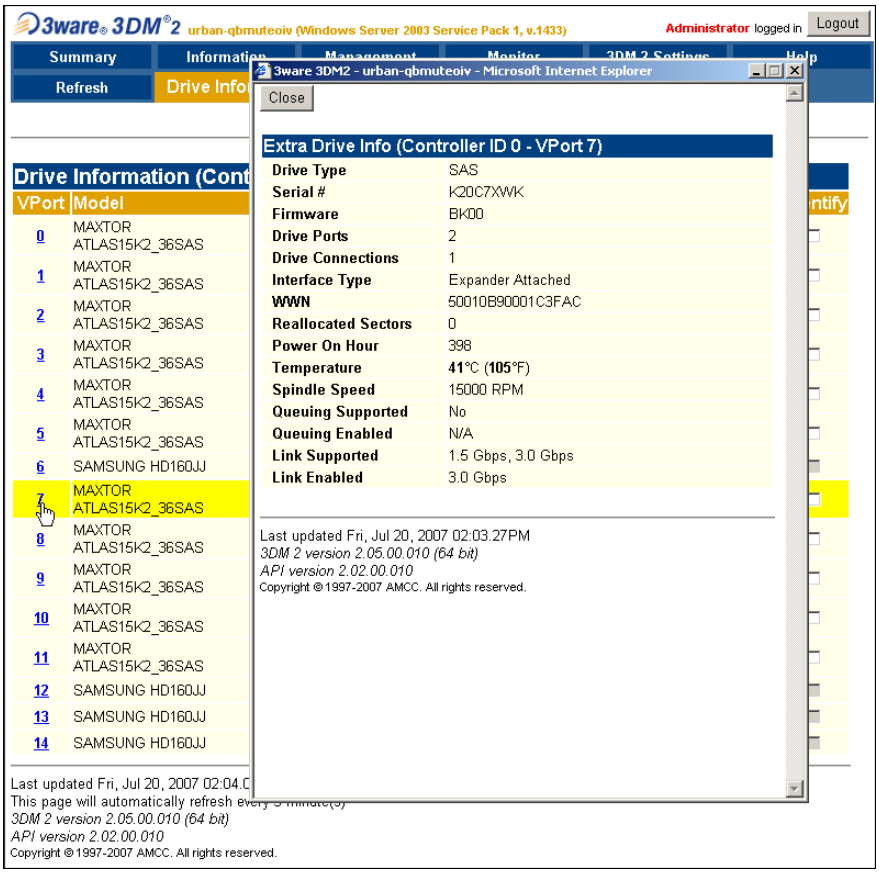
Status. The status of the drive: OK, Not Supported, Not Present, and so forth. If you need help regarding a status displayed here, please contact Technical Support. For more information, see “Drive Statuses” on page 130.

Note: In most cases, the status of the drive will not correspond to the status of the unit, shown on the Unit Information page. Different status information is provided for drives and for units.

Identify. Check this box to cause the LED for this drive to blink in the enclosure. If the box is grayed, identify is not supported.

Drive Details window

Figure 98. Drive Details Page



The Drive Details window displays when you click a VPort # on the Drive Information page.

This Drive Details window shows some Extra Drive Information, including Queuing and SATA Link Speed support, and the SMART data for SATA drives. SMART data is not displayed for SAS drives.

Extra Drive Information

Drive Type. The type of drive: SAS or SATA.

Serial #. The serial number of the drive.

Firmware. The firmware version of the drive.

Drive Ports. The number of physical ports on the drive.

Drive Connections. The number of connections made to the drive ports.

Interface Type. The drive interface, direct or expander.

SAS WWN. The SAS drive's unique World Wide Number.

Reallocated Sectors. The number of sectors that have been re-allocated due to bad sectors on the drive.

Power On Hour. The total number of hours the drive has been powered-on.

Drive Temperature. The temperature of the drive.

Spindle Speed. The drive speed in RPM.

Queuing Supported and **Queuing Enabled.** (Not applicable to SAS drives) SATA-2 drives support NCQ (Native Command Queuing), which can result in increased performance for some applications, usually server-type applications. In order to make use of Native Command Queuing, the feature must be enabled at both the drive and the controller. Not all drives support queuing.

The queuing values in this window indicate whether the feature is supported and enabled at the drive. At the controller level, queuing is enabled or disabled for all drives in a unit on the Controller Settings page.

Link Supported and **Link Enabled.** These fields show the fastest link speed that the disk drive supports and the current link speed.

SMART Data

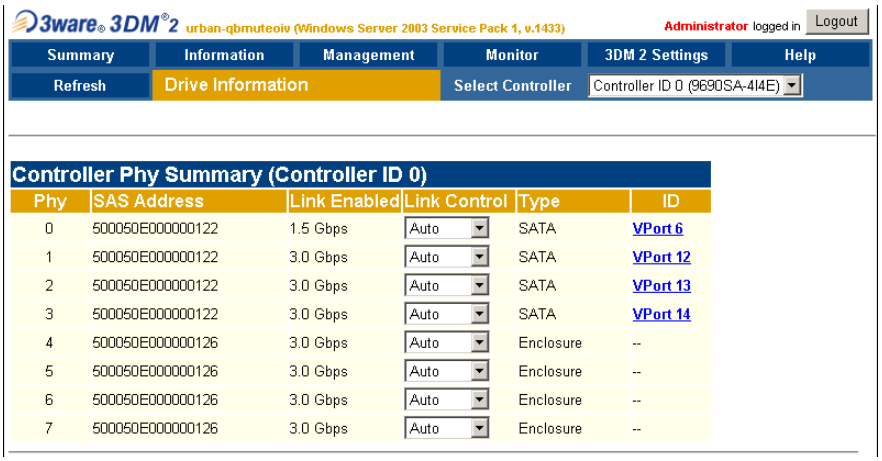
SMART data is displayed as hex values.

Consult your disk drive manufacturer for information on how to interpret the SMART data. The SMART data meaning varies by disk drive manufacturer and model.

SMART data is not presently displayed for SAS drives.

Controller Phy Summary page

Figure 99. Controller Phy Summary Page



The Controller Phy Summary page shows the properties of controller phys.

The Controller Phy Summary page can be accessed in two ways.If you have a direct-attached drive you can access this page from the **Information > Drive Information** page by clicking the phy ID for the drive. If all drives are connected via expanders, navigate to the **Management > Controller Settings** page. Under **Other Controller Settings** click the # link for **Number of Controller Phys**.

Phy. The ID number assigned to the phy connection.

SAS Address. The SAS address of the phy. Phys within each wide port have the same SAS address when they are connected to an enclosure. For directly-connected drives, each phy has a unique SAS address.

Link Enabled. The existing link speed between the controller and the hard drive or enclosure to which it is connected.

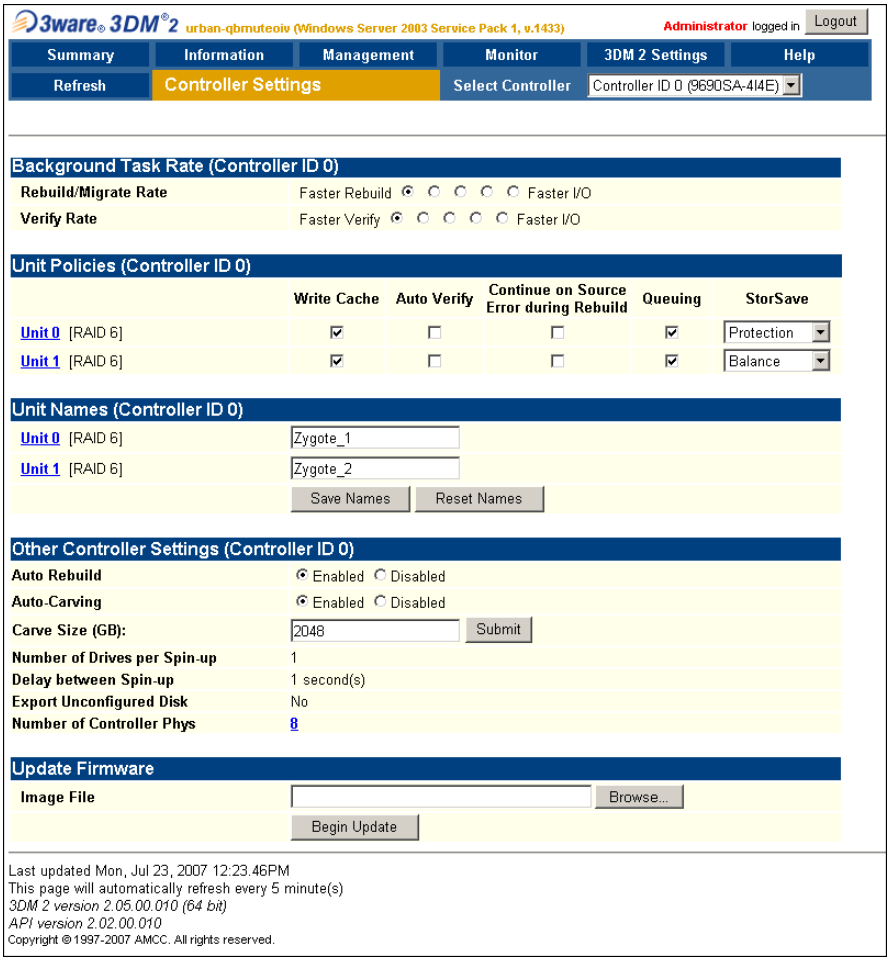
Link Control. Selectable field for setting the link speed between the device and the controller. The options are 1.5 Gbps, 3.0 Gbps, and Auto.The default is Auto. See “Changing the Phy Link Speed” on page 83.

Type. Shows the type of device connected by the phy—either SATA, SAS, or enclosure. A type of SATA or SAS means that the connection is a direct connection to the drive. Enclosure connections are made through an expander.

ID. The VPort address of directly-attached devices. Enclosures do not have VPort numbers, although the drives attached to them do. To find the VPort for a drive in an enclosure, click the ID link to go to the Drive Information page. The drive you selected will be highlighted.

Controller Settings page

Figure 100. Controller Settings Page



The Controller Settings page appears when you choose **Management > Controller Settings** from the menu bar.

This page lets you view and change settings that affect the units on the controller specified in the drop-down list on the menu bar.

There are four main sections on this page:

- Background Task Rate
- Unit Policies
- Unit Names
- Other Controller Settings
- Update Firmware

Background Task Rate

The Background Task Rate fields let you change the balance of background tasks and I/O (reading and writing to disk) performed by the controller.

There are separate settings for Rebuild/Migrate Rate and Verify Rate, Figure 100. The Rebuild/Migrate Rate also applies to initialization. Although the same rate is used for rebuilding, migrating, and initializing, migrating has the highest priority.

The five radio buttons let you set the ratio at which background tasks are performed in comparison to I/O. For additional information, see “Setting Background Task Rate” on page 149.

Unit Policies

You can enable or disable these policies: **Write Cache**, **Auto-verify, Continue on Source Error During Rebuild, Queuing**, and you can select a **StorSave Profile**. 3DM lists each unit on the current controller, and shows you whether the policies are currently enabled or disabled for each unit.

Write Cache. When write cache is enabled, data is stored locally in memory on the drive before it is written to the disk drive media, allowing the computer to continue with its next task. This improves performance. However, in the event of a power failure, the data in the controller's write cache will be lost if you do not have a battery backup unit (BBU) or an uninterruptable power supply (UPS).

For additional information, see “Enabling and Disabling the Unit Write Cache” on page 102.

Auto Verify. When the Auto Verify policy is enabled, a verify task is performed automatically once every 24 hours. This feature is designed to make regular verification of units easier.

If a verify scheduling window has been set up and enabled, then Auto Verify will wait until the scheduled time window to start the automatic verify process.

When Auto Verify is not enabled, verify tasks are only run if you manually request one on the 3DM **Management** page. If a verify scheduling window is set and enabled, then manual verifies will wait until the scheduled time to start.

Continue on Source Error During Rebuild. This policy applies only to units which are redundant. (For units which are not redundant, a check box is not available.) When this policy is set, ECC errors are ignored when they are encountered during a rebuild. When this policy is not set, a rebuild will abort upon encountering an ECC error and the unit will be set back to Degraded.

Since this option could result in the loss of some source data in the event of source errors, select this option only if you want to ensure that a rebuild will complete successfully without manual intervention. If the rebuild fails and **Continue on Source Error During Rebuild** is not selected, then you have the option to start a rebuild manually. It is recommended that you execute a file system check when the rebuild completes. Under Windows, you can do this by right-clicking on the Drive and choosing Properties; then on the Tools tab, click Check Now. Under Linux use `fsck /dev/sda1`.

Note: The policy **Continue on Source Error During Rebuild** is equivalent to the "Force continue on source errors" option in 3DM v 1.x and the "ignoreEcc" option in the CLI.

Queuing. (Not applicable for SAS drives) This policy enables or disables Native Command Queuing (NCQ) for SATA drives in the unit. By default, queuing is disabled. You can enable it, if desired.

NCQ only operates when the feature is enabled at both the drive and the controller. If a drive does not support NCQ, the policy setting for the controller is ignored.

Enabling NCQ can improve performance in many applications; it causes command reordering to be done on the drive itself.

StorSave Profile. The StorSave feature includes an option that lets you change the StorSave Profile used for a unit. Three profiles are available: Protection, Balanced, and Performance. These profiles automatically adjust several different factors that affect protection and performance, including whether FUA (Forced Unit Access) is honored, whether Write Journaling is enabled, and whether Disable Cache on Degrade is enabled. For additional information, see "Setting the StorSave Profile for a Unit" on page 106.

Note: If the write cache setting is disabled for a unit, the StorSave Profile capability does not apply and is automatically disabled.

Unit Names

Units can be assigned names. A name can be assigned when the unit is created and can be changed from this screen. For additional information, see "Naming a Unit" on page 99.

Other Controller Settings

The Other Controller settings displays information about additional settings, some of which can only be changed in the BIOS (3BM).

Auto Rebuild. The Auto Rebuild policy determines how the controller firmware will attempt to rebuild degraded units.

When Auto Rebuild is disabled, only spares will be used to automatically rebuild degraded units. When Auto Rebuild is enabled, the firmware will automatically select drives to use for rebuilding a degraded unit using the following priority order.

- Smallest usable spare.
- Smallest usable unconfigured (available) drive.
- Smallest usable failed drive.

For additional information, see “Setting the Auto Rebuild Policy” on page 77.

Auto-Carving. Auto-carving can be enabled or disabled by selecting the appropriate radio button.

When this feature is enabled, any unit that is over a specified size (known as the *carve size*) will be broken down into multiple volumes of that size, plus a remainder volume. The default carve size is 2048 GB (2 TB). For example, using the default carve size, if the unit is 2.5 TB then it will contain two volumes, with the first volume containing 2 TB and the second volume containing 0.5 TB. If the unit is 5.0 TB then it will contain 3 volumes, with the first two volumes containing 2 TB each and the last volume containing 1 TB. If a specific Boot Volume was also specified in 3BM, the first volume will be the size specified for the Boot Volume, and then the carve size will be applied to the remainder of the unit.

Carve Size. Sets a size for dividing up units into volumes when Auto-Carving is enabled. This setting can be between 1024 and 2048 GB.

Number of Drives Per Spin-up. Number of drives that will spin up at the same time when the controller is powered up. (This setting only applies when the feature is supported by the disk drives.)

Delay between Spin-ups. The delay time (in seconds) between drive groups that spin up at one time on this particular controller.

Export Unconfigured Disks. By default, this setting is No. If you have individual drives attached to a 9000-series 3ware RAID controller that you want to make available to the operating system, it is recommended that you configure them as Single Disk units.

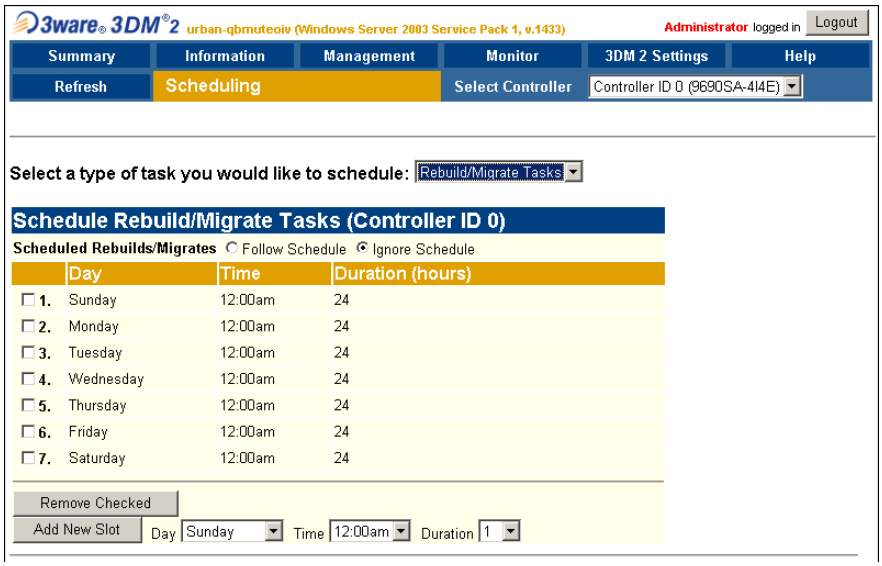
Number of Controller Phys. The number of phy connections possible on the controller. The 3ware 9690SA RAID controller has 8 phys.

Update Firmware

The Update Firmware function allows you to update the firmware of your 3ware RAID controller to the latest version. This keeps the firmware compatible with updates to your operating system and allows you to take advantage of new features 3ware may have added to your controller's functionality. For additional information, see "Updating the Firmware Through 3DM 2" on page 159.

Scheduling page

Figure 101. Scheduling Page



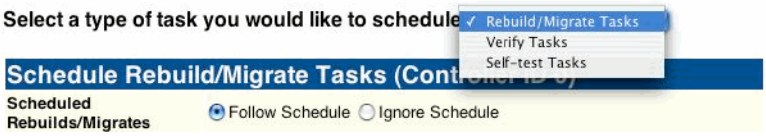
The Scheduling page appears when you choose **Management > Scheduling** from the menu bar.

The Scheduling page lets you set up a schedule for when background tasks (rebuild, migrate, initialize, verify, and self-test) should occur. Background tasks can have impact on the performance of your system, so you may prefer to schedule them at times when they will be least disruptive, such as in the middle of the night or on a weekend.

Select a type of task you would like to schedule. You start by selecting the type of task for which you want to set the schedule from the drop-down list at the top of the page.

- Rebuild/migrate tasks (also applies to initialization)
- Verify tasks (also applies to media scans)
- Self-tests

3DM then updates the page to show you schedule details for that type of task.



Follow Schedule/Ignore Schedule. You can enable or disable the schedule for the Rebuild/Migrate and Verify tasks by selecting either **Follow Schedule** or **Ignore Schedule**. When schedules are set to be ignored, these tasks can be performed at any time, and are not restricted to the scheduled times.

For details about the different background tasks, see “Background Tasks” on page 137.

Task Schedules

Initially, 7 schedule slots are defined, for 24 hours each. Even if **Follow Schedule** is enabled, this schedule is equivalent to **Ignore Schedule**, because tasks can run at any time, round the clock.

A maximum of 7 slots can be created, so to set a different schedule, start by deleting one or more of the existing scheduled slots, and then add new slots.

For step-by-step instructions for adding and removing schedules, and setting schedules to be followed or ignored, see “Scheduling Background Tasks” on page 150.

Self-test Schedules

Unlike scheduling of rebuilds and verifies, scheduling of self-tests is always followed. To disable self-tests you either remove all schedule times, or uncheck the tests listed in the Tasks column.

Note: Only the checked tasks will be run during the scheduled times. If none of the tasks are checked, self-tests will never run, even if you have scheduled time slots set.

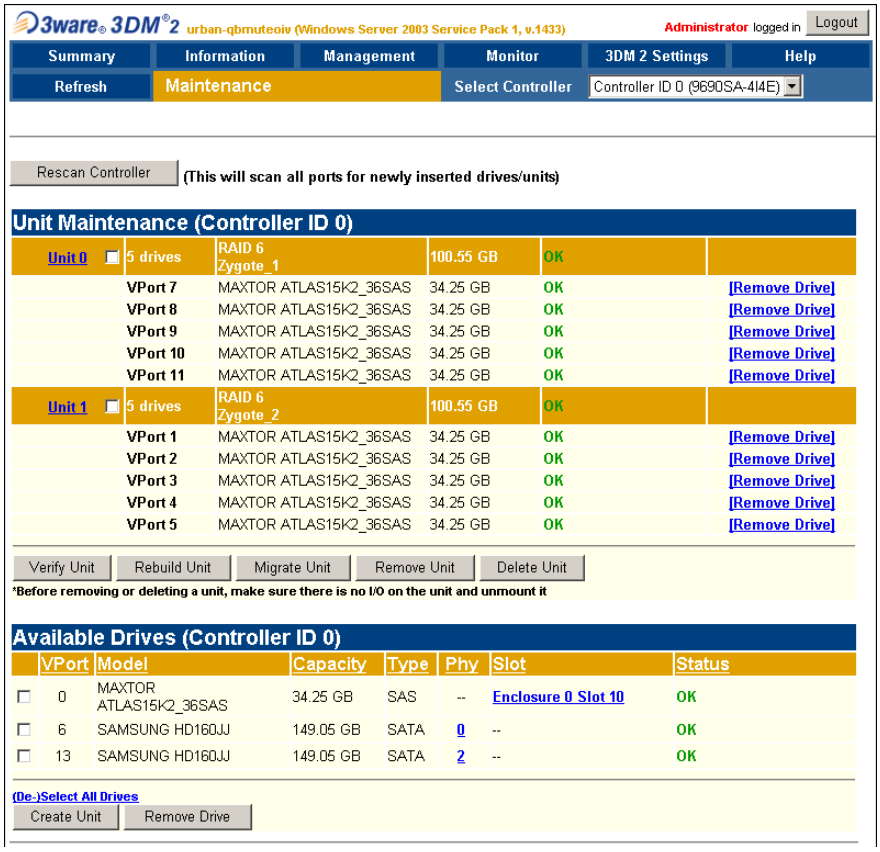
Check SMART Thresholds. This test checks to see whether SMART thresholds have been exceeded.

The SMART thresholds indicate when a drive is likely to fail, based on the number of errors that have been recorded through SMART (Self-Monitoring, Analysis and Reporting Technology).

If any of the disk drives have detected a “threshold exceeded” condition, then an AEN is logged to the 3DM Alarms page. Moreover, if anything unusual is found during any self-test, it will be logged as an Alarm.

Maintenance page

Figure 102. Maintenance Page



The Maintenance page appears when you choose **Management > Maintenance** from the menu bar.

The Maintenance page lets you perform maintenance tasks on existing units on the current controller and lets you create new units by configuring available drives.

Information about the Maintenance page is organized under these headings:

- Rescan Controller
- Unit Maintenance
- Maintenance Task Buttons
- Available Drives (to Create Units)

Rescan Controller

The **Rescan Controller** button scans the ports on the controller. Rescanning updates the list of available drives shown and updates the status of all attached disks. If error conditions have been fixed, the status is updated to reflect that.

Rescanning is useful in a variety of maintenance tasks. For example, if you physically plug in a drive and want the controller to recognize the newly plugged-in drive, Rescan will find it.

Note: If you unplug a drive without first removing it through 3DM, Rescan may not recognize it as gone unless the drive was in use or until it is required by the system. Always use the **Remove** link to remove a drive before unplugging it.

Warning: Physically removing or adding drives which are not in hot swap bays can result in a system hang or may even damage the system and the drive.

Rescan checks all ports. It checks empty ports for newly plugged-in drives. If those drives were previously part of a 3ware RAID configuration and they still have valid DCB (Disk Configuration Block) information on them, the controller tries to piece them back together into a working unit. If a working unit can be formed, it will appear in the Unit Maintenance list when the scan is complete, and the operating system will be notified of the unit. In Linux, a device node will be associated with each unit created. In Windows, the device manager will reflect the changes under the disk drives icon. This process is known as importing drives.

If new drives do not have any data indicating they were previously part of a 3ware RAID configuration, they will appear in the Available Drives list.

In addition, if there is a unit with the status Inoperable before a rescan (for example, a RAID 5 unit missing 2 or more drives), and a rescan finds drives that complete the unit, the inoperable unit will become a valid unit.

Unit Maintenance

The Unit Maintenance section of the page lists all existing units on the current controller, and displays summary information about them.

The top row shows information about the unit, while subsequent rows show summary information about each drive in the unit.

Unit Information

Unit Number. The unit number assigned to the unit by the firmware. Use the checkbox next to the unit to select a unit before clicking one of the task buttons.

 # Drives. Number of drives in the unit.

Type of Unit. Type of unit: RAID 0, RAID 1, RAID 5, RAID 6, RAID 10, RAID 50, Single Disk, or Spare. If the unit has been given a unique name, it shows beneath the RAID type.

Name of Unit. User-assigned unique name of the unit. The default setting is blank.

Capacity. The usable capacity (size) of the unit.

Status. Operational status of the unit: Ok, Rebuilding, Initializing, Verifying, Migrating, Degraded, or Inoperable (missing drives). When Rebuilding, Initializing, Migrating, or Verifying, the percentage (%) complete is also shown. The percentage complete can be active or paused. To see whether this task is currently active or paused, click on the unit number to display the Unit Details page, which has that information. For an explanation of the statuses, see “Unit Statuses” on page 129.

Drive Information

VPort. The VPort (virtual port) to which the drive is connected.

Model. The model of the drive.

Capacity. The capacity (size) of the drive.

Status. The status of the drive: OK, Not Supported, Not Present, and so forth. If you need help regarding a status displayed here, please contact Technical Support. For more information, see “Drive Statuses” on page 130.

Remove Drive. The **Remove Drive** link removes a drive from the controller so that you can safely unplug it. In the Unit Maintenance section, this link is only provided for drives that can be safely removed without creating an inoperable unit. (For example, a RAID 5 missing 2 or more drives or a RAID 0 missing 1 or more drives would become inoperable.) If you remove a drive from a redundant unit, the unit will become degraded. Once a unit has become degraded, additional drives cannot be removed without making it inoperable, so no **Remove Drive** link will display.

Warning: Physically removing drives which are not in hot swap bays can result in a system hang, data loss, or may even damage the system and the drive.

Maintenance Task Buttons

Below the list of units, a row of task buttons lets you perform maintenance and configuration tasks related to the unit. Before clicking one of these buttons, select the appropriate unit.

Verify Unit. Puts the selected unit in verifying mode. If verify scheduling is enabled on the Scheduling page, the unit will not start actively verifying until the scheduled time, and the status will indicate "Verify-Paused." (The Unit Details page will indicate whether a unit is actively verifying.) If verify scheduling is not enabled, clicking Verify Unit begins the verification process.

If the unit you selected to verify is a redundant unit, the redundancy of the unit will be verified. For example it will check parity for a RAID 5 or check data consistency for a RAID 1. If the unit you checked is not a redundant unit, verify will do a surface scan of the media. During verification, I/O continues normally. For RAID 0, single disks, and spares, there is only a slight performance loss. For redundant units, you can set the background task rate on the Controller Settings page to specify whether more processing time should be given to verifying or to I/O. For more information, see "About Verification" on page 141 and "Setting Background Task Rate" on page 149.

While a unit is verifying, the status changes to Verifying and a **Stop Verify** link appears in the right-most column of the Unit Maintenance table.

Note: If the unit has not previously been initialized and you click **Verify Unit**, the initialization process starts. Initialization cannot be halted, so no Stop Verify link appears. (Initialization can be paused, however, through Scheduling. Initialization follows the Rebuild schedule, so turning on scheduling for Rebuild will pause initialization, as well.) For more information about initialization, see "About Initialization" on page 137.

Rebuild Unit. Replaces a failed drive in a degraded unit with an available drive and begins rebuilding the RAID. When you select a degraded unit and click **Rebuild Unit**, a dialog box listing available drives appears, so that you can select the drive you want to use. If the degraded unit has more than one failed drive (for example, a RAID 10 where both mirrored pairs each have a failed drive), you will repeat this process a second time.

If rebuild scheduling is enabled on the Scheduling page, the unit will not start actively rebuilding until the scheduled time, and the status will change to say "Rebuild-Paused." (The Unit Details page indicates whether a unit is actively rebuilding.) If rebuild scheduling is not enabled, the rebuild process will begin right away.

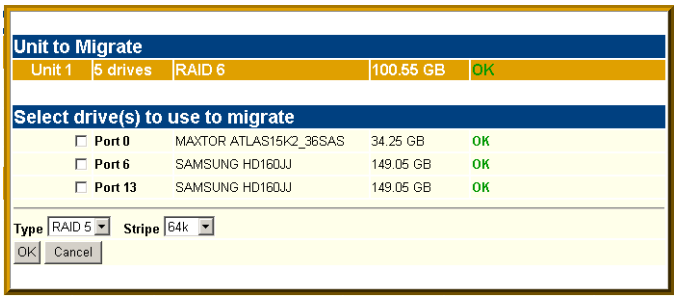
For more information about rebuilds, see “To verify a unit through 3BM” on page 143.

Migrate Unit. Reconfigures a unit while it is on-line. Migration can be used to change the RAID level, to expand the capacity by adding additional drives, or to change the stripe size.

Warning: Once migration of a unit is started, it cannot be cancelled.

When you select a unit and click **Migrate Unit**, a dialog box appears which lists the drives in the unit and any additional available drives. In the dialog box are two drop-down menus, one for choosing the RAID level and one for choosing stripe size.

Figure 103. Migrating a unit



You can only migrate a unit to a RAID level that will be larger than the original unit. For example, you can migrate from a RAID 5 array with 4 drives to a RAID 0 with four drives but you cannot migrate from a RAID 5 with four drives to a RAID 10 with four drives.

After you have specified changes to the unit, the Unit Maintenance screen reflects your changes and shows the percentage of migration completed.

While the unit is migrating, you can still access the unit as normal but the performance will be lower. You can adjust the I/O rate with the radio buttons on the Controller Settings page. (See “Setting Background Task Rate” on page 149.)

Remove Unit. Removes a selected unit and allows you to unplug the drives and move the unit to another controller. The data on the unit remain intact.

Caution: Before you click **Remove Unit**, make sure the unit you are removing is unmounted from the operating system and that the system is not accessing it.

If a unit is not unmounted and you remove it, it is the equivalent of physically yanking a hard drive out from under the operating system. You could lose data, the system could hang, or the controller could reset.

To unmount a unit under windows, use Administrative Tools > Computer Management > Disk Management. In the Computer Management window, right-click on the partition and Remove the logical drive letter associated with the unit.

To unmount a unit under Linux, unmount the mount point to where the RAID unit is mounted. For example, if you want to remove unit 0 and you know that 0 corresponds to /dev/sdb, you should unmount all partitions for sdbx (where x is the number of the partition).

```
umount /dev/sdbx
```

When you click **Remove Unit**, you will be asked to confirm that you want to proceed. When you confirm the removal, the unit number and information will be removed from 3DM. (Units created in the future can reclaim this unit number.)

The operating system is notified that the unit was removed. In Linux the device node associated with this unit is removed. In Windows the Device Manager will reflect the changes under the disk drives icon.

Information about the unit remains intact on the drives. This allows the drive or drives to be reassembled into a unit again on this controller, or if moved to another controller.

Warning: Physically removing drives which are not in hot swap bays can result in a system hang, data loss, or may even damage the system and the drive.

Delete Unit. Deletes the selected unit and allows you to use the drives to create another unit. The drives appear in the list of Available Drives.

Caution: Before you click **Delete Unit,** make sure the unit you are removing is unmounted from the operating system and that the system is not accessing it.

Devices can be unmounted through the operating system. For details, see the discussion under **Remove Unit,** above.

Warning: When a unit is deleted, the data will be permanently deleted: the drives cannot be reassembled into the same unit. If you want to reassemble the drives on another controller and access the existing data, use **Remove Unit** instead of **Delete Unit.**

After deletion, the operating system is notified that the unit was deleted. In Linux the device node associated with this unit is removed. In Windows the Device Manager will reflect the changes under the disk drives icon.

Available Drives (to Create Units)

This section lists the drives on the controller which are not currently configured as part of a unit. The VPort number, model, capacity, type, phy, slot, and status are all displayed, as they are for drives in existing units.

The available drives can be sorted by VPort, model, capacity, type, phy, or slot by clicking on the column headings. (For details about these attributes, see “Drive Information page” on page 193.)

Remove Drive. The Remove Drive button removes a drive from the controller so that you can safely unplug it. Select the box for any drive in the Available Drives list you wish to remove.

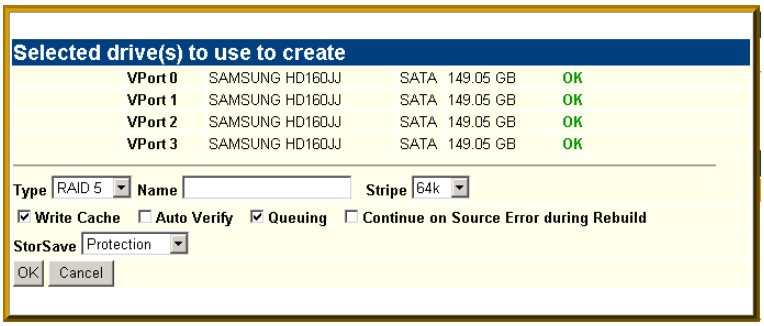
Warning: Physically removing drives which are not in hot swap bays can result in a system hang or may even damage the system and the drive.

Create Unit

Use the **Create Unit** button to create a unit for use on the current controller. Begin by selecting the drives you want to use in the list of Available Drives, and then click **Create Unit**. You will be prompted to select the unit Type, Name, Stripe size (if applicable), and unit policy settings.

A window like the one below shows the drives you selected, and lets you specify configuration settings.

Figure 104. Configuration Window in 3DM



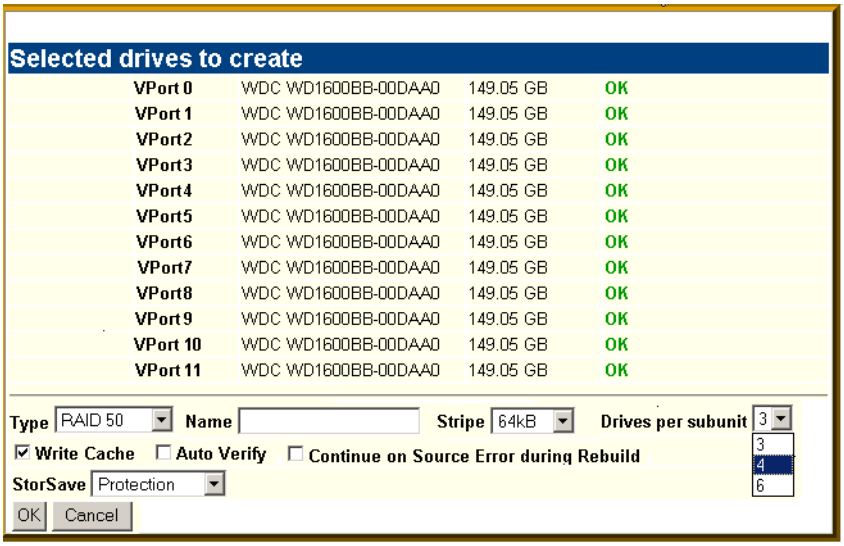
For more detailed instructions, see “Configuring a New Unit” on page 85.

Type. The drop-down list lists the possible RAID configurations for the drives selected in the list of Available Drives. Available configurations may include RAID 0, RAID 1, RAID 5, RAID 6, RAID 10, RAID 50, Single Disk, and

Spare Disk. For information about these configurations, see “Available RAID Configurations” on page 5.

Depending on the size of the unit, a RAID 50 unit will contain 2 or more subunits. For example, when you are configuring a RAID 50 with twelve drives, an additional field appears, in which you select the number of drives per subunit—3, 4, or 6.

Figure 105. Configuring a RAID 50 with 12 Drives



Name. You can enter a name for the unit.

Stripe. The drop-down list of stripe sizes lists the possible stripe sizes for the configuration you selected in the RAID level drop-down.

The default stripe size of 64KB will give the best performance with applications that have many sequential reads and writes. A larger stripe size will give better performance with applications that have a lot of random reads and writes. In general, the smaller the stripe size, the better the sequential I/O and the worse the random I/O. The larger the stripe size, the worse the sequential I/O and the better the random I/O.

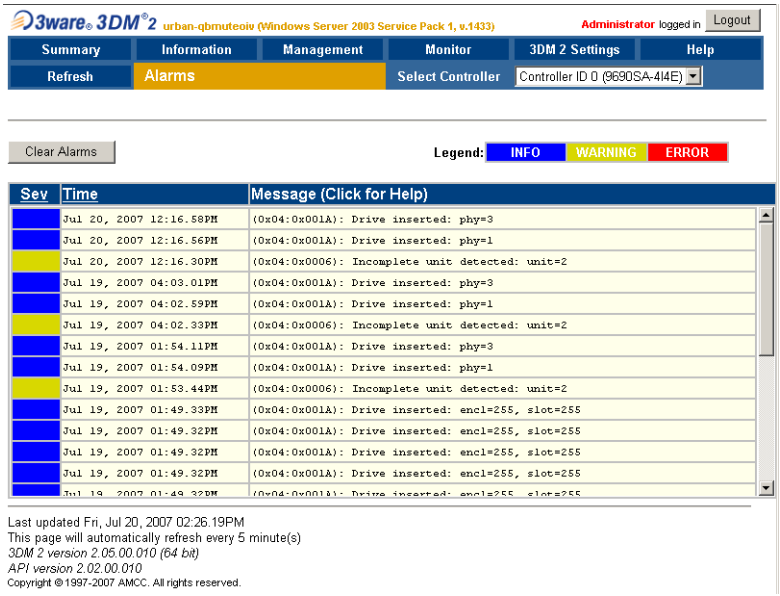
Write Cache, **Auto Verify**, and **Continue on Source Error during Rebuild.** These check boxes let you set the policies for the unit. These policies can also be set and changed on the Controller Settings page. For details about these policies, see “Unit Policies” on page 199.

Note: If the configuration window disappears while you are selecting drives, 3DM 2 may have refreshed. Click **Create Unit** again. If desired, you can reduce the frequency with which information refreshes in 3DM 2, or disable refresh temporarily, on the 3DM 2 Settings page.

StorSave. You can specify the StorSave Profile to be used for the unit. Three profiles are available: Protection, Balanced, and Performance. For more information, see “Setting the StorSave Profile for a Unit” on page 106.

Alarms page

Figure 106. Alarms Page



The Alarms page appears when you click **Monitor > Alarms** on the menu bar.

This page displays a list of AENs (asynchronous event notifications) received from the controller displayed in the drop-down list in the menu bar.

Up to 1000 events can be listed. After the 1000-limit is reached, the oldest events are deleted, as new ones occur.

You can sort the events by severity or time. To do so, just click the column header.

For information about a particular event, click it on the Alarms page; the 3DM Help will open with information about the event. For a complete listing of the alarms that appear on the Alarms page, see “Error and Notification Messages” on page 228.

Clear Alarms. The **Clear Alarms** button removes all alarms shown in the list.

Sev. Shows the severity of the event. Three levels are provided:

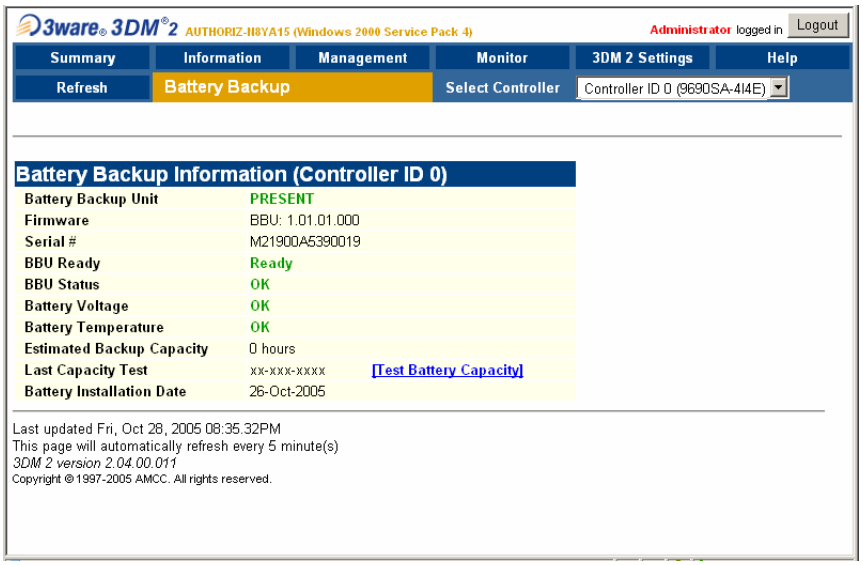
- Errors are shown next to a red box
- Warnings are shown next to a yellow box
- Information is shown next to a blue box

Time. The time shown for alarms is the time the alarm was received by the driver from firmware.

Message. The specific text relating to the alarm condition.

Battery Backup page

Figure 107. Battery Backup Page



The Battery Backup page appears when you choose **Monitor > Battery Backup** on the menu bar. Use this page to determine whether a backup battery is present, see details about it, and perform a battery test.

Battery Backup Unit. Indicates whether the BBU is present.

Firmware. Indicates the BBU firmware version.

Serial Number. Indicates the BBU serial number.

BBU Ready. Indicates if the BBU is able to backup the 3ware RAID controller or not. If the BBU is “Ready”, write cache can be enabled on the 3ware RAID controller. When the status is not “Ready,” write caching is automatically disabled on all units attached to the controller.

BBU Status. Indicates the status of the BBU. Possibly BBU statuses include the following:

- **OK**. The BBU is functioning normally.
- **Not Present**. The BBU was not detected or is disabled. (The BBU can be disabled using CLI.)
- **No Battery**. No battery pack is installed in the BBU.

- **Testing**. A battery capacity test is in process.
- **Charging**. The battery is being charged. Charging of the battery occurs automatically if the battery voltage falls too low. This normally occurs about once a week to top off the charge level; the process does not change the BBU readiness state.

  If the battery is ever discharged through a backup cycle or if the system power is off for more than two weeks, the battery status changes to "Charging" the next time the system is powered on. This indicates the BBU is not able to backup the 3ware RAID controller. When the BBU is in the charging state, write caching is disabled automatically on all units attached to the controller.
- **Fault**. The BBU detected a fault. This occurs if the voltage or temperature is outside the acceptable range.
- **Error**. Other BBU error. Please contact AMCC Technical Support.
- **Weak Battery**. The battery should be replaced soon. The results of a battery health test or capacity test indicate that the battery is below the warning threshold (48 hours).
- **Failed Battery**. The battery failed a test and must be replaced. A "Failed Battery" status is displayed if the battery failed the health test or the battery capacity is below the error threshold (24 hours). The battery must be replaced.

Battery Voltage. Indicates the voltage status of the battery. The BBU measures and evaluates the battery voltage continuously. If the voltage falls outside the normal range, warning or error level AENs are generated. In the case of a voltage error the BBU status will change to "Fault" and the battery will be disconnected electronically.

Battery Temperature. Indicates the temperature status of the battery. The BBU measures and evaluates the battery pack temperature continuously. If the temperature falls outside the normal range, warning or error level AENs are generated based on the measured temperature. In the case of a temperature error, the BBU status will change to "Fault" and the battery will be disconnected electronically.

Estimated Backup Capacity. Indicates the estimated backup capacity in hours. This is the amount of time that the battery backup unit can protect the data in the 3ware RAID controller's cache memory. This field is set to zero at the start of a new test and is updated after the test completes. A capacity of zero will also show if the BBU is disconnected and then reconnected.

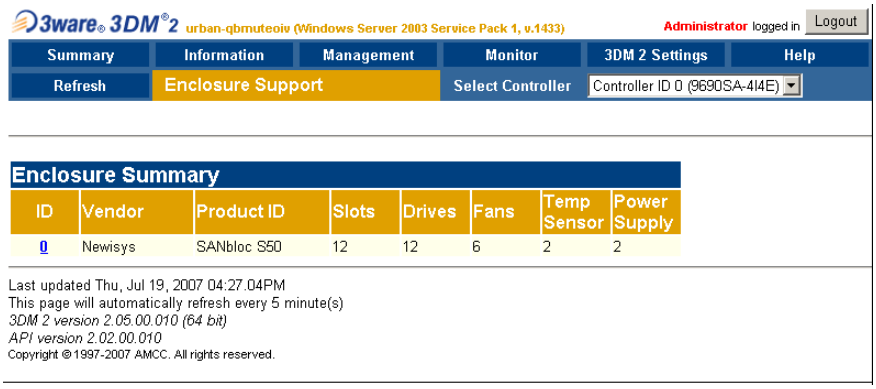
Under optimal conditions, a battery can protect for up to 72 hours. However, with a fresh battery, you may see a higher number in this field. As the battery ages, the backup capacity diminishes.

Last Capacity Test. Indicates the date when the last battery test was completed. To test the battery click the **Test Battery Capacity** link. For details, see “Testing Battery Capacity” on page 176.

Battery Installation Date. Indicates when the BBU last detected the battery pack was removed and replaced.

Enclosure Summary page

Figure 108. Enclosure Summary Page



The Enclosure Summary page appears when you choose **Monitor > Enclosure Support** from the menu bar.

The Enclosure Summary page provides basic information about any enclosures attached to your system. The specific details that display depend upon your enclosure. For a list of supported enclosures, see http://www.3ware.com/support/sys_compatibility.asp.

ID. The ID that the 3ware firmware assigns to the enclosure. This ID is also a link to a page with more detailed information about the enclosure.

Vendor. The name of the manufacturer of the enclosure.

Product ID. The product ID of the enclosure.

Slots. The number of slots in the enclosure.

Drives. The number of drives in the enclosure.

Fans. The number of fans in the enclosure.

Temp Sensor. The number of temperature sensors in the enclosure.

Power Supply. The number of power supplies in the enclosure.

Enclosure Details page

Figure 109. Enclosure Details Page

The Enclosure Details page appears when you click the ID of an enclosure on the Enclosure Summary page.

Use this page to view information about the enclosure, fans, temp sensors, power supplies, and drive slots.

Information about the Enclosure Details page is organized under these headings:

- Enclosure ID
- Fan Summary
- Temp Sensor Summary
- Power Supply Summary
- Slot Summary

Enclosure ID

Vendor. The manufacturer of the enclosure.

Product ID. The product ID of the enclosure.

Revision. The manufacturer's revision number for the enclosure.

Diagnostic. Click the **Diagnostic Text** link to download a log of enclosure diagnostic information to your computer. If you contact AMCC for support with your controller, they may ask you to use this feature. It may help AMCC identify the problem you encountered.

Controller ID. The ID of the controller connected to the enclosure.

Fan Summary

Fan. Lists the ID number associated with the fan.

Status. Will be one of OK, Failure, Not Installed, Unknown, or Off. For status definitions, see "Fan Status" on page 183.

State. Will be **ON** or **OFF**.

Speed. Fan speed is automatically controlled by the enclosure monitoring software to maintain correct enclosure temperature. Possible settings are Stopped, Lowest, Second Lowest, Third Lowest, Intermediate, Third Highest, Second Highest, Highest, and Unknown.

RPM. The fan speed in revolutions per minute.

Identify. If supported by the enclosure manufacturer, checking this box will cause an LED to blink on the enclosure containing the specified fan. If the box is grayed, identify is not supported.

Temp Sensor Summary

Temp Sensor. The ID number of the specified temperature sensor.

Status. The status of the temperature sensor. Can be OK, Failure, Not Installed, Off, or Unknown. In addition, there are threshold warnings of Over Temp Failure, Over Temp Warning, Under Temp Warning, and Under Temp Failure. For status definitions, see "Temp Sensor Status" on page 183.

Temperature. The temperature of the enclosure in Centigrade and Fahrenheit.

Identify. If supported by the enclosure manufacturer, checking this box will cause an LED to blink on the enclosure containing the specific temperature sensor. If the box is grayed, identify is not supported.

Power Supply Summary

Power Supply. The ID number associated with the specified power supply.

Status. Can be OK, Failure, Not Installed, Off, or Unknown. For status definitions, see “Power Supply Status” on page 183.

State. Indicates if the power supply is ON or OFF.

Voltage.The status of the dc voltage output of the power supply. Can be Normal, Over Voltage, Under Voltage, or Unknown.

Current. The status of the dc amperage output of the power supply. Can be Normal, Over Current, or Unknown.

Identify. If supported by the enclosure manufacturer, checking this box will cause an LED to blink on the enclosure containing the specific power supply. If the box is grayed, identify is not supported.

Slot Summary

Slot Summary. Lists the enclosure slots and indicates which ones contain drives, and the status of each drive.

Slot. The ID of the slot for a drive in the enclosure.

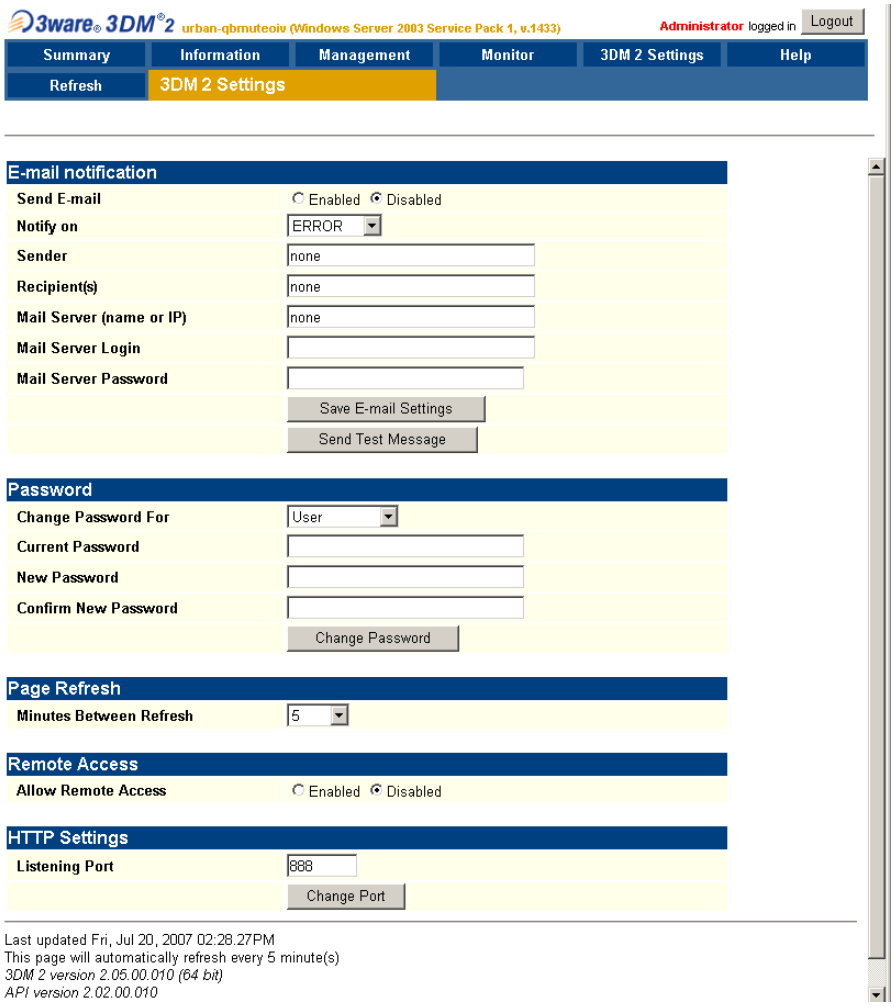
Status. The status of the drive in the slot. Can be **Inserted**, **Ready To Insert**, **Ready To Remove**, or **Activated**.

VPort. The VPort assigned to the drive in the slot. Clicking the link takes you to the Drive Information page. The drive you selected will be highlighted.

Identify. Check the box to cause the LED associated with that slot to blink.

3DM 2 Settings page

Figure 110. 3DM 2 Settings Page



The 3DM 2 Settings page appears when you click **3DM 2 Settings** on the menu bar. Use this page to set preferences, including email notification for alarms, passwords, page refresh frequency, whether remote access is permitted, and the incoming port for 3DM to listen for requests.

The initial settings for most of these preferences are specified during installation of 3DM.

Information about the 3DM 2 Settings page is organized under these headings:

- E-mail Notification
- Password
- Page Refresh

- Remote Access
- HTTP Settings

E-mail Notification

Use the fields in this section to set up and manage notifications of events by e-mail.

Send E-mail. This field determines whether e-mail notification is **Enabled** or **Disabled**. It is a good idea to enable this feature, so that you receive email when your units or drives have problems.

Notify On. Specifies the type of events for which notifications should be sent. A severity of **Information** will send e-mails for all alarms, a severity of **Warning** will send e-mail for alarms with severity of Warning and Error. A severity of **Error** will send e-mail for alarms with severity of Error.

Sender. Enter the email address which will appear in the “From” field.

Recipient. The e-mail address to which notifications should be sent. You can enter multiple addresses, separated by commas (,).

Mail Server (name or IP). If the machine on which you are running 3DM has access to a name server, you may enter the machine name of the mail server in the Server field. Otherwise, use the IP address.

Mail Server Login. If your email server requires authentication, enter the login for the server. If you are uncertain of the login, contact the administrator of the email server.

Mail Server Password. If your email server requires authentication, enter the password for the Mail Server login.

Save E-mail Settings button. Saves the e-mail notification settings.

Send Test Message button. Sends a test message using the saved e-mail settings.

Password

Use the fields in this section to set the passwords for the User and Administrator. When 3DM is first installed, the default password for both is `3ware`.

Change Password For. Select the access level for which you are setting the password: **User** or **Administrator**. Users can only view status information in 3DM, while Administrators can make changes and administer the controller and associated drives.

Current Password. Enter the current password.

New Password. Enter the new password.

Confirm New Password. Enter the new password a second time, to be sure you have entered it correctly.

Change Password button. Saves password changes.

Page Refresh

Minutes Between Refresh. Displays how frequently pages in 3DM will be refreshed with new data from the controller. To change this setting, select another option from the drop-down. If you prefer 3DM to only refresh when you click **Refresh Page**, select **Never**.

The Login, Help and Drive SMART data pages do not automatically refresh. All other 3DM pages do.

Remote Access

Allow Remote Access. This field enables or disables the ability for users and administrators to access 3DM from a remote computer.

HTTP Settings

Listening Port. This field specifies the HTTP: port to be used by 3DM when listening for communications. The default port setting is 888.

If you change this port, make sure the port you specify is not being used. Failure to do so will cause 3DM to stop responding and you will have to restart it by hand.

Change Port button. Saves a new port number.

13

Troubleshooting

This troubleshooting section includes the following sections:

- Web Resources
- Before Contacting Customer Support
- Basic Troubleshooting: Check This First
- Command Logging
- Problems and Solutions
- Error and Notification Messages

Web Resources

For support, troubleshooting tips, frequently asked questions, software releases, and compatibility information related to 3ware RAID controllers, refer to:

- 3ware support page at:
  http://www.3ware.com/support/
- 3ware knowledgebase:
  http://www.3ware.com/KB/kb.asp
- 3ware software downloads:
  http://www.3ware.com/support/download.asp
- 3ware documentation:
  http://www.3ware.com/support/userdocs.asp
- 3ware Compatibility Lists:
  http://www.3ware.com/support/sys_compatibility.asp

If you have a degraded unit or problem drive, see “Maintaining Units” on page 125.

Before Contacting Customer Support

Three screens in 3DM 2 provide controller version and status information that can be helpful when contacting 3ware Customer Support with questions or for troubleshooting: Controller Summary, Unit Details, and Unit Information.

You can copy and paste the information from these screens into an email using the system clipboard. When each page is displayed on the screen, highlight it using your mouse (or press Ctrl-A to select all text), press Ctrl-C to copy it to the clipboard, and then Ctrl-V to paste it into an e-mail.

You may also want to take a screen capture of these pages so that you can respond to questions about your system configuration to the Customer Support representative.

Additional useful information can be gathered from the error logs.For instructions for collecting error logs, see knowledgebase article 12278: http://www.3ware.com/KB/article.aspx?id=12278.

Basic Troubleshooting: Check This First

Many error messages can be traced to improperly connected hardware. Hardware can appear to be connected, yet not be in full contact. This can cause intermittent errors that are hard to identify.

Reseat the following items to make sure they are in full contact and are not loose:

- Cables
- Power cords and power connectors
- BBU connectors
- RAID controller
- Hard drives

If you have insured that all connections are secure and the errors still occur, one strategy to confirm or rule out hardware problems is to swap suspected bad drives, cables or power cords with known good ones. You can also:

- Move the drive to a different drive slot on the controller.
- In the case of a controller, try a different computer.

Command Logging

All changes that are made to RAID configurations using 3DM or CLI are automatically stored in a special log file, tw_mgmt.log. This log can be helpful to AMCC technical support for troubleshooting problems with your RAID controller and units.

Under Linux, tw_mgmt.log is in the /var/log directory.

Under Windows, tw_mgmt.log is in the 3DM2 installation directory if 3DM2 is installed on your system. If 3DM2 is not installed, the log file is in the home directory of the current user.

When you install 3DM, you are given the option of turning Command logging on or off. If you later want to disable it, you can do so through the CLI. (For details see the *3ware SAS/SATA RAID Controller CLI Guide*.)

There are other logs that may be useful to technical support. For instructions in how to collect the system logs, see http://www.3ware.com/KB/article.aspx?id=15123.

Problems and Solutions

This section covers some common problems and solutions. It is organized into the following sections:

- Enclosure-Related Problems
  - An LED is blinking red on an enclosure.
- Hardware Installation Problems
  - The 3ware BIOS screen never appears
  - Need to boot from a non-3ware device without changing the boot order
- Software Installation Problems
  - The 3ware RAID controller was configured without problems, but the system does not boot
  - A unit shows up as unusable, because of missing drives:
- Problems in 3DM and 3BM
  - A 3ware RAID controller does not show in the list of controllers
  - When booting a system, a drive is not showing up in the startup screens, in 3BM, or in 3DM

Enclosure-Related Problems

An LED is blinking red on an enclosure.

A blinking red LED on an enclosure may indicate that there is a “predicted fault” on the drive in that slot. Actual LED behavior will depend on the enclosure manufacturer. Refer to the user guide for your enclosure.

Such an error can result from a number of different factors, including a SMART error, read error, or cable error. The drive has not failed yet, but may fail soon.

For additional information about the LED indicators on an enclosure, see “Enclosure Drive LED Status Indicators” on page 128.

Hardware Installation Problems

Two common problems during hardware installation are listed below. For details related to other issues, check the 3ware KnowledgeBase: http://www.3ware.com/KB/kb.asp.

The 3ware BIOS screen never appears

- The 3ware RAID controller may not be installed properly. Reinstall the hardware and reboot.
- The motherboard may be functional, but may not be compatible. Please check the Motherboard Compatibility List on the 3ware website at http://www.3ware.com/products/compatibility.asp to see if you motherboard has been tested by 3ware. If you have a different type of motherboard available, you may want to test the controller in it to see if the 3ware BIOS screen appears.
- The motherboard's BIOS may need to be upgraded. Check the web site of the motherboard manufacturer to download and install their latest BIOS.
- The motherboard may not be functional.
- You may not have the latest 3ware firmware and driver. To see what version you have, see “Determining the Current Version of Your 3ware Driver” on page 156.To download the most recent software, see http://www.3ware.com/support/download.asp.

Need to boot from a non-3ware device without changing the boot order

If the operating system is installed on a 3ware unit, you can temporarily bypass the 3ware BIOS and prevent the OS from booting from that unit by pressing Alt-b. This saves the step of changing the boot order in the motherboard BIOS and 3BM and having to change it back again.

Software Installation Problems

The 3ware RAID controller was configured without problems, but the system does not boot

The problem could be one or more of the following:

- The BIOS may have changed the order of the boot devices. Check your system BIOS boot sequence.
- The 3ware BIOS will only boot from the first unit listed in 3BM. You can change the unit from which the 3ware controller boots by moving it to the top of the list of units by highlighting the unit and pressing the 'Page Up'/ 'Page Down' keys.
- The operating system is installed on a device that is not in your system's boot order. Use your system's Setup utility to include the StorSwitch controller in the boot order.
- If your operating system was installed before you configured your RAID units, you may have overwritten your operating system. Remember that creating or deleting a RAID unit overwrites any existing data on the member drives. Reinstall your operating system.
- There may be a compatibility problem between the motherboard system BIOS and the 3ware BIOS. Check the 3ware website (www.3ware.com) to see if your motherboard is compatible with the 3ware BIOS, and check with your motherboard manufacturer for potential BIOS updates.

A unit shows up as unusable, because of missing drives:

```
Unusable Arrays:

   3 drive 64K RAID 5 558.77 GB (Unit 1)

      SATA - Maxtor  6B300S0      279.86 GB  (Port 6)

The unit has some but not all of its members available. The
unit will be unusable. If this unit is your boot device, your
system will not boot. You must either return the missing
disks to complete the unit, or release the member disks by
deleting the incomplete unit(s) listed in the display.
Remember that deleting a RAID unit overwrites any existing
data on the member drives.
```

CAUTION: Do not delete the inoperable unit and recreate it, as this will overwrite the data and make data recovery very difficult.

If you get this error, contact technical support at http://www.3ware.com/support/.

Problems in 3DM and 3BM

A 3ware RAID controller does not show in the list of controllers

You may not the most recent driver for your controller, the driver may not be loaded, or you may not have the most recent version of the CLI or 3DM.

To find out the driver version currently installed, see “Determining the Current Version of Your 3ware Driver” on page 156

Current drivers and software are available for download on the 3ware website at
http://www.3ware.com/support/download.asp.

When booting a system, a drive is not showing up in the startup screens, in 3BM, or in 3DM

This could be due to one or more of the following:

- Defective cable
- Defective drive
- Defective RAID cage/chassis slot
- Poorly seated drive
- Poorly connected power cable
- Poorly connected data cable
- Defective connector on the 3ware controller

If a drive that previously showed up in 3DM or 3BM does not show up, try the following:

1. Power the system down, then reseat the drive in the slot, reseat the data cable, and reseat the power cable.
2. Power the system back up.
3. If the drive still does not show up in 3DM or 3BM, then swap that drive with a drive that is showing up.
4. If the drive now shows up, and drive you swapped it with does not, then the drive is OK. The problem could be the controller connector, the cable, the power connector, or the RAID cage/chassis slot.
5. Change each of these things, one at a time
   - Try a different connector on the controller
   - Try a different data cable
   - Power the drive with a different power connector from the power supply
   - Try connecting the drive directly to the motherboard, bypassing the RAID cage/chassis slot

If the drive shows up, then you will know which hardware was defective.

If the drive still does not show up, contact 3ware Technical Support.

Error and Notification Messages

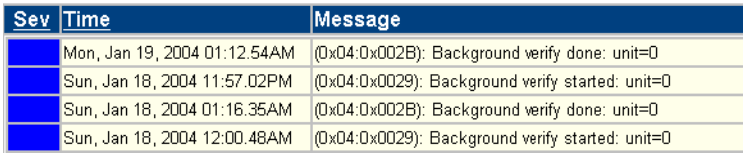
Error and notification messages are issued by the 3ware RAID controller when an error is detected or when an action is completed. These messages are sometimes referred to as AENs (asynchronous event notifications).

AEN messages are displayed on the 3DM 2 Alarms page and CLI Show Alarms page.

On the 3DM 2 Alarms page, you can click on the message to jump to help text about that message. You can also look the message up in the list below. In 3DM 2, the message number is the last few digits within the parentheses at the beginning of the message description. For example, in the string `(0x04:0x002B)`, "`002B`" is the message number. To find additional information about the message 2B, you would look up 002B in the list below.

Note that the messages are listed below in hex order, since the message numbers are in hex.

Error and notification messages are listed in Table 12. Descriptions of each are provided after the table.



Sev	Time	Message
	Mon, Jan 19, 2004 01:12.54AM	(0x04:0x002B): Background verify done: unit=0
	Sun, Jan 18, 2004 11:57.02PM	(0x04:0x0029): Background verify started: unit=0
	Sun, Jan 18, 2004 01:16.35AM	(0x04:0x002B): Background verify done: unit=0
	Sun, Jan 18, 2004 12:00.48AM	(0x04:0x0029): Background verify started: unit=0

Table 12: Error and Notification Message List

Value	Message
0001	Controller reset occurred
0002	Degraded unit
0003	Controller error occurred
0004	Rebuild failed
0005	Rebuild completed
0006	Incomplete unit detected
0007	Initialize completed
0008	Unclean shutdown detected

Table 12: Error and Notification Message List

Value Message
0009 Drive timeout detected
000A Drive error detected
000B Rebuild started
000C Initialize started
000E Initialize failed
000F SMART threshold exceeded
0019 Drive removed
001A Drive inserted
001E Unit inoperable
001F Unit Operational
0021 Downgrade UDMA mode
0022 Upgrade UDMA mode
0023 Sector repair completed
0024 Buffer integrity test failed
0025 Cache flush failed; some data lost
0026 Drive ECC error reported
0027 DCB checksum error detected
0028 DCB version unsupported
0029 Verify started
002A Verify failed
002B Verify completed
002C Source drive ECC error overwritten
002D Source drive error occurred
002E Replacement drive capacity too small
002F Verify not started; unit never initialized
0030 Drive not supported
0032 Spare capacity too small
0033 Migration started
0034 Migration failed
0035 Migration completed

Table 12: Error and Notification Message List

Value Message
0036 Verify fixed data/parity mismatch
0037 SO-DIMM not compatible
0038 SO-DIMM not detected
0039 Buffer ECC error corrected
003A Drive power on reset detected
003B Rebuild paused
003C Initialize paused
003D Verify paused
003E Migration paused
003F Flash file system error detected
0040 Flash file system repaired
0041 Unit number assignments lost
0042 Primary DCB read error occurred
0043 Backup DCB read error detected
0044 Battery voltage is normal
0045 Battery voltage is low
0046 Battery voltage is high
0047 Battery voltage is too low
0048 Battery voltage is too high
0049 Battery temperature is normal
004A Battery temperature is low
004B Battery temperature is high
004C Battery temperature is too low
004D Battery temperature is too high
004E Battery capacity test started
004F Cache synchronization skipped
0050 Battery capacity test completed
0051 Battery health check started
0052 Battery health check completed
0053 Battery capacity test is overdue

Table 12: Error and Notification Message List

Value Message
0055 Battery charging started
0056 Battery charging completed
0057 Battery charging fault
0058 Battery capacity is below warning level
0059 Battery capacity is below error level
005A Battery is present
005B Battery is not present
005C Battery is weak
005D Battery health check failed
005E Cache synchronization completed
005F Cache synchronization failed; some data lost
0062 Enclosure removed
0063 Enclosure added
0064 Local link up
0065 Local link down

Error and Notification Message Details

0001 Controller reset occurred

Event Type
Information

Cause
The device driver has sent a soft reset to the 3ware RAID controller. The driver does this when the controller has not responded to a command within the allowed time limit (30 sec.). After the soft reset command has been sent, the driver will resend the command.

Action
If this message occurs more than three times a day, collect the system logs and contact Technical Support.

See Also

For how to collect the system logs, see http://www.3ware.com/kb/article.aspx?id=12278

0002 Degraded unit

Event Type

Error

Cause

An error was encountered and the unit is now operating in degraded (non-redundant) mode. This is usually due to a drive failure or the physical removal of a drive from a redundant unit.

Action

Check hardware connections and reseat the drive or drives. Rescan the controller from 3DM or CLI to see if the unit has been restored. If you are able to restore the unit before any data has been written to the unit, a rebuild will not be necessary. If the unit remains degraded, replace the missing or dead drives and initiate a rebuild.

See Also

“About Degraded Units” on page 130

“Rebuilding Units” on page 144

0003 Controller error occurred

Event Type

Error

Cause

The 3ware RAID controller has encountered an internal error.

Action

Please collect log files and contact AMCC Customer Support, as a replacement board may be required. Technical support is at http://www.3ware.com/support/index.asp. Information on collecting logs is at http://www.3ware.com/KB/article.aspx?id=12278.

0004 Rebuild failed

Event Type
Error

Cause

The 3ware RAID controller was unable to complete a rebuild operation. This error can be caused by drive errors on either the source or the destination of the rebuild. However, because ATA drives can reallocate sectors on write errors, the rebuild failure is most likely caused by the source drive of the rebuild detecting a read error.

Action

The default operation of the 3ware RAID controller is to abort a rebuild if an error is encountered. If you want rebuilds to continue when there is a source error, you can set a unit policy to Continue on Source Error During Rebuild in 3DM or CLI.

The consequence of continuing a rebuild when there is a source error is that there may be corrupt data in your rebuilt unit. In some cases, however, this may be your only alternative for recovering as much data as possible from a unit that has become degraded.

To lower the likelihood of getting this error, schedule regular verifications.

See Also

“Setting Continue on Source Error During Rebuild” on page 104.

“Scheduling Background Tasks” on page 150

0005 Rebuild completed

Event Type
Information

Cause

The 3ware RAID controller has successfully completed a rebuild. The data is now redundant.

Action
None required.

0006 Incomplete unit detected

Event Type

Warning

Cause

The 3ware RAID controller has detected an incomplete unit.

An incomplete unit is a unit in which the 3ware RAID controller is unable to detect one or more drives. The drives may be missing, dead, or improperly connected. A unit that is incomplete is also degraded (although a degraded unit can be complete if all drives are still detected, including the failed drive).

Action

Check hardware connections and reseat the drives. Rescan the controller from 3DM to see if the unit has been restored. If you are able to restore the unit before any data has been written to the unit, a rebuild will not be necessary. If the unit remains incomplete, replace the missing or dead drives and initiate a rebuild.

0007 Initialize completed

Event Type

Information

Cause

The 3ware RAID controller completed the “synching” background initialization sequence of RAID levels 1, 6, 10, 50, or 5. For RAID 5, RAID 6, and RAID 50, the data on the unit was read and the resultant new parity was written. For RAID 1 and 10, one half of the mirror was copied to the other half (mirrors are synchronized).

This message will not appear for a foreground initialization.

See Also

“Foreground Versus Background Initialization” on page 138

0008 Unclean shutdown detected

Event Type

Warning

Cause

The 3ware RAID controller detected an unclean shutdown of the operating system, either from a power failure or improper shutdown procedure. The controller will force the unit to begin verifying, due to the possibility that data on a redundant unit could be out of synchronization.

Action

Allow the verification to complete. Verifications have little overhead in terms of system performance and keep your units in optimum condition.

To prevent unclean shutdowns, always go through the normal shutdown procedure. It is also recommended to use an uninterruptible power supply (UPS) to prevent unclean shutdowns due to sudden power loss.

See Also

“About Verification” on page 141

0009 Drive timeout detected

Event Type

Error

Cause

A drive has failed to respond to a command from a 3ware RAID controller within the allowed time limit (20 secs.). After sending this error message, the controller will attempt to recover the drive by sending a reset to that drive and retrying the failed command.

Possible causes of drive time-outs (also known as ATA-Port time-outs) include a bad or intermittent disk drive, power cable or interface cable.

Action

If you have checked hardware connections and no cause other than the drive can be found, replace the drive.

You may also want to use the drive manufacturer’s diagnostic and repair utilities on the drive.

See Also

For links to drive manufacturer diagnostic utilities and troubleshooting advice, see http://www.3ware.com/KB/article.aspx?id=14924.

“Basic Troubleshooting: Check This First” on page 223

000A Drive error detected

Event Type

Error

Cause

A drive has returned an error to the 3ware RAID controller that it is unable to complete a command. The error type is not a time-out (000A) or uncorrected ECC (0026).

This message may be seen as part of a recovery operation initiated by the 3ware RAID controller on the drive. One possible cause is multiple write commands to a sector forcing the drive to remap a defective sector. This message may be seen if error recovery operations initiated by the 3ware RAID controller are unsuccessful.

Action

If you see this message, the drive repairs may lie outside of the 3ware RAID controller’s abilities.Try running the drive manufacturer’s diagnostic and repair utilities on the drive.

If necessary, replace the drive.

See Also

For links to drive manufacturer diagnostic utilities and troubleshooting advice, see http://www.3ware.com/KB/article.aspx?id=10894.

000B Rebuild started

Event Type

Information

Cause

The 3ware RAID controller started to rebuild a degraded unit. The rebuild may have been initiated by you, may have started automatically on a hot spare or may have started after drive removal or insertion (due to the Auto Rebuild policy).

Action

Allow the rebuild to complete. This will return the unit to its normal redundant state.

See Also

“Scheduling Background Tasks” on page 150
“Rebuilding Units” on page 144
“Background Task Prioritization” on page 150

000C Initialize started

Event Type

Information

Cause

The 3ware RAID controller started an initialization. This is always a “synching” background initialization and does not erase user data. Initialization either occurs at unit creation time for larger RAID 5, 6, or 50 units or later during the initial verification of redundant units.

Action

Allow the initialization to complete. This will return the unit to its normal redundant state.

See Also

For more information, see “About Initialization” on page 137

000E Initialize failed

Event Type

Error

Cause

The 3ware RAID controller was unable to complete the initialization. This error can be caused by unrecoverable drive errors.

If this unit was a redundant unit, and the initialization failed because of a problem on a particular disk drive, then the unit will be degraded.

Action

If the unit was degraded, then rebuild the unit. This may necessitate replacing the drive.

Check physical cable and power connections. You can also run the drive manufacturer's diagnostic and repair utilities on the drive.

See Also

For links to drive manufacturer diagnostic utilities and troubleshooting advice, see http://www.3ware.com/KB/article.aspx?id=10894.

"Basic Troubleshooting: Check This First" on page 223

000F SMART threshold exceeded

Event Type

Warning

Cause

SMART monitoring is predicting a potential drive failure.

The 3ware RAID controller supports SMART monitoring, whereby the individual drives automatically monitor certain parametric information such as error rates and retry counts.This type of monitoring may be able to predict a drive failure before it happens, allowing you to schedule service of the unit before it becomes degraded. The SMART status of each drive attached to the 3ware RAID controller is monitored daily.

Action

AMCC recommends that you replace any drive that has exceeded the SMART threshold.

If the drive is part of a redundant unit, remove the drive through 3DM2 or CLI. Replace the drive and start a rebuild.

If the drive is not part of a redundant unit, then you will need to backup your data before replacing the drive.

See Also

"Viewing SMART Data About a Drive" on page 136

"Rebuilding Units" on page 144

0019 Drive removed

Event Type
Warning

Cause
A drive was physically removed from the controller while the controller was powered on.

Action
If the drive is not part of a redundant unit, return the drive as soon as possible. You may need to rescan the controller to have the drive recognized. If at all possible, do not remove a drive from a non-redundant unit as this may cause data loss or a system hang.

001A Drive inserted

Event Type
Information

Cause
A drive was connected to the controller while the controller was powered on.

Action
The drive is now available for use. If the drive is part of a unit add the remaining drives and rescan the controller, in 3DM or CLI, to bring the unit online.

001E Unit inoperable

Event Type
Error

Cause
The 3ware RAID controller is unable to detect sufficient drives for the unit to be operable. Some drives have failed or are missing.

Examples of inoperable units are as follows:

- RAID 0 missing any drives.

- A RAID 5 or 50 unit with two or more drives missing from the same RAID 5 unit or subunits.
- A RAID 10 unit with both drives missing from one of the RAID 1 subunits.
- A RAID 6 unit with three or more drives missing.

Note: The controller only generates this message if the unit is missing drives for more than 20 seconds. This allows a hot swap of a drive to be completed without generating this error.

Action

The unit is no longer available for use. Return all missing drives to the unit. If the drives are physically present, check all data and power connections.

CAUTION: Do not delete the inoperable unit and recreate it as this will overwrite the data and make data recovery very difficult.

You may wish to contact technical support at http://www.3ware.com/support.

See Also

"About Inoperable Units" on page 131

001F Unit Operational

Event Type

Information

Cause

Drive insertion caused a unit that was inoperable to become operational again. Any data that was on that unit will still be there. This message is only sent if the unit was inoperable for more than 20 seconds. That means that if the hot swap of a drive occurred within 20 seconds, messages are not generated.

Action

None Required. The unit is available for use.

0021 Downgrade UDMA mode

Event Type

Warning

Cause

The 3ware RAID controller has downgraded the UDMA transfer rate between the controller and the ATA disk drives. This message only applies to parallel ATA and certain legacy serial ATA drives.

Background Information

The 3ware RAID controller communicates to the ATA disk drives through the Ultra DMA (UDMA) protocol. This protocol ensures data integrity across the ATA cable by appending a Cyclical Redundancy Check (CRC) for all ATA data that is transferred. If the data becomes corrupted between the drive and the 3ware RAID controller (because of an intermittent or poor quality cable connection) the 3ware RAID controller detects this as a UDMA CRC or cable error. The 3ware RAID controller then retries the failed command three times at the current UDMA transfer rate. If the error persists, it lowers the UDMA transfer rate (for example, from UDMA 100 to UDMA 66) and retries another three times.

Action

Check for possible causes of UDMA CRC errors such as defective or poor quality interface cables or cable routing problems through electrically noisy environments (for instance, cables are too close to the power supply). Also check for cables which are not standard or exceed the ATA specification. A list of cables for use with 3ware controllers is available at http://3ware.com/products/cables.asp.

0022 Upgrade UDMA mode

Event Type

Warning

Cause

During a self-test, the controller found that a drive was not in the optimal UDMA mode and upgraded its UDMA transfer rate.

Action

None required. The drive and cable are working in optimal mode.

0023 Sector repair completed

Event Type

Warning

Cause

The 3ware RAID controller moved data from a bad sector on the drive to a new location.

Background Information

The 3ware RAID controller supports a feature called dynamic sector repair that allows the unit to recover from certain drive errors that would normally result in a degraded unit situation. For redundant units such as RAID 1, 5, 6, 10, and 50, the 3ware RAID controller essentially has two copies of your data available. If a read command to a sector on a disk drive results in an error, it reverts to the redundant copy in order to satisfy the host's request. At this point, the 3ware RAID controller has a good copy of the requested data in its cache memory. It will then use this data to force the failing drive to reallocate the bad sector, which essentially repairs the sector.

Action

Sector repairs are an indication of the presence of grown defects on a particular drive. While typical modern disk drives are designed to allow several hundred grown defects, special attention should be paid to any drive in a unit that begins to indicate sector repair messages. This may be an indication of a drive that is beginning to fail. You may wish to replace the drive, especially if the number of sector repair errors exceeds 3 per month.

0024 Buffer integrity test failed

Event Type

Error.

Cause

The 3ware RAID controller performs diagnostics on its internal RAM devices as part of its data integrity features. Once a day, a non-destructive test is performed on the cache memory. Failure of the test indicates a failure of a hardware component on the 3ware RAID controller. This message is sent to notify you of the problem.

Action

You should replace the 3ware RAID controller.

If the controller is still under warranty, contact 3ware Technical Support for a replacement controller.

0025 Cache flush failed; some data lost

Event Type

Error

Cause

The 3ware RAID controller was not able to commit data to the drive(s) during a caching operation.This is due to a serious drive failure, possibly from a power outage.

Background Information

The 3ware RAID controller uses caching layer firmware to improve performance. For write commands this means that the controller acknowledges it has completed a write operation before the data is committed to disk. If the 3ware RAID controller cannot commit the data to the drive after it has acknowledged to the host, this message is posted.

Action

To troubleshoot the reasons for the failure, collect the logs for your system and contact 3ware technical support at http://www.3ware.com/support/index.asp. For information on what error logs are and how to collect them, see http://www.3ware.com/KB/article.aspx?id=12278.

0026 Drive ECC error reported

Event Type

Error

Cause

Drive ECC errors are an indication of grown defects on a particular drive. For redundant units, this typically means that dynamic sector repair has been invoked (see message “0023 Sector repair completed” on page 241). For non-redundant units (Single Disk, RAID 0 and degraded units), which do not have another copy of the data, drive ECC errors result in the 3ware RAID controller returning failed status to the associated host command.

Action

Schedule periodic verifications of all units so that drive ECC errors can be found and corrected. If the unit is non-redundant a unit file system check is recommended.

Under Windows, right-click on your drive icon and choose **Properties> Tools> Check Now.**

Under Linux use `fsck /dev/sda1`. If you have more than one SATA device, substitute the correct drive letter and partition number, such as sdb2, for sda1.

See Also

"Setting Auto Verify for a Unit" on page 103

"Scheduling Background Tasks" on page 150

0027 DCB checksum error detected

Event Type

Error

Cause

The drive's Drive Configuration Block (DCB) has been corrupted.

The 3ware RAID controller stores certain configuration parameters on a reserved area of each disk drive called the Drive Configuration Block. As part of power-on initialization, the 3ware RAID controller performs a checksum of the DCB area to ensure consistency.

Action

If this error occurs, please contact 3ware technical support at http://www.3ware.com/support/index.asp for assistance.

0028 DCB version unsupported

Event Type

Error

Cause

The unit that is connected to your 3ware RAID controller was created on a legacy 3ware product that is incompatible with your new controller.

During the evolution of the 3ware product line, the format of the Drive Configuration Block (DCB) has been changed to accommodate new features. The DCB format expected by the 3ware RAID controller and the DCB that is written on the drive must be compatible. If they are not, this message is sent.

Action

Return the drives back to their original controller and contact 3ware technical support at http://www.3ware.com/support/index.asp for further assistance.

0029 Verify started

Event Type

Information

Cause

The 3ware RAID controller has started verifying the data integrity of a unit. The verification functions for different RAID levels are as follows:

- **Single and Spare.** Verify = Media scan
- **RAID 0.** Verify = Media scan
- **RAID 1 and 10.** Verify = Comparison of mirror sides
- **RAID 5, 6, and 50.** Verify = Comparison of parity data with user data

Action

Allow verify to complete to identify any possible data integrity issues.

See Also

For information on scheduling a verify process, see “Scheduling Background Tasks” on page 150. For information on verification of a unit, see “About Verification” on page 141.

002A Verify failed

Event Type

Error

Cause

Verification of a unit has terminated with an error. For each RAID level being verified, this may mean:

- **Single and Spare.** A single drive returned an error, possibly because of a media defect.
- **RAID 0.** A single drive returned an error, possibly because of a media defect.
- **RAID 1 and 10.** One side of the mirror does not equal the other side.

- **RAID 5, 6, and 50.** The parity data does not equal the user data.

For any RAID type, the most likely cause of the error is a grown defect in the drive. For out-of-synchronization mirrors or parity, the error could be caused by improper shutdown of the unit. This possibility applies to RAID 1, 5, 6, 10, and 50.

Action

When a verify fails, redundant units will automatically resynchronize user data through a background initialization. The initialize will not erase user data, but will recalculate and rewrite user parity data.

If the unit was non-redundant, any data in the error location is lost. (However, the error could be in a part of the drive that did not contain data.) A unit file system check is recommended.

Under Windows, right-click on your drive icon and choose **Properties> Tools> Check Now**.

Under Linux use `fsck /dev/sda1`. If you have more than one SATA device, substitute the correct drive letter and partition number, such as sdb2, for sda1.

The resynchronization of data that takes place during a background initialization can slow down access to the unit. Once initialization has begun, it cannot be canceled. You can pause it, however, by scheduling it to take place during off-hours. For more information, see “Scheduling Background Tasks” on page 166. You can also set the initialization process to go slower and use fewer system resources. For more information, see “Setting Background Task Rate” on page 165. (Initialization occurs at the Rebuild rate.)

See Also

“About Initialization” on page 137

002B Verify completed

Event Type

Information

Cause

Verification of the data integrity of a unit was completed successfully.

See Also

“About Verification” on page 141

002C Source drive ECC error overwritten

Event Type

Error

Cause

A read error was encountered during a rebuild and the controller is configured to ‘ignore ECC’ or to ‘Force continue on source errors’. The sector in error was reallocated.This will cause uncorrectable blocks to be rewritten, but the data may be incorrect.

Action

It is recommended that you execute a file system check when the rebuild completes.

Under Windows, right-click on your drive icon and choose **Properties> Tools> Check Now**.

Under Linux use `fsck /dev/sda1`. If you have more than one SATA device, substitute the correct drive letter and partition number, such as sdb2, for sda1.

002D Source drive error occurred

Event Type

Error

Cause

An error on the source drive was detected during a rebuild operation. The rebuild has stopped as a result.

Action

The controller will report an error, even if the area of the source drive that had the error did not contain data. Scheduling regular verifies will lessen the chance of getting this error.

You can force the rebuild to continue by setting the Overwrite ECC Error policy through 3DM, CLI, or 3BM, and then rebuilding the unit again. This will cause uncorrectable blocks to be rewritten, but the data may be incorrect. It is recommended that you execute a file system check when the rebuild completes.

Under Windows, right-click on your drive icon and choose **Properties> Tools> Check Now**.

Under Linux use `fsck /dev/sda1`. If you have more than one SATA device, substitute the correct drive letter and partition number, such as sdb2, for sda1.

See Also

"Starting a Verify Manually" on page 143

"Setting Auto Verify for a Unit" on page 103

"Setting Continue on Source Error During Rebuild" on page 104

002E Replacement drive capacity too small

Event Type

Error

Cause

The storage capacity of the drive you are using as a replacement drive is too small and cannot be used.

Action

Use a replacement drive equal to or larger than the drives already in use

002F Verify not started; unit never initialized

Event Type

Warning

Cause

A verify operation has been attempted by the 3ware RAID controller, but the unit has never been initialized before. The unit will automatically transition to initializing mode and then start a verify.

Action

None required.

This is considered a normal part of operation. Not all types of RAID units need to be initialized in order to have full performance. The initialize will not erase user data, but will calculate and write parity data or mirror data to the drives in the unit.

See Also

“About Initialization” on page 137

0030 Drive not supported

Event Type

Error

Cause

3ware 8000 and 9500S Serial ATA controllers only support UltraDMA-100/133 drives when using the parallel-to-serial ATA converter. This message indicates that an unsupported drive was detected during rollcall or a hot swap. This message could also indicate that the parallel-to-serial converter was jumpered incorrectly.

Action

Use a parallel ATA drive which supports UDMA 100 or 133 and check that the parallel-to-serial converter was correctly jumpered to correspond to UDMA 100 or 133 drives.

See Also

For a list of compatible drives, see
http://www.3ware.com/products/compatibility_sata.asp

0032 Spare capacity too small

Event Type

Warning

Cause

There is a valid hot spare but the capacity is not sufficient to use it for a drive replacement in existing units.

Action

Replace the spare with a drive of equal or larger capacity than the existing drives.

0033 Migration started

Event Type
Information

Cause
The 3ware RAID controller has started the migration of a unit.

Migration changes can include:

- Expanding capacity of a unit by adding drives
- Changing RAID levels, for example, from RAID 1 to RAID 5

See Also
"RAID Level Migration (RLM) Overview" on page 110

0034 Migration failed

Event Type
Error

Cause
The migration of a unit has failed.

Migration changes can include:

- Expanding capacity of a unit by adding drives.
- Changing RAID levels, for example, from RAID 1 to RAID 5

Action
Review the list of events on the Alarms page for other entries that may give you an idea of why the migration failed (for example, a drive error on a specific port).

You may also wish to get the logs and contact technical support at http://www.3ware.com/support/index.asp. For information on what error logs are and how to collect them, see http://www.3ware.com/KB/article.aspx?id=12278.

See Also
"RAID Level Migration (RLM) Overview" on page 110

0035 Migration completed

Event Type
Information

Cause
The migrated unit is now ready to be used.

Migration changes can include:

- Expanding capacity of a unit by adding drives
- Changing RAID levels, for example, from RAID 1 to RAID 5.

Action
If the capacity of the unit did not change, then you do not need to do anything else. If the capacity of the migrated unit is larger, you will need to inform the operating system of the change. See “Informing the Operating System of Changed Configuration” on page 113.

0036 Verify fixed data/parity mismatch

Event Type
Warning

Cause
A verify error was found and fixed by the 3ware RAID controller.

Some examples of errors that can be fixed include:

- A parity inconsistency for a RAID 5 or RAID 50 unit.
- A data mismatch for a RAID 1 or RAID 10 unit.

Action
None required.

0037 SO-DIMM not compatible

Event Type
Error

Cause

There is incompatible SO-DIMM memory connected to the 9500S controller.

Note: This message only applies to the 3ware 9500S controller, which has removable memory. Other 3ware controller models do not have memory that can be removed.

Action

Replace the incompatible SO-DIMM with a compatible one.

See Also

For a list of SODIMMs compatible with the 9500S, see http://www.3ware.com/KB/article.aspx?id=11748.

0038 SO-DIMM not detected

Event Type

Error

Cause

The 3ware 9500S RAID controller is inoperable due to missing SO-DIMM memory.

Note: This message only applies to the 3ware 9500S controller, which has removable memory. Other 3ware controller models do not have memory that can be removed.

Action

Install a compatible SO-DIMM on the controller.

See Also

For a list of SODIMMs compatible with the 9500S, see http://www.3ware.com/KB/article.aspx?id=11748.

0039 Buffer ECC error corrected

Event Type

Warning

Cause

The controller has detected and corrected a memory ECC error.

Action

None required.

If errors persist, contact technical support at http://www.3ware.com/support/index.asp.

003A Drive power on reset detected

Event Type

Error

Cause

The controller has detected that a drive has lost power and then restarted. The controller may degrade the unit if it is a redundant unit (non-redundant units cannot be degraded).

Action

If this drive was the only one to lose power, check the cable connections. Also, check that your power supply is adequate for the type and number of devices attached to it.

See Also

For troubleshooting information and a link to drive manufacturer diagnostic utilities, see http://www.3ware.com/KB/article.aspx?id=14927.

003B Rebuild paused

Event Type

Information

Cause

The rebuild operation is paused.

Rebuilds are normally paused for two (formerly ten) minutes after a system first boots up and during non-scheduled times when scheduling is enabled.

Disabling or modifying the schedule with 3DM or CLI will allow the rebuild to resume.

See Also

“Scheduling Background Tasks” on page 150

003C Initialize paused

Event Type

Information

Cause

The initialization is paused.

Initializations are normally paused for two (formerly ten) minutes after a system first boots up. Initialization is also paused during non-scheduled times when scheduling is enabled. Initializations follow the rebuild schedule.

Action

If you want the initialize to resume, you can disable or modify the schedule through 3DM or CLI.

See Also

“Viewing Current Task Schedules” on page 151

“About Initialization” on page 137

003D Verify paused

Event Type

Information

Cause

The verify operation is paused.

Verifies are normally paused for 2 (formerly 10) minutes after a system first boots up. Verifies are also paused during non-scheduled times when scheduling is enabled.

Action

If you want the verification to resume, you can disable or modify the schedule through 3DM or CLI

See Also

“About Verification” on page 141

“Scheduling Background Tasks” on page 150

003E Migration paused

Event Type

Information

Cause

Migration is paused. Migration follows the rebuild schedule.

Action

If you want the migration to resume, you can disable or modify the schedule through 3DM or CLI

See Also

“RAID Level Migration (RLM) Overview” on page 110

“Scheduling Background Tasks” on page 150

003F Flash file system error detected

Event Type

Warning

Cause

A corrupted flash file system was found on the 3ware RAID controller during boot-up.

The 3ware RAID controller stores configuration parameters as files in its flash memory. These files can be corrupted when a flash operation is interrupted by events such as a power failure. The controller will attempt to restore the flash files from a backup copy.

Action

Update to the latest firmware, as earlier firmware resets corrupted files to default settings.

We recommend using 3DM, CLI or 3BM to check your settings, in case they were not able to be restored.

0040 Flash file system repaired

Event Type
Information

Cause
A corrupted flash file system has been successfully repaired.

Some of the flash files with insufficient data may have been lost in the operation. The configuration parameters which are lost will then return to their default values.

Action
We recommend using 3DM, CLI or 3BM to check your settings, in case they were not able to be restored.

0041 Unit number assignments lost

Event Type
Warning

Cause
The unit number assignments have been lost.

This may have occurred as a result of a soft reset.

Action
Please contact AMCC 3ware technical support at http://www.3ware.com/support/index.asp.

0042 Primary DCB read error occurred

Event Type
Warning

Cause
The controller found an error while reading the primary copy of the Disk Configuration Block (DCB).

The controller will attempt to correct the error by reading the back-up copy of the DCB. If a valid DCB is found, the primary DCB is re-written to rectify the errors.

Action

AMCC recommends verifying the unit. See “Starting a Verify Manually” on page 143.

0043 Backup DCB read error detected

Event Type

Warning

Cause

The controller has detected a latent error in the backup Disk Configuration Block (DCB).

The 3ware RAID controller checks the backup DCB, even when the primary DCB is OK. If an error is found, the controller will attempt to correct the error by reading the primary copy. If the primary copy is valid, the backup DCB will be rewritten to rectify the errors.

Action

AMCC recommends verifying the unit. See “Starting a Verify Manually” on page 143.

0044 Battery voltage is normal

Event Type

Information

Cause

The battery pack voltage being monitored by the Battery Backup Unit fell outside of the acceptable range and then came back within the acceptable range.

Action

None required

0045 Battery voltage is low

Event Type
Warning

Cause
The battery pack voltage being monitored by the Battery Backup Unit has fallen below the warning threshold.

Action
The Battery Backup Unit is presently still able to backup the 3ware RAID controller, but you should replace the battery pack if the warning continues.

0046 Battery voltage is high

Event Type
Warning

Cause
The battery pack voltage being monitored by the Battery Backup Unit has risen above the warning threshold.

Action
The Battery Backup Unit is presently still able to backup the 3ware RAID controller, but you should replace the battery pack if the warning continues.

0047 Battery voltage is too low

Event Type
Error

Cause
The battery pack voltage being monitored by the Battery Backup Unit is too low to backup the 3ware RAID controller.

You may see this message during a battery capacity test. In this case, it is not a sign of battery failure.

You may also see this message if the battery pack is plugged in while the computer is on. This is not advised.

Action

Replace the battery pack if none of the above causes apply and the warning continues.

0048 Battery voltage is too high

Event Type

Error

Cause

The battery pack voltage being monitored by the Battery Backup Unit is too high to backup the 3ware RAID controller.

Action

The battery pack must be replaced.

This may be a fault in the BBU control module. If you get this error, do the following:

1 Turn off the computer and remove the 3ware RAID controller.
2 Remove the BBU control module from the 3ware RAID controller and the battery module from the remote card.
3 Unplug the battery from the control module.
4 Return the BBU control module and battery module to 3ware.

For more details on removing the BBU, see the installation guide that came with your 3ware RAID controller.

0049 Battery temperature is normal

Event Type

Information

Cause

The battery pack temperature being monitored by the Battery Backup Unit fell outside of the acceptable range and then came back within the acceptable range.

Action

None required

004A Battery temperature is low

Event Type

Warning

Cause

The battery pack temperature being monitored by the Battery Backup Unit has fallen below the acceptable range. The most likely cause is ambient temperature.

Action

The Battery backup Unit is presently still able to backup the 3ware RAID controller, but you should replace the battery pack if the temperature warning persists and is not due to environmental reasons.

004B Battery temperature is high

Event Type

Error

Cause

The battery pack temperature being monitored by the Battery Backup Unit has risen above the acceptable range. However, the BBU is still able to backup the 3ware RAID controller.

Action

Check for sufficient airflow around the card. To increase airflow you can:

- Leave the PCI slots next to the controller empty
- Add fans to your computer case
- Move and bundle wiring that is blocking air circulation

The Battery Backup Unit is presently still able to backup the 3ware RAID controller, but you should replace the battery pack if the temperature warning persists.

Contact 3ware technical support at http://www.3ware.com/support/index.asp if this problem is not due to environmental reasons or improper case cooling.

004C Battery temperature is too low

Event Type
Error

Cause
The battery pack temperature being monitored by the Battery Backup Unit is too low.

The BBU is unable to backup the 3ware RAID controller.

Action
Contact 3ware technical support at http://www.3ware.com/support/index.asp.

The battery pack must be replaced if the problem persists and is not due to environmental reasons.

004D Battery temperature is too high

Event Type
Error

Cause
The battery pack temperature being monitored by the Battery Backup Unit is too high.

The BBU is unable to backup the 3ware RAID controller.

Action
Check for sufficient airflow around the card. To increase airflow you can:

- Leave the PCI slots next to the controller empty
- Add fans to your computer case
- Move and bundle wiring that is blocking air circulation

Contact 3ware technical support at http://www.3ware.com/support/index.asp if this problem is not due to environmental reasons or improper case cooling.

004E Battery capacity test started

Event Type
Information

Cause

A battery test was started through CLI or 3DM.

Background Information

The test estimates how many hours the Battery Backup Unit will be able to back up the 3ware RAID controller in case of a power failure.

This test performs a full battery charge/discharge/re-charge cycle and may take up to 20 hours to complete. During this test the Battery Backup Unit cannot backup the 3ware RAID controller. In addition, all units have their write cache disabled until the test completes.

Action

None required.

See Also

See the Install Guide for your controller.

004F Cache synchronization skipped

Event Type

Warning

Cause

The cache synchronization that is normally performed when power is restored after a power failure was skipped and write data is still being backed up in the controller cache. This can occur if a unit was physically removed or became inoperable during the power outage.

Action

Return missing drive(s) to the controller so that the missing write data can be saved.

0050 Battery capacity test completed

Event Type

Information

Cause

The Battery Backup Unit has completed a battery capacity test.

The BBU is again able to backup the 3ware RAID controller and write cache has been re-enabled for all units. (During the test, backup and write cache were disabled).

0051 Battery health check started

Event Type
Information

Cause

The Battery Backup Unit periodically evaluates the health of the battery and its ability to backup the 3ware RAID controller in case of a power failure. This health check has started.

0052 Battery health check completed

Event Type
Information

Cause

The Battery Backup Unit evaluates periodically the health of the battery and its ability to backup the 3ware RAID controller in case of a power failure. This message is posted to the host when this health check has completed.

0053 Battery capacity test is overdue

Event Type
Information

Cause

There has not been a battery capacity test run in the last 6 months, which is the maximum recommended interval. This message will be sent once every week until the test is run.

Action
AMCC recommends running the test at least once every 6 months, if the measured battery capacity is longer than 120 hours. If the measured battery capacity is less than 120 hours the recommended test interval is 4 weeks.

0055 Battery charging started

Event Type
Information

Cause
The Battery Backup Unit has started a battery charge cycle.

Action
None required

0056 Battery charging completed

Event Type
Information

Cause
The Battery Backup Unit has completed a battery charge cycle.

0057 Battery charging fault

Event Type
Error

Cause
The Battery Backup Unit has detected a battery fault during a charge cycle. The Battery Backup Unit is not ready and is unable to backup the 3ware RAID controller.

Action
Replace the battery pack.

See Also
See the Install Guide for your controller

0058 Battery capacity is below warning level

Event Type
Information

Cause
The measured capacity of the battery is below the warning level. The Battery Backup Unit is presently still able to backup the 3ware RAID controller, but it is weakening.

Action
Replace the battery pack if the warnings persist.

See Also
See the Install Guide for your controller.

0059 Battery capacity is below error level

Event Type
Error

Cause
The measured capacity of the battery is below the error level. The Battery Backup Unit is not ready and is unable to backup the 3ware RAID controller.

Action
Replace the battery pack.

See Also
See the Install Guide for your controller.

005A Battery is present

Event Type
Information

Cause
A battery pack is connected to the 3ware RAID controller.

005B Battery is not present

Event Type
Error

Cause
The battery pack has been removed from the 3ware RAID controller.

Action
Reinstall the battery pack.

005C Battery is weak

Event Type
Warning

Cause
The Battery Backup Unit periodically evaluates the health of the battery and its ability to backup the 3ware RAID controller in case of a power failure. This message is posted when the result of the health test is below the warning threshold.

Action
Replace the battery pack if warnings persist.

005D Battery health check failed

Event Type
Error

Cause
The Battery Backup Unit is not able to backup the 3ware RAID controller.

The Battery Backup Unit periodically evaluates the health of the battery and its ability to backup the 3ware RAID controller in case of a power failure. This message is posted when the result of the health test is below the fault threshold.

Action

Replace the battery pack. The BBU cannot presently backup the controller.

005E Cache synchronization completed

Event Type

Information

Cause

The 3ware RAID controller performs cache synchronization when system power is restored following a power failure. This message is posted for each unit when the cache synchronization completes successfully.

You will also see this message if drive insertion causes a unit to become operational and retained write cache data was flushed.

005F Cache synchronization failed; some data lost

Event Type

Error

Cause

The 3ware RAID controller performs cache synchronization when system power is restored following a power failure. The cache synchronization was not successful for some reason.

0062 Enclosure removed

Event Type

Warning.

Cause

Applies to only the 9690SA controller.

An enclosure is no longer accessible to the 9690SA RAID controller. The likely cause is that the enclosure has been powered down or that a cable has been unplugged.

0063 Enclosure added

Event Type
Information.

Cause
Applies to only the 9690SA controller.

An enclosure is now accessible to the 9690SA RAID controller. The likely cause is that an enclosure connected to the controller has been powered up or that a cable has been plugged in.

0064 Local link up

Event Type
Information.

Cause
Applies to only the 9690SA controller.

A cable has been plugged in, restoring a link to a controller phy.

0065 Local link down

Event Type
Warning.

Cause
Applies to only the 9690SA controller.

A cable has been unplugged, removing a link to a controller phy.

Appendices

The following information is available in the appendices:

A

Glossary

- **3BM.** The 3ware BIOS Manager, used on PC machines. The 3ware BIOS (Basic Input Output System) manager is a basic interface used to view, maintain, and manage 3ware controllers, disks, and units, without having to boot the operating system. 3BM is included with the controller and is updated when the controller firmware is upgraded. The latest firmware and code set is available for download from the 3ware web site: http://www.3ware.com/support/
- **3DM 2.** 3ware Disk Manager. The 3ware disk manager is a web-based graphical user interface that can be used to view, maintain, and manage 3ware controllers, disks, and units. It is available on the 3ware CD that came with your controller and can be downloaded from http://www.3ware.com/support/download.asp.
- **3ware.** Named after the 3 computer wares: hardware, software and firmware. A leading brand of high-performance, high-capacity Serial ATA (SATA) and SAS (Serial Attached SCSI) RAID storage solutions.
- **A-Chip**. AccerATA chip. Automated data port to handle asynchronous ATA disk drive interface.
- **AMCC.** Applied Micro Circuits Corporation provides the essential building blocks for the processing, moving and storing of information worldwide.
- **Array.** One or more disk drives that appear to the operating system as a single unit. Within 3ware software (3BM and 3DM), arrays are typically referred to as units.
- **Array Roaming.** The process of swapping out or adding in a configured unit without having to shut down the system. This is useful if you need to move the unit to another controller.
- **Background rebuild rate**. The rate at which a particular controller initializes, rebuilds, and verifies redundant units (RAID 1, RAID 5, RAID 6, RAID 10, RAID 50).
- **Boot volume size.** The size to be assigned to volume 0 when creating a unit through 3BM or CLI on a PC machine. Note that the resulting

volume does not have to be used as a boot volume. However, if the operating system is installed on the unit, it is installed in volume 0.

- **Carve size.** The size over which a unit will be divided into volumes, if auto-carving is enabled.
- **CLI**. Command Line Interface. The 3ware CLI is a text program, rather than a GUI (graphical user interface). It has the same functionality as 3DM, and can be used to view, maintain, and manage 3ware controllers, disks, and units.
- **Configuration**. The RAID level set for a unit.
- **Controller.** The physical card from 3ware that you insert into a computer system and connect to your disk drives or enclosure. The controller contains firmware that provides RAID functionality. 3ware makes a number of different models of SATA RAID controllers. (See “System Requirements” on page 2.)
- **Controller ID number.** Unique number assigned to every 3ware controller in a system, starting with zero.
- **Create an array**. The process of selecting individual disk drives and selecting a RAID level. The array will appear to the operating system as a single unit. Overwrites any existing unit configuration data on the drives. Note that in 3ware software tools, arrays are referred to as units.
- **DCB.** Disk configuration block. This is 3ware proprietary RAID table information that is written to disk drives that are in a RAID unit, single disk, or spare. The DCB includes information on the unit type, unit members, RAID level, and other important RAID information.
- **Delete an array.** Deleting an array (or unit) is the process of returning the drives in a unit to individual drives. This erases the DCB information from the drives and deletes any data that was on them. When a unit is deleted from a controller, it is sometimes referred to as being “destroyed.” If you want to remove a unit without deleting the data on it, do not delete it; instead use the Remove feature in 3DM, and then physically remove the drives.
- **Destroying**. Same as deleting a unit.
- **Degraded unit.** A redundant unit that contains a drive that has failed.
- **Disk roaming.** When moving a unit from one controller to another, refers to putting disks back in a different order than they initially occupied, without harm to the data.
- **Distributed parity.** Parity (error correction code) data is distributed across several drives in RAID 5, RAID 6, and RAID 50 configurations. Distributing parity data across drives provides both protection of data and good performance.

- **Drive ID**. A unique identifier for a specific drive in a system. Also called a port ID.
- **Drive Number**. The SCSI number, or channel number, of a particular drive.
- **ECC.** Error correction code. ECC Errors are grown defects that have occurred on a drive since it was last read.
- **ECC Error policy**. Determines whether an error detected during a rebuild stops the rebuild or whether the rebuild can continue in spite of the error. Specified by the Continue on Source Error During Rebuild unit policy.
- **Enclosure.** An enclosure houses drives and a backplane. The backplane may have an expander.
- **Expander.** Expanders are simple switches in enclosures that provide connectivity between the 3ware 9690SA RAID controller and the other devices in the SAS domain. Expanders allow one phy to connect to multiple drives. Expanders in enclosures attached to an external wideport of the 9690SA RAID controller can be cascaded up to 4 times.
- **Export a unit**. To remove the association of a unit with a controller. Does not affect the data on the drives. Used for array roaming, when you want to swap out a unit without powering down the system, and move the unit to another controller. Compare to Delete, which erases all unit configuration information from the drive.
- **Exportable unit or drive**. In 3BM (BIOS), exportable units and drives are those that will be available to the operating system when you boot your computer.
- **Fault tolerant**. A RAID unit which provides the ability to recover from a failed drive, either because the data is duplicated (as when drives are mirrored) or because of error checking (as in a RAID 5 unit).
- **Firmware.** Computer programming instructions that are stored in a read-only memory on the controller rather than being implemented through software.
- **Grown defect.** Defects that arise on a disk from daily use.
- **Hot spare.** A drive that is available, online, and designated as a spare. When a drive fails in a redundant unit, causing the unit to become degraded, a hot spare can replace the failed drive automatically and the unit will be rebuilt.
- **Hot swapping**. The process of removing a disk drive from the system while the power is on. Hot swapping can be used to remove units with data on them, when they are installed in hot swap bays. Hot swapping can also be used to remove and replaced failed drives when a hot swap bay is used.

- **Import a unit**. Attach a set of disk drives with an existing configuration to a controller and make the controller aware of the unit. Does not affect the data on the drives.
- **Initialize.** For 3ware SATA RAID controllers, initialize means to put the redundant data on the drives of redundant units into a known state so that data can be recovered in the event of a disk drive failure. For RAID 1 and 10, initialization copies the data from the lower port to the higher port. For RAID 5, 6, and 50, initialization calculates the RAID 5 parity and writes it to disk (background initialization). This is sometimes referred to as *resynching*, and does not erase user data. **Note:** If foreground initialization is done before the operating system has loaded, zeroes are written to all of the drives in the unit. This process, done through the 3ware BIOS, does erase existing data.
- **Logical Units.** This term is used in the 3ware CLI. It is usually shortened to "units." These are block devices presented to the operating system. A logical unit can be a one-tier, two-tier, or three-tier arrangement. Spare and Single logical units are examples of one-tier units. RAID 1, RAID 5, and RAID 6 are examples of two-tier units and as such will have sub-units. RAID 10 and RAID 50 are examples of three-tier units and as such will have sub-sub-units.
- **JBOD.** An unconfigured single drive. The acronym is derived from "just a bunch of disks." Note that earlier versions of the 3ware RAID controller exported JBODs to the OS. By default, this is not the case in 9000-series controllers. Individual drives should be configured as Single Disks in order to be made available to the OS.
- **Migration.** The process of changing the characteristics of a unit. The change can be to expand the capacity of the unit (OCE), change the stripe size of the unit, change the unit from redundant to non-redundant, change the unit from non-redundant to redundant, and to change the unit from one type of redundant unit to another type of redundant unit (for example RAID 1 to RAID 5).
- **Mirrored disk array (unit).** A pair of drives on which the same data is written, so that each provides a backup for the other. If one drive fails, the data is preserved on the paired drive. Mirrored disk units include RAID 1 and RAID 10.
- **NCQ (Native Command Queuing). See "Queuing"**
- **Non-redundant units.** A disk array (unit) without fault tolerance (RAID 0 or single disk.).
- **OCE (Online Capacity Expansion).** The process of increasing the size of an existing RAID unit without having to create a new unit. See also *migration*.
- **Parity.** Information that the controller calculates using an exclusive OR (XOR) algorithm and writes to the disk drives in RAID 5, RAID 6, and

RAID 50 units. This data can be used with the remaining user data to recover the lost data if a disk drive fails.

- **PCB**. Printed circuit board.
- **P-Chip.** PCI interface chip that connects the PCI bus to the high-speed internal bus and routes all data between the two using a packet switched fabric. There is one P-chip per controller card.
- **Phy.** Phys are transceivers that transmit and receive the serial data stream that flows between the controller and the drives. 3ware 9690SA controllers have 8 phys. These phys are associated with virtual ports (vports) by 3ware software to establish up to 128 potential connections with the SAS or SATA hard drives.
- **Phy Identifier.** The ID number (0-7) assigned to each of the 8 phys on the 9690SA controller.
- **Port.** 3ware controller models prior to the 9690SA series have one or many ports (typically 4, 8, 12, 16, or 24). Each port can be attached to a single disk drive. On a controller with a Multi-lane™ serial port connector, one connector supports four ports (eight if 24-port controller). On 9690SA series controllers, connections are made with phys and vports (virtual ports). See “phy” and “VPort”.
- **Port ID**. A unique identifier for a specific port in a system. Also called a drive ID.
- **Queuing.** SATA drives can use Native Command Queuing (NCQ) to improve performance in applications that require a lot of random access to data, such as server-type applications. When NCQ is enabled, the commands are reordered on the drive itself.

  NCQ must be supported by the drive. NCQ must be turned on in both the drive and the RAID controller. By default, the RAID unit’s queue policy is disabled when creating a unit.
- **RAID.** Redundant array of inexpensive disks, combined into a unit (array), to increase your storage system’s performance and provide fault tolerance (protection against data loss).
- **Rebuild task schedule**. The specification for when rebuilding, may occur, including start time and duration.
- **Rebuild a unit**. To generate data on a new drive after it is put into service to replace a failed drive in a fault tolerant unit (for example, RAID 1, 10, 5, 6, or 50).
- **Redundancy.** Duplication of data on another drive or drives, so that it is protected in the event of a drive failure.
- **Remove a drive.** The process of making a drive unavailable to the controller.

- **Remove a unit.** The process of making a unit unavailable to the controller and the operating system. After a unit is removed it can be hot swapped out of the system. This is sometimes referred to as exporting a unit.
- **RLM (RAID Level Migration).** The process of using an existing unit of one or more drives and converting it to a new RAID type without having to delete the original unit. For example, converting a single disk to a mirrored disk or converting a RAID 0 unit to a RAID 5 unit.
- **Self-test.** A test that can be performed on a scheduled basis. Available self-tests include Upgrade UDMA mode and Check SMART Thresholds.
- **Stagger time.** The delay between drive groups that will spin up, at one time, on a particular controller.
- **SAS.** SAS (Serial Attached SCSI) is a serial communication protocol for storage devices. The SAS protocol includes support for SAS and SATA devices.
- **SAS address.** Each SAS device (SAS drives, controllers, and expanders) has a worldwide unique 64-bit SAS address. Also known as World Wide Number (WWN). SATA drives do not have a WWN and are identified by a VPort ID.
- **SAS device.** SAS devices include SAS drives, controllers, and any expanders present in the SAS domain. Each SAS device has a unique 64-bit World Wide Number (WWN). SATA drives do not have a WWN and are identified by their VPort IDs
- **SAS domain.** The SAS domain includes all SAS and SATA devices that are connected to the 9690SA controller, either directly or through expanders.
- **SES (SCSI Enclosure Services).** The SES protocol allows the 9650SE and 9690SA RAID controllers to manage and report the state of the power supplies, cooling devices, displays, indicators, individual drives, and other non-SCSI elements installed in an enclosure.
- **Stripe size**. The size of the data written to each disk drive in RAID unit levels that support striping. The size of stripes can be set for a given unit during configuration. In general, smaller stripe sizes are better for sequential I/O, such as video, and larger strip sizes are better for random I/O (such as databases). The stripe size is user-configurable at 64KB, 128KB, or 256KB.

  This stripe size is sometimes referred as a “minor” stripe size. A major stripe size is equal to the minor stripe size times the number of disks in the unit.
- **Striping.** The process of breaking up files into smaller sizes and distributing the data amongst two or more drives. Since smaller amounts

of data are written to multiple disk drives simultaneously, this results in an increase in performance. Striping occurs in RAID 0, 5, 6, 10 and 50.

- **Subunit.** A logical unit of storage that is part of another unit. For example, the mirrored pairs (RAID 1) in a RAID 10 unit are subunits of the RAID 10 unit.
- **UDMA mode.** UDMA mode is a protocol that supports bursting data up to 133 MB/sec with PATA disk drives. This protocol is supported for earlier versions of 3ware RAID controllers, however it is not supported for the 9690SA series.
- **Unit ID**. A unique identifier for a specific unit in a system.
- **Unit Number**. The SCSI number, or channel number, of a particular unit.
- **Unit**. A logical unit of storage, which the operating system treats as a single drive. A unit may consist of a single drive or several drives. Also known as an array.
- **Verify**. A process that confirms the validity of the redundant data in a redundant unit. For a RAID 1 and RAID 10 unit, a verify will compare the data of one mirror with the other. For RAID 5, RAID 6, and RAID 50, a verify will calculate RAID 5 parity and compare it to what is written on the disk drive.
- **VPort.** The 3ware 9690SA RAID controller has 128 addresses available to assign to hard drives. These addresses are known as virtual port (vport) IDs. By using vport IDs and expanders, one controller phy can connect to multiple drives. This is in contrast to standard port connections which are one-to-one physical connections.
- **Wide Port**. A SAS port can consist of one or more phys. When a SAS port consists of one phy it is known as a narrow port, when it contains multiple phys it is known as a wide port. The 3ware 9690SA controller has two wide port connectors that contain 4 phys each. These phys can function individually, in which case each phy has its own SAS address, or the 4 phys can be banded together, in which case they share the same SAS address. A 9690SA wideport can have a bandwidth of up to 12.0 Gbps.
- **WWN (World Wide Number).** The unique worldwide 64-bit SAS address assigned by the manufacturer to each SAS port and expander device in the SAS domain. Many SAS drives have 2 ports and thus 2 WWNs.

B

Software Installation

This appendix provides detailed instructions for installing the 3ware management software for your 3ware RAID controller and the 3ware HTML Bookshelf.

You can install all software at once, or you can use the installer to install some or all of the following specific components:

- 3DM 2
- CLI (Command Line Interface)
- tw_update (Linux only), for updating the firmware
- 3ware HTML Bookshelf

If you install the disk management tool 3DM 2, you will be asked to specify some settings, such as email notifications and security settings. All of these settings can be modified later from the 3DM 2 software. You do not have to complete them at this time.

There are two versions of the installer: one for use in a graphical user interlace (Windows or Linux), and a console version, for use at a Linux command line.

Installing Software from a Graphical User Interface (GUI)

The steps below describe how to install the 3ware RAID management software from a windowing graphical user interface such as Microsoft Windows or X Windows in Linux.

To install the 3ware management software

1 With your computer on, insert the AMCC 3ware CD that came with your 3ware RAID controller.

The CD should automatically launch and display the AMCC License window. If it does not, you can start it manually.

- Under Windows, open **My Computer**, select the CD, right-click and choose **AutoPlay**.

- Under Linux, manually mount the CD by typing

  ```
  mount /dev/cdrom /mnt
  ```

  Start autorun by typing:

  ```
  /mnt/autorun
  ```

2 When the License screen appears, review and agree to the license in order to continue.

3 When the 3ware menu appears, click **Install Tools** to launch the installer.

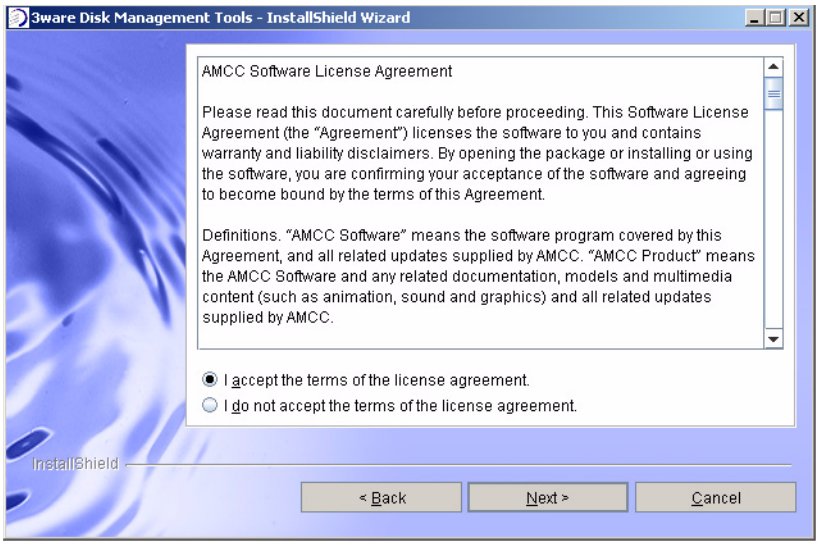
The installer will start and the welcome screen appears.

4 From the Welcome screen, click **Next** to start the installation process.

Figure 111. Welcome Installation Screen

5 On the License Agreement page, accept the agreement and click **Next**.

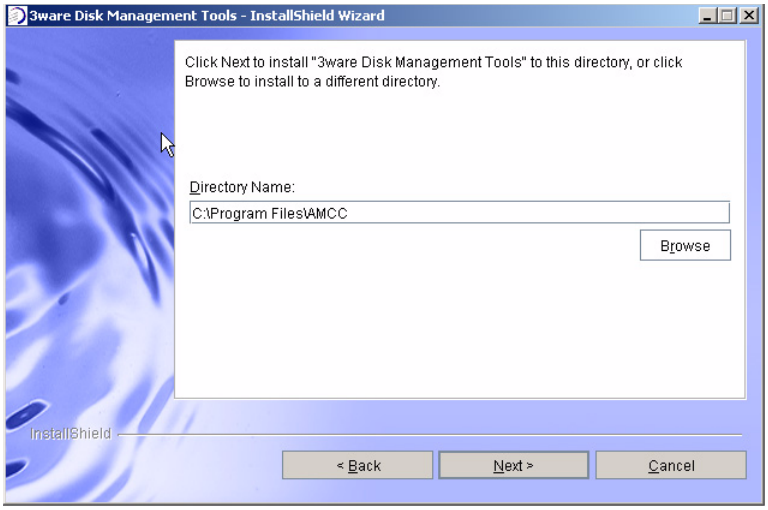
Figure 112. License Agreement Screen



6 If you want to change where the 3ware Disk Management tools 3DM and CLI will be installed, you can change the path and directory.

When you are ready, click **Next**.

Figure 113. Specify Directory Path Screen



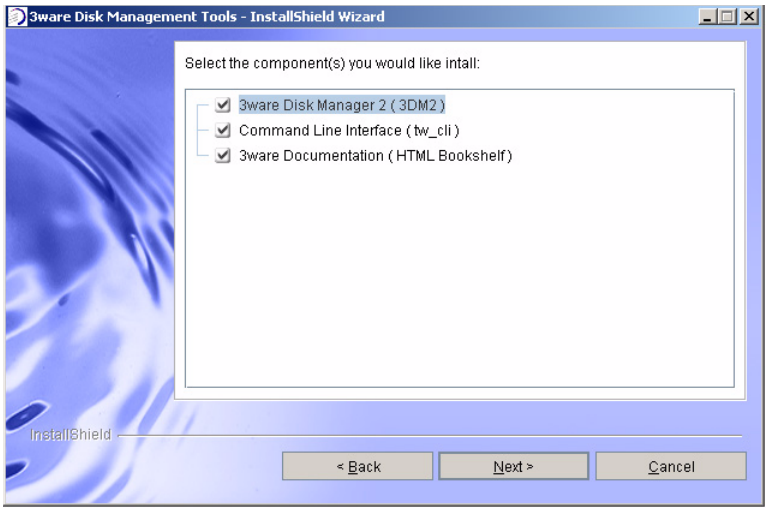
7 Select what components you want to install and click **Next**.

3DM and CLI are applications that let you set up and manage RAID units. 3DM is browser-based; CLI is a command line interface.

The Firmware Upgrade Utility lets you update the firmware on your controller, if required.

The 3ware Documentation option installs the 3ware HTML Bookshelf on your computer. This is a combined HTML version of the User Guide and CLI Guide.

Figure 114. Select Components to Install Screen



8 To configure email notification, check the box and complete the 3DM 2 Email Configuration screen.

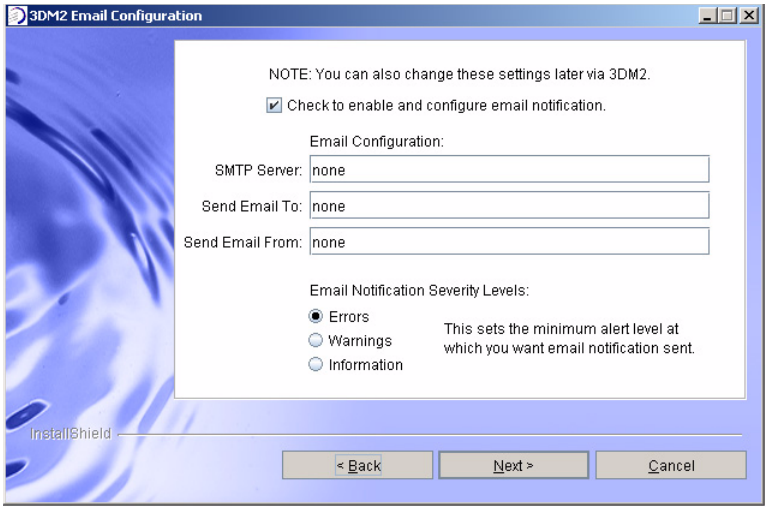
This features allows you to receive notification of problems with your 3ware RAID controller and units. For details about completing these fields, see “Managing E-mail Event Notification” on page 69.

You can select what level of notifications you want to be emailed about.

- **Errors.** You will be notified of Errors only.
- **Warnings.** You will be notified of Warnings and Errors.
- **Information.** You will be notified of Information, Warnings, and Errors.

When you are ready, click **Next** to continue.

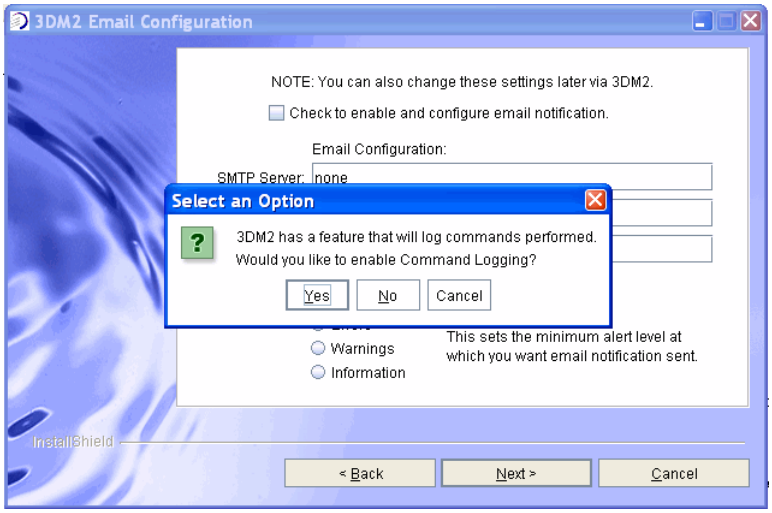
Figure 115. 3DM2 Email Configuration Screen



9 When a message asks you whether you want to enable 3DM command logging, click Yes to enable it, or No to disable it.

Command logging saves all changes you make to RAID configurations using 3DM to a special file. This information can be useful for troubleshooting problems with AMCC technical support.

Figure 116. 3DM2 Command Logging Message

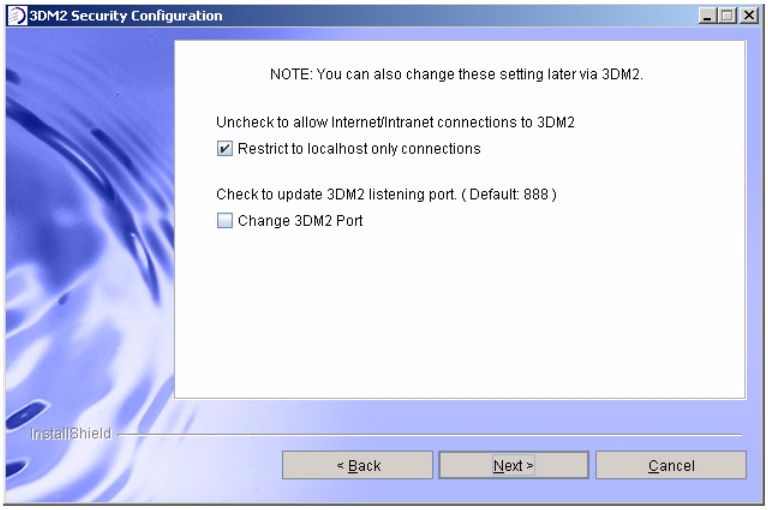


10 [Optional] On the 3DM 2 Security Configuration screen, specify whether you want to restrict access to localhost connections.

Enabling this feature prevents people from checking the status and administering the controller from across the Internet or Intranet.

If you want to allow people to remotely administer the controller, uncheck this box. For more information, see “Enabling and Disabling Remote Access” on page 70.

Figure 117. 3DM2 Security Configuration Screen

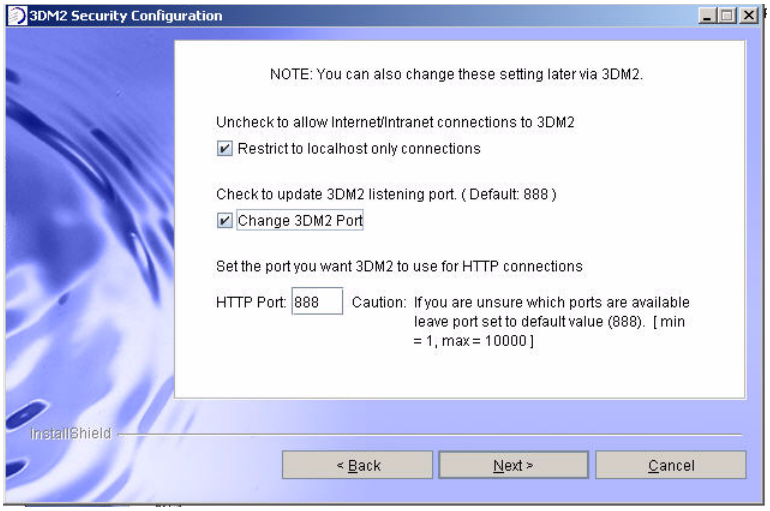


11 [Optional] On the same 3DM 2 Security Configuration screen, you can specify a different listening port than the default (888), if appropriate.

For more about this feature, see “Setting the Listening Port #” on page 70.

When you are ready, click **Next** to continue.

Figure 118. 3DM2 Specify Listening Port

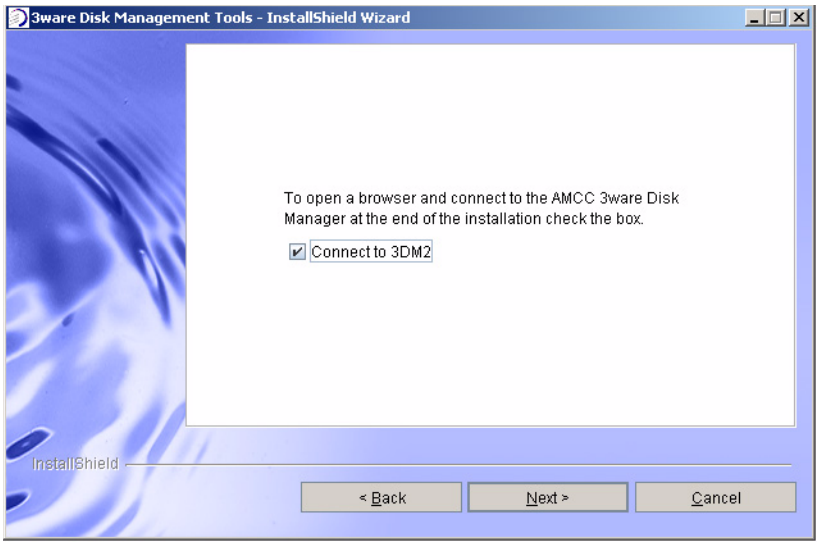


12 If you want the Installation Wizard to connect to 3DM 2 after you finish the wizard, check the **Connect to 3DM2** box. This allows you to log into 3DM and configure a RAID unit right away.

If you do not want to connect to 3DM 2 at this time, leave the box unchecked.

When you are ready, click **Next** to continue.

Figure 119. Final Installation Screen

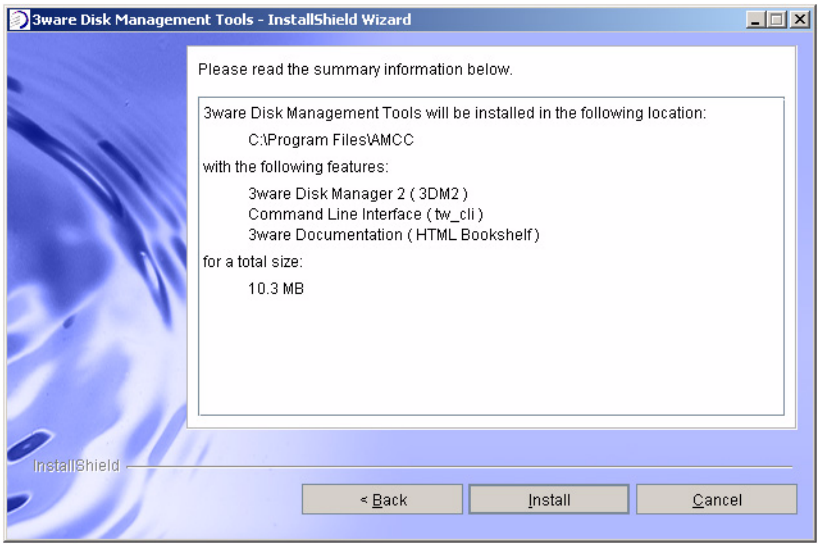


13 On the summary screen, review the installation that is about to occur.

If you want to make changes, use **Back** to move back through the screens.

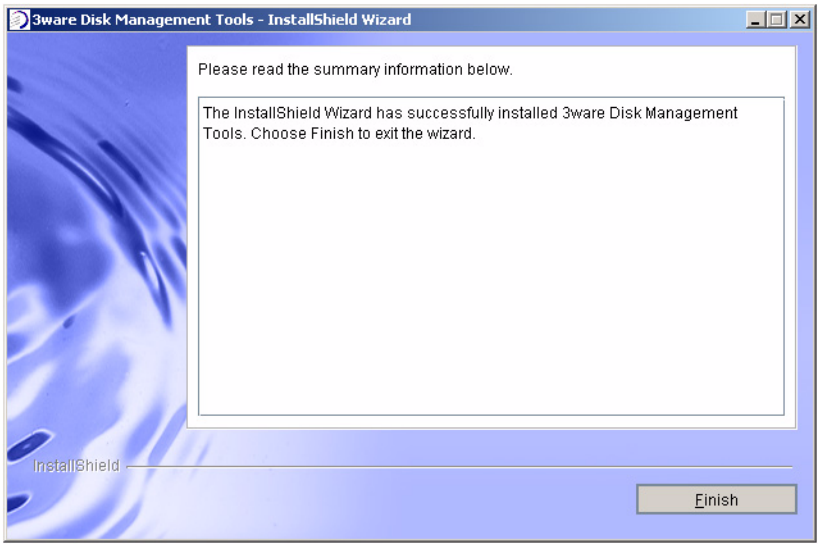
When you are ready, click **Install** to continue.

Figure 120. Installation Summary Screen



14 When the final installation screen lets you know that installation is complete, click **Finish**.

Figure 121. Final Installation Screen



Tip: You can now access the documentation through the 3ware HTML Bookshelf. For Windows, from the Start menu, choose **Programs > AMCC > Bookshelf shortcut**. For Linux, open a browser window to the following location:

```
/opt/AMCC/Documentation/index.html
```

For more information, see “Using the 3ware HTML Bookshelf” on page ix.

Installing Software on Linux from the Command Line

The following steps describe how to install software on Linux at a command line, using a console application.

To install software on Linux from the command line

1 Navigate to the folder containing the installer for your operating system and processor type (x86 or x64). It will be one of the following:

```
/packages/installer/linux/x86
/packages/installer/linux/x86_64
```

2 Type:

`./` [name of install file] `-console`

and press **Enter**.

The install file name will be one of the following, depending on your operating system and processor type.

```
./setupLinux_x86.bin -console
./setupLinux_x64.bin -console
```

3 After you press **Enter**, the application starts in text mode.

4 Respond to each screen as it walks you through the installation process.

The Console installation screens mirror those that display using the GUI installer. For specific information about the screens, see the previous section in this chapter.

To navigate in text mode, type:

1 for Next

2 for Previous

3 to Cancel

5 to Redisplay

0 to Continue Installing

Tip: You can now access the documentation through the 3ware HTML Bookshelf. Open your browser and enter `/opt/AMCC/Documentation/index.html`.
For more information, see “Using the 3ware HTML Bookshelf” on page ix.

Uninstalling Software

The steps below tell you how to remove 3ware software from your system.

Note: If 3DM is reinstalled or restarted, close any open web browsers before starting 3DM again to close the server socket.

Uninstalling 3DM under Microsoft Windows

Use the **Add or Remove Programs** control panel to uninstall 3DM.

- From the **Startup** menu, choose **Control Panels > Add or Remove Programs**.
- In the Add or Remove Programs control panel, select **3ware Disk Management Tools** and click **Change/Remove**.

Uninstalling 3DM under Linux

The following steps describe how to uninstall software on Linux from the command line. If you do not use the `-console` option, the installer will assume you want GUI mode. You must be root or superuser.

To uninstall 3DM for Linux

1 Navigate to the directory where you installed the software. The default directory is /opt/AMCC.

2 Change to the subdirectory "_uninst".

3 Type `./uninstaller.bin -console` and press Enter.

4 Follow the prompts to remove the installed components.

C

Compliance and Conformity Statements

This section is organized into the following topics:

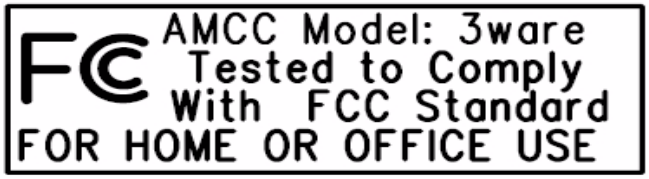
- FCC Radio Frequency Interference Statement
- Microsoft Windows Hardware Quality Lab
- European Community Conformity Statement

FCC Radio Frequency Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC (Federal Communications Commission) Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

To maintain compliance with FCC radio frequency emission limits, use shielded cables and connectors between all parts of the computer system.



Microsoft Windows Hardware Quality Lab

AMCC is committed to Microsoft Windows Hardware Quality Labs (WHQL) certification for all its products. However, a product's software drivers are typically submitted for certification at nearly the same time as their release to market. Since the certification process may lag behind the release of the drivers, please refer to our WEB site at www.3ware.com for current certification information.

European Community Conformity Statement

The Controller Models 9650SE, 9590SE, 9550SX, and 9690SA are in conformity with the following Common Technical Regulations and/or normative documents:

EN 55022 Limits and methods of measurements of radio interference characteristics of information technology equipment

EN 61000-4-2 Electromagnetic compatibility (EMC) Part 4: Testing and measurement techniques Section 2: Electrostatic discharge immunity test

EN 61000-4-3 Electromagnetic compatibility (EMC) Part 4: Testing and measurement techniques Section 3: Radiated, Radio-Frequency, Electromagnetic Field Immunity Test

EN 61000-4-4 Electromagnetic compatibility (EMC) Part 4: Testing and measurement techniques Section 4: Electrical fast transient/burst immunity test

EN 60950 Safety of information technology equipment, including electrical business equipment following the provisions of the Electromagnetic Compatibility Directive 89/23/EEC Low Voltage Directive

CE

.

D

Warranty, Technical Support, and Service

This section is organized into the following topics:

- Limited Warranty
- Warranty Service and RMA Process
- AMCC Technical Support and Services
- Sales and ordering information
- Feedback on this manual

Limited Warranty

RAID Controller Hardware. 3-Year Hardware Warranty: AMCC warrants this product against defects in material and workmanship for a period of thirty-six (36) months from the date of original purchase. AMCC, at no charge and at its option, will repair or replace any part of this product which proves defective by reason of improper workmanship or materials. Repair parts or replacement products will be provided by AMCC on an exchange basis and will be either new or refurbished to be functionally equivalent to new. Products or parts replaced under this provision shall become the property of AMCC.

Battery Backup Unit (BBU) Hardware. 1-Year Hardware Warranty: AMCC warrants this product against defects in material and workmanship for a period of twelve (12) months from the date of original purchase. AMCC, at no charge and at its option, will repair or replace any part of this product which proves defective by reason of improper workmanship or materials. Repair parts or replacement products will be provided by AMCC on an exchange basis and will be either new or refurbished to be functionally equivalent to new. Products or parts replaced under this provision shall become the property of AMCC.

Software Warranty: AMCC will replace a defective media purchased with this product for a period of up to 30 days from the date of purchase.

AMCC warranty service is provided by returning the defective product to AMCC.

Exclusions

This warranty does not cover any damage to this product which results from accident, abuse, misuse, natural or personal disaster, or any unauthorized disassembly, repair or modification. AMCC shall not be liable for any incidental or consequential damages, including but not limited to loss of profits, other loss, damage or expense directly or indirectly arising from the customer's misuse of or inability to use the product, either separately or in combination with other equipment, regardless of whether AMCC has been advised of the possibility of such damages. AMCC is not liable for and does not cover under warranty, any costs associated with servicing and/or the installation of AMCC products. This warranty sets for the entire liability and obligations of AMCC with respect to breach of warranty and the warranties set forth or limited herein are the sole warranties and are in lieu of all other warranties, expressed or implied, including warranties or fitness for particular purpose and merchantability.

State Law Provisions

This warranty gives you specific legal rights and you may have other rights which vary from state to state. Some states do not allow the exclusion of incidental or consequential damages or allow limitation of implied warranties or their duration, so that the above exclusions or limitations may not apply.

Warranty Service and RMA Process

To obtain warranty service during the warranty period, register at the 3ware website and submit an RMA request online at https://www.3ware.com.

You will be issued a return material authorization (RMA) number. AMCC will send a replacement in approximately two business days after receipt of the defective unit (transit time not included).

Advanced replacement is available with a credit card number with authorization in the amount equaling the then current list price of the 3ware Serial ATA RAID Controller, including shipping costs. As soon as practicable thereafter, AMCC will ship the advanced replacement to you at the address of your choosing. Upon receipt of the advanced replacement, we ask that you immediately ship the defective AMCC 3ware Serial ATA RAID Controller to AMCC, RAID Products RMA DEPT, 6290 Sequence Drive, San Diego, CA 92121. If AMCC receives the defective AMCC 3ware Serial ATA RAID Controller from you within thirty (30) days of the date of shipment of the advanced replacement, AMCC will destroy your credit card authorization and you will not be charged for the advanced replacement.

Please use the original packing material contents of the box when exchanging or returning a product.

For information about the status of a replacement, please contact AMCC Technical Support.

AMCC Technical Support and Services

Product information, Frequently Asked Questions, software upgrades, driver files and other support are available through the AMCC World Wide Web site at http://www.3ware.com. AMCC's 3ware software library is accessible at: http://www.3ware.com/support/download.asp

Web-based software downloads feature upgrading multiple switches simultaneously.

For specific answers to questions or to give feedback about the product, visit our Web site at http://www.3ware.com/support and use our convenient e-mail form. AMCC also offers toll-free 1 (800) 840-6055 or 1 (858) 535-6517 direct phone support during normal business hours.

Sales and ordering information

For sales information, send an electronic mail message to 3wareSales@amcc.com.

Feedback on this manual

Your feedback is welcome. If anything in the guide seems unclear please let us know. You can contact support by logging in and using Web Support at http://www.3ware.com/support/support.asp.

Index

Q

R

S