AMCC

STORAGE

User Guide

3ware®

Serial ATA RAID Controller

Supports the 9000 Series

PN 720-0114-01
March 2005

Table of Contents

About This Guide

3ware 9000 Series Serial ATA RAID Controller User Guide provides instructions for configuring and maintaining your 3ware controller.

This guide assumes that you have already installed your controller in your system. If you have not yet done so, see *3ware 9000 Series Serial ATA RAID Controller Installation Guide* for instructions.

How this Guide is Organized

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: one at the BIOS level (3ware BIOS Manager, or 3BM) and one that runs in a browser (3ware Disk Manager 2, or 3DM 2). 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, available from the 3ware software CD and from 3ware's website: *3ware 9000 Series Serial ATA RAID Controller CLI Guide*.

Basic information about using the two tools (3BM and 3DM), such as starting the tool, navigating between screens, and so forth, is described in sections about each of those tools: "3ware BIOS Manager (3BM)" on page 19 and "3ware Disk Manager (3DM 2)" on page 27.

Step-by-step instructions for performing specific tasks are organized by tasks throughout other sections of this guide. For example, the instructions for "Creating a New Unit" on page 85 include information about how to create a unit from 3DM, followed by how to create a unit from 3BM.

Table 1: Sections in this Guide

Section	Description
Introduction	Provides an overview of product features for the 3ware 9000 series controllers. Includes system requirements and an introduction to RAID concepts and levels.
Getting Started	Provides a summary of the steps required to install and set up your 3ware RAID controller.
3ware BIOS Manager (3BM)	Describes the basics of using 3BM.
3ware Disk Manager 2 (3DM 2)	Describes the basics of using 3DM and includes a reference of all the 3DM pages.
Configuring Your Controller	Describes how to view details about the controller, check it's status, and change configuration settings that affect the controller and all associated drives.
Configuring Units	Describes how to configure new units and spares, change existing configurations, and set unit policies.
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.
Maintaining Your Controller	Describes how to update the driver, move a unit from one controller to another, and replace an existing 3ware controller with a new one. Also includes information about checking battery status on a BBU (Battery Backup Unit).
Troubleshooting	Provides common problems and solutions, and explains error messages.
Glossary	Includes definitions for terms used throughout this guide.
Appendices	Provides compliance and conformity statements, warranty information, and tells you how to contact technical support.

Conventions

The following conventions are used through this guide:

- 3BM refers to the 3ware BIOS Manager

- 3DM refers 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 this 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.

Introducing the 3ware 9000 Series Controller

This chapter includes the following sections:

- "Product Features" on page 5
- "What's New With the 3ware 9000 Series Controller" on page 6
- "System Requirements" on page 6
- "Understanding RAID Concepts and Levels" on page 8
- "Determining What RAID Level to Use" on page 12

Product Features

The 3ware 9000 Series Serial ATA family includes 9500S-4LP, 9500S-8, 9500S-12, 9500S-8MI, 9500S-12MI.

Features of the 3ware 9000 series controllers include:

- Advanced RAID features for greater data protection and management.
- Support for battery backup provides added data protection in the event of a power outage. (Battery Backup unit sold separately)
- Support for RAID units greater than 2 terabytes with 64-bit LBA support.
- An enhanced firmware platform allows future upgrades. Anticipated upgrades include Enclosure Management Services (EMS).
- AMCC's remote management software, 3ware Disk Manager 2 (3DM®2) simplifies storage configuration and management via a web browser.

What's New With the 3ware 9000 Series Controller

Enhancements and changes in version 9.2 of the 9000-series controllers include the following:

- MultiLUN support with auto-carving of units greater than 2 terabytes into 2 terabyte volumes
- RAID Level Migration (RLM) and Online Capacity Expansion (OCE)
- Unit naming and unit serial number support
- Improved write performance in writes with multiple concurrent streams using Stream Fusion technology.
- Extended drive and unit status information.

System Requirements

3ware RAID controllers require the following

- **A workstation-class or server-class motherboard** which meets the following criteria:

  - PCI slots that comply with PCI 2.2 or above standards.
  - PCI slot that meets the Plug and Play and PC99 specifications.

  Note: For all 3ware 9000 series models, install the card in a 64-bit, 66 MHz PCI or PCI-X slot for best performance.

- **Drives**

  Depending on the particular model, the 3ware RAID controller may be connected to up to two, four, eight, or twelve SATA drives using the supplied interface cables.

  Drives must meet serial ATA 150 (SATA-1)or serial ATA 300 (SATA 2) Gb/s standards. Drives may be of any capacity or physical form factor.

  The length of shielded and unshielded interface cables may not exceed 1M (39") for serial ATA controllers.

- **Operating System**

  3ware RAID controllers may be used with:

  - Windows 2000 (SP3 or newer), Windows XP (SP1 or newer), Windows Server 2003, both 32-bit and 64-bit x64
  - Red Hat Linux, 32-bit and 64-bit x86
  - SuSE Linux, 32-bit and 64-bit x64

- Other versions of Linux using the open source Linux driver
- FreeBSD

■ **Other Requirements**

- Adequate air flow and cooling

- Adequate power supply for drives

3DM 2 (3ware Disk Manager) displays information in a browser. It requires the following:

- Internet Explorer 5.5 and later or Mozilla 1.2 or later

- JavaScript must be enabled

- Cookies must be enabled

- For best viewing, screen resolution should be 1024 x 768, with 16-bit color or more

For a complete listing of features and system requirements, refer to the 9000 Series Datasheet, available from the website at http://w.3ware.com/products/serial_ata9000.asp.

Understanding RAID Concepts and Levels

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

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 you work with 3ware software, "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 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 achieve highest transfer rates and performance at the expense of fault tolerance.

- **Distributed Parity**. Parity works in combination with striping on RAID 5 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 degraded drive or a bad drive in a redundant array.

- **Array Roaming.** The process of swapping out or swapping in a configured unit without having to shut down the system. This is useful if you need to move the unit to another controller.

- **Disk 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 can be attached to different ports than they were originally attached to, without harm to the data. The disks may be attached to the same ports or different ports on the controller.

For definitions of other terms used throughout the documentation, see the "Glossary" on page 179.

Available RAID Configurations

The following RAID levels and configurations are available for drives attached to a 3ware RAID controller:

- RAID 0
- RAID 1
- RAID 5
- RAID 10
- RAID 50
- Single Disk
- JBOD
- Hot Spare

RAID 0

Provides striping, but no mirroring or redundancy of any kind. Striped disk arrays achieve high transfer rates because they can read and write data on more than one drive simultaneously. The stripe size is configurable in the 3ware BIOS Manager (3BM) and in the 3ware Disk Manager (3DM 2). Requires a minimum of two drives.

When drives are configured in a striped disk array (see Figure 1), 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.

```
          RAID 0
         480 GB
        64K Stripe
```

```
   A        B        C        D
 120 GB   120 GB   120 GB   120 GB
```

Figure 1.   RAID 0 Configuration Example

RAID 1

Also known as a mirrored array. Mirroring is done on pairs of drives. Mirrored disk arrays write data to two drives using RAID 1 algorithms (see

Figure 2). 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 mission 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.

```
RAID 1
30 GB
MIRROR
```

Figure 2. RAID 1 Configuration Example

RAID 5

Combines striping data with parity (exclusive OR) to restore data in case of a drive failure. This array type provides performance, fault tolerance, high capacity, and storage efficiency. Requires a minimum of three drives.

Parity information is distributed across all drives rather than being concentrated on a single disk (see Figure 3). This avoids throughput loss due to contention for the parity drive.

RAID 5

A Blocks	B Blocks	C Blocks	D Blocks	E Blocks
0 parity	B0	C0	D0	E0
A1	1 parity	C1	D1	E1
A2	B2	2 parity	D2	E2
A3	B3	C3	3 parity	E3
A4	B4	C4	D4	4 parity
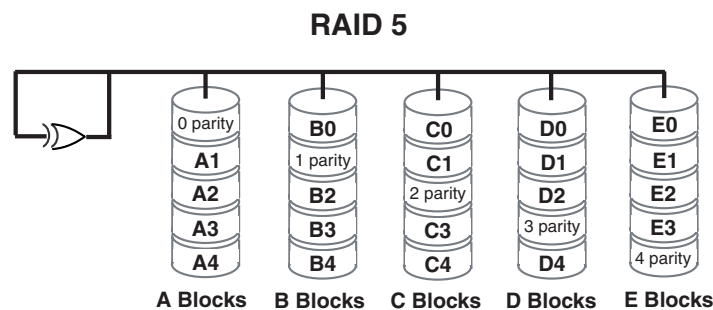
Figure 3. RAID 5 Configuration Example

RAID 10

This array is a combination of RAID 1 with RAID 0. Striped and mirrored arrays for fault tolerance and high performance. Requires a minimum of four drives to use both RAID 0 and RAID 1 techniques.

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 4). 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. RAID 10 is available on the four, eight, and twelve port 3ware Serial ATA RAID Controllers.
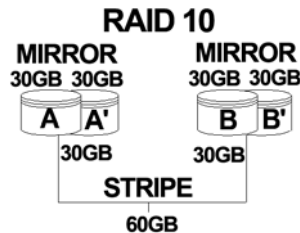
Figure 4.   RAID 10 Configuration Example

RAID 50

This array is a combination of RAID 5 with RAID 0. This array type provides fault tolerance and high performance. 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.

Single Disk

A single drive that has been 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 take to prevent system hangs and data loss.

JBOD

A JBOD is an unconfigured disk attached to your 3ware RAID controller. JBOD configuration is no longer supported in the 3ware 9000 series. AMCC recommends that you use Single Disk as a replacement for JBOD, to take advantage of advanced features such as caching, OCE, and RLM.

JBOD units 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 single drive, available online, so that a redundant array can be automatically rebuilt in case of drive failure.

For additional information about RAID levels, see the article "RAID Primer" on the 3ware website, at: http://www.3ware.com/products/pdf/RAID_Primer.pdf.

Determining What RAID Level to Use

Select the RAID configuration to use based on the applications to be used on the system, whether performance or data protection is of primary importance, and the number of disk drives available for use.

Review the information under "Understanding RAID Concepts and Levels" on page 8 to determine the type of RAID configuration most appropriate for your needs and use the tables below to determine what RAID levels are available, based on your particular controller model and the number of available drives.

The RAID configurations available to you are determined by the number of ports on your controller, and the number of drives attached to those ports. You can configure all drives in one unit, or you can configure multiple units, if you have enough drives.

Table 2: Possible Configurations Based on Number of Drives

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

Table 2: Possible Configurations Based on Number of Drives

# Drives	Possible RAID Configurations
6 or more	RAID 50 Depending on the number of drives, a RAID 50 may contain from 2 to 4 subunits. For example, with 12 drives, possible RAID 50 configurations include 2 subunits of 6, 3 subunits of 4, or 4 subunits of 3. With 10 drives, a RAID 50 will contain 2 subunits of 5 drives each. Combination of RAID 0, 1, 5, 10, hot spare, and single disk

Drive Capacity Considerations

The capacity of each drive is limited to the capacity of the smallest drive in the array. The total array capacity is defined as follows:

Table 3: Drive Capacity

RAID Level	Capacity
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 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), 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 drives will be rounded. down to 120 GBytes. For more information, see the discussion of drive coercion under "Creating a Hot Spare" on page 92.

Support for Over 2 Terabytes

Windows 2000, Windows XP, Linux 2.4, and FreeBSD 4.x, 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.

For more information, see See "Multi LUN Support and Auto-Carving" on page 79.

3ware Tools for Configuration and Management

3ware software tools lets 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 several tools for use in configuring and managing units attached to the 3ware controller:

- 3BM (3ware BIOS Manager)
- 3DM 2 (3ware Disk Manager)
- 3ware CLI (Command Line Interface)

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 "3ware BIOS Manager (3BM)" on page 19.

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. 3DM supports hot spare and hot swap for redundant units.

3DM can be used locally (on the system that contains the 9000) or remotely (on a system connected via a network to the system containing the 9000).

For details about working with 3DM, see "3ware Disk Manager (3DM 2)" on page 27.

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

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 also use it to remotely administer controllers in a system by first logging into the system.

The 3ware CLI is described in *3ware 9000 Series Serial ATA RAID Controller CLI Guide*.

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. (For details, see "Viewing SMART Data About a Drive" on page 118.)

- **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). For details, see "Enabling and Setting Up Staggered Spinup" on page 78.

- **Verification and Media Scans.** The verify task verifies all redundant units, and checks for media errors on single disks, spares, JBODS 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.

- **Error Correction**. Bad sectors can be dynamically repaired through error correction (Dynamic Sector Repair). Reallocation of blocks will try to be 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.

- **Write Cache**. Write cache can be enabled or disabled using 3BM, 3DM2 and CLI. When write cache is enabled, data will be stored in system cache, 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 occurred. With a Battery Backup Unit (BBU) installed, the cache stored on the 3ware controller can be restored. For more information, see "Updating the 3ware Driver Under Windows XP" on page 146.

Getting Started with Your 3ware RAID Controller

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

- Physically Install the Controller and Drives
- Configure the RAID Unit and Drives
- Install the Drivers 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.

Physically Install the Controller and Drives

To install your controller and drives, follow the instructions in *3ware 9000 Series Serial ATA RAID Controller Installation Guide*. If you do not have a hardcopy of this manual, you can download it from the 3ware website at http://www.3ware.com/support/userdocs.asp

Configure the RAID Unit and Drives

You may want to review the information under "Understanding RAID Concepts and Levels" on page 8 before configuring your drives. This information will help you choose the appropriate RAID level for your situation.

If you will 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 in the installation guide, following the instructions for installing the card.

Information about using 3BM is also included in this user guide, but the installation guide offers a sequential set of steps for initial installation.

If the operating system is already installed on another drive in your system, you can configure the drives through either 3BM or through 3ware Disk Manager (3DM). If you want to use 3DM for configuration, go ahead and boot to the OS, install the drivers and the 3DM 2 software, and then configure your units. For details about using 3DM, see "3ware Disk Manager (3DM 2)" on page 27.

> **Note:** The ability to configure RAID units, single drives, and hot spares through 3DM is new with version 2 of 3DM (3DM 2). If you previously used 3DM version 1.x, configuration was not available in that version.

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

Complete instructions for installing drivers and completing the installation under Windows, Red Hat Linux, SuSE Linux, and FreeBSD are provided in *3ware 9000 Series Serial ATA RAID Controller Installation Guide*.

You will also find instructions for updating the driver under "Updating the Driver and Firmware" on page 140.

Set Up Management and Maintenance Features

3ware RAID controllers come with software that 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 staggered spinup, use of write cache, and how unconfigured disks (JBODs) are handled
- 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.

Details about these features are described in this user guide and can be looked up individually. When you first set up your controller, you may want to review these sections in particular:

- "Configuring Your Controller" on page 73
- "Setting Unit Policies through 3DM" on page 97
- "Setting Background Task Rate" on page 124
- "Scheduling Background Tasks" on page 125

3ware BIOS Manager (3BM)

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 9000-series RAID controller.

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

Note: While the basics of working with 3BM for the 9000 series are similar to working with the 3ware Disk Array Configuration utility for the 7000 and 8000 series, the screens have changed, and some additional features are provided. If you have a 7000- or 8000-series controller, the BIOS screens you see will be somewhat different than those shown in this chapter. For instructions specific to the BIOS manager for 3ware 7000- and 8000-series controllers, see the *3ware Escalade ATA User Guide for 7000 & 8000 Series Controllers*, available from the 3ware website, `http://www.3ware.com/support/userdocs.asp`

This section is organized into the following topics:

- "Starting 3BM" on page 20
- "Working in the 3BM Screens" on page 22
- "Displaying Advanced Details" on page 25
- "Getting Help While Using 3BM" on page 25
- "Exiting the 3BM Configuration Utility" on page 26

Starting 3BM

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

To start 3BM

1 Power up or reboot your system.

2 While the system is starting, watch for a screen similar to Figure 5.

```
3ware ATA RAID Controller: Escalade 9500S-12
BIOS: BE9X X.XX.XX.XXX   Firmware: FE9X X.XX.XX.XXX

Unit 0 -         Mirror            111.74GB
  Port 0    - IC35L120AVVA07-0            115.03 GB
  Port 1    - IC35L120AVVA07-0            115.03 GB

Following drives will not be exported to OS:
Port 2   - IC35L120AVVA07-0           115.03 GB Unconfigured Disk
Port 3   - IC35L120AVVA07-0           115.03 GB Unconfigured Disk

----Press <Alt-3> to access 3ware BIOS Manager ----
```

Figure 5.   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 have more than one 9000-series controller in your system, a screen lists the available boards. (See Figure 6.) In this case, highlight the board with which you want to work and press **Enter**.

```
                      3ware Boards selection
   Board at slot:  3

   Board at slot:  5













        Help  ↕↔ Previous/Next     Enter Go into highlighted board
                          Esc Cancel              F8 Done
```

Figure 6.   3ware Controller Board Selection Screen

You see a screen similar to Figure 7, warning you that changing your disk array configuration may overwrite data on the disks.

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.
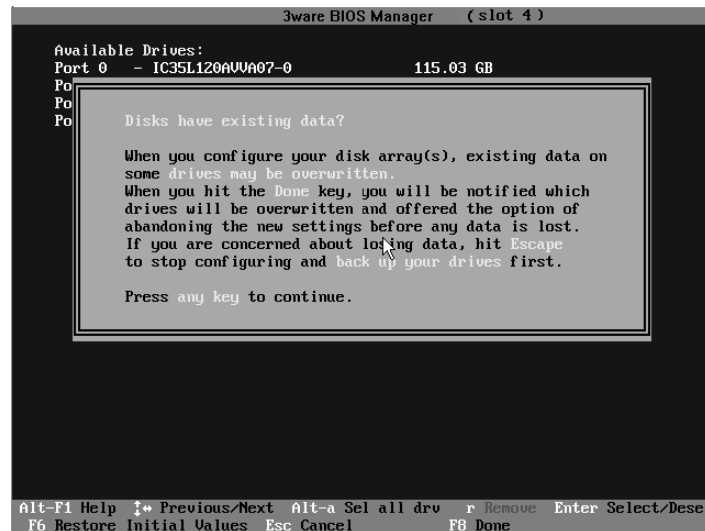
Figure 7.   Warning Message When you Start 3BM

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

> **Note:** If you have a combination of 7000/8000-series and 9000-series controllers in your system, the 7000/8000-series controllers are not listed on the selection screen shown in Figure 6. Instead, an additional BIOS summary will appear for the 7000/8000-series controller, similar to Figure 5. To access the BIOS utility for the 7000/8000-series board, press **Alt-3** when the information for that controller appears, to enter the BIOS software. Although similar to 3BM, some screens and features are different for the 7000/8000-series. For detailed information, see the version of the *3ware Escalade ATA RAID Controller User Guide* that supports the 7000 and 8000 series controllers.
>
> If you have two 9000 controllers that have different versions of the BIOS installed, they will also appear in different BIOS summaries, and will launch different versions of 3BM.

Working in the 3BM Screens

The main **3BM** screen (Figure 8) 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.
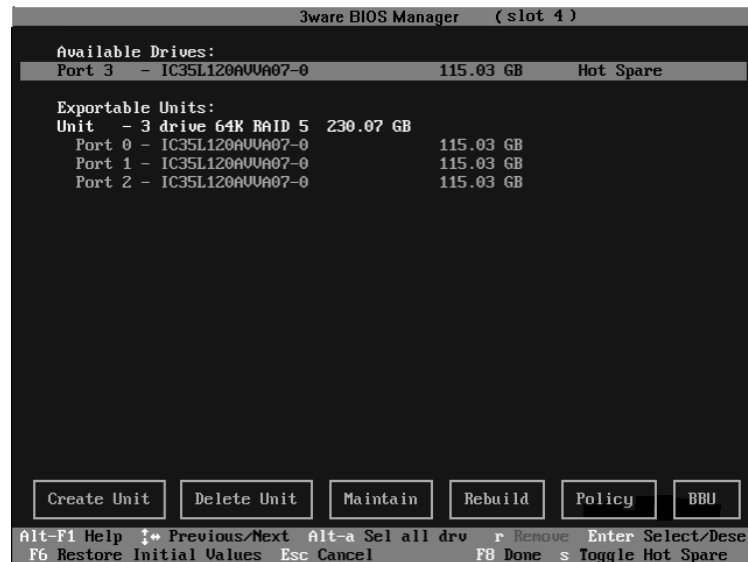
Figure 8. 3BM Main Display

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

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

- **Exportable Units** lists the existing units, along with the drives contained in each. 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, drives that are not usable, and drives that were part of a unit on a 3ware 7000/8000-series controller, and contain data that needs to be updated before your 3ware 9000 series controller can use them. (If you want to move a unit from a 7/8000 controller to the 9000 controller, you must convert the drives first. For more information, see the

section "Replacing an Existing Controller with a New Controller," in the
3ware 9000 Series Serial ATA RAID Controller Installation Guide.)

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 103.

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

Table 4 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 4: Working in 3BM

To do this	Use these keys
Move between units or drives in a list, and between fields, and 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
Highlight one of the primary buttons on the main screen: ■ Create ■ Delete ■ Maintain ■ Rebuild ■ Policy ■ BBU	 Alt+C Alt+D Alt+M Alt+R Alt+P Alt-B
Specify (or unspecify) a drive as a hot spare	S

Table 4: Working in 3BM

To do this	Use these keys
Unlock the drives in a unit, so that they can be removed and used with a controller other than a 9000-series controller.	R (Remove)
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.
Display the Advanced Detail screen, where you can see the software versions (BIOS, Firmware, monitor), serial number, controller and model number, cache memory size, slot # of the 3ware card, and whether or not BBU-support is available.)	Shift+F5
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

Displaying Advanced Details

The Advanced Details screen shows you details about your controller, and about the version of associated software installed on your system.

To see the advanced details

◼ Press **Shift**+**F5** from the main screen.

(Note that the particular versions shown in the screen shot below may not be current.)

Figure 9. Advanced Detail Screen

To return to the main screen

◼ Press **any key**.

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.

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: Any changes made to policies are saved when you leave the Policy screen. Pressing **F8** is not required to save those changes. For details about changing policies, see "Setting Policies for a Controller through 3BM" on page 76.

3ware Disk Manager (3DM 2)

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 view the status of and manage 3ware RAID controllers and associated drives. 3DM runs as a service under Microsoft Windows, and as a daemon under Linux. When it is running, you can use your browser to view status and perform administrative tasks locally or remotely.

3DM 2 can display information about 3ware RAID 7000-, 8000- and 9000-series RAID controllers. However, some version 2 features are only available for 9000-series controllers.

Two levels of access are provided: user and administrator. Users have view-only access—they can check the status of drives and units—while 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 overview, information is organized into the following topics:

- "Browser Requirements for 3DM" on page 28
- "Installing 3DM" on page 29
- "Starting 3DM and Logging In" on page 34
- "Working with the 3DM Screens" on page 37
- "Setting Up 3DM Preferences" on page 41
- "3DM 2 Reference" on page 45, which contains information about the fields and settings on each page in 3DM.

For additional information about doing particular tasks in 3DM, see the remaining sections in this guide

Browser Requirements for 3DM

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

- Mozilla 1.2 and above

- Internet Explorer 5.5 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 chapter are examples only. (Screenshots were taken in Internet Explorer.) The actual "look" of the windows will depend on the browser, 3DM version and operating system in use.

Setting up Mozilla

Details about accessing all ports, including port 888, by adding a list of ports to /Mozilla/default/all.js

> **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 to add a comma-separated list of ports to default/all.js (in your Mozilla installation directory). For example, to unblock port 888, use 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 main 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.

3DM must be installed on the system in which the controller is installed. 3DM does not have to be installed on remote systems in order to remotely manage a 3ware controller.

During installation, you will be asked to enter the following preferences for 3DM use. (Each of these preferences can be changed later, from within 3DM.)

- The HTTP port to be used as the listening port
- Whether remote access will be allowed
- Whether you want email alerts to be sent when errors occur, and who should receive them

Installing 3DM on a Microsoft Windows system

The 3ware RAID controller works with Windows 2000, Windows XP, and Windows Server 2003. The latest service packs should be installed for any Windows release.

To install 3DM on a Windows system

1 Insert the 3DM CD-ROM and click **Install 3DM 2** when the menu appears.

   Or, if you downloaded 3DM from the website, find the file setup.exe and double-click it to launch the setup.

2 If a command window opens, press any key to begin the installation process.

3 When the License Agreement screen appears, read and agree to the license information; then let the InstallShield Wizard guide you through the installation process.

4 On the **3DM Remote Monitoring and Security Configuration** screen (see Figure 10), use the settings to specify these things:

   - To change the HTTP port that 3DM will use as a listening port, check the first box.

     If you do not know which port to use, leave the box unchecked and use the default port.

   - To allow remote administration, uncheck the second checkbox.

     When the second checkbox is checked, only localhost connections are allowed. Internet and Intranet connections are not allowed.

(You can change this setting later in 3DM.)

Figure 10. 3DM Remote Monitoring and Security Configuration Display

5   If the **3DM HTTP listening port setup** screen appears, enter the HTTP port you want to use.

This screen only appears when you check the first box on the **3DM Remote Monitoring and Security Configuration** screen.

(You can change this setting later within 3DM.)

6   On the **E-mail Notification Preferences** screen (see Figure 11) use the fields to specify initial email settings.

> **Note:** If you do not want email alerts to be sent to anyone, leave "None" in these fields and click **Next** to go on to the next screen.

■   In the **Server** field, enter the name or IP address of your email server.

You can get the IP address of your mail server by typing

nslookup <file server name>

To find the mail server name, ask your system administrator or check the e-mail preferences or setup options on your e-mail client.

■   In the **Recipients** field, enter the e-mail address of the user who should receive the 3DM e-mail status messages.

You may enter multiple e-mail addresses, separating each entry with a comma (,).

■   In the **Sender** field, enter the email address from which the email notifications will be sent. This is typically the local host name.

(You can change these settings later within 3DM.)
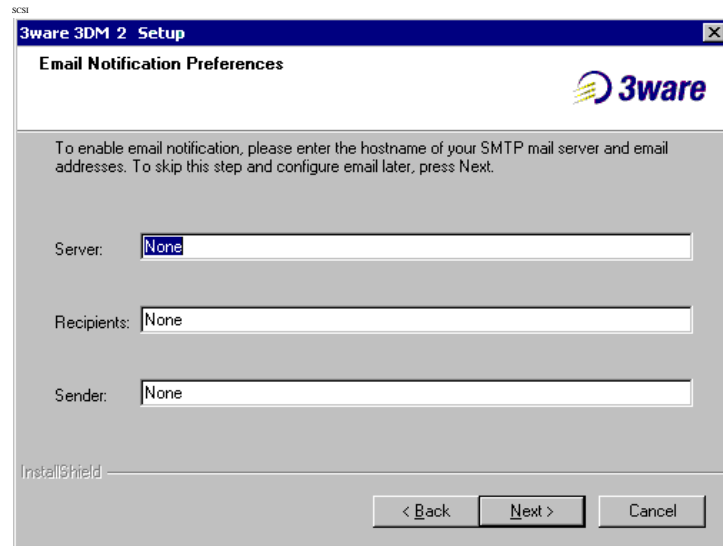
Figure 11.   3DM E-mail Notification Preferences

7   Continue with the installation as prompted, clicking **Next** to move to the next screen, and **Finish** when you reach the last screen.

3DM Installation gives you the option of starting 3DM and opening the browser window.

8   If you elect to launch the web interface, a Security Alert may appear, as shown in Figure 12. Click **Yes** continue.

You may install the certificate if you do not want to see this alert in the future. To do so, click View Certificate and then click Install Certificate.
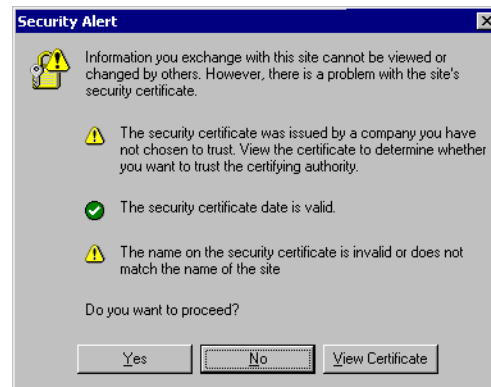
Figure 12.   Security Alert dialog box

9   When the first 3DM screen appears in your browser, log in as Administrator and use the default password, 3ware.

> **Notes:**
> You can start 3DM later by choosing **3DM** from the **Start** menu.
>
> If you change, add, or remove an IP address, or change the machine name of the machine on which you have installed 3DM 2, you will need to recreate the security certificate. You can do so by re-installing 3DM 2, or by deleting the file 3dm2.pem and restarting the 3DM 2 service. Under Windows, this file is located in the same directory in which you installed 3DM 2. Under Linux, the file resides in /etc/3dm2. You may also want to delete the installed/cached security certificate from your browser.

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 **3DM** and click **Change/Remove**.

Installing 3DM for Linux or FreeBSD

You can install 3DM from the command line, or from a GUI. The steps below describe how to install 3DM from the command line. If you are using a GUI, you can access the CD-ROM and folders from the windows in the GUI.

> **Note:** If you downloaded 3DM_Linux.zip from the website, unzip the file to root (or to any other working directory) and change Directory (CD) to that directory (for example: `/root`). Then start the following procedure at step 3, substituting `/mnt` with `/root` or your installation directory.

To start the installation

1 Insert the 3ware software installation CD-ROM for Linux into the CD-ROM drive.

2 Mount the CD-ROM disk:

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

3 Change the directory and run the install script:

For Linux:32-bit x86 systems
```
cd /mnt/packages/3dm2/linux/x86
./install.3dm
```

For Linux:64-bit systems
```
cd /mnt/packages/3dm2/linux/x86_64
./install.3dm
```

For FreeBSD 32-bit x86 systems:
```
cd /mnt/packages/3dm2/freebsd/x86
./install.3dm
```

To specify initial setup for 3DM 2

During installation, you will be prompted with a series of questions that determine initial 3DM settings. You can change these later, from within 3DM.

(The first question appears for Linux, but not for FreeBSD.)

1   Was RPM used to install the Escalade driver and/or 3DM?

   The default answer is no. ("RPM" stands for RedHat Package Manager.)

2   Please enter the location of the help documentation (default is /usr/local/doc/3dm)

   Press Enter to accept the default location and display the next question, or enter the path at which you want the documentation to be installed.

3   Would you like to have e-mail notification enabled (Y/N)?

   E-mail notification sends an email message when an event occurs.

   The default answer to this question is "yes".

   If you enable e-mail notification you will be asked to provide additional information: the name of the mail server, the user name for the person who will send the E-mail notification (typically the local host name) and the user name for the person who will receive the e-mail notification (typically the system administrator).

```
Please enter the name of your mail server: (default is local
host name)
Please enter the name of the user you want sending e-mail
notification: (default is root)
Please enter the name of the user you want receiving e-mail
notification: (default is 3ware_admin)
```

   To enter multiple e-mail addresses, separate them by a comma or a semicolon:

4   Please enter the port number you would like to use for web monitoring (default is 888)

   If you do not know what port to use, select the default:

5   Would you like 3DM connection security to limit connections to localhost only? (default is yes)

   If you want to be able to use 3DM for remote administration, change this to No.

6   Change the directory and then eject the CD-ROM disk when finished:
```
cd /home
eject cdrom
```

Uninstalling 3DM under Linux or FreeBSD

To uninstall 3DM for Linux or FreeBSD

1 Insert the 3ware software installation CD-ROM into the CD-ROM drive.

2 Mount the CD-ROM disk:

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

3 Change the directory and run the uninstall script:

(For FreeBSD, replace "linux" with "freebsd" in the path shown in this step.)

For Linux:32-bit x86 systems
```
cd /mnt/packages/3dm2/linux/x86
./install.3dm --u
```

For Linux:64-bit systems
```
cd /mnt/packages/3dm2/linux/x86_64
./install.3dm --u
```

Note that if you downloaded 3DM from the web, replace "/mnt/" in the previous command with "/root/"

4 Eject the CD-ROM disk when finished:
```
cd /home
eject cdrom
```

> **Note:** If 3DM Linux is reinstalled or restarted, close any open web browsers before starting 3DM again to close the server socket.

Starting 3DM and Logging In

3DM runs as a service under Windows, and as a daemon under Linux.

It is a good idea to leave 3DM 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.

You can access the 3DM screens to check status information and manage your 3ware RAID controller by logging in to the 3DM screens in your browser.

Starting 3DM under Linux

3DM should start automatically after installation and upon bootup.

To start 3DM manually

1   Login as root.

1   Afterwards, type:

For Red Hat Linux:
```
/etc/rc.d/init.d/3dm start
```

For SuSE Linux:
```
/etc/rc.d/3dm start
```

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

The default URL is `https://localhost:888/` for 32-bit versions of Linux.

For 64-bit versions of Linux, use: `http://localhost:888/`

(Note that 32-bit versions require https, while 64-bit versions require http—without the "s.")

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 are using a 64-bit AMD processor with a 64-bit version of Linux, use "http://" instead of "https://".

The 3DM login screen appears.

Starting 3DM under Microsoft Windows

■ From the Start menu, choose **Programs > 3ware > 3DM 2.**

Your default browser opens and displays the URL for your local controller.

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

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 close your browser, 3DM continues to run in the background on the system.

Viewing 3DM Remotely via a Standard Web Browser

When remote administration is enabled, 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.

Remote connections can be enabled or disabled from the 3DM 2 Settings Page.

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

  If you don't 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`.

Logging In

When you first view 3DM in a browser, you must log in before you can view or change any information.

Two levels of access are provided:

- Users can check the status of the controller, units, and drives attached to it.

- Administrators can check status, configure, and maintain the equipment.

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

To log in to 3DM

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

2   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`.

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 13. 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.

3DM Menus

The 3DM menu bar groups access to a number of 3DM pages on menus, and provides direct link access to others.
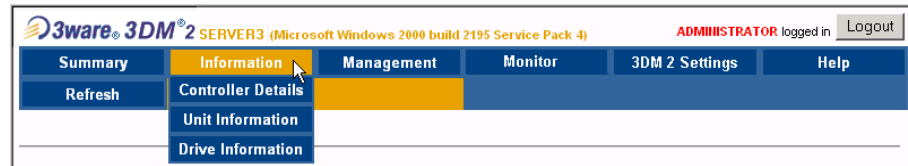
Figure 14.   3DM Menu Bar

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 names, enabling of unit write cache, and policies 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 and the BBU 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 **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.

Help lets you access information about using 3DM, and provides access to an electronic copy of this User Guide.

Viewing Information About Different Controllers in 3DM

If you have more than one 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.

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

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 43.

Note: If you click Refresh on the browser window, you will be taken back to the Summary page.

3DM Screens and What They're Used For

Table 5 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 the section "3DM 2 Reference" on page 45. The page names in Table 5 provide links to details about that page.

Table 5: 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.

Table 5: List of 3DM Pages

3DM Page	Description
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.
SMART Details About Drive at Particular Port Page	Shows the SMART data for a specific drive. To see this page, click the Port # for a drive on the Drive Information page.
Controller Settings Page	Lets you view and change settings that affect the units on the current controller. 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.
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 Incoming 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.

Event notification can only occur while 3DM is running, so it is recommended that 3DM be left running 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 alarms

- **Warning** will send e-mail for alarms with severity of Warning and Error only.

- **Error** will send e-mail for alarms with severity of Error only.

For more information about events and alarms, see "Viewing Alarms" on page 117.

Event notification is initially set up during 3DM installation, but 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 your mail server.

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.

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 Incoming 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 incoming port

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

2   In the **Incoming 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's 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 don't 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.

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 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
- SMART Details About Drive at Particular Port Page
- Controller Settings Page
- Scheduling Page
- Maintenance Page
- Alarms Page
- Battery Backup Page
- 3DM 2 Settings Page

Controller Summary Page

Figure 15. Controller Summary Page

> **Note:** The software version shown in the screenshots in this manual are preliminary examples only. For the current released and tested version number, refer to the 9000 release notes.

The Summary page appears after you first logon to 3DM, and when you click the Summary link in the menu bar.

The Summary 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.

> **Note:** The controller ID you see in 3DM 2 may not match the number that you see for the same controller in 3DM version 1.x.

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.

Controller Details Page
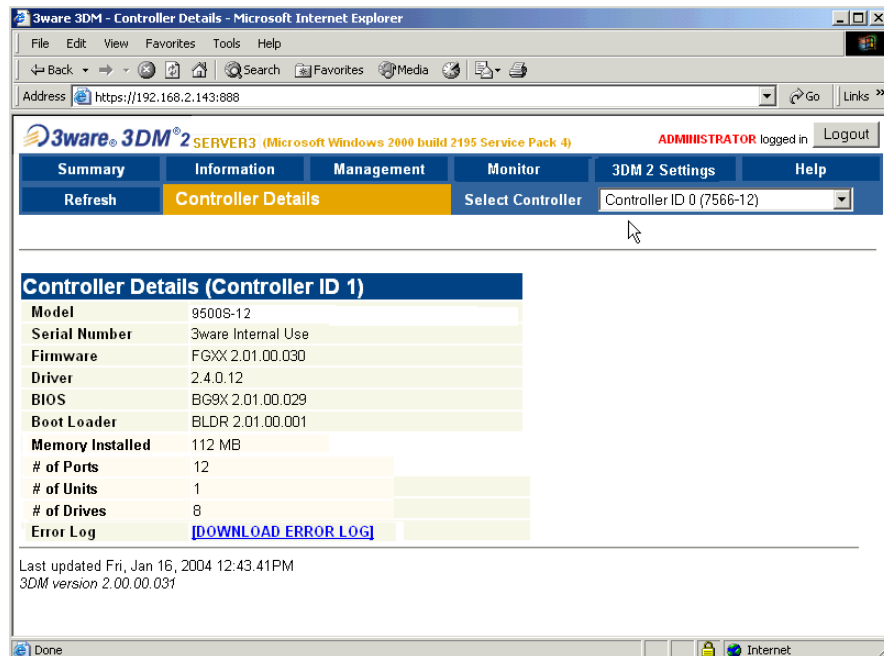
Figure 16. Controller Details Page

The Controller Details page appears when you choose **Information > Controller Details** from the menu bar.

The Controller Details 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.

Monitor. The Monitor version on the controller.This field appears only for 7000- and 8000-series controllers.)

Boot Loader. Boot Loader version on the controller. This field appears only for 9000-series controllers.

# of Ports. The number of total ports on the controller, regardless of whether each currently has a drive connected.
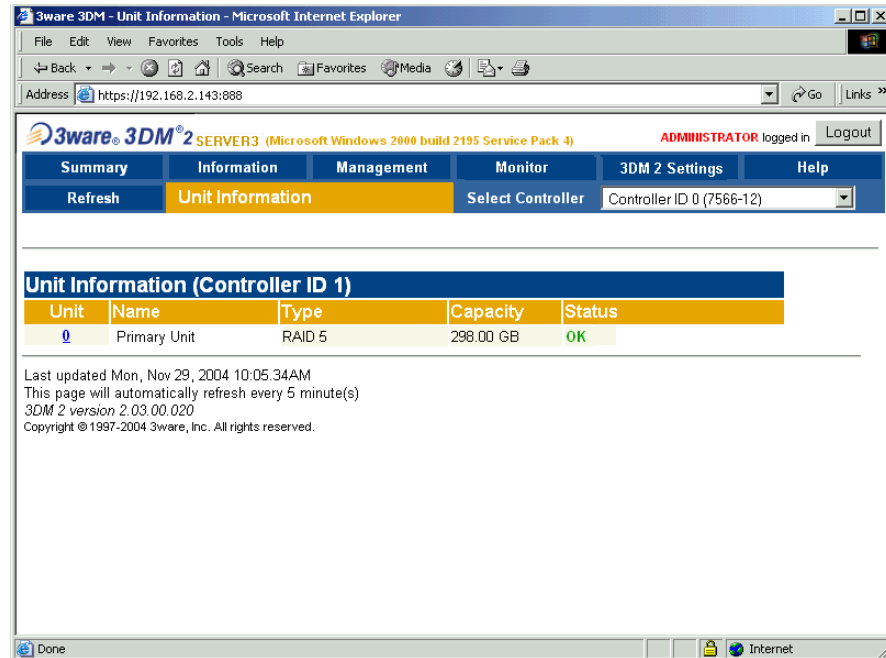
# of Units. The number of units on the controller.

# of Drives. The number of drives connected to the controller.

Download Error Log: Click on this 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 17. 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.

The Unit Information page shows a list of the units on the controller specified in the drop-down list on the menu bar 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. For 9000-series controllers, unit numbers are in sequential order.

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 10, RAID 50, Single Disk, JBOD, or Spare. For details about each of the RAID levels, see "Understanding RAID Concepts and Levels" on page 8.

Capacity. The logical capacity (size) of the unit.

> **Note:** 3DM 2 displays the capacity (in MBytes or GBytes) the same way that Microsoft Windows and Linux operating systems do: as 1KB = 1024 bytes. Previous versions of 3DM 1.x used the 1KB = 1000 bytes definition. Consequently capacities of units listed under 3DM v 1.x may appear to be larger than they do under 3DM 2.

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.

Unit Details Page

Figure 18.   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. To return to the list of units, click **Unit Information** in the menu bar.

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 18. 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 Port #. 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.

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 10, RAID 50, Single Disk, Spare, JBOD, or Disk

Volumes. Displays the number of volumes in a unit. This is usually 1. If you have a unit with more than 2TB and 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 "Multi LUN Support and Auto-Carving" on page 79.

Stripe. The stripe size of the unit, if applicable.

Subunits. If the unit has subunits, details of the subunits are shown.

Port #. If the Type is Disk, Single Disk, JBOD, or Spare, the port to which the drive is connected is shown. For multiple drive units, the port numbers are shown in the subunits section. The port number is a link to the Drive Information page.

Drive Information Page

Figure 19.   Drive Information Page

The Drive Information page appears when you choose **Information > Drive Information** from the menu bar, or when you click a port # on the Unit Details page. If you arrive at this page from the port # hyperlink on the Unit Information page, the line showing the port # you clicked on is highlighted.

The Drive Information page shows a list of drives on the controller specified in the drop-down list on the menu bar, and a summary of each one.

To see the SMART data for a drive, click the link in the Port # column.

Port #. The port to which the drive is connected.

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 1K = 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.

Serial #. The serial number of the drive.

Firmware. The firmware version of the drive.

Unit. The unit the drive belongs to, if applicable.

Status. The status of the drive: OK, Not Supported, Read Timeout, Read Failure, Orphan, DCB Data Check, Unsupp DCB, Unconv DCB, Offline JBOD, or Not Present. (In the event of a problem, the status shown for the drive can be useful to customer support.)

> **Note:** In most cases, the status of the drive will not correspond to the status of the unit, shown on the Unit Information page.

SMART Details About Drive at Particular Port Page

Figure 20.   S.M.A.R.T Data Page

The SMART Details page appears when you click a Port # on the Drive Information page.

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.

Controller Settings Page

Figure 21. Controller Settings Page

The Controller Settings page appears when you choose **Management > Controller Settings** from the menu bar.

The Controller Settings page lets you view and change settings that affect the units on the controller specified in the drop-down list on the menu bar.

Background Task Rate

The Background Task Rate fields let you change the balance of background tasks and I/O performed by the controller.

9000-series controllers show separate settings for Rebuild/Migrate Rate and Verify Rate, as shown in Figure 21. The Rebuild/Migrate Rate also applies to initialization. Although the same rate is used for rebuilding, migrating, and initializing, migrating has the highest priority.

7000- and 8000-series controllers show only one setting for Task Rate; it applies to both rebuild and verify rates. Note that this rate is not persistent following a reboot for 7/8000 controllers.

The 5 radio buttons let you set the ratio at which background tasks are performed in comparison to I/O. The furthest left buttons set the firmware to the fastest settings for background tasks settings. This means, maximum

processing time will be given to background tasks rather than I/O. The furthest right buttons set the firmware to the slowest background rates, giving maximum processing time to I/O.

For additional information, see"Setting Background Task Rate" on page 124.

Unit Policies

For units on 9000-series controllers, you can enable or disable three policies: **Write Cache**, **Auto-verify** and **Continue on Source Error During Rebuild**. 3DM lists each unit on the controller specified in the drop-down list on the menu bar, and shows you whether the policies are currently enabled or disabled for each unit.

This section does not appear for 7000- and 8000- series controllers.

Unit Write Cache. You can enable or disable write cache for each unit. 3DM lists each unit on the controller specified in the drop-down list on the menu bar, and shows you whether the write cache is currently enabled or disabled for it.

Write cache is a combination of the physical hard drives' write cache as well as the controller's memory, depending on what type of unit you are using.

For 9000-series controllers, a **Disable Write Cache on Unit Degrade** setting can be set in 3ware BIOS Manager (3BM). You can see if this setting is enabled in the **Other Controller Settings** field at the bottom of this Controller Settings page. If **Disable Write Cache on Unit Degrade** is enabled, upon degrade of a unit, the write cache will automatically be disabled, even if you enable write cache in the Unit Write Cache field.

For additional information, see "Enabling and Disabling the Unit Write Cache" on page 95

Auto-verify. The Auto-verify policy causes verify tasks to be performed automatically, whenever the controller firmware algorithms determine that a verify task is needed. This feature is designed to make verification of units easier. When you check this box, the controller will run verify tasks as they are required.

If there is no schedule set up for verify tasks, then the controller firmware can initiate a verify task at any time. If a verify time window is scheduled, then the controller will not start a verify task for that unit outside the time window, and may or may not start a verify task for that unit within the time window, depending on whether one is needed.

If Auto-verify is not set and there is no schedule, you must manually specify when you want to run a verify, on the 3DM Management page.

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

---

3ware 9000 Series Serial ATA RAID Controller User Guide

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 manually 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 a file system check be executed when the rebuild completes.

> **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.

Unit Names

On 9000-series controllers, 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 114.

Other Controller Settings

For 9000-series controllers, the Other Controller settings displays information about additional settings, most of which can only be changed in the BIOS (3BM). For more information see "Setting Policies for a Controller through 3BM" on page 76.

This section does not appear for 7000- and 8000- series controllers.

2TB 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 2TB will be broken down into multiple volumes of 2TB each, plus a remainder volume. For example, 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 2TB each and the last volume containing 1TB.

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 and has been enabled in 3BM.)

**Delay between Spin-ups.** The delay time (in seconds) between drive groups that spin up at one time on this particular controller.

Export JBOD (Unconfigured) Disks. Indicates whether unconfigured disks (JBODs) should be exported to the operating system. By default, this setting is disabled and JBOD drives are not exported to the operating system. For more information about this feature, see "Exporting JBOD Disks" on page 77.

Disable Write Cache on Unit Degrade. Indicates whether write cache will be automatically disabled on a unit if it becomes degraded. After the unit is rebuilt, the write cache will be re-enabled automatically.

For additional information, see "Viewing Controller Policies in 3DM" on page 75.

Scheduling Page
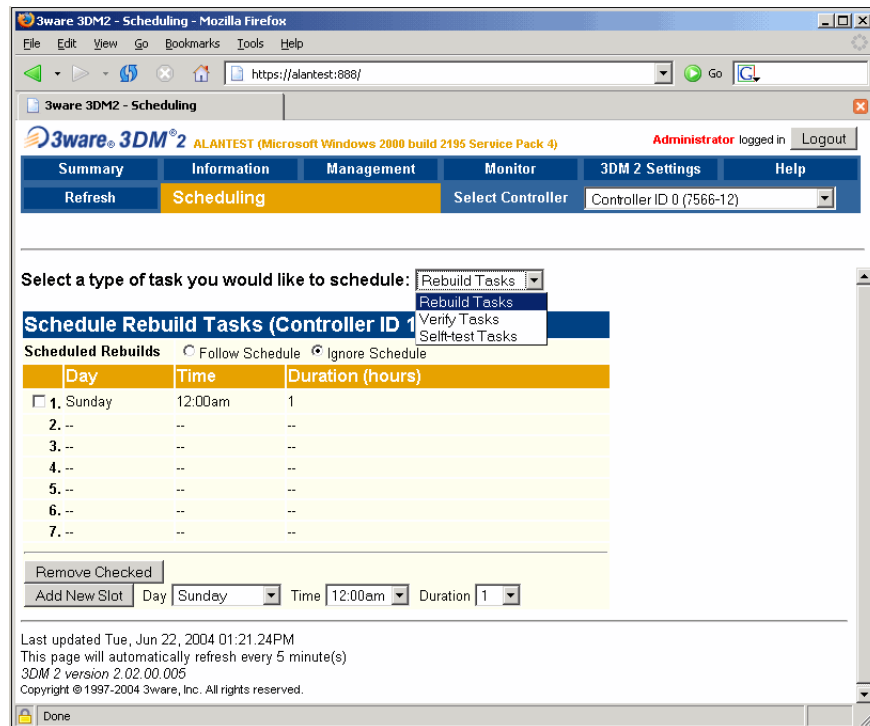
Figure 22.   Scheduling Page

For 9000-series controllers, the Scheduling page appears when you choose **Management > Scheduling** from the menu bar.

The Scheduling page is not available for 7000- and 8000- series controllers. If you want to schedule tasks for one of those controllers, use 3DM Version 1.x.

The Scheduling page lets you view and change the schedule for background tasks that affect all units on the controller specified in the drop-down list on the menu bar, including:

- Rebuild tasks (also applies to initialization and migration tasks)

- Verify tasks (also applies to media scans)

- Self-tests

You select the type of task for which you want to set the schedule from the drop-down list at the top of the page.

You can also enable or disable use of the schedule for the selected background tasks by selecting either **Follow Schedule** or **Ignore Schedule**. When these schedules are set to be ignored, these tasks can be performed at any time, and are not restricted to the scheduled times.

> **Note:** Scheduling of these tasks is only available on the 9000-series controllers.

For details about the different background tasks, see "About Background Tasks" on page 119.

About Task Schedules

Each type of task may be scheduled for up to 7 times per week. This limits active initializing, rebuilding, verifying, migrating, and testing of a unit to the times you specify, so that the task does not interfere with peak I/O times.

If all 7 schedule slots are filled, you must first remove one or more schedule times before you can add another.

You may set schedule times whether scheduling is set to be followed or ignored. This is useful if you want to temporarily disable the schedule.

If you remove all the schedule times for a particular background task, initializations, rebuilds, and migrations will run anytime, as they are needed. Verify will only run if started by the CLI or if the Verify Unit button is clicked.

For information about adding and removing schedules, and setting schedules to be followed or ignored, see "Scheduling Background Tasks" on page 125

About Self-tests

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.

Two self-tests can be scheduled:

Upgrade UDMA mode. This test checks the speed at which data transfer to drives is occurring, to see if the UDMA mode can be increased. (If you are already running at the fastest UDMA mode, then this self-test has no effect.)

The UDMA mode can become downgraded in the event that cable CRC errors are encountered, requiring multiple retries to read sectors. In severe cases, the

UDMA mode may be downgraded from ATA 150 to ATA 133, to ATA 100, to 66, to 33.

This check is also done every time the system is booted.

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 23. 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 (shown in the drop-down list on the menu bar), 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

Rescan Controller

Use the **Rescan Controller** button to have 3DM scan the available drives in the controller and update the list of available drives shown. This is useful in variety of maintenance tasks. For example, if you physically plug in a drive and want the controller to recognize the newly plugged in drive.

Note: If you unplug a drive without first removing it through 3DM, Rescan will 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 hotswap carriers can result in a system hang or may even damage the system and the drive.

In 9000-series controllers, rescan 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 or FreeBSD, 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.

> **Note:** In 8000-series controllers, only JBOD units can be removed and rescanned while keeping the data intact. Clicking Rescan Controller after removing units other than a JBOD unit (e.g. RAID 5) will cause the drives that make up the unit to be seen as individual available drives; they will not be pieced together to form a unit. This is unlike the 9000 series controllers, which will piece together the unit for you and display the drives as a unit. If you still want to use the drives together as a unit, restart the computer before creating a new unit with those drives. Creating a new unit with those drives will destroy any existing data on them. After you restart, the 8000 will again see the drives as 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. Unit numbers for 9000 series are in sequential order. Unit numbers for the 7/8000 series will begin with the lowest port number of the unit. 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 10, RAID 50, Single Disk, Spare, or JBOD. 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 Information page, which has that information.

Drive Information

Port. The 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.

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 hotswap carriers can result in a system hang or may even damage the system and the drive.

Maintenance Task Buttons

Below the list of units, a row of task buttons lets you preform 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, JBODs, 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.

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 119.

Rebuild Unit. Replaces a degraded 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 degraded drives (for example, a RAID 10 where both mirrored pairs each have a degraded 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 "About Rebuilds" on page 121.

Migrate Unit. Reconfigures a unit while it is on-line. Migration can be used to change only the RAID level, to expand the capacity by adding additional drives, or to change the stripe size.

⚠️ **Caution:** 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.

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.

For more information, see "About Migration" on page 123.

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 and no I/Os are being issued. (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.)
>
> 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. Resulting behavior depends on which operating system you are using and what kind of I/O is being done, however you will typically see really bad results, bad errors, and most likely a reset of the controller or a system hang.
>
> 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
> ```
> For FreeBSD, the command would be
> ```
> umount /dev/twedx
> ```

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 hotswap carriers can result in a system hang 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 and no I/Os are being issued. 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. Resulting behavior depends on which operating system you are using and what kind of I/O is being done, however you will typically see really bad results, bad errors, and most likely a reset of the controller or a system hang.

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 Port number, model, capacity, and status are all displayed, as they are for drives in existing units.

Remove Drive. The Remove Drive link removes a drive from the controller so that you can safely unplug it. Any drive in the Available Drives list can be removed.

⚠ **Warning**: Physically removing drives which are not in hotswap carriers 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, Stripe size (if applicable), Write Cache, and Auto Verify settings.

A window like the one in Figure 24 shows the drives you selected, and lets you specify configuration settings.

Figure 24.   Configuring a Unit in 3DM

For more detailed instructions, see "Configuring Units in 3DM via the Maintenance Page" on page 84.

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 10, RAID 50, Single Disk, and Spare Disk. For information about these configurations, see "Available RAID Configurations" on page 9.

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 25.   Configuring a RAID 50 with 12 Drives

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 54.

> **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.

Alarms Page

Figure 26.   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 alarms can be listed. After the 1000-limit is reached, the oldest alarms are deleted, as new ones occur.

You can sort the alarms by severity or time. To do so, just click the column header.

For 8000 and 9000-series controllers, alarms can be used by either 3DM or CLI, but not both. Whichever issues an alarms command first determines which can see alarm data.

For more information about any of the alarms that appear on the Alarms page, see "AEN Messages" on page 163.

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 generated by 7000- and 8000- series controllers is the time retrieved from the driver by 3DM. The time shown for alarms generated by 9000-series controllers is the time received by the driver from firmware.

Message. The specific text relating to the alarm condition.

Battery Backup Page
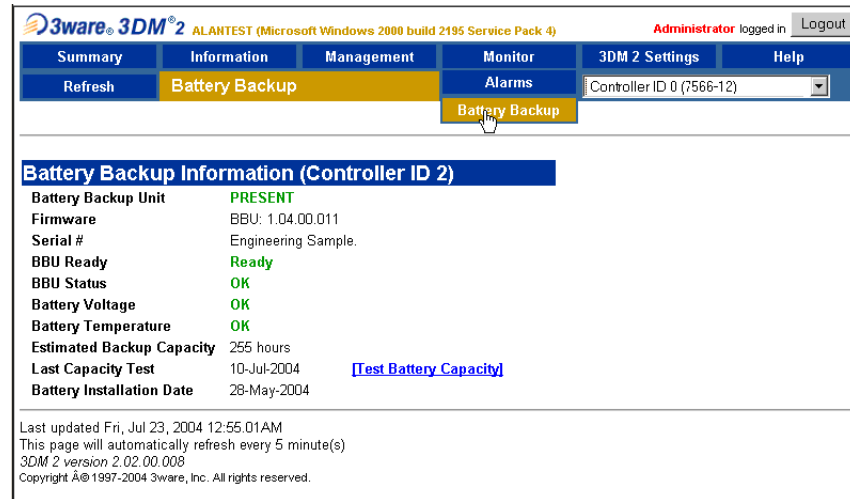
Figure 27. Battery Backup Page

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.

- **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 157.

Battery Installation Date. Indicates when the BBU last detected the battery pack was removed and replaced.

3DM 2 Settings Page
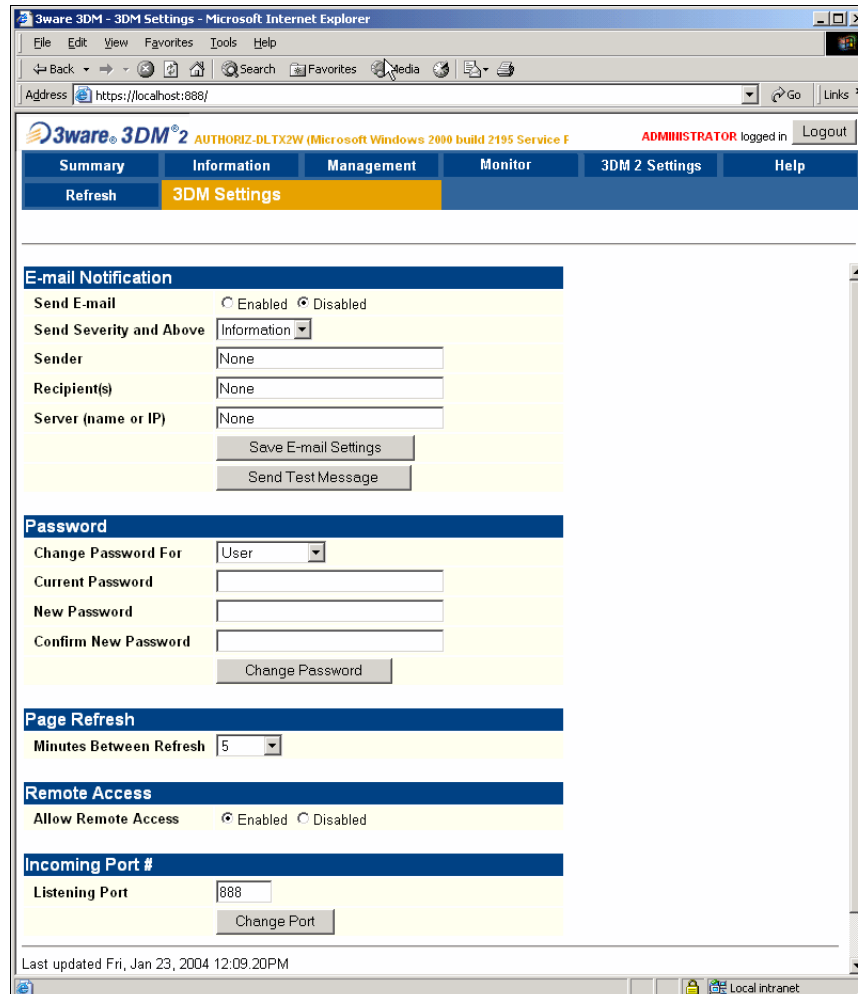
Figure 28. 3DM 2 Settings Page

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.

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**.

3ware 9000 Series Serial ATA RAID Controller User Guide

Send Severity and Above. 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 (,).

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.

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 Connections. This field enables or disables the ability for users and administrators to access 3DM from a remote computer.

Incoming Port

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.

Configuring Your Controller

This section describes how to view details about the controller, check it's 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 Different Controllers

■ Viewing Controller Policies in 3DM

■ Setting Policies for a Controller through 3BM

> **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 124.

Viewing Information About Different Controllers

If you have more than one controller in your system, you can easily view information about each one using 3DM, in the same session. If you are working at the BIOS level, you access 3BM for each controller separately. The following steps tell you how to display information about the controller you want to work with.

To see details about a particular controller in 3DM

1   Start 3DM and log in.

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

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

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.

For more information about this page, see "Controller Summary Page" on page 45.

2   To see details about a particular controller, click the ID link for that controller.

The Controller Details page appears.

For more information about this page, see "Controller Details Page" on page 47.

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 to see details about 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 manual, 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

For details about working with 3BM, see "3ware BIOS Manager (3BM)" on page 19.

Viewing Controller Policies in 3DM

You can view the current state of controller policies in 3DM, in the **Other Controller Settings** section of the bottom of the Controller Settings Page.
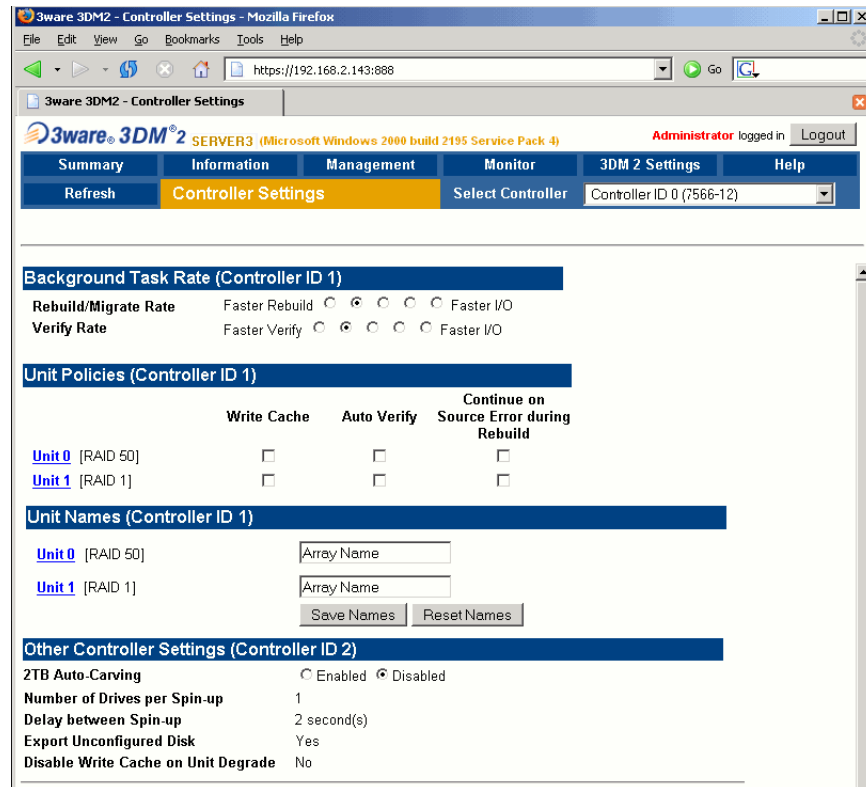
Changes to these policies can only be made in 3ware BIOS Manager (3BM).

- **Number of drives per spinup**

- **Delay between spinup**

- **Export unconfigured disks**

- **Disable write cache on unit degrade**

- **2TB Auto-carve**:

Setting Policies for a Controller through 3BM

3BM allows you to set policies for all units on the controller. These policies can only be set or changed in 3BM, however you can check the settings for them in 3DM.

- **Export JBOD (unconfigured) disks.** This setting indicates whether JBOD disks should be exported to the operating system. JBOD configuration is strongly discouraged for newly added disks on the 9000 series controller, in favor of Single Disk, so by default, this setting is disabled. If you have a JBOD configuration from a 7000/8000 controller that you want to use on the 9000 controller, you should enable this setting.

- **Staggered spinup.** Spinup 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. This setting determines whether all of the drives will spin up at the same time or in a staggered fashion.

  If staggered spinup is enabled, then compatible drives will be sent a spin up command as defined by the **Number of drives per spinup** and **Delay between spinup settings**.

  If staggered spinup is disabled, then the spin up command is sent to all of the drives at boot time, resulting in all of the drives spinning up simultaneously.

- **Number of drives per spinup.** Number of drives that will spin up at the same time when the controller is powered up, if staggered spinup is enabled.

- **Delay between spinup.** The delay time (in seconds) between drive groups that spin up at one time on this particular controller, if staggered spinup is enabled.

- **Disable write cache degraded array.** Indicates whether write cache will be automatically disabled on a unit if it becomes degraded.

  Selecting **Yes** will cause the unit write cache and the disk drive write cache to be disabled if the unit degrades. This setting has no effect on non-redundant arrays. Write cache will be automatically re-enabled when the unit returns to normal.

  Selecting **No** will cause the unit and disk drive write cache to remain enabled (if it is enabled), in the event that the unit degrades.

- **Staggered method.** Indicates whether the type of staggered spinup is ATA-6 or SATA OOB (Out Of Band). By default, when Staggered Spinup is enabled, the ATA-6 scheme is used. If your drives support the SATA OOB method, select that method here. There is no electronic method for the controller to know if a drive supports this method, so it must be set

manually. For staggering to work properly, the drives must support the selected method.

■ **2TB Auto-Carving.** When this feature is enabled, any unit that is over 2TB will be broken down into multiple volumes with 2TB each, plus a remainder volume. For example, 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 2TB each and the last volume containing 1TB.

This auto-carving feature is sometimes referred to as multi-LUN, where each volume that is created is referred to as a "LUN."

All of these policies.can be set and changed on the 3BM Policy screen, shown in Figure 29.
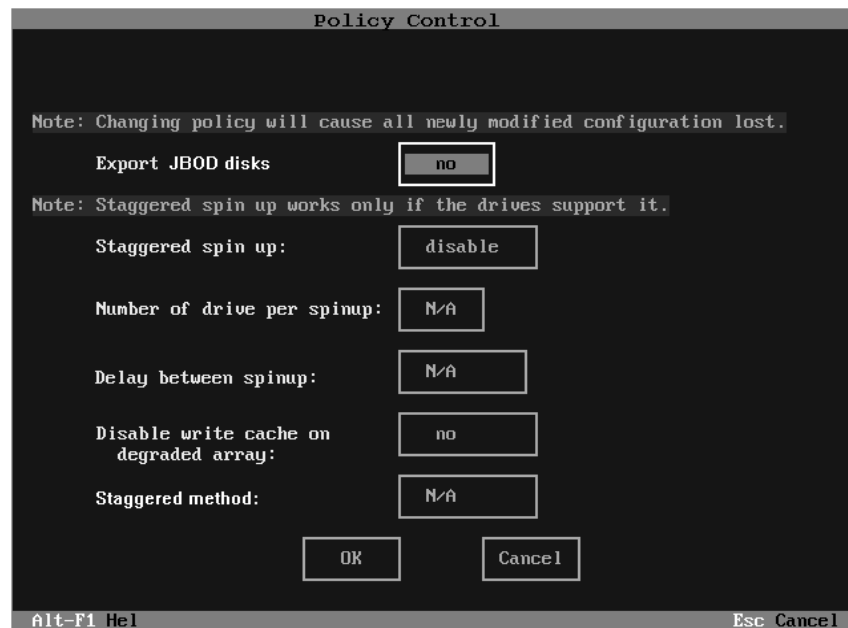
Figure 29.   3BM Policy Screen

Exporting JBOD Disks

By default, JBOD disks (unconfigured disks) connected to the 3ware RAID controller are not exported to the operating system. This means that any drives you leave unconfigured are not seen by the operating system, and cannot be used for storage. When Export JBOD Disks is set to No, you make individual disks available for use by configuring them as Single Disks.

If you want unconfigured disks to be available on your computer, you can change this setting.

> **Note:** It is recommended that JBODs not be made available to the operation system. The advantages of working with configured Single Disks over JBOD are:
>
> ■Single disk media scan will continue where it left off, while JBOD media scan always must restart from the beginning.
>
> ■Single disks can take advantage of the controller caching and configuration is persistent.
>
> ■Single disks will be able to be migrated to redundant units in the future (e.g. A single disk will be able to be mirrored to another drive, creating a RAID 1 array).

If JBOD disks are not exported to the operating system, they will appear as available drives in 3DM, and can be configured as single disks or spares, and included in other RAID configurations. If you change the policy to allow JBOD disks to be exported to the operating system, they will appear as units in 3DM.

To enable or disable the export of unconfigured disks

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

2   On the **Policy Control** screen, **Tab** to **Export Unconfigured Disks**, press **Enter** to display the choices, use the **arrow keys** to select **Yes** (to enable), or **No** (to disable) and press **Enter** again to choose it.

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

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

> **Note:** If you enable the Export JBOD Disks option, the controller recognizes and displays as JBODs brand new drives, and drives that were previously connected to 7000/8000-series controllers as JBODs. Drives that were previously connected to a 9000-series controller and configured will not be seen as JBODs.

Enabling and Setting Up Staggered Spinup

Four policy settings let you enable or disable spinup of drives, 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 drives support staggered spinup. If you enable staggered spinup and have drives that do not support it, the setting will be ignored.

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:** Select **enabled** to enable staggered spinup; **disabled** to disable it.

■   **Number of Drives Per Spinup:** Select the number of drives—from 1 to 4, 8, or 12, depending on the number of ports on the controller.

■   **Delay between spinup:** Select the number of seconds—from 1 to 6.

■   **Staggered Method:** Select either ATA-6 or SATA OOB as the type of staggered spinup you want to use. For staggering to work correctly, the drives must support the selected method.

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

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

Disabling Write Cache on Unit Degrade

You can choose whether you want the write cache to be automatically disabled when a unit degrades. This enables some higher level recovery, to cover the case where there is a software RAID layer (using some redundancy) on top of the 3ware RAID configuration. If case of a second drive failure, the software RAID layer can still provide redundancy since no data was lost.

When this setting is set to **Yes,** it overrides the write cache setting specified for a particular unit.

For more information about enabling and disabling the write cache, see"Enabling and Disabling the Unit Write Cache" on page 95.

To disable write cache when a unit degrades

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

2   On the Policy Control screen, **Tab** to **Disable Write Cache on Unit Degrade**.

3   Press **Enter** to display the choices, use the **arrow keys** to select **Yes**, and press **Enter** again to select it.

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

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

Multi LUN Support and Auto-Carving

Windows 2000, Windows 2003, Windows XP, and FreeBSD 4.x, do not currently recognize unit capacity in excess of 2 TB. To gain use of the full capacity in units greater than 2 TB, you can enable auto-carving.

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. These chunks are sometimes known as multiple LUNs (logical units), however through the 3ware documentation, they are referred to as *volumes*. 3ware firmware supports a maximum of 8 volumes per controller, up to a total of 16 TB.

> **Note:** Operating systems without this limitation include Linux 2.6 and FreeBSD 5.x. Microsoft plans to overcome this limitation in Win XP-64bit and Windows 2003, SP 1.

You must turn on the 2TB Auto-Carving policy before creating the unit. Units created with this policy turned off will not be affected. 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 2 TB auto-carving feature. You can do so using 3DM, 3BM, or the 3ware CLI.

In 3DM, enable 2TB auto-carving at the bottom of the **Management > Controller Settings** page.

In 3BM, you enable auto-carving on the Policies page.

In CLI, use the command tw_cli /cx set autocarve=on. For more information, see the *3ware 9000 Series Serial ATA RAID Controller CLI Guide*.

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

With auto-carving enabled, if the combined capacity of the drives exceeds 2 TB, up to 8 individual 2 TB volumes will be created from the unit.

For example, a 5 TB unit would become 3 volumes; two 2 TB volumes and one 1 TB volume.

3 Verify the creation of the volumes through 3DM 2 or the CLI.

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 TBs, 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 is always used as the boot device.

Configuring Units

A unit is any configured disk or array of disks connected to your 3ware RAID controller.

This section includes instructions for performing the following configuration tasks:

- Creating a New Unit
- Creating a Hot Spare
- Enabling and Disabling the Unit Write Cache
- Setting Unit Policies through 3DM
- Changing An Existing Configuration (RAID Level Migration)
- Deleting a Unit
- Removing a Unit
- Adding a Drive through 3DM
- Removing a Drive
- Rescanning the Controller
- Naming a Unit

Configuring Units in 3DM via the Maintenance Page

You can configure units via the 3DM web interface or from the BIOS, using 3BM. In 3DM, configuration starts from the **Maintenance** page (Figure 30), where you can configure a new unit, designate an available drive as a hot spare, delete a unit, and remove units or drives. You can also have 3DM rescan the controller, if you have added drives or units.

For information about working in 3DM, see "3ware Disk Manager (3DM 2)" on page 27.
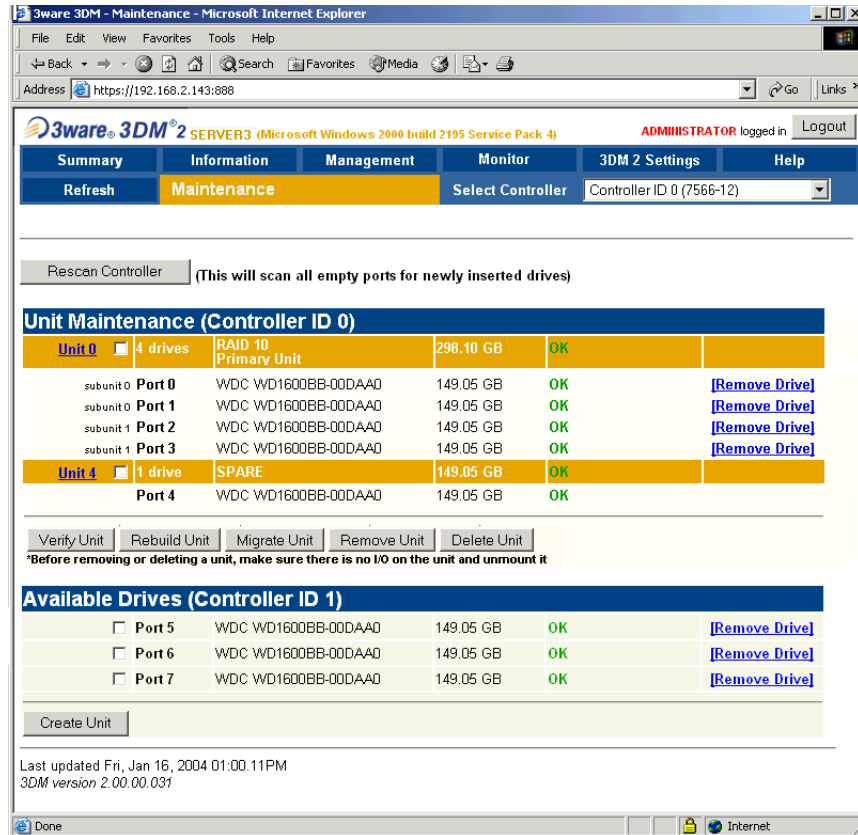

Figure 30.   3DM Maintenance Page

Configuring Units in 3BM via the main 3BM Screen

In 3BM, configuration tasks start from the main 3ware BIOS Manager screen shown in Figure 31. From this screen you can configure new units, delete existing ones, or perform maintenance tasks.

For information about working in 3BM, see "3ware BIOS Manager (3BM)" on page 19.

```
                          3ware BIOS Manager   ( slot 4 )

      Available Drives:
      Port 3   - IC35L120AVVA07-0              115.03 GB      Hot Spare

      Exportable Units:
      Unit   - 3 drive 64K RAID 5  230.07 GB
        Port 0 - IC35L120AVVA07-0              115.03 GB
        Port 1 - IC35L120AVVA07-0              115.03 GB
        Port 2 - IC35L120AVVA07-0              115.03 GB




        Create Unit      Delete Unit     Maintain     Rebuild     Policy     BBU

   Alt-F1 Help  ↕↔ Previous/Next  Alt-a Sel all drv   r Remove   Enter Select/Desel
    F6 Restore Initial Values  Esc Cancel            F8 Done  s Toggle Hot Spare
```

Figure 31. 3BM Main Display

Creating a New Unit

Whether you create a unit through 3BM or 3DM, when you create a new unit, you specify the following:

- Drives to be included in the unit

- Type of configuration

- Name for the unit (optional)

- Stripe size, if appropriate for the RAID level

You can make some changes to the unit later. For details, see "Changing An Existing Configuration" on page 98.

Drives to be included in the unit

You may include from one to twelve drives in the unit, depending on the number available. (For information about how many drives to select for a given RAID level, see Table 2 on page 12.)

You may only select available drives that are not currently part of a unit. If you want to use drives that are currently part of a different unit, you must delete that unit, first, to make the drives available. (For details, see "Deleting a Unit" on page 103.) 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 through 3DM" on page 110.

Type of configuration

Available configuration types include RAID 0, RAID 1, RAID 5, RAID 10, RAID 50, and Single Disk. For information about the different RAID levels, see "Understanding RAID Concepts and Levels" on page 8.

> **Note:** Creating a unit erases all data on all drives. Although creating a RA1D 1 (mirror) creates a unit that will have a duplicate of data on both drives after it is put in use, creating a RAID 1 cannot be used to make a backup copy of data that currently exists on a single drive unless you migrate from a RAID 1 to two individual single disks.

Name of the unit (optional)

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

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 smaller or larger stripe size.

Creating a Unit through 3DM

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 Port number for each one.

   If you are creating single drive units (single disks or hot spares), you can configure multiple drives at once.

   (For details about this screen, see "Maintenance Page" on page 58.)

3 Click **Create Unit**.

4 In the dialog box that appears, select the RAID configuration you want.

5 If stripe size applies to the RAID type you select, select a Stripe Size.

6   Optional: In the Name box, enter a name for the unit (up to 21 characters, including dashes and underscores). To rename the unit, see "Naming a Unit" on page 114

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.

8   Click **Ok**.

The new unit will appear in the Unit Maintenance list at the top of the page and the operating system will be notified of the new unit.

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.

9   Partition and format the unit. (Steps will vary depending on the operating system.)

10 Mount the new unit.

> **Note:** For RAID 5 units with 5 or more disks, and RAID 50 units with 10 or 12 disks and only two subunits, initialization of the unit begins immediately.
> The unit can be used while it is initializing and is fault-tolerant.

11 Partition and format the unit. For details, see "Partitioning and Formatting Units" on page 91.
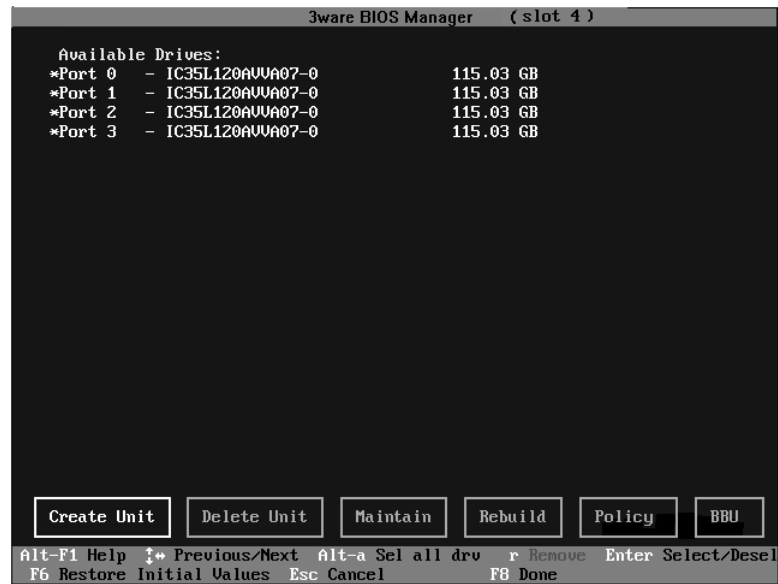
Creating a Unit through 3BM

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 32).

Tip: If you want to use all available drives, press **Alt-A** to select them all.
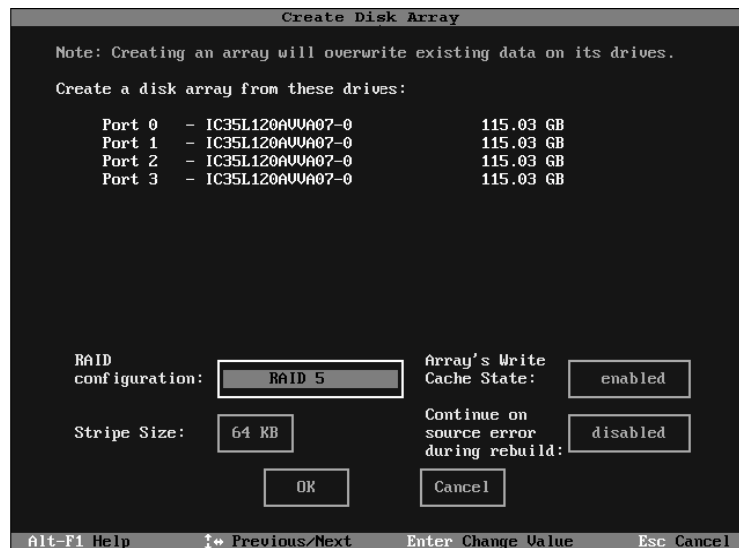
Figure 32. Asterisks Next to Selected Drives

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 (see Figure 33 for an example for RAID 5).

Figure 33. Create Disk Array Display, RAID 5 Example

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

**Figure 34.   List of Configuration Choices for Four Drives**

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

6   (Optional) **Tab** to the field **Array's Write Cache State** and select whether you want the write cache to be enabled or disabled for this unit.

Note: You can enable or disable the write cache again later without affecting the configuration. For more information about write cache, see "Enabling and Disabling the Unit Write Cache" on page 95.

7   **Tab** to the field **Stripe Size** and select the desired striping size (16, 64, or 256 KB).
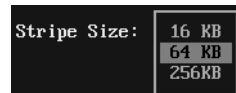
Figure 35.   Stripe Sizes for a RAID 5

8   (Optional) **Tab** to the field **Continue on source error during rebuild**. Normally this is left disabled, however if you want any rebuilds of this unit to continue in the event of source errors, you can enable it. For more information, see the discussion of the "Overwrite ECC errors" feature in 3DM, under "Controller Settings Page" on page 53.

Note: You can enable or disable this setting later without affecting the configuration.

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

You are returned to the main 3BM screen.

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

10 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.
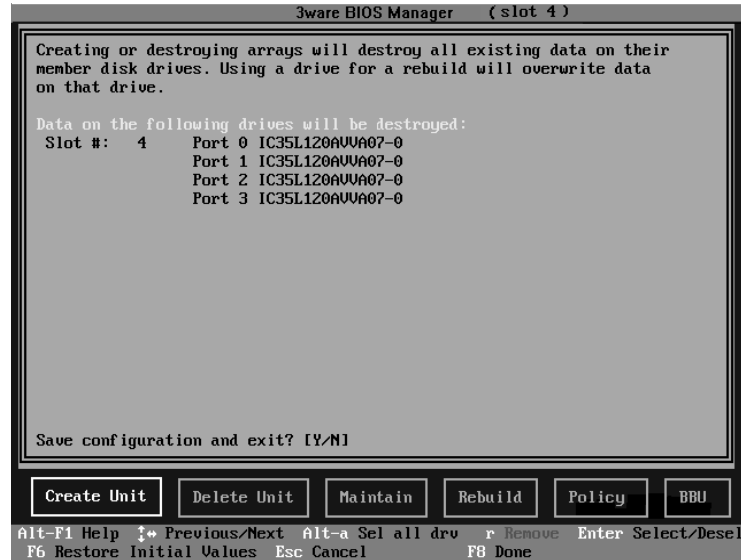
Figure 36.   Confirmation Message when Saving and Exiting

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.

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

> **Note:** For RAID 5 units with 5 or more disks, and RAID 50 units with 10 or 12 disks configured into two subunits, 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 "Initializing Units" under "Configuring Units" in *3ware 9000 Series Serial ATA RAID Controller Installation Guide*.

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 and Formatting Units

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

To partition and format 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**.

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

To partition and format under Linux

1   Boot the system and log in as root.

2   Open a terminal window.

---

3   Partition the unit:

```
fdisk /dev/sda
```

If the unit is over 2 TB, use:
```
parted /dev/sda
```

4   Create or make the file system:

```
mkfs /dev/sda1
```

If you have kernel 2.6.8.1 or higher, for partitions over 4 TB, specify the XFS filesystem when using parted. Use of the -j option to turn on journaling is recommended for large partitions.

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

To partition and format under FreeBSD

1   Boot the system and log in as root.

2   Open a terminal window.

3   Partition the unit:

```
fdisk -BI /dev/da0;
disklabel /dev/da0 | disklabel -B -R -r da0
```

4   Create or make the file system:

```
newfs /dev/da0c
```

You can also use sysinstall to format and partition the unit.

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. When this occurs, an event notification is generated and appears in the list of alarms in 3DM.

It's 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 drives it is replacing.

> **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), 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 drives 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 through 3DM" on page 110.
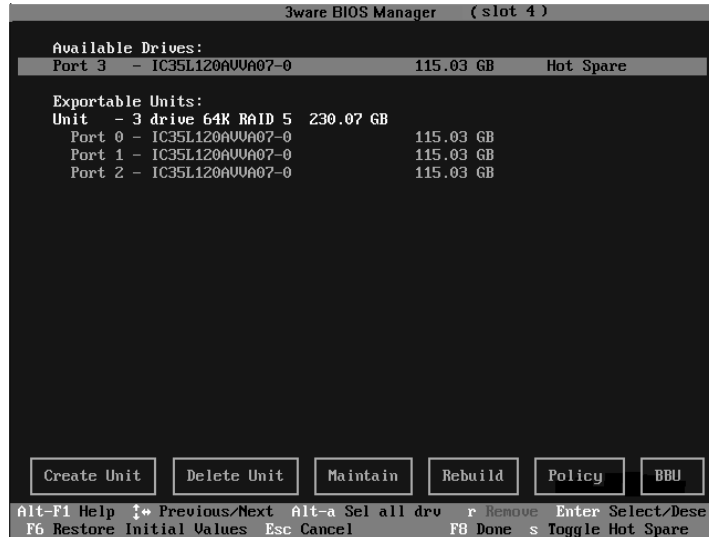
To specify a hot spare after the system is booted

1   In the **Available Drives** section of the Maintenance Page, select the drive by checking the box next to it.

2   Click **Create Unit**.

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

4   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.

```
                          3ware BIOS Manager    ( slot 4 )

       Available Drives:
       Port 3   - IC35L120AVVA07-0            115.03 GB       Hot Spare

       Exportable Units:
       Unit    - 3 drive 64K RAID 5   230.07 GB
         Port 0 - IC35L120AVVA07-0            115.03 GB
         Port 1 - IC35L120AVVA07-0            115.03 GB
         Port 2 - IC35L120AVVA07-0            115.03 GB

















       Create Unit     Delete Unit     Maintain     Rebuild     Policy     BBU

  Alt-F1 Help  ↕↔ Previous/Next  Alt-a Sel all drv   r Remove   Enter Select/Desel
  F6 Restore Initial Values  Esc Cancel              F8 Done  s Toggle Hot Spare
```

Figure 37.   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.

Enabling and Disabling the Unit Write Cache

Write cache is used to store data locally on the drive before it is written to the disk, allowing the computer to continue with its next task. Enabling write cache results in the most efficient access times for your computer system. However, there may be instances when you always 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.

Write cache can be turned on or off for individual units in both 3DM 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.

Notes:
For 9000-series controllers, a setting at the BIOS level in 3BM can specify that the cache should be disabled in the event the unit degrades. When that option is selected, unit write cache cannot be enabled until the array is rebuilt and again in optimal mode. In 3DM, you can see whether **Disable write cache on unit degrade** is set in the **Other Controller Settings** section of the **Controller Settings page**. For more information, see "Disabling Write Cache on Unit Degrade" on page 79.

Write cache settings are not applicable for an unconfigured disk (JBOD).

Note: Do not use Windows Control Panel to enable or disable cache on 3ware RAID units.

Enabling and Disabling the Unit Write Cache through 3DM

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

2   In the **Unit Write Cache** section of the Controller Settings Page, select the Enabled or Disabled option for each unit.

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

For more information about the write cache settings, see the reference section, "Controller Settings Page" on page 53.

Enabling or Disabling the 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 In the Maintain Array screen, **Tab** to the field **Array's Write Cache State**.
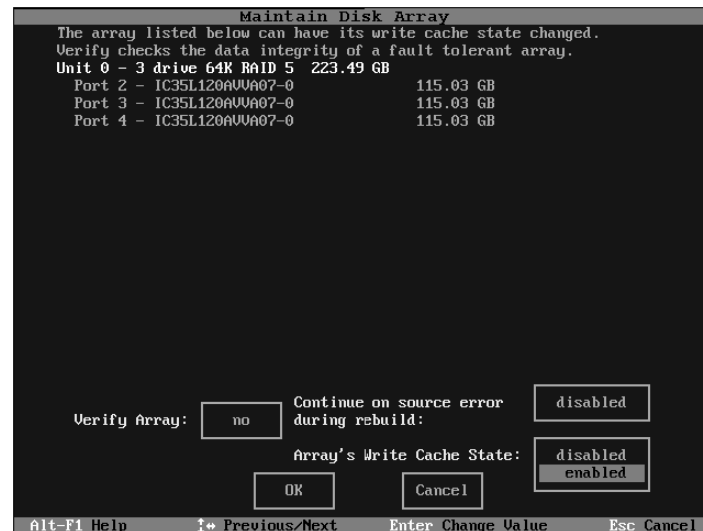
Figure 38. Unit Write Cache State in 3BM

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

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

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

You return to the main 3BM screen.

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

Setting Unit Policies through 3DM

For 9000-series controllers, you can enable or disable two policies: Auto-verify and Configure on Source Error during Rebuild. (For details about these unit policies, see the 3DM Reference section, "Controller Settings Page" on page 53.)

To set unit policies

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

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 (Figure 39).

Figure 39.   Setting Unit Policies in 3DM

Note: You can also set both of these policies when you create units through 3DM, and when using 3BM, you can set the policy "Continue on source error during rebuild" when creating a unit.

Changing An Existing Configuration

With 3ware 9000 series RAID controllers you can convert one RAID configuration into another while the unit is online. This process is known as RAID Level Migration (RLM).

Note: Units on a 7xxx/8xxx series controller cannot be migrated.

You can use RAID Level Migration to make two main types of configuration changes:

- RAID Level

- Unit Capacity Expansion

You can also use RLM to change the stripe size of a unit.

These changes can be made using 3DM2 or the CLI. Instructions for using migrate in 3DM2 are described below. For information about CLI, see *3ware 9000 Series Serial ATA RAID Controller CLI Guide*.

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

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 40 shows an example of how data is reconfigured during a migration. In this example, the migration is from a 4-drive RAID 0 to a 6-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.

4-Drive R0   6-Drive R5
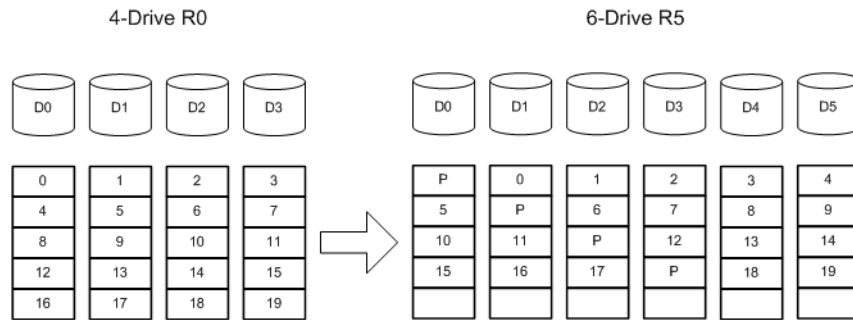
Figure 40.   RAID Level Migration Example

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.

It is possible to reduce the number of drives included in a unit through a migration, as long as the new RAID configuration still has the same or more capacity. For example, if the unit consists of four 200 GB drives in a RAID 5, then 1 drive could be removed after migrating to RAID 0 with no loss of data. However, drive reduction typically also results in the loss of redundancy, or less redundancy, so be sure to weigh the trade-offs choices carefully.

Note: Removing a drive while migrating a unit must be done through the CLI.

.

Table 6: Valid Migration Paths

Source	Destination							
	R0	R1	R5	R10	R50	Single	JBOD	Spare
R0	Yes	No	Yes	Yes	Yes	No	No	No
R1	Yes	No	Yes	Yes	Yes	Yes	No	No
R5	Yes	No	Yes	Yes	Yes	No	No	No
R10	Yes	No	Yes	Yes	Yes	No	No	No
R50	Yes	No	Yes	Yes	Yes	No	No	No
Single	Yes	Yes	Yes	Yes	Yes	No	No	No
JBOD	No	No	No	No	No	No	No	No

Table 6: Valid Migration Paths

Source	Destination							
	R0	**R1**	**R5**	**R10**	**R50**	**Single**	**JBOD**	**Spare**
Spare	No	No	No	No	No	No	No	No

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, and in some cases you can remove a drive. 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. If you want to migrate and reduce drives, you must use the *3ware 9000 Series Serial ATA RAID Controller CLI Guide*

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 adding or removing drives from the unit. Making physical changes to 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.

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.

> **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 four-drive RAID 0 unit cannot migrate to a four-drive RAID 5, without adding another drive, due to the need for additional storage capacity for parity bits.

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.)

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 Maintenace 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   Inform the operating system of the change, as described below.

Note: You can also perform these steps using the CLI. For more information, see the *3ware 9000 Series Serial ATA RAID Controller CLI Guide*.

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.

Resizing the file system to match the new partition size is not automatic. It may be necessary to expand or contract the file-system using tools specific to your operating system.

In addition, in order to use the new capacity, you need to either resize the existing partition or add a new partition.

Note: This step can only be done after the system has completed the migration or online capacity process. The operating system will not see the capacity until that process is complete.

To inform the operating system that secondary storage has been upgraded:

1   If you change the configuration of the boot unit (the unit containing the operating system), you must reboot the system in order to see the new unit capacity.

2   Unmount all file systems.

Under Windows, go to **Start > Administrative Tools > Computer Management**, and select **Disk Management.** Remove the logical drive letter for the unit.

Under Linux and FreeBSD, from a command prompt, type sync <enter>, sync <enter>, sync <enter>.

You can then unmount the unit with this command: umount <mount location>

3   If the reconfigured unit is secondary storage, you must have the controller rescan, in order to update unit information.

   d   In 3DM2, select the appropriate unit and choose **Management > Maintenance**. Click the **Remove Unit** button.

   e   After the unit has been removed, click the **Rescan** button. The new unit capacity displays.

4   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, you must either convert it to a dynamic disk or use a 3rd party tool to rubrication the unit.

■ 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 and FreeBSD, 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/FreeBSD 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 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 them 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 109.

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 the 9000 controller, you must convert the drives first. For more information, see the section "Replacing an Existing Controller with a New Controller," in the *3ware 9000 Series Serial ATA RAID Controller Installation Guide*.)

Deleting a Unit through 3DM

1 Make sure no I/Os are being issued to 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 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. Resulting behavior depends on which operating system you are using and what kind of I/O is being done, however you will typically see really bad results, bad errors, and most likely a reset of the controller or a system hang.

Under Windows, go to **Start > Administrative Tools > Computer Management**, and select **Disk Management.** Remove the logical drive letter for the unit.

Under Linux and FreeBSD, you can unmount the unit with this command: `umount <mount location>`

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

5   In the Unit Maintenance table on the Maintenance Page, select the unit you want to remove and click **Delete Unit** (Figure 41).
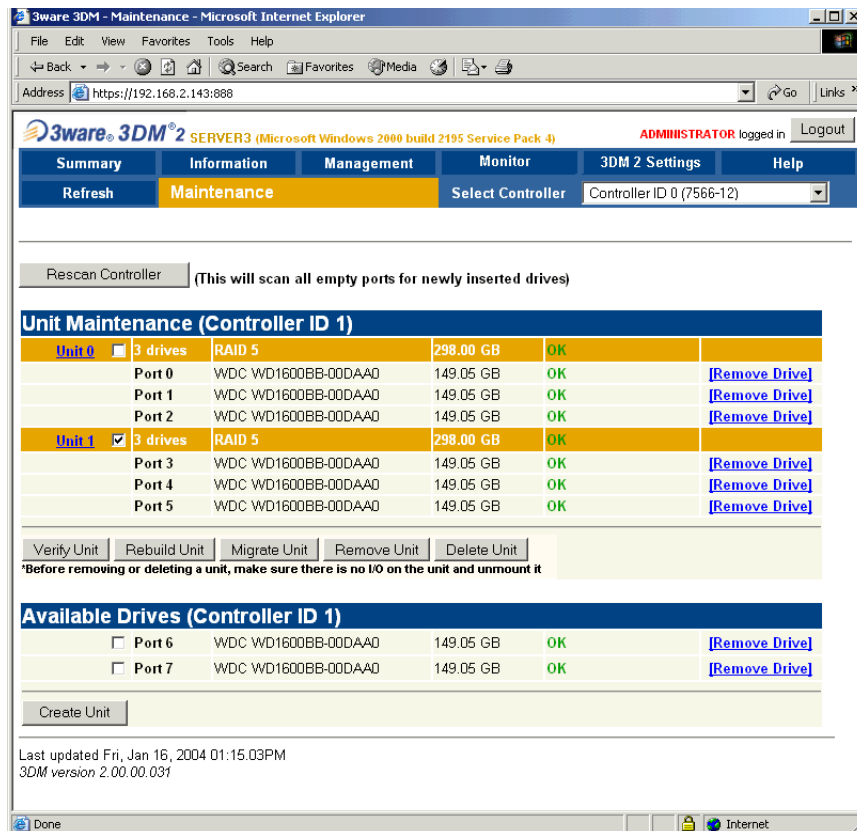
Figure 41.   Deleting a Unit Through 3DM

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 42). You can now use them as part of another unit, or designate them as Spares, for use in a rebuild.

Figure 42.   Unit Successfully Deleted through 3DM

Deleting 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.

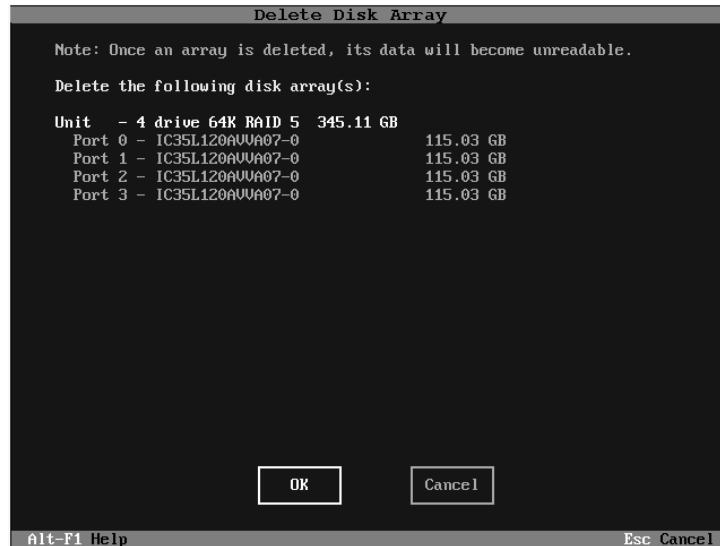2   **Tab** to the **Delete Unit** button and press **Enter.**

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.

```
                        Delete Disk Array
   Note: Once an array is deleted, its data will become unreadable.

   Delete the following disk array(s):

   Unit    - 4 drive 64K RAID 5  345.11 GB
     Port 0 - IC35L120AVVA07-0                115.03 GB
     Port 1 - IC35L120AVVA07-0                115.03 GB
     Port 2 - IC35L120AVVA07-0                115.03 GB
     Port 3 - IC35L120AVVA07-0                115.03 GB




                        OK          Cancel

 Alt-F1 Help                                     Esc Cancel
```

Figure 43.   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 allows you to safely remove drives from a controller in order to move the unit to another controller or to store the drives for safekeeping purposes. This process is sometimes referred to as "array roaming." Hot swap carriers are required unless you power down first.

When you remove a unit (in contrast to deleting a unit), information about the unit remains intact on the drives. This allows the drives to be reassembled into a unit again on this controller, or if moved to another controller.

⚠️ **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.

📓 **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 111.

Removing a Unit Through 3DM

📓 **Note:** If you do not have hot swap carriers, 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 you do have hot swap carriers, follow the steps below.

1   Make sure no I/Os are being issued to 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. Resulting behavior depends on which operating system you are using and what kind of I/O is being done, however you will typically see really bad results, bad errors, and most likely a reset of the controller or a system hang.

    Under Windows, go to **Start > Administrative Tools > Computer Management**, and select **Disk Management.** Remove the logical drive letter for the unit.

    Under Linux and FreeBSD, 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 you have a hotswap carrier, you can do this without shutting down the system. If you do not have a hot-swap carrier, power-down the system and ground yourself before making changes to the hardware.

If you change your mind and want to reuse the drives and unit on the current controller, 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.

1   If your drives are not in hot swap carriers, 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 carriers 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.

3   Press the R key.

The unit is immediately removed from the screen.

You can now physically remove the drives and move them to another controller. If you have a hot swap carrier, 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 ports 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 do this 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 106 and "Rescanning the Controller" on page 113.

⚠ **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 9500-8, 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 the 9xxx 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. You will also need to unlock the drives, as described under "Unlocking Drives Configured on a 9000 Series Controller" on page 109.

Unlocking Drives Configured on a 9000 Series Controller

When drives are configured into a unit on a 9000 series controller, they become locked for use with 9000 series controllers.

If you want to use these drives on an older 3ware controller, a non-3ware controller, or connect them directly to a motherboard ATA controller, you must first unlock them.

You can unlock drives in the following ways:

■   In 3BM, highlight the unit you want to unlock, and press the **r** key (for remove). Then shut down the system.

- In either 3BM or 3DM, delete the unit, as described under "Deleting a Unit" on page 103. All data on the drives will be permanently deleted, and the drives will be unlocked.

- Boot to the operating system. Put a file system on the unit by formatting and partitioning it. Shut down the operating system cleanly. The drives will be unlocked.

Adding a Drive through 3DM

If you have a hot-swap carrier, you can add a drive to your system and make it available through 3DM without powering down the system.

Without hot swap carriers, you should not add a drive via 3DM. Simply power down to add the applicable drives. Refer to the *3ware 9000 Series Serial ATA RAID Controller Installation Guide* for more details.

> **Warning:** Physically adding a drive without a hotswap carrier and without powering down your system can result in a system hang or may even damage the system and the drive

To add a drive through 3DM when you have hot-swap carriers

1 Connect the drive physically to the controller.

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, or as a replacement drive in the event that another drive degrades.

4 If you want to use this drive as a spare, see "Creating a Hot Spare" on page 92.

Removing a Drive

If you have a hot-swap carrier and want to physically remove a drive from your system without powering it down, you must first remove it through the 3ware software.

This is useful 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 carrier can result in a system hang or may even damage the system and the drive.

If you unplug a drive without first removing it through 3DM or 3BM, Rescan will not recognize it as gone. Always use the **Remove Drive** command to remove a drive before unplugging it.

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 106. 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.*

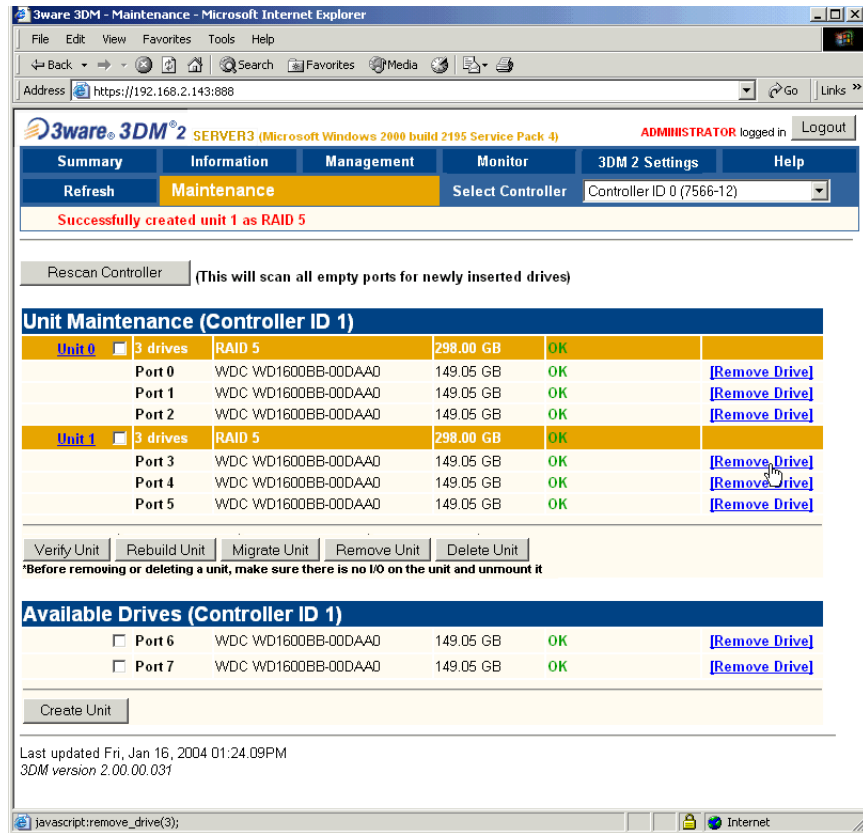**To remove a drive**

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 44).

(You can remove a drive that is part of a unit, or that is shown in the list of Available Drives.)

Figure 44. Removing a Drive in 3DM

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.

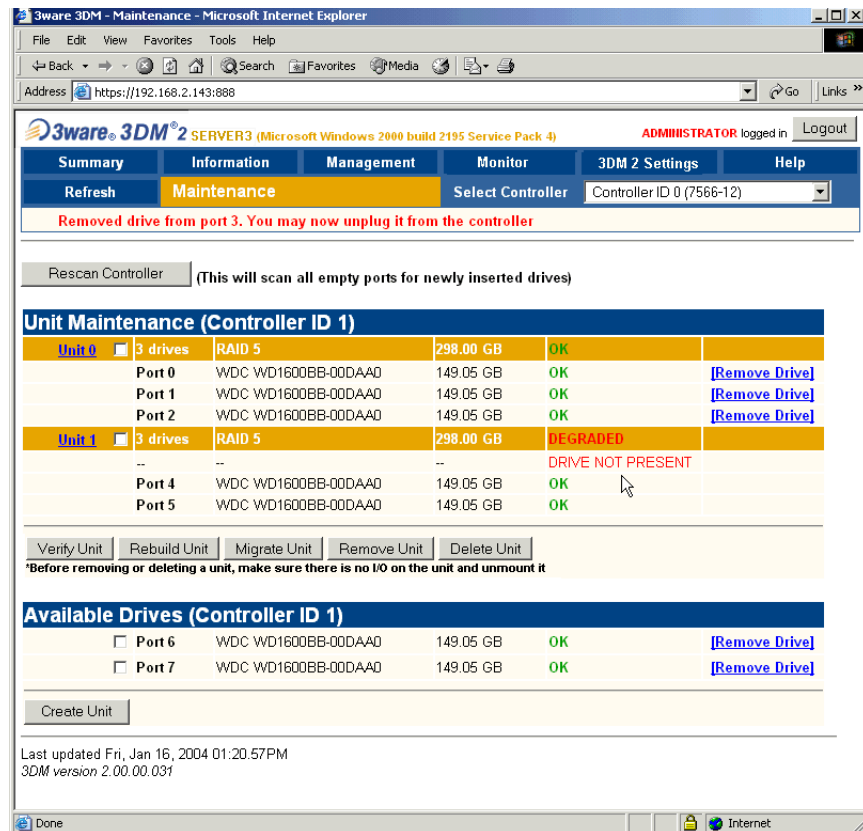If you removed a drive that was part of a unit, the unit may become degraded, as shown in (Figure 45).

Figure 45. Result of Removing Drive from Unit in 3DM

Rescanning the Controller

When you make a change by physically adding drives or units, you can have 3DM rescan the controller to update the list of units and available drives shown on the **Maintenance** page. For more information, see "Adding a Drive through 3DM" on page 110.

This is useful in variety of circumstances. For example, if you added new drives to the controller, you can make them available by rescanning the controller.

For more details about how the Rescan feature works, see the information in the Reference section, under "Maintenance Page" on page 58.

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

There is not an explicit "rescan" command in 3BM. However, if you restart the computer, it will rescan the controllers. You can then start 3BM and use it for configuration or maintenance tasks.

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. The name can also be added or changed later.

To name or rename a unit

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.

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.

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.

This section includes the following tasks to help you maintain your units:

- Checking Unit and Drive Status through 3DM
- Reviewing Alarms and Errors
- About Background Tasks
- Scheduling Background Tasks
- Rebuilding Units
- Verifying Units

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 in 3DM. 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).

Figure 46 illustrates how you can drill down to get additional detail about units and drives in your system.
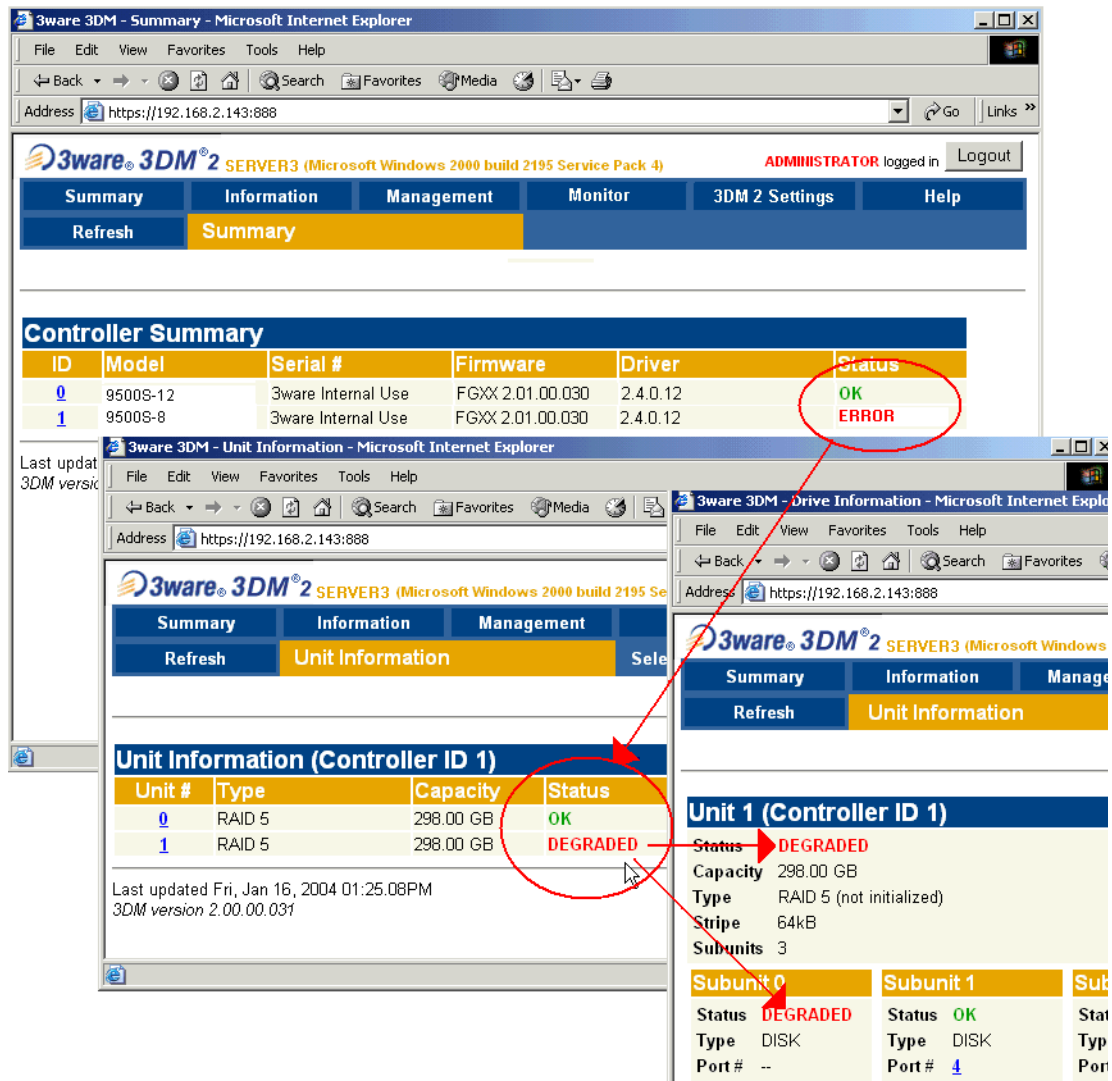
Figure 46. Drilling Down to Check Status Information

For details about specific pages with summary and detailed status information, see these topics in the 3DM Reference section:

- "Controller Summary Page" on page 45
- "Controller Details Page" on page 47
- "Unit Information Page" on page 48
- "Unit Details Page" on page 49
- "Drive Information Page" on page 51
- "SMART Details About Drive at Particular Port Page" on page 52

Reviewing Alarms and Errors

3DM provides several levels of detail about events:

- A summary log of all alarms on the **Alarms** page

- A detailed error listing, available for download from the **Controller Details** page

- **SMART** data for individual drives

Viewing Alarms

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.

Alarm messages are categorized by the following levels of severity:

- Errors, shown next to a red box

- Warnings, shown next to a yellow box

- Information, shown next to a blue box

3DM can e-mail notifications of these events to one or more recipients. For more information, see "Managing E-mail Event Notification" on page 42.

To view alarms

- Choose **Monitor > Alarms**.

  For detailed information about the Alarms page, see "Alarms Page" on page 66.

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   Choose **Information > Controller Details** from the menu bar.

2   Make sure the correct controller is displayed in the **Select Controller** field in the men 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 drive to help troubleshoot problems that occur. SMART data is available on all disk drives (unit members, Single Disks, and Hot Spares).

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 129.

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.

About Background Tasks

Background tasks are maintenance tasks that help maintain the integrity of your drives and data. These tasks include

- Initialization of new units

- Rebuilds when units have become degraded

- Unit verification

- Migration of an on-line RAID from one RAID configuration to another

- Self-tests

About Initialization

Some RAID levels must be initialized for best performance. (For specifics, see "Initialization of Different RAID Types" on page 120.) Initialization can take place before the units are put into service (foreground initialization) or while the units are being used (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. Background initialization uses an algorithm to perform initialization and does not rewrite existing data.

Foreground Versus Background Initialization

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 boot to the operating system. Background initialization will then start automatically within about 10 minutes. Background initialization does not write zeroes to the drives or harm your data, so you can partition, format, and use the unit safely. For the 9000 series, the unit is fully fault-tolerant while the initialization takes place. That is, if the array 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. (For more information, see "Setting Background Task Rate" on page 124.) You can also postpone initialization until a scheduled time. (For details, see "Scheduling Background Tasks" on page 125).

> **Note:** Units that do not need to be immediately initialized for full performance will be automatically initialized using foreground initialization if they are ever verified. (Verification requires that the unit 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.

Initialization of RAID 0 Units

RAID 0 units do not need to be initialized and are immediately available for use with full performance when created.

Initialization of RAID 5 and RAID 50 Units

Regardless of the size, all 9000-series RAID-5 and 50 arrays are fully fault tolerant upon creation. This is because 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 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. Similarly, RAID 50 units with 6, 8, or 9 disks, and RAID 50 with 12 disks configured into 3 subunits of 4 or 4 subunits of 3, do not need to be initialized for full performance.

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, RAID 10 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 channel 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 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).

Auto Initialization After Power Failure

The 3ware controller detects and handles power failures. This mechanism is intended to ensure 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. For redundant units, if a unit or sub-unit is detected to have been shutdown uncleanly, the unit or sub-unit will change its mode to either 'Initializing' or 'Verifying'.

3ware's auto-initialization feature determines if this is required. During driver startup, a flag is set that indicates that the driver loaded. Upon an orderly shutdown, the flag is rewritten, indicating that there was a clean shutdown. During the next system power cycle the firmware queries the flag. If there was a power failure, the flag will indicate that there was not a clean shutdown. This means that the data on the drives may not be correct.

When the initialization is complete, the unit is guaranteed to be redundant again. The initialization does not erase user data.

About Rebuilds

Fault tolerant RAID units provide data security by duplicating information on multiple drives.

- RAID 1 and 10 units each use mirroring, where identical data is stored on two or more drives to protect against drive failure.

- RAID 5 and 50 units achieve fault tolerance by using a simple (exclusive OR) function to generate the parity data that is distributed on all drives.

When one of the drives in a fault-tolerant unit is removed, unplugged or fails on read or write requests, the unit is said to be "degraded." Rebuilding is the process by which the RAID unit is made fault tolerant again.

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.

In all cases, 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 a hot spare is specified and a redundant unit degrades, an event notification is generated and the hot spare automatically replaces the failed drive in the redundant unit without user intervention. 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 rebuild process is complete.

With the 3ware 9000 series controller, rebuilds on multiple units can take place simultaneously.

About Verification

For the 3ware 9000 series, the verify feature combines verification of redundant units (confirming the validity of the redundant data) and media scans for non-redundant units. (3ware software for the 7000 and 8000 series provided separate features for verify and media scan.)

Verification is useful because it can provide early warning of a disk drive problem or failure. For example, if the verification process encounters many error locations, it may be an indication of an excessive number of grown defects on the drive. This allows you to replace drives before they fail.

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.

For a RAID 1 or RAID 10 unit, a verify compares the data of one mirror with the other. For RAID 5 and RAID 50, a verify calculates RAID 5 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.

About Verifies of Non-Redundant Units

Verification of non-redundant units (single disks, JBODs, 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.

About Verifies of Redundant Units

Verifies of redundant units also read 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.

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 026h AEN_DRIVE_ECC_ERROR" on page 169.)

If the disk drive is part of a redundant array 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. The result is a restoration of drive and data integrity; the primary and redundant data are again both valid.

If the array 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 array, and reinstall the data.

About Migration

Migration allows on-line units to be reconfigured. You can make two types of configuration changes:

- RAID Level
- Unit Capacity Expansion

RAID level migration and unit capacity expansion tasks can be done together or separately.

Migration tasks follow the same schedule as rebuild and initialization tasks.

Because of the controller and disk resources required during migration, when migration is active, it has priority over other background tasks. When migration starts, it will take the highest priority over rebuild, initialize and verify.

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.

Migrate tasks are always done in the background, and can be initiated through either 3DM or the CLI. (Foreground migrations through 3BM are not supported.)

A unit be 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 affect this has on performance by setting the background task rate. For more information, see "Setting Background Task Rate" on page 124.

Moving a Unit to Another Controller During Migration

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.

For more information about migration, see "Changing An Existing Configuration" on page 98.

About Self-tests

Two self-tests can be set, to check whether UDMA Mode can be upgraded, and whether SMART thresholds have been exceeded.

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. For more information, see "Selecting Self-tests to be Performed" on page 129.

Setting Background Task Rate

In 3DM, you can set the relative performance of background tasks (initializing, rebuilding, and verifying) in relation to normal I/O activity.

9000-series controllers show separate settings for Rebuild Rate and Verify Rate. (Initialization occurs at the Rebuild rate.) 7000- and 8000-series controllers show only one setting for Task Rate, which applies to both rebuild and verify rates.

Rebuild and verify tasks can be started manually or scheduled. For details about manually starting these processes, see "Rebuilding Units" on page 130 and "Verifying a Unit through 3DM" on page 135. For details about scheduling rebuild, verify, and other tasks, see "Scheduling Background Tasks" on page 125.

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.

For more information about these settings, see the reference section, "Controller Settings Page" on page 53.

Scheduling Background Tasks

You can set up scheduling windows for when background tasks can occur, so that routine maintenance of storage media occurs at times that will be least likely to interfere with peak I/O times. By creating and using schedules, you can limit active rebuilding, verifying, and testing of units to times that are least disruptive.

Note: Initialization and migration operations follow the rebuild schedule.

Although rebuild/migrate, verify, and self-test tasks are scheduled separately, you set up the schedules for each in a 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 scheduled task, you first remove the scheduled item and then add it back with the desired day, time, and duration.

Sometimes you may want to manually start rebuild and verify tasks. For information about how to do so, see the procedures under "Rebuilding Units" on page 130 and "Verifying Units" on page 135.

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 124.

For more information about background tasks themselves, see "About Background Tasks" on page 119.

Prioritization of Background Tasks

Rebuilding preempts verify operations. If a unit requires rebuilding, that process will take place before the unit is verified.

Migration receives higher priority than all other background tasks.

3ware 9000-series RAID 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.

Scheduled Task Duration

If a rebuild completes within a scheduled time, it will not start over come next schedule time block, unless someone degrades the unit and starts another rebuild on the unit in the meantime.

Rebuilds occur at the scheduled time when a drive degrades and there is a hot spare, or when a rebuild has been manually requested. If a rebuild does not complete in the scheduled time block, it will continue where it left off at the next schedule 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.
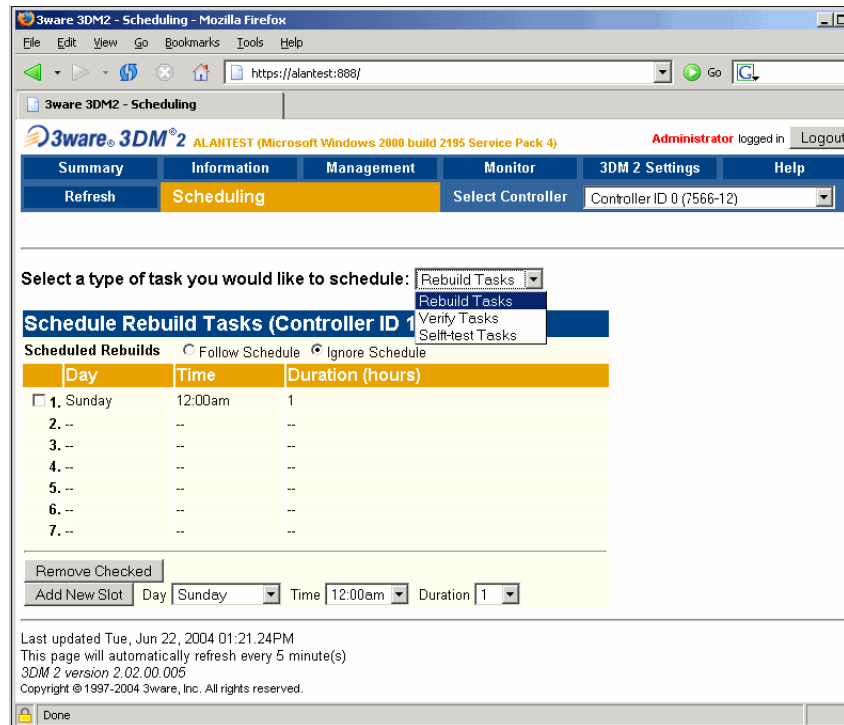
Turning On or Off Use of a Task Schedule

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, are manually started, or if the 'Auto-verify' policy is enabled for a particular unit (verifies only).

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 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 129.

Removing a Task Schedule

When you first use 3DM, 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

Two self-tests can be set, to check whether UDMA Mode can be upgraded, and whether SMART thresholds have been exceeded. (For more information about these self-tests, see the 3DM Reference section, "Scheduling Page" on page 56.)

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.

Rebuilding Units

If a hot spare is specified and a redundant unit degrades, an event notification is generated and the hot spare dynamically replaces the failed drive in the redundant unit without user intervention. 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 few minutes). If 3DM is running and E-mail notification is enabled, an event notification will be sent to specified users when the rebuild process starts and when it completes.

If a hot spare is not specified, or if there is not a hot spare large enough to replace the degraded drive, you can manually replace the drive 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.

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 mirror 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 50 unit can also sustain multiple drive failures, as long there is only one failed drive in each RAID 5 set.

When a RAID 5 is running in Degraded mode, the missing data is reconstructed from all non-degraded 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.

Rebuilding a Unit Through 3DM

When a drive on a unit degrades, you replace it with an available drive and then rebuild the unit.

To rebuild a unit through 3DM

1   If necessary, add a new drive to be used to replace the failed drive. (For details, see "Adding a Drive through 3DM" on page 110.)

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 degraded drive and click **OK.**
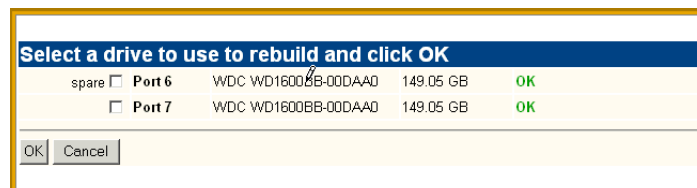
5 If the degraded unit has more than one degraded drive (for example, a RAID 10 where both mirrored pairs each have a degraded drive), repeat steps 3 and 4.

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 47, shows an example of how a degraded RAID 5 unit appears in 3BM.

```
                        3ware BIOS Manager   (slot 4)

      Available Drives:
      Port 5   - IC35L120AVVA07-0              115.03 GB

      Exportable Units:
      Unit 0 - 3 drive 64K RAID 5  223.49 GB      DEGRADED
         Port 2 - IC35L120AVVA07-0              115.03 GB   Not in Use
         Port 3 - IC35L120AVVA07-0              115.03 GB
         Port 4 - IC35L120AVVA07-0              115.03 GB














    [ Create Unit ]  [ Delete Unit ]  [ Maintain ]  [ Rebuild ]  [ Policy ]  [ BBU ]
    Alt-F1 Help  ↕↔ Previous/Next  Alt-a Sel all drv   r Remove    Enter Select/Desel
    F6 Restore Initial Values  Esc Board Selection  F8 Done  s Toggle Hot Spare
```

Figure 47.   Degraded RAID 5 Array to be Rebuilt

To rebuild 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 48 shows an example of a degraded-array message.
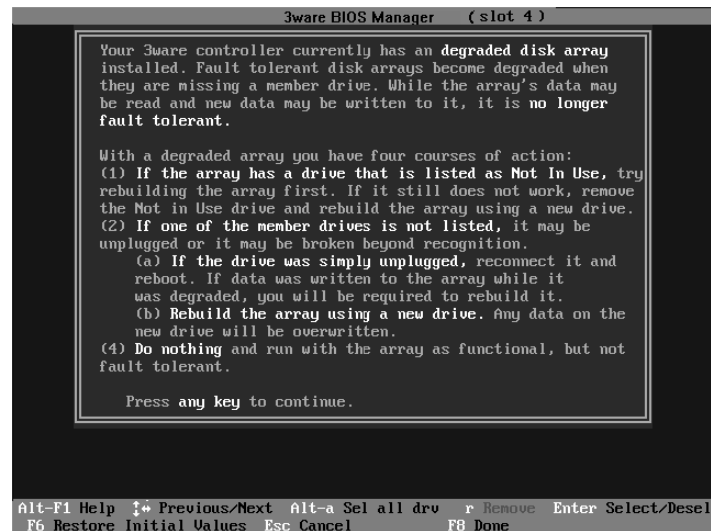
Figure 48. Degraded Disk Array Warning Message

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, you must power down the system and replace the failed or **Not In Use** drive. Then power on the system and start 3BM.

1 At the main 3BM screen, highlight an available drive to replace the faulted drive and press **Enter** to select it (see Figure 49).

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.

Figure 49. Select Available Drive to Replace Faulted Drive

3   **Tab** to the **Rebuild Unit** button and press **Enter**.

4   Navigate to and select the **OK** button to continue.

You are returned to the main screen; "Rebuilding" appears next to the unit you selected.

5   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 you can cancel a rebuild from within 3DM by using the **Remove Drive** link on the Maintenance page.

If you do not want to boot the operating system and launch 3DM, you can also cancel a rebuild by 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 132.

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.

Verifying Units

For redundant units, verify checks the redundancy of the unit. 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 performs a surface scan of the media. During verification, I/O continues normally, but with a slight performance loss, depending on your verify rate setting. For more details about how verification works, see "About Verification" on page 122. For details about verify rates, see "Setting Background Task Rate" on page 124.

For 9000 series controllers, 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 this involves recalculating and rewriting the RAID 5 parity that was incorrect. AEN 36 (AEN_VERIFY_ERROR) is posted to the Alarms page.

When this occurs for 7000/8000 series controllers, AEN 36 AEN_VERIFY_ERROR is logged and the entire unit is initialized. For RAID 1 and 10, initialization involves copying the data from the lower port(s) to the higher port(s) of the mirror. For RAID 5 this involves recalculating and rewriting the RAID 5 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.

Note: If the unit has not previously been initialized and you manually select **Verify Unit** in either 3BM or 3DM, the initialization process starts.

Verification of units can be done automatically, on a schedule, or can be started manually, as described below. For information about scheduling, see "Scheduling Background Tasks" on page 125.

You can manually start a verify through either 3DM or 3BM. as described below.

Verifying 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.)

Verifying 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 **Maintain Disk Array** screen, review the information about the unit to make sure it is the one you want to verify.

4   **Tab** to the **Verify Array** field, change the setting to **Yes.**
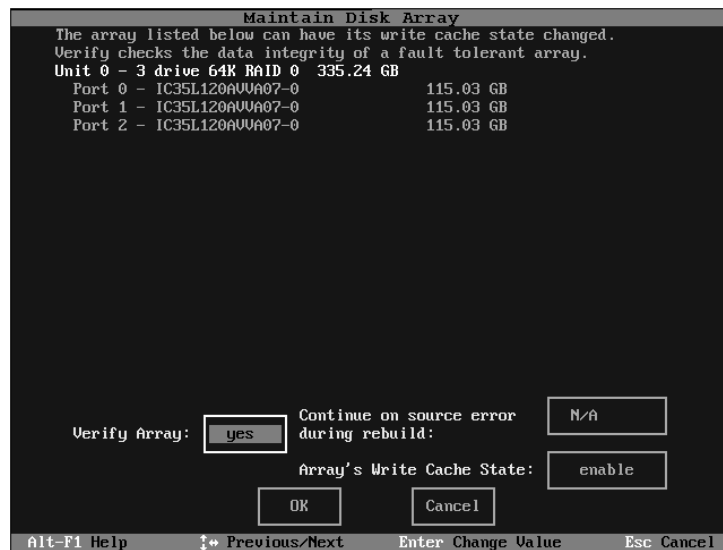
Figure 50.   Verifying a Unit

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

Verification of the selected unit starts immediately.

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.

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 Driver and Firmware
- 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 (see the "Controller Summary Page" on page 45)
- Using 3BM (see "Displaying Advanced Details" on page 25)

Under Linux, you can also type the following command if you have a 2.4 kernel or earlier:

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

where the asterisk (*) represents controller number and "9xxx" represents the version of the controller. For example:

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

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 8 steps under "Updating the 3ware Driver Under Windows XP" on page 146.

You can also use the 3ware Command Line Interface to check the version. For more information, see *3ware 9000 Series Serial ATA RAID Controller CLI Guide*.

Updating the Driver and Firmware

You can download the latest driver from the 3ware website, at www.3ware.com. For Linux and FreeBSD, updating the driver also updates the firmware. For Windows, you can update both driver and firmware, or only the driver.

> **Note:** For Linux, do not use the driver from the external Linux distribution, as it will not include the firmware image, due to size limitations, and 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

1   On the 3ware website (www.3ware.com), navigate to **Service and Support > Software Downloads**.

2   Select the product and release desired.

3   Select Driver as the item to download.

4   Select the Operating System you are using.

5   Click **Next**.

6   When details about the download you requested appear, click the link for the driver you want to download.

7   Read and agree to the license agreement that appears.

8   Click **Save** to save the file to disk.

9   Uncompress the file to extract the driver files to a diskette or to a local directory.

10 Turn to the section for your operating system, below:

- Windows, on page 146
- RedHat Linux, on page 153

- SuSE Linux, on page 154
- FreeBSD, on page 155

To make a driver diskette

If you want to create a driver diskette, extract the driver files to a floppy in step 9 above. Refer to the user manual for your operating system for more details.

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 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 146.

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 on page 140.

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.
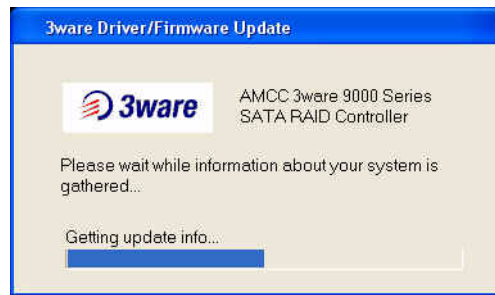
Figure 51.   Update Utility Progress Dialog (System Check)

When the 3ware Driver/Firmware Update dialog box appears, it shows available updates for the device driver and for the firmware.
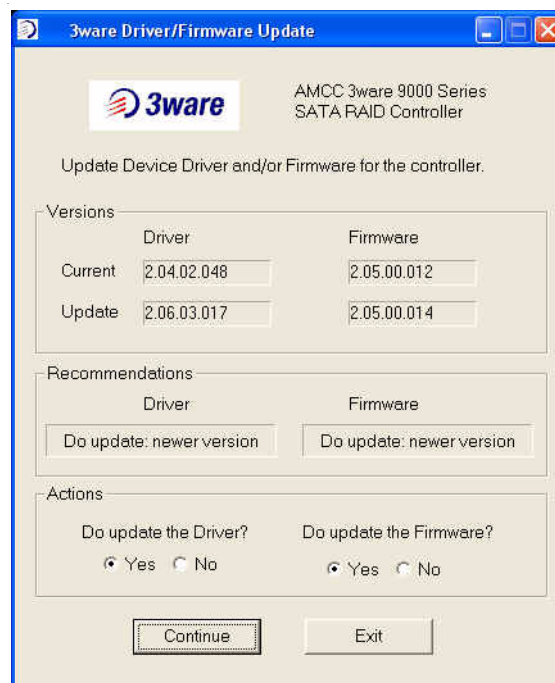
The updater tells you whether newer updates are available, and makes recommendations for whether you should update.

Figure 52.   Update Utility Showing Available Drivers

If either your driver or firmware are current, the screen reflects that.
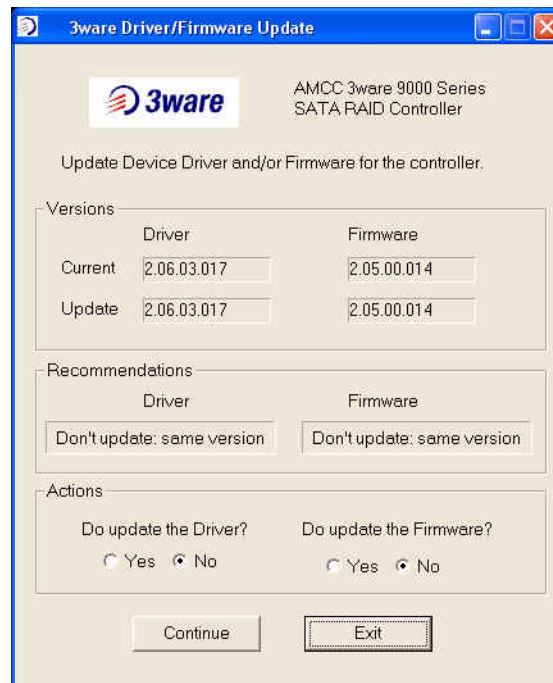
Figure 53. Update Utility Showing Drivers Already Current

If the firmware image is not found with the driver files, you will see an error message, and the 3ware Driver/Firmware Update dialog box will show only the Driver as available.

Figure 54. Error Message When the Firmware Image is Missing
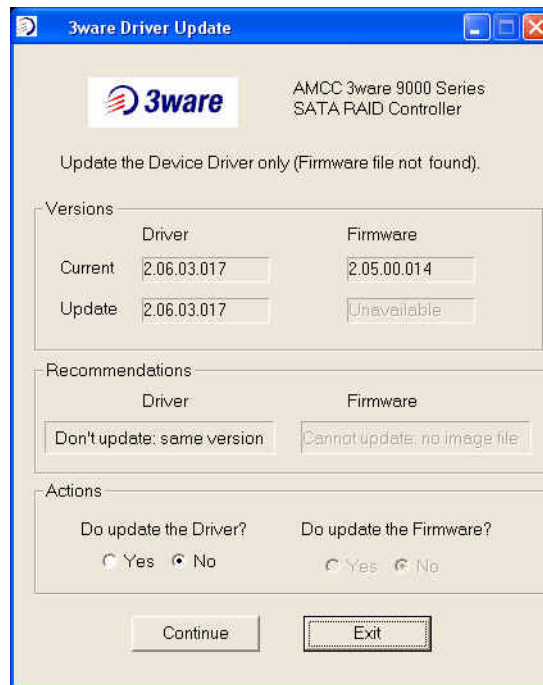
Only the driver is available, because the firmware image was not found.

Figure 55. Update Utility Showing Only Driver Available

> **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 145.

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 your computer, click **Yes** to do so.

(If you were working from a driver diskette, be sure to remove the floppy diskette before Windows reboots.)
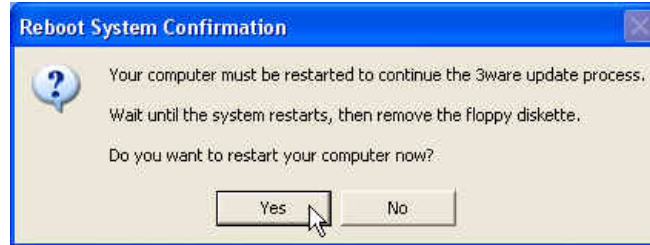
8   If the driver you are installing is unsigned, you will receive a message to that effect.

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.)

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 141.

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.
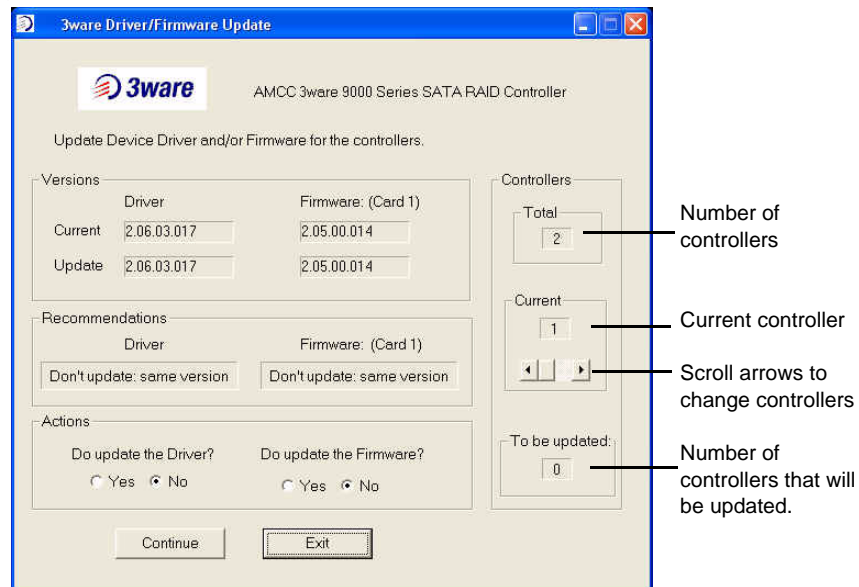
Figure 56. Update Utility Showing Available Drivers

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 on page 140

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 Escalade 9000 Series ATA RAID Controller Properties** dialog box appears.

9   Click the **Driver** tab (Figure 57).
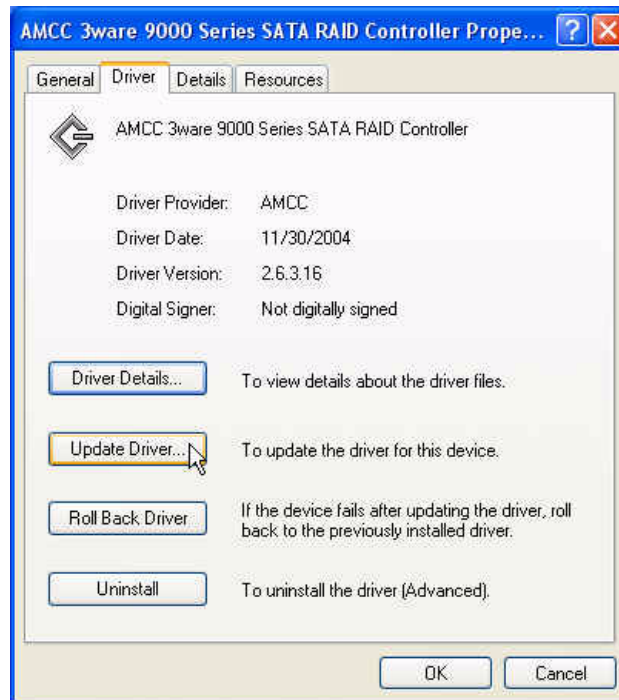
Figure 57. 3ware Serial ATA RAID Controller Properties Dialog

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 58.   Windows XP Service Pack 2 Windows Update Query

12 When you reach the **Hardware Update Wizard** screen shown in Figure 59, select "Install from a list or specific location (Advanced)" and then click **Next**.
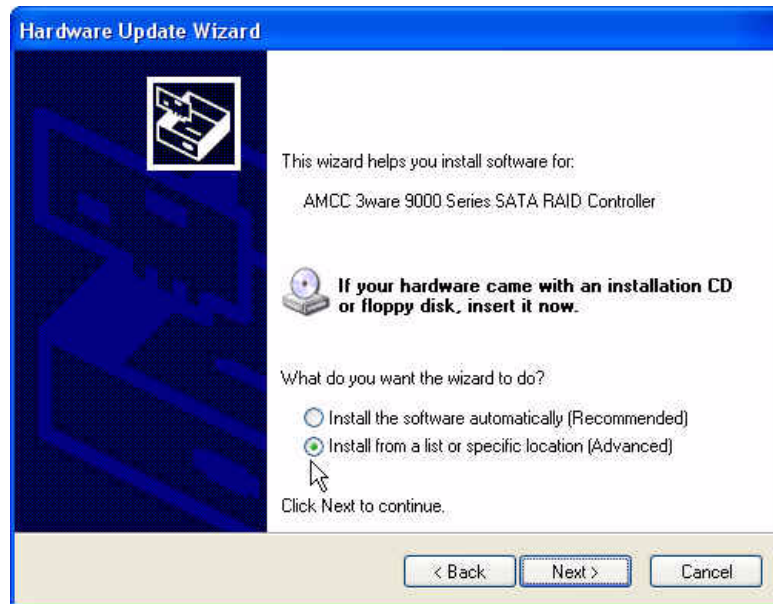
Figure 59.   Upgrade/Install Device Driver Wizard

13 At the next screen (Figure 60) choose "Don't search. I will choose the driver to install" and click **Next**.
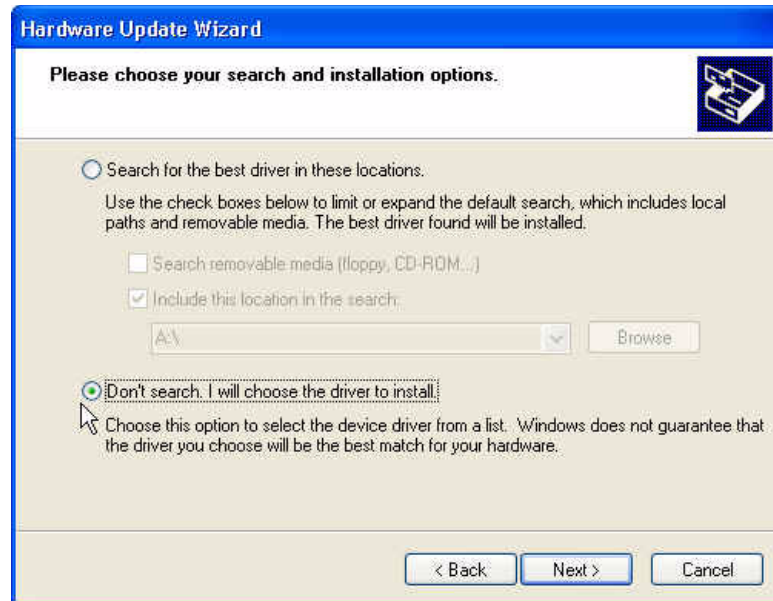
Figure 60.   Search for Driver Screen

14 When the **Select the Device Driver** screen appears (Figure 61), click the **Have Disk…** button.
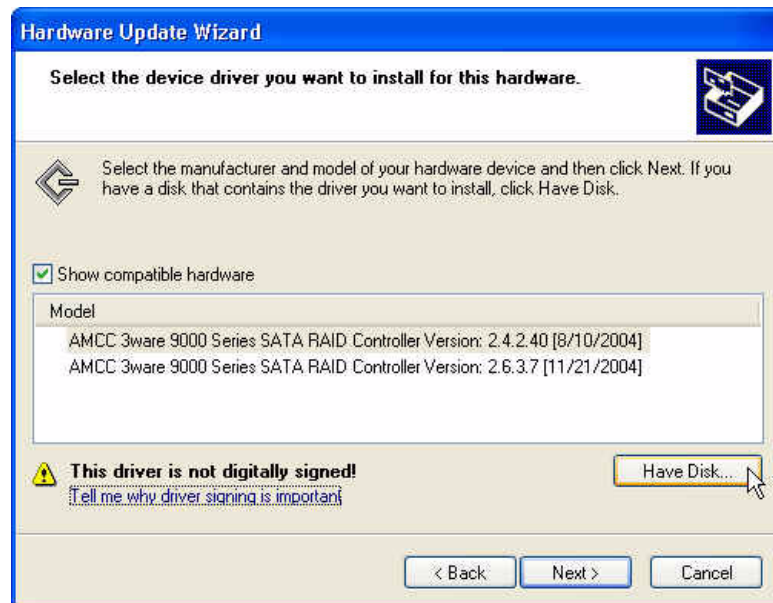
Figure 61.   Select the Device Driver Screen

15 When the **Install from Disk** dialog box appears (Figure 62), 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 62. Install From Disk Dialog Box

16 When the **Select the Device Driver** dialog box reappears, select the appropriate driver (Figure 63) and click **Next**.

Be sure to select the correct driver name, otherwise the driver upgrade will not be successful.
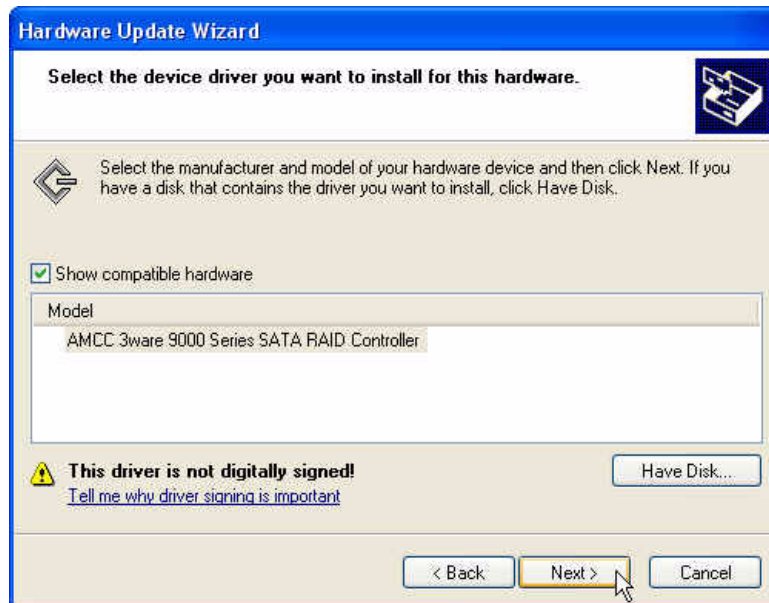
Figure 63. Select a Device Driver

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.

3ware 9000 Series Serial ATA RAID Controller User Guide

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 64).

Figure 64. 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 65.   Completing Found New Hardware Wizard

Updating the 3ware Driver Under Red Hat

1   Download and extract the driver, as described on page 140.

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 version, such as ws3_x86, and replace <kernel> with the applicable kernel, for example 2.4.20-8)

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.o for 2.4 kernels, or 3w-9xxx.ko for 2.6 kernels

For Red Hat Uniprocessor
```
cp <version>/3w-9xxx.o /lib/modules/
<kernel>/drivers/scsi/3w-9xxx.o
```

For Red Hat SMP
```
cp <version>/3w-9xxx.smp /lib/modules/
<kernel>/drivers/scsi/3w-9xxx.o
```

For Red Hat Bigmem
```
cp <version>/3w-9xxx.big /lib/modules/
<kernel>/drivers/scsi/3w-9xxx.o
```

For Red Hat Hugemem
```
cp <version>/3w-9xxx.hug /lib/modules/
<kernel>/drivers/scsi/3w-9xxx.o
```

5   **For 2.4 Kernels**, add the following line to /etc/modules.conf:
```
alias scsi_hostadapter 3w-9xxx.o
```

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

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> with the applicable kernel, for example 2.4.20-8)

For Red Hat Uniprocessor
```
mkinitrd -v -f initrd-<kernel>.img <kernel>
```

For Red Hat SMP

`mkinitrd –v –f initrd-<kernel>smp.img <kernel>smp`

For Red Hat Bigmem

`mkinitrd –v –f initrd-<kernel>bigmem.img <kernel>bigmem`

For Red Hat Hugemem

`mkinitrd –v –f initrd-<kernel>hugmem.img <kernel>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

> **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.

1   Download and extract the driver, as described on page 140.

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 su91)

Replace <kernel> with applicable kernel (i.e.: 2.6.21-4GB)

For SuSE Uniprocessor (2.6 kernels)

`cp <version>/3w-9xxx.ko /lib/modules/<kernel>/drivers/scsi`

For SuSE SMP (2.6 kernels)

`cp <version>/3w-9xxx.smp /lib/modules/<kernel>/kernel/`
`drivers/scsi/3w-9xxx.ko`

For SuSE high memory systems (2.6 kernels)

`cp <version>/3w-9xxx.big /lib/modules/<kernel>/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.o, 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. Details are described in chapter on Linux Driver Installation in the
3ware 9000 Series Serial ATA RAID Controller Installation Guide.

Updating the 3ware Driver Under FreeBSD

1   Download and extract the driver, as described on page 140.

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.

    For FreeBSD 4.x, copy the driver into `/modules`

    For FreeBSD 5.x, copy the driver into `/boot/kernel`.

5   Load the driver
    `kldload twa.ko`

If units are present, you should see unit information in the system log (usually, `/var/log/messages`).

6 `If you wish to load the driver automatically every time the system is rebooted,` add the line `'twa_load="YES"'` to the file
`/boot/loader.conf`

Viewing Battery Information

The Battery Backup Unit (BBU) is an add-on card that can be attached to a 3ware 9000 RAID controller 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.

Note: When the BBU status is not "Ready," write caching is automatically disabled on all units attached to the controller.

You can see information about a battery backup unit attached to your controller in both 3DM 2 and 3BM.

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 68.

To view information about a BBU in 3BM

■ At the main 3BM screen, tab to the **BBU** button 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 68.

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.

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.
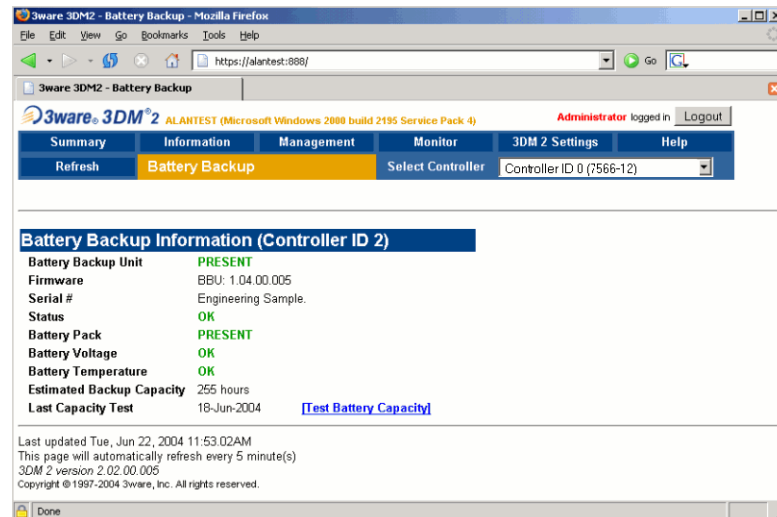
Figure 66.   Battery Backup Information Screen in 3DM

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.
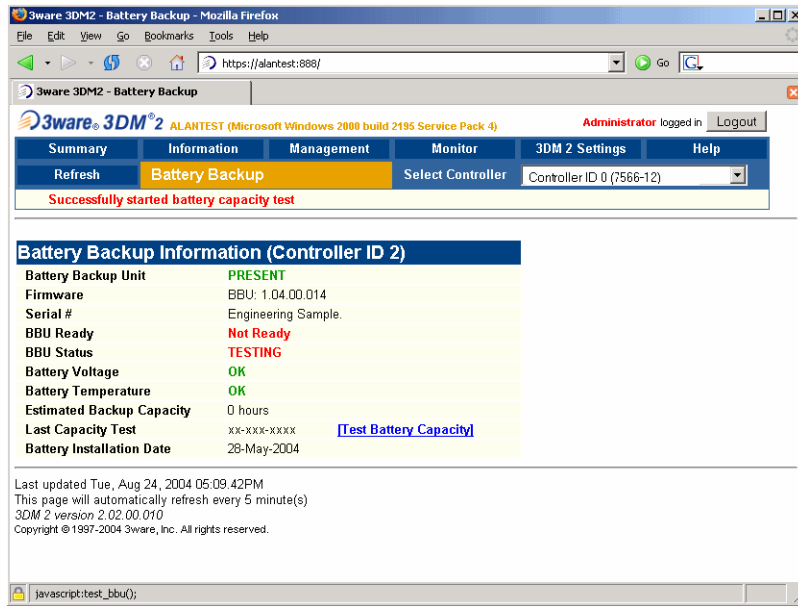
Figure 67.   BBU Information Screen While Battery is Testing

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 68.   Battery Backup Information Screen in 3BM

Troubleshooting: Problems and Solutions

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

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 using your mouse, 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 snapshot of these pages so that you can respond to questions about your system configuration to the Customer Support representative.

Problems in 3DM

Q1: A 3ware RAID controller does not show in the list of controllers.

The appropriate driver may not be installed on the computer in which the controller is installed.

For 7000 or 8000 controllers, you must use the most recent driver. For 9000 controllers, you must use the most recent 9000 driver.

To find out the driver number currently installed, see "Determining the Current Version of Your 3ware Driver" on page 139

Current drivers are available for download on the 3ware website at http://www.3ware.com/downloads.

Instructions for installing drivers are provided in the *3ware 9000 Series Serial ATA RAID Controller Installation Guide*.

Hardware Installation

Q1: The rail on the 3ware RAID controller doesn't fit in the case.

Use a screwdriver to remove the black end rail. It aligns and secures the 3ware RAID controller in the computer chassis but is not critical for operation.

Q2: The system doesn't begin booting (no BIOS runs) when the 3ware RAID controller is installed but boots OK when the controller is removed.

Check the cabling between the drives and the 3ware RAID controller. A cable plugged in upside down can prevent your system from running its BIOS.

Q3: The 3ware BIOS screen never appears.

The 3ware RAID controller is not installed properly. Reinstall the hardware and reboot. There may also be a problem with the motherboard. 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.

Q4: Some of the drives do not appear in the Disk Array Configuration Utility's main display.

Your drives are not connected properly to the 3ware RAID controller. Check that both the power and ATA cables are connected properly and that the drives are all properly jumpered. To operate properly the 3ware

RAID controller requires that drives be set as **Single** (if available on your drive) or **Master**.

Q5: **I am using a Dell Dimension system that locks-up when booting after a 3ware card is installed. What is going on?**

This symptom is caused by a Dell BIOS bug. Basically, this bug sees the system boot drive as two primary master drives. That causes the system to hang. Enter the Dell BIOS setup and reload the BIOS defaults.

Software Installation

Q6: **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 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 disk arrays, you may have overwritten your operating system. Remember that creating or deleting a disk array overwrites any existing data on the member drives. Reinstall your operating system.

- If you installed your operating system when you installed the 3ware RAID controller, you may have made a mistake in installing the operating system. Reinstall your operating system.

There is most likely a compatibility problem between the motherboard system BIOS and the 3ware BIOS. Check the 3ware website to see if your motherboard is compatible with the 3ware BIOS, and check with your motherboard manufacturer for potential BIOS updates.

Q7: **An array shows up as incomplete in the Disk Array Configuration Utility's main display similar to the following:**

```
Array Unit 1 - Incomplete      6.5 GB
     Port 1 - FUJITSU MPC3065AH      6.5 GB
```

The array has some but not all of its members available. The array will be unusable. If this array is your boot device, your system will not boot. You must either find the missing disk and replace it to complete the array, or release the member disks by deleting the incomplete array(s) listed in the display. Remember that deleting a disk array overwrites any existing data on the member drives.

Screen Display Messages

Figure 69 through Figure 73 are screen messages that might appear during installation.
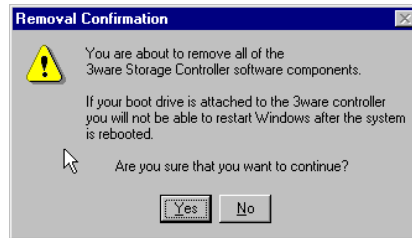
Figure 69.   A Warning for All Software Removal Requests
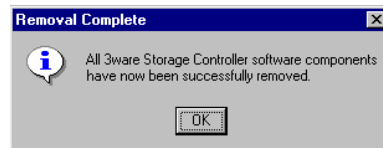
Figure 70.   Confirmation of Successful Software Removal
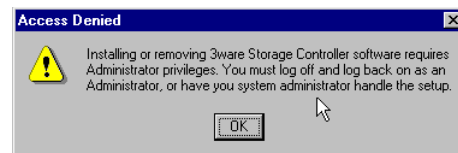
Figure 71.   Administrator Privileges Required Warning
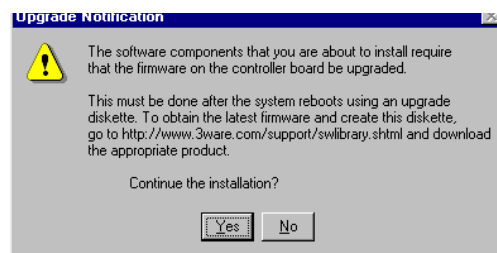
Figure 72.   Firmware Upgrade Requirement Warning
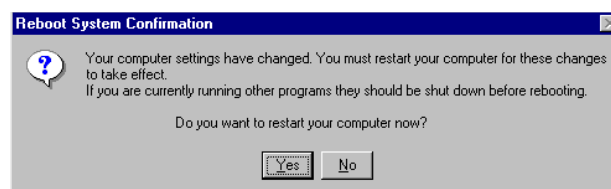
Figure 73.   System Reboot Request

AEN Messages

AEN (automatic event notifications) are messages issued by the 3ware RAID controller when an error is detected such or when an action is completed. These are summarized in Table 7. Descriptions of each are provided at the end of the table.

If you use 3DM 2, AEN messages are displayed on the Alarms page. If you use the CLI, AEN messages can be listed using the `show alarms` command.

On the 3DM 2 Alarms page, the AEN number is the last few digits within the parentheses at the beginning of the message description. For example, in the string `(0x04:0x002B)`, "2B" is the AEN number. To find additional information about the AEN 2B, you would look up 02Bh on the pages below.

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 7: AEN Error Messages

Value	Message
001h	AEN SOFT_RESET
002h	AEN_DEGRADED_UNIT
003h	AEN_CONTROLLER_ERROR
004h	AEN_REBUILD_FAIL
005h	AEN_REBUILD_DONE
006h	AEN_INCOMP_UNIT
007h	AEN_INIT_DONE
008h	AEN_UNCLEAN_SHUTDOWN
009h	AEN_APORT_TIMEOUT
00Ah	AEN_DRIVE_ERROR
00Bh	AEN_REBUILD_STARTED
00Ch	AEN_INIT_STARTED
00Eh	AEN_INIT_FAILED
00Fh	AEN_SMART_FAIL
021h	AEN_UDMA_DOWNGRADE
022h	AEN_UDMA_UPGRADE

Table 7: AEN Error Messages

Value	Message
023h	AEN_SECTOR_REPAIR
024h	AEN_SBUF_FAIL
025h	AEN_LOST_CACHED_WRITE
026h	AEN_DRIVE_ECC_ERROR
027h	AEN_DCB_XSUM_ERROR
028h	AEN_DCB_BAD_VERSION
029h	AEN_VERIFY_STARTED
02Ah	AEN_VERIFY_FAILED
02Bh	AEN_VERIFY_DONE
02Ch	AEN_SECTOR_OVERWRITE
02Dh	AEN_RBLD_SOURCE_ERROR
02Eh	AEN_REPLACE_DRIVE_TOO_SMALL
02Fh	AEN_UNIT_NOT_ZEROED
030h	AEN_DRIVE_NOT_SUPPORTED
032h	AEN_SPARE_INADEQUATE
036h	AEN_VERIFY_ERROR
037h	AEN_INCOMPATIBLE_SODIMM
038h	AEN_NO_SODIMM
039h	AEN_COR_SBUF_ECC
03Ah	AEN_DRIVE_POR_DETECTED
03Bh	AEN_REBUILD_PAUSED
03Ch	AEN_INIT_PAUSED
03Dh	AEN_VERIFY_PAUSED
03Fh	AEN_FLASH_FILE_CORRUPT
040h	AEN_FLASH_FILE_REPAIRED
041h	AEN_UGT_CORRUPT
042h	AEN_PRIMARY_DCB_ERROR
043h	AEN_BACKUP_DCB_ERROR
044h	AEN_VOLTAGE_NORMAL
045h	AEN_VOLTAGE_LOW_WARN

3ware 9000 Series Serial ATA RAID Controller User Guide

Table 7: AEN Error Messages

Value	Message
046h	AEN_VOLTAGE_HIGH_WARN
047h	AEN_VOLTAGE_BELOW_OPERATING
048h	AEN_VOLTAGE_ABOVE_OPERATING
049h	AEN_TEMPERATURE_NORMAL
04Ah	AEN_TEMPERATURE_LOW_WARN
04Bh	AEN_TEMPERATURE_HIGH_WARN
04Ch	AEN_TEMPERATURE_BELOW_OPERATING
04Dh	AEN_TEMPERATURE_ABOVE_OPERATING
04Eh	AEN_LOW_CURRENT_TEST_STARTED
04Fh	AEN_CACHE_SYNC_SKIPPED
050h	AEN_LOW_CURRENT_TEST_STOPPED
051h	AEN_HIGH_CURRENT_TEST_STARTED
052h	AEN_HIGH_CURRENT_TEST_STOPPED
053h	AEN_NEED_CAPACITY_TEST
055h	AEN_CHARGE_STARTED
056h	AEN_CHARGE_STOPPED
057h	AEN_CHARGE_FAULT
058h	AEN_CAPACITY_WARN
059h	AEN_CAPACITY_ERROR
05Ah	AEN_BATTERY_PRESENT
05Bh	AEN_BATTERY_NOT_PRESENT
05Ch	AEN_HIGH_CURRENT_TEST_WARN
05Dh	AEN_HIGH_CURRENT_TEST_FAULT
05Eh	AEN_CACHE_SYNC_PASS
05Fh	AEN_CACHE_SYNC_FAIL
0FFh	AEN_QUEUE_FULL

AEN   001h SOFT_RESET

The 3ware RAID controller has detected a soft reset from the device driver. If the 3ware RAID controller fails to respond to the device driver within a

reasonable amount of time, the device driver may issue a soft reset to the 3ware RAID controller and retry the command packet.

AEN 002h AEN_DEGRADED_UNIT

An error has been encountered and the array is operating in degraded (non-redundant) mode. The user should replace the bad drive as soon as possible and initiate a rebuild.

AEN 003h AEN_CONTROLLER_ERROR

The 3ware RAID controller has encountered an internal error. Please contact 3ware Customer Support as a replacement board may be required.

AEN 004h AEN_REBUILD_FAIL

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, due to ATA drives' ability to reallocate sectors on write errors, the rebuild failure is most likely caused by the source drive of the rebuild detecting some sort of read error. The default operation of the 3ware RAID controller is to abort a rebuild if an error is encountered. If it is desired to continue on error, you can set the Continue on Source Error During Rebuild policy for the unit on the Controller Settings page in 3DM.

AEN 005h AEN_REBUILD_DONE

The 3ware RAID controller has successfully completed a rebuild. The completion of the rebuild changes the state of the array from rebuilding to OK. The data is now redundant.

AEN 006h AEN_INCOMP_UNIT

At power-on initialization time, the 3ware RAID controller performs a "rollcall" of all drives attached to the card. After detection of the drives, the 3ware RAID controller then uses an internal algorithm to logically connect drives that belong to the same array. If after rollcall a member of an array is not found, the **INCOMPLETE UNIT AEN** is sent. Examples of incomplete units are as follows:

- 4 drive RAID 5 with 1 drive missing.

- 2 drive RAID 1 with 1 drive missing.

Replacing the missing or dead drive and initiating a rebuild will change the state of the array from an incomplete unit to OK. No rebuild is required if you replace the missing drive before loading the driver.

AEN 007h AEN_INIT_DONE

The 3ware RAID controller has completed the initialization sequence of RAID levels 1, 10, 5, or 50. For RAID 5, the data on the array is read and the resultant parity is written to the parity area on the array. For RAID 1 and 10, one half of the mirror is copied to the other half (mirrors are synchronized).

AEN 008h AEN_UNCLEAN_SHUTDOWN

The 3ware RAID controller has the ability to detect if the system has been shutdown via the standard shutdown mechanism of the operating system (clean shutdown). If the system loses power or is reset without going through the normal shutdown procedure, it is possible that the data on a redundant array may be out of synchronization. The unclean shutdown detection will detect this case and force the array to enter the rebuilding state. This has the effect of synchronizing the array back to a fully redundant state.

To prevent unclean shutdowns, the user should always go through the normal shutdown procedure for the operating system in use and use an uninterruptible power supply (UPS) to prevent unclean shutdowns due to sudden power loss.

AEN 009h AEN_APORT_TIMEOUT

The 3ware RAID controller has a sophisticated recovery mechanism to handle various types of failures of a disk drive. One such possible failure of a disk drive is a failure of a command that is pending from the 3ware RAID controller to complete within a reasonable amount of time. If the 3ware RAID controller detects this condition, it notifies the user, prior to entering the recovery phase, by displaying this AEN.

Possible causes of APORT time-outs include a bad or intermittent disk drive, power cable or interface cable.

AEN 00Ah AEN_DRIVE_ERROR

As part of the recovery mechanism of the 3ware RAID controller, various drive failures can be detected and, if possible, corrected. One such drive failure is when the drive indicates back to the 3ware RAID controller that it was unable to complete a command. If the drive returns an error to the 3ware RAID controller, the user is notified by this AEN.

AEN 00Bh AEN_REBUILD_STARTED

The 3ware RAID controller notifies the user whenever it starts a rebuild. The rebuild start may be user-initiated (by selecting the rebuild button in the 3DM Disk Management Utility) or it may be auto-initiated by a hot spare failover. In either case, the user is notified of the event by this AEN.

AEN 00Ch AEN_INIT_STARTED

The 3ware RAID controller notifies the user by this AEN whenever it starts an initialization. Initialization either occurs at array creation time for larger RAID 5 or 50 arrays or later during the initial verification of redundant arrays.

AEN 00Eh AEN_INIT_FAILED

The 3ware RAID controller was unable to complete the initialization. This error can be caused by unrecoverable drive errors. When this error occurs, the unit will go back to degraded mode if possible.

AEN 00Fh AEN_SMART_FAIL

The 3ware RAID controller supports SMART Monitoring, whereby the individual drives automatically monitor certain parametric information such as error rates and retry counts. By monitoring this data, SMART may be able to predict a drive failure before it happens, allowing a user to schedule service of the array before it becomes degraded. The SMART status of each drive attached to the 3ware RAID controller is monitored daily. If a failure of any drive is determined to be likely, the user is notified by this AEN.

AEN 021h AEN_UDMA_DOWNGRADE

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 (e.g., an intermittent 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 (e.g., from UDMA 100 to UDMA 66) and retries another three times. This AEN is sent to the user when the 3ware RAID controller lowers the UDMA transfer rate.

Possible causes of UDMA CRC errors are intermittent or bad ATA interface cables or cable routing problems through electrically noisy environments (e.g., cables are too close to the power supply).

AEN 022h AEN_UDMA_UPGRADE

During the self-test, if a drive is found to not be in the optimal UDMA mode, the controller will upgrade its UDMA mode to be optimal.

AEN 023h AEN_SECTOR_REPAIR

The 3ware RAID controller supports a feature called dynamic sector repair to allow the unit to recover from certain drive errors that would normally result

in a degraded array situation. For redundant arrays such as RAID 1, 10, 50, and 5, the 3ware RAID controller essentially has two copies of the users 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. When a sector repair occurs, the user is notified by this AEN.

The fact that a sector repair AEN has been sent to the user is 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 an array that begins to indicate sector repair messages. This may be an indication of a drive that is beginning to fail. The user may wish to replace the drive, especially if the number of sector repair errors exceeds 3 per month.

AEN 024h AEN_SBUF_FAIL

The 3ware RAID controller, as part of its data integrity features, performs diagnostics on its internal RAM devices. 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 AEN is sent to notify the user of the problem. Contact Technical Support for a replacement controller.

AEN 025h AEN_LOST_CACHED_WRITE

To improve performance, this 3ware RAID controller features caching layer firmware. For write commands this means that it acknowledges it has completed a write operation before the data is committed to disk. If the 3ware RAID controller can not commit the data to the media after it has acknowledged to the host, this AEN is posted to the user.

Typically, the LOST CACHED WRITE notification would be an indication of a catastrophic failure of the drives in the array, such as loss of power to multiple drives in an array.

AEN 026h AEN_DRIVE_ECC_ERROR

This AEN may be sent when a drive returns the ECC error response to an 3ware RAID controller command. The AEN may or may not be associated with a host command. Internal operations such as Background Media Scan post this AEN whenever drive ECC errors are detected.

Drive ECC errors are an indication of a problem with grown defects on a particular drive. For redundant arrays, this typically means that dynamic sector repair would be invoked (see AEN 023h). For non-redundant arrays

(JBOD, RAID 0 and degraded arrays), drive ECC errors result in the 3ware RAID controller returning failed status to the associated host command.

AEN 027h AEN_DCB_XSUM_ERROR

The 3ware RAID controller stores certain configuration parameters on a reserved area of each disk drive called the Drive Configuration Block (DCB). As part of power-on initialization, the 3ware RAID controller performs a checksum of the DCB area to ensure consistency. If an error occurs, please contact 3ware technical support. The drive's DCB has been corrupted.

AEN 028h AEN_DCB_BAD_VERSION

During the evolution of the 3ware product line, the format of the 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 an array that was created on a very old 3ware product is connected to a newer 3ware RAID controller, this AEN is posted and the 3ware RAID controller rejects the drive. Please contact 3ware technical support if this event occurs.

AEN 029h AEN_VERIFY_STARTED

The 3ware RAID controller allows the user to verify data integrity on an array.The verification functions for different RAID levels are as follows:

- Single, JBOD, and Spare. Verify = Media Scan

- RAID 0. Verify = Media Scan

- RAID 1. Verify = Compare of Mirror Sides

- RAID 10. Verify = Compare of Mirror Sides

- RAID 5 and 50. Verify = Compare of Parity Data with User Data

When the verification starts, this AEN is posted to the user.

AEN 02Ah AEN_VERIFY_FAILED

This AEN indicates that the data integrity verification function (see AEN 029h) has terminated with an error. For each RAID level being verified, this may mean:

- Single, JBOD, 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. One side of the mirror does not equal the other side.

- RAID 10. One side of the mirror does not equal the other side.

■ RAID 5 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 array. This possibility applies to RAID 1, 10, 5, and 50. A rebuild will re-synchronize the array.

AEN 02Bh AEN_VERIFY_DONE

This AEN indicates the data integrity verification function (see AEN 029h) was completed successfully. No errors were encountered.

AEN 02Ch AEN_SECTOR_OVERWRITE

If a read error is encountered during a rebuild and the user chooses to ignore the error, the sector in error is reallocated. The user is notified of the event by this AEN.

AEN 02Dh AEN_RBLD_SOURCE_ERROR

If an error is encountered during a rebuild operation, this AEN is generated if the error was on a source drive of the rebuild. Knowing if the error occurred on the source or the destination of the rebuild is useful for troubleshooting.

AEN 02Eh AEN_REPLACE_DRIVE_TOO_SMALL

The 3ware RAID controller notifies the user by this AEN when the replacement drive capacity is smaller than required. The replacement drive must be equal to or greater capacity than the drive it's replacing.

AEN 02Fh AEN_UNIT_NOT_ZEROED

This AEN will be sent by the controller when a verify operation is attempted but the unit has never been initialized before. The unit will transition to initializing mode.

AEN 030h   AEN_DRIVE_NOT_SUPPORTED

3ware 8000 and 9000 series Serial ATA Controller only support UltraDMA-100/133 drives when using the parallel to serial ATA converter. This AEN indicates that an unsupported drive was detected during rollcall or a hot add. This AEN also could indicate that the Serial to Parallel converter was jumpered in the wrong place. The converter must be correctly jumpered to correspond to UDMA 100 or 133 drives.

AEN 032h AEN_SPARE_INADEQUATE

This AEN is sent by the controller when it finds a valid hot spare but the capacity is not sufficient to use it for a drive replacement.

AEN 036h AEN_VERIFY_ERROR

This AEN is sent by the controller when a verify error is found (parity inconsistency for RAID5/50 or data mismatch for RAID1/10 configuration) and recovered. If the error is not recovered the AEN_VERIFY_FAILED is returned instead.

AEN 037h   AEN_INCOMPATIBLE_SODIMM

This AEN will be sent if an incompatible SODIMM memory has been connected to the controller. In this case, the controller is inoperable.

AEN 038h   AEN_NO_SODIMM

This AEN will be sent if there is no SODIMM memory connected to the controller. In this case, the controller is inoperable.

AEN 039h   AEN_COR_SBUF_ECC

This AEN will be sent when the controller has detected and corrected a memory ECC error.

AEN 03Ah   AEN_DRIVE_POR_DETECTED

If the controller detects that a drive has been power-cycled, it will send this AEN. The controller may degrade the unit (if possible).

AEN 03Bh   AEN_REBUILD_PAUSED

This AEN will be sent when the rebuild operation is paused.

AEN 03Ch   AEN_INIT_PAUSED

This AEN will be sent when the initialization is paused.

AEN 03Dh   AEN_VERIFY_PAUSED

This AEN will be sent when the verify operation is paused.

AEN 03Fh AEN_FLASH_FILE_CORRUPT

The 3ware RAID controller stores some configuration parameters as files in its flash memory. This AEN will be sent when a corrupted flash file system is found on the controller during boot-up. A further attempt will be made to

repair the flash file system. These files usually get corrupted when a flash operation is interrupted by events such as power failures.

AEN 040h AEN_FLASH_FILE_REPAIRED

This AEN will be sent if a corrupted flash file system is successfully repaired. Some of the flash files with insufficient data may be lost in the operation. The configuration parameters which are lost will then return to their default values.

AEN 041h AEN_UGT_CORRUPT

The 3ware RAID controller tries to keep the unit numbers persistent across soft resets. This AEN will be sent if unit number assignments were lost from some unknown reasons.(This event rarely happents. Please contact AMCC 3ware technical support if this event occurs.

AEN 042h AEN_PRIMARY_DCB_ERROR

This AEN will be sent when the controller finds error in reading the primary copy of the Disk Configuration Block (DCB). The back-up copy of the DCB will be read if this error occurs. If a valid DCB is found, the primary DCB is re-written to rectify the errors found.

AEN 043h AEN_BACKUP_DCB_ERROR

This AEN will be sent when the controller sees a latent error in the backup Disk Configuration Block (DCB). A scrubbing activity will be started to repair any sector errors on getting this error. An effort is made to read the backup DCB even when the primary DCB is successfully read. When an error occurs here, this is a latent error that needs to be addressed before any future errors so this DCB is re-written with the primary copy to rectify the errors found.

AEN 044h AEN_VOLTAGE_NORMAL

The Battery Backup Unit measures and evaluates the battery pack voltage on a continuous basis. If the voltage falls outside the acceptable range then comes back within the acceptable range, this AEN will be posted to the host.

AEN 045h AEN_VOLTAGE_LOW_WARN

The Battery Backup Unit measures and evaluates the battery pack voltage on a continuous basis. If the voltage is below the warning threshold, this AEN will be posted to the user. When this event happens, the Battery Backup Unit is still able to backup the 3ware RAID controller, but the user should replace the battery.

AEN 046h AEN_VOLTAGE_HIGH_WARN

The Battery Backup Unit measures and evaluates the battery pack voltage on a continuous basis. If the voltage is above a warning threshold, this AEN will be posted to the user. When this event happens, the Battery backup Unit is still able to backup the 3ware RAID controller but the user should replace the battery.

AEN 047h AEN_VOLTAGE_BELOW_OPERATING

The Battery Backup Unit measures and evaluates the battery pack voltage on a continuous basis. If the voltage is too low to operate, this AEN will be posted to the user. This indicates that the battery pack must be replaced. The Battery Backup Unit becomes not ready and is unable to backup the 3ware RAID controller.

AEN 048h AEN_VOLTAGE_ABOVE_OPERATING

The Battery Backup Unit measures and evaluates the battery pack voltage on a continuous basis. If the voltage is too high to operate, this AEN will be posted to the user. The Battery Backup Unit becomes not ready and is unable to backup the 3ware RAID controller. This indicates that the Battery Backup Unit must be replaced.

AEN 049h AEN_TEMPERATURE_NORMAL

The Battery Backup Unit measures and evaluates the battery pack temperature on a continuous basis. If the temperature falls outside the acceptable range then comes back within the acceptable range, this AEN will be posted to the host.

AEN 04Ah AEN_TEMPERATURE_LOW_WARN

The Battery Backup Unit measures and evaluates the battery pack temperature on a continuous basis. If the temperature is below a warning threshold, this AEN will be posted to the user. When this event happens, the Battery Backup Unit is still able to backup the 3ware RAID controller but the user should replace the battery pack.

AEN 04Bh AEN_TEMPERATURE_HIGH_WARN

The Battery Backup Unit measures and evaluates the battery pack temperature on a continuous basis. If the temperature is above a warning threshold, this AEN will be posted to the user. The user should check that there is enough airflow around the Battery Backup Unit. When this event happens, the Battery Backup Unit is still able to backup the 3ware RAID controller but the user should replace the battery pack if the temperature warning persists.

AEN 04Ch AEN_TEMPERATURE_BELOW_OPERATING

The Battery Backup Unit measures and evaluates the battery pack temperature on a continuous basis. If the temperature is too low to operate, this AEN will be posted to the user. When this event happens, the Battery Backup Unit becomes not ready and is unable to backup the 3ware RAID controller. The user must replace the battery pack.

AEN 04Dh AEN_TEMPERATURE_ABOVE_OPERATING

The Battery Backup Unit measures and evaluates the battery pack temperature on a continuous basis. If the temperature is too high to operate, this AEN will be posted to the user. The user should check that there is enough airflow around the Battery Backup Unit. When this event happens, the Battery Backup Unit becomes not ready and is unable to backup the 3ware RAID controller. The user must replace the battery pack if the temperature error persists. The use of a PCI card in the slot adjacent to the BBU is not recommended and may result in the battery temperature being exceeded.

AEN 04Eh AEN_LOW_CURRENT_TEST_STARTED

This AEN is posted when the Battery Backup Unit starts a battery test. The test estimates the battery capacity in hours, which is how long the Battery Backup Unit can back up the 3ware RAID controller. 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; all units have their write cache disabled until the test completes.

AEN 04Fh AEN_CACHE_SYNC_SKIPPED

The 3ware RAID controller performs cache synchronization when system power is restored following a power failure. This AEN is posted when the cache synchronization was skipped and write data is still being backed up in the controller cache. This can occur if a unit that was present before the power failure was physically removed or became inoperable before system power was restored.

AEN 050h AEN_LOW_CURRENT_TEST_STOPPED

This AEN is posted when the Battery Backup Unit completes a battery capacity test. All units will have their write cache settings restored to their original values since the Battery Backup Unit is now able to backup the 3ware RAID controller.

AEN 051h AEN_HIGH_CURRENT_TEST_STARTED

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 AEN is posted to the host when this health check is started.

AEN 052h AEN_HIGH_CURRENT_TEST_STOPPED

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 AEN is posted to the host when this health check has completed.

AEN 053h AEN_NEED_CAPACITY_TEST

The recommended time interval for running the battery capacity test is once every 4 weeks. If a battery capacity test has not been completed in the last 4 weeks this AEN will be sent to the host, and once every week thereafter.

AEN 055h AEN_CHARGE_STARTED

This AEN is posted when the Battery Backup Unit starts a battery charge cycle.

AEN 056h AEN_CHARGE_STOPPED

This AEN is posted when the Battery Backup Unit completes a battery charge cycle.

AEN 057h AEN_CHARGE_FAULT

This AEN is posted when the charger of the Battery Backup Unit has detected a battery fault during a charge cycle. The Battery Backup Unit becomes not ready and is unable to backup the 3ware RAID controller.

AEN 058h AEN_CAPACITY_WARN

The measured capacity of the battery is below the warning level. When this occurs the Battery Backup Unit is still able to backup the 3ware RAID controller but it signals that the battery pack should be replaced soon.

AEN 059h AEN_CAPACITY_ERROR

The measured capacity of the battery is below the error level. When this occurs the Battery Backup Unit becomes not ready and is unable to backup the 3ware RAID controller. The user must replace the battery pack.

AEN 05Ah AEN_BATTERY_PRESENT

This AEN is posted to the host when the Battery Backup Unit detects that a battery pack has been connected.

AEN 05Bh AEN_BATTERY_NOT_PRESENT

This AEN is posted to the host when the Battery Backup Unit detects that the battery pack has been removed.

AEN 05Ch AEN_HIGH_CURRENT_TEST_WARN

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 AEN is posted when the result of the health test is below the warning threshold. This indicates that the battery pack should be replaced soon because the battery is becoming weak.

AEN 05Dh AEN_HIGH_CURRENT_TEST_FAULT

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 AEN is posted when the result of the health test is below the fault threshold. This indicates that the battery pack must be replaced. The Battery Backup Unit becomes not ready and is unable to backup the 3ware RAID controller.

AEN 05Eh AEN_CACHE_SYNC_PASS

The 3ware RAID controller performs cache synchronization when system power is restored following a power failure. This AEN is posted for each unit when the cache synchronization completed successfully.

AEN 05Fh AEN_CACHE_SYNC_FAIL

The 3ware RAID controller performs cache synchronization when system power is restored following a power failure. This AEN is posted when cache synchronization was not successful for some reason.

AEN 0FFh AEN 0FFh AEN_QUEUE_FULL

This is an internal error. Please contact 3ware Technical Support.

Glossary

- **3BM.** 3ware BIOS Manager. 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. It is available for download from ww.3warecom/downloads as part of the firmware image. For 9000 Linux and FreeBSD users, it is included in the driver.

- **3DM.** 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 for download from ww.3ware.com/downloads.

- **A-Chip**. AccerATA chip. Automated data port to handle asynchronous ATA disk drive interface.

- **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 10, RAID 50).

- **CLI**. Command Line Interface. The 3ware CLI is a text program, rather than a GUI (graphical user interface), for Windows, Linux, and FreeBSD. 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 ID number.** The unique SCSI number in the Windows environment, or the Channel number in the Linux environment, of a particular controller. Typically assigned by the operating system.

- **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. If you want to attach and access an existing array without overwriting the configuration data, see Array Roaming.

- **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 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 Error policy**. Determines whether an error detected during a rebuild stops the rebuild or whether the rebuild can continue in spite of the error.

- **EMS (Enclosure Management Services).** Chassis-monitoring functions for environmental, power, mechanical monitoring, and control using the I²C bus port.

- **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).

- **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 degraded 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 carriers. This is referred to as array roaming. Hot swapping can also be used to remove and replaced failed drives when a hot-swap carrier is used.

- **I²C-(or Inter-IC) bus**. A two-wire serial bus solution used as a control, diagnostic, environmental, and power management for EMS (enclosure management services).

- **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.** 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 and 50, initialization calculates the RAID 5 parity and writes it to disk (background initialization) or writes zeroes to all of the drives in the array (foreground initialization). Initialization does not erase user data if done while the operating system is running. However, RAID 5 initialization done through the 3ware BIOS does erase any existing data.

- **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. However, a policy in 3BM can be set that allows JBODs to be seen by the OS. By default, individual drives must be configured as Single Disks in order to be made available to the OS.

- **Mirrored disk array.** 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 arrays include RAID 1 and RAID 10.

- **Non-redundant units.** A disk array without fault tolerance (RAID 0, single disk, or JBOD.).

- **OCE (Online Capacity Expansion).** The process of increasing the size of an existing RAID unit without having to create a new array.

- **Parity.** Information that the controller calculates using an exclusive OR (XOR) algorithm and writes to the disk drives in RAID 5 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.

- **Port ID**. A unique identifier for a specific port in a system. Also called a drive ID.

- **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 degraded drive in a fault tolerant unit (for example, RAID 1, 10, 5, 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 unit test that can be performed on a scheduled basis. in 3DM, 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.

- **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 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, 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 and 1500 Mbit/sec with SATA disk drives.

- **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 and RAID 50, a verify will calculate RAID 5 parity and compare it to what is written on the disk drive.

Appendix A. Compliance and Conformity Statements

Federal Communications Commission 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 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.

3ware, Inc.   Model: DiskSwitch 4D

FC Tested to Comply
With FCC Standards

FOR HOME OR OFFICE USE
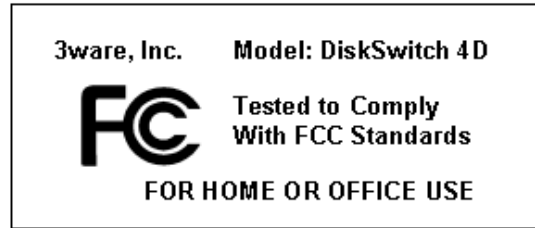
Microsoft Windows Hardware Quality Lab (WHQL)

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 StorSwitch Controller Card Model StorSwitch 4D is 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 **PCI** LOCAL BUS

.

Appendix B. Warranty, Technical Support and Service

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.

For detailed terms and conditions, please see the Limited Hardware Warranty and Software License Agreement at our website: http://www.3ware.com/support/rma_form.asp

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.

Obtaining Warranty Protection

To obtain warranty service during the warranty period call AMCC toll free at (800)-945-7273 or (408) 523-1145 (direct) as soon as you have identified a problem with your AMCC 3ware Serial ATA RAID Controller unit. 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 (800) 945-7273 and (408) 523-1145 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 by sending e-mail to 3wareSupport@amcc.com.

Index

update utility 141

V
verification 15
  about 122
  error handling 123
  media scans 122
  non-redundant units 122
  redundant units 123
verify unit, 3DM 61
verifying
  definition 183
verifying units 135
viewing 3DM remotely 36
ving 79
volumes
  in a unit 50
  resulting from auto-carvings 50

W
warnings, installation 162
Warranty 187
WHQL 186
working in 3BM 23
write cache 16, 54
  disabling on degrade in 3BM 79
  enabling 95
  enabling in 3BM 96
  enabling in 3DM 95

3ware 9000 Series Serial ATA RAID Controller User Guide