



3ware®

Serial ATA RAID Controller

PN 720-0161-00
March 2007

User Guide for Mac® OS X

Copyright

©2004-2007 Applied Micro Circuits Corporation (AMCC). All rights reserved. This publication may be copied or reproduced for reference purposes only. All other purposes require the express written consent of AMCC, 215 Moffett Park Drive, Sunnyvale, CA 94089. AMCC shall not be responsible or liable for, and shall be held harmless against, any and all damages, claims, and/or disputes that arise from the copying or reproduction of this publication.

Trademarks

3ware®, Escalade®, 3DM®, and TwinStor® are all registered trademarks of AMCC. The 3ware logo, 3BM, Multi-Lane, StorSave, StorSwitch, StreamFusion, and R5 Fusion are all trademarks of AMCC. Apple®, the Apple logo, and PowerMac® are trademarks of Apple Computer Inc., registered in the United States and/or other countries. Safari is a trademark of Apple Computer, Inc. PowerPC and the PowerPC logo are trademarks of International Business Machines Corporation. Linux® is a registered trademark of Linus Torvalds in the United States, other countries, or both. Windows® is a registered trademark of Microsoft Corporation in the United States and other countries. Firefox® is a registered trademark of the Mozilla Foundation. PCI Express® is a registered trademark of PCI-SIG®. All other trademarks herein are property of their respective owners.

Disclaimer

While every attempt is made to make this document as accurate as possible, AMCC assumes no responsibility for errors or omissions in this document, nor does AMCC make any commitment to update the information contained herein.

Table of Contents

About this User Guide	vi
How this User Guide is Organized	vi
Conventions	vii
Screenshots	viii
Using the 3ware HTML Bookshelf	viii
Chapter 1. Getting Started with Your 3ware RAID Controller	1
Chapter 2. Introducing the 3ware® SATA RAID Controller	4
System Requirements	5
Understanding RAID Concepts and Levels	6
RAID Concepts	6
Available RAID Configurations	7
Determining What RAID Level to Use	10
3ware Tools for Configuration and Management	11
Monitoring, Maintenance, and Troubleshooting Features	12
Chapter 3. 3DM 2 (3ware Disk Manager) Introduction	14
Browser Requirements for 3DM	15
Starting 3DM and Logging In	15
Logging In to the 3DM Web Application	16
Starting and Stopping the 3DM Process Manually on the Macintosh	17
Viewing 3DM Remotely Using a Web Browser	18
Working with the 3DM Screens	19
3DM Menus	20
Viewing Information About Different Controllers	21
Refreshing the Screen	21
3DM Screens and What They're Used For	21
Setting Up 3DM Preferences	23
Setting and Changing 3DM Passwords	24
Managing E-mail Event Notification	24
Enabling and Disabling Remote Access	25
Setting the Incoming Port #	26
Setting the Frequency of Page Refreshes	26
Chapter 4. Configuring Your Controller	27
Viewing Information About a Controller	27
About Controller Policies	29
Viewing Controller Policies	29
Setting the Auto Rebuild Policy	30
Using Auto-Carving for Multi LUN Support	31
Setting the Size of Volumes Created with Auto-Carving	32

Chapter 5. Configuring Units	33
Configuring a New Unit	33
Configuration Options When Creating a Unit	33
Creating a Unit	35
Initializing (Formatting) and Partitioning Units	37
Creating a Hot Spare	40
Naming a Unit	41
Setting Unit Policies	42
Enabling and Disabling the Unit Write Cache	43
Setting Auto Verify for a Unit	44
Setting Continue on Source Error During Rebuild	45
Enabling and Disabling Queuing for a Unit	46
Setting the StorSave Profile for a Unit	46
Changing An Existing Configuration by Migrating	48
RAID Level Migration (RLM) Overview	49
Changing RAID Level	50
Expanding Unit Capacity	51
Informing the Operating System of Changed Configuration	52
Deleting a Unit	53
Removing a Unit	55
Moving a Unit from One Controller to Another	56
Adding a Drive	56
Removing a Drive	57
Rescanning the Controller	58
Chapter 6. Maintaining Units	60
Checking Unit and Drive Status	60
Enclosure LED Status Indicators	63
Unit Statuses	63
Drive Statuses	64
About Degraded Units	65
About Inoperable Units	65
Alarms, Errors, and Other Events	66
Viewing Alarms, Errors, and Other Events	66
Downloading an Error Log	67
Viewing SMART Data About a Drive	67
Background Tasks	68
About Initialization	69
About Verification	70
Starting a Verify Manually	73
Rebuilding Units	73
Cancelling a Rebuild and Restarting It with a Different Drive	75
Setting Background Task Rate	75
Background Task Prioritization	76
Scheduling Background Tasks	76
Viewing Current Task Schedules	77
Turning On or Off Use of a Task Schedule	78
Removing a Task Schedule	79
Adding a New Task Schedule Slot	79
Selecting Self-tests to be Performed	80
Locating a Drive by Blinking Its LED	81

Chapter 7. Maintaining Your Controller	83
Determining the Current Version of Your 3ware Driver	83
Updating the Firmware and Driver	84
Updating the Firmware Through 3DM 2	85
Viewing Battery Information	85
Testing Battery Capacity	86
Chapter 8. 3DM 2 Reference	88
Controller Summary page	89
Controller Details page	90
Unit Information page	91
Unit Details page	92
Drive Information page	93
Drive Details window	95
Controller Settings page	96
Scheduling page	100
Maintenance page	102
Alarms page	109
Battery Backup page	110
Enclosure Summary page	112
Enclosure Details page	113
3DM 2 Settings page	114
Chapter 9. Troubleshooting	117
Web Resources	117
Before Contacting Customer Support	118
Basic Troubleshooting: Check This First	118
Command Logging	119
Enclosure-Related Problems	119
Error and Notification Messages	119
Error and Notification Message Details	123
Appendices	158
Appendix A. Glossary	159
Appendix B. Driver and Software Installation	165
Uninstalling 3DM on the Macintosh	172
Appendix C. Compliance and Conformity Statements	173
FCC Radio Frequency Interference Statement	173
European Community Conformity Statement	174
Appendix D. Warranty, Technical Support, and Service	175
Limited Warranty	175
Warranty Service and RMA Process	176
AMCC Technical Support and Services	177
Sales and ordering information	177
Feedback on this manual	177
Index	178

About this User Guide

This document, *3ware Serial ATA RAID Controller User Guide for Mac OS X*, provides instructions for configuring and maintaining RAID units on 3ware 9650SE and 9590SE controllers used with Mac OS X systems.

This guide assumes that you have already installed your controller in your system and connected it to your 3ware® Sidecar external enclosure. If you have not yet done so, see the installation guide that came with your controller. If you do not have the printed copy, a PDF of the installation guide is available on your 3ware CD, or you can download it from: <http://www.3ware.com/support/userdocs.asp>. (Note that there are different installation guides for different 3ware RAID controller models. The 9650SE-4LPME is part of the 3ware Sidecar Kit.)

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 3ware Disk Manager 2, referred to as 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: *3ware Serial ATA RAID Controller CLI Guide*. Information from both this Users Guide and the CLI Guide are also available in the *3ware HTML Bookshelf*, available in the 3ware Documentation folder and on your 3ware CD. (For more information, see "Using the 3ware HTML Bookshelf" on page viii.)

How this User Guide is Organized

Table 1: Chapters and Appendices in this User Guide

Chapter/Appendix	Description
1. Getting Started with Your 3ware RAID Controller	Provides a summary of the process you should follow to get started using your 3ware RAID controller.
2. Introducing the 3ware SATA RAID Controller	Provides an overview of 3ware 9650SE and 9590SE RAID controller features. Includes system requirements and an introduction to RAID concepts and levels.

Table 1: Chapters and Appendices in this User Guide

Chapter/Appendix	Description
3. 3ware Disk Manager (3DM 2) Introduction	Describes the basics of using 3DM. Also includes information about installing and uninstalling 3DM, and how to start the 3DM process manually, if required.
4. Configuring Your Controller	Describes how to view details about the controller, check its status, and change configuration settings that affect the controller and all associated drives.
5. Configuring Units	Describes how to configure new units and spares, change existing configurations, and set unit policies.
6. 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.
7. 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.
8. 3DM 2 Reference	Describes the features and functions on each of the pages in 3DM.
9. Troubleshooting	Provides common problems and solutions, and explains error messages.
A. Glossary	Includes definitions for terms used throughout this guide.
B. Driver and Disk Management Tool Installation	Describes how to install the driver for the 3ware controller and other 3ware software tools.
C. Compliance and Conformity Statements	Provides compliance and conformity statement.
D. Warranty, Technical Support, and Service	Provides warranty information and tells you how to contact technical support.

Conventions

The following conventions are used through this guide:

- 3DM and 3DM 2 both refer to the 3ware Disk Manager, version 2.
- In the sections that describe using 3DM, *current controller* is used to refer to the controller which is currently selected in 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.

Screenshots

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

Using the 3ware HTML Bookshelf

The 3ware HTML Bookshelf is an HTML version of this user guide and the CLI Guide, combined as one resource. It is available on your 3ware CD, in the /doc folder.

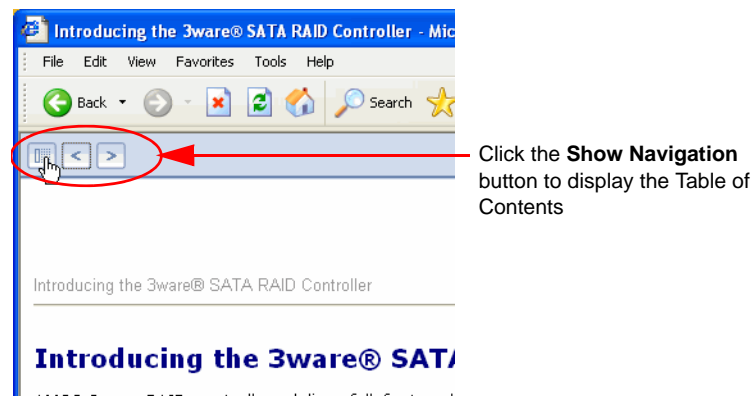
To make use of the 3ware HTML Bookshelf

- 1 Copy the compressed version of the guide (3wareHTMLBookshelf.zip or 3wareHTMLBookshelf.tgz, depending on your operating system) to a local drive on your computer and extract it.
- 2 To launch the bookshelf at the opening page, open the 3wareHTMLBookshelf folder and double click the file index.html.

Opening the file from “index.html” automatically displays a navigation panel at the left that includes a Table of Contents, Index, and Search.

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

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



Getting Started with Your 3ware RAID Controller

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

- Physically Install the RAID Controller and Drives
- Install the 3ware Driver and Disk Management Software
- Configure a RAID Unit
- Set Up Management and Maintenance Features

Tip: When you are first setting up your system, you may want to review “System Requirements” on page 5.

Physically Install the RAID Controller and Drives

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

For drive installation, see the instructions that came with your 3ware Sidecar or other external enclosure. If you are installing drives in a computer case, follow the manufacturer’s instructions.

Install the 3ware Driver and Disk Management Software

Instructions for installing the drivers and software are in the *3ware Sidecar Kit with the 9650SE-4LPME: Installation Guide* and in Appendix B, “Driver and Software Installation”

Configure a RAID Unit

If you would like more information about what RAID level to choose for your situation, review the information under “Understanding RAID Concepts and Levels” on page 6. Then turn to “Configuring a New Unit” on page 33.

Set Up Management and Maintenance Features

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

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

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

- “Configuring Your Controller” on page 27
- “Setting Unit Policies” on page 42
- “Setting Background Task Rate” on page 75

Initial Settings for Policies and Background Tasks

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

Table 2: Default Settings for Policies and Background Tasks

Policy	Default Value	Where to Change
Controller-Level Settings (For details, see “Configuring Your Controller” on page 27)		
Auto-Rebuild	Enabled	3DM, CLI
Auto-Carving	Disabled	3DM, CLI
Auto-Detect	Enabled	CLI
Carve Size or Factor	2048 GB	3DM, CLI
Unit-Level Settings (For details, see “Setting Unit Policies” on page 42)		
Auto Verify	Disabled	3DM, CLI
Continue on Source Error During Rebuild	Disabled	3DM, CLI

Table 2: Default Settings for Policies and Background Tasks

Policy	Default Value	Where to Change
Queuing (NCQ)	Enabled	3DM, CLI
StorSave Profile	Protection	3DM, CLI
Write Cache	Enabled	3DM, CLI

Background Task Settings
(For details, see “Scheduling Background Tasks” on page 76 and “Setting Background Task Rate” on page 75)

Verify Task Schedules	Daily, starting at 12:00 am and running for 24 hours	3DM, CLI
Follow Verify Task Schedule	No	3DM, CLI
Rebuild Task Schedules	Daily, starting at 12:00 am and running for 24 hours	3DM, CLI
Follow Rebuild Task Schedule	No	3DM, CLI
Self-test Task Schedules ^a	Daily, starting at 12:00 am and running for 24 hours	3DM, CLI
Follow Self-test Task Schedule	Yes	3DM, CLI

- a. Although the default Self-test Task Schedule is for 24 hours, self-test tasks are run only at the beginning of that time period and take just a few minutes. For more information about task schedules, see “Scheduling Background Tasks” on page 76.

2

Introducing the 3ware[®] SATA RAID Controller

Two 3ware SATA RAID controllers are available for use with Mac OS X: the 9650SE-4LPME and the 9590SE-4ME. Both of these controllers are 4-lane (x4) PCI Express[®] cards and can be installed in any of the available x4 or x8 PCI Express slots on your Mac Pro or Power Mac[®] G5. (The x16 slot is normally reserved for your graphics card.)

These 3ware RAID controllers feature:

- Support for up to 4 SATA drives.
- AMCC's remote management software, 3ware Disk Manager 2 (3DM[®]2) which simplifies storage configuration and management through a web browser.
- An enhanced firmware platform that allows future upgrades.
- Advanced RAID features for greater data protection and management.
- PCI Express connectivity
- Transfer rate of up to 2.5Gbps per lane
- 7th generation StorSwitch(TM) technology
- Support for 3Gbps and Native Command Queuing (NCQ)
- StorSave profiles that let you set the desired level of protection versus performance for a unit
- Drive Locate which allows you to easily identify a drive in the 3ware Sidecar enclosure by blinking the LED associated with it
- The ability to define a carving size to be used when carving units into volumes.



Note: The 9650SE-4LPME and 9590SE-4ME are each part of a 3ware Sidecar Kit, which includes the 3ware Sidecar Enclosure. Information about setting up the 3ware Sidecar itself is included in the installation guide that comes with the 3ware Sidecar Kit. Make sure you get the appropriate RAID controller model for the type of Mac you own (Mac Pro or Power Mac G5).

System Requirements

Drive Requirements

Drives must be 3.5" and meet SATA-1 or SATA-2 standards.

A list of drives that have been tested is available at http://www.3ware.com/products/compatibility_sata2.asp

Operating System and Computer Requirements

Mac OS 10.4.6 or later, running on a Mac Pro or a Power Mac G5 (PowerPC-based) with PCI Express.

Other Requirements

- 3DM 2 (3ware Disk Manager) displays information in a browser. It requires one of the following browsers:
 - Safari™ 2.0.4 or newer
 - Firefox® 1.5.0.4 or newer

In addition:

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



Note: When using the 3ware HTML Bookshelf, if you use the Safari browser, the Back button does not step you back through pages accessed in the bookshelf. You can use the navigation features built into the bookshelf, however, including the Previous/Next arrows at the top of each page, the breadcrumbs, and the Contents/Index/Search pane at the left.

Tip: The Back button does work correctly when viewing the 3ware HTML Bookshelf in Firefox.

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

Understanding RAID Concepts and Levels

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

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

- “RAID Concepts” on page 6
- “Available RAID Configurations” on page 7
- “Determining What RAID Level to Use” on page 10

RAID Concepts

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

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

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

Available RAID Configurations

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

For how to configure RAID units, see “Configuring a New Unit” on page 33.

RAID 0

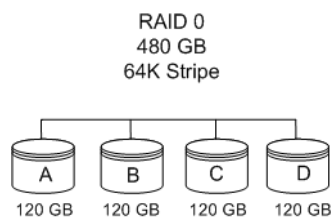
RAID 0 provides improved performance, but no fault tolerance. Since the data is striped across more than one disk, RAID 0 disk arrays achieve high transfer rates because they can read and write data on more than one drive simultaneously. The stripe size is configurable during unit creation. RAID 0 requires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

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

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

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

Figure 2. RAID 0 Configuration Example



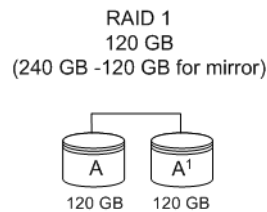
RAID 1

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

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

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

Figure 3. RAID 1 Configuration Example



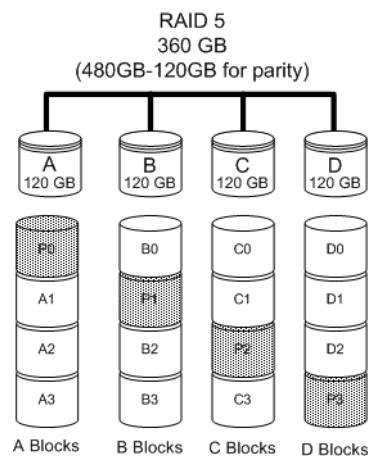
RAID 5

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

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

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

Figure 4. RAID 5 Configuration Example



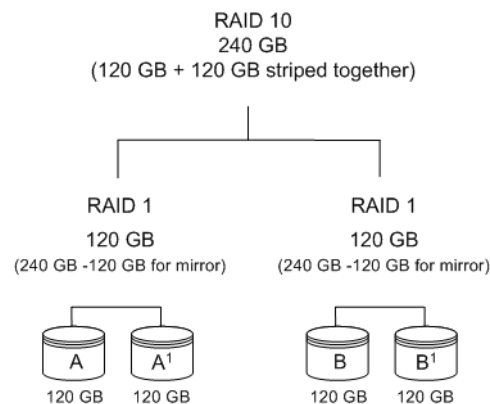
RAID 10

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

When drives are configured as a striped mirrored array, the disks are configured using both RAID 0 and RAID 1 techniques, thus the name RAID 10 (see Figure 5). A minimum of four drives are required to use this technique. The first two drives are mirrored as a fault tolerant array using RAID 1. The third and fourth drives are mirrored as a second fault tolerant array using RAID 1. The two mirrored arrays are then grouped as a striped RAID 0 array using a two tier structure. Higher data transfer rates are achieved by leveraging TwinStor and striping the arrays.

In addition, RAID 10 arrays offer a higher degree of fault tolerance than RAID 1 and RAID 5, since the array can sustain multiple drive failures without data loss. Please note that if both halves of a mirrored pair in the RAID 10 array fail, then all of the data will be lost.

Figure 5. RAID 10 Configuration Example



Single Disk

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

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

Hot Spare

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

Determining What RAID Level to Use

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

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

Table 3: RAID Configuration Types

RAID Type	Description
RAID 0	Provides performance, but no fault tolerance.
RAID 1	Provides fault tolerance and a read speed advantage over non-RAID disks.
RAID 5	This type of unit provides performance, fault tolerance, and high storage efficiency. RAID 5 units can tolerate one drive failing before losing data.
RAID 10	A combination of striped and mirrored units for fault tolerance and high performance.
Single Disk	Not a RAID type, but supported as a configuration. Provides for maximum disk capacity with no redundancy.

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

Using Drive Capacity Efficiently

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

The total unit capacity is defined as follows:

Table 4: Drive Capacity

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

Through drive coercion, the capacity used for each drive is rounded down so that drives from differing manufacturers are more likely to be able to be used as spares for each other. The capacity used for each drive is rounded down to the nearest GB for drives under 45 GB (45,000,000,000 bytes), and rounded down to the nearest 5 GB for drives over 45 GB. For example, a 44.3 GB drive will be rounded down to 44 GB, and a 123 GB drive will be rounded down to 120 GB. For more information, see the discussion of drive coercion under “Creating a Hot Spare” on page 40.

3ware Tools for Configuration and Management

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

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

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

3DM runs in the background on the controller’s host system, and can be accessed through a web browser to provide ongoing monitoring and administration of the controller and associated drives. It can be used locally or remotely.

For details about working with 3DM, see “3DM 2 (3ware Disk Manager) Introduction” on page 14.

Using 3DM to manage your 3ware RAID controller is discussed throughout this manual.

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

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

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

The 3ware CLI is described in *3ware Serial ATA RAID Controller CLI Guide* and in the *3ware HTML Bookshelf*.

Monitoring, Maintenance, and Troubleshooting Features

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

- **SMART Monitoring** (Self-Monitoring, Analysis and Reporting Technology) automatically checks a disk drive's health every 24 hours and reports potential problems. This allows you to take proactive steps to prevent impending disk crashes. SMART data is checked on all disk drives (array members, single disks, and hot spares). Monitoring of SMART thresholds can be turned on and off in 3DM. (For details, see “Viewing SMART Data About a Drive” on page 67.)
- **Verification.** The verify task verifies all redundant units, and checks for media errors on single disks, spares, and RAID 0 unit members. If the disk drive is part of a redundant unit, error locations that are found and are deemed repairable are rewritten with the redundant data. This forces the drive firmware to reallocate the error sectors accordingly. (For more information, see “About Verification” on page 70.)
- **Error Correction.** Bad sectors can be dynamically repaired through error correction (Dynamic Sector Repair). Reallocation of blocks is based intelligently on the location of the block in relation to the stripe.
- **Scheduled Background Tasks.** Initialize, rebuild, verify, and self-test tasks can all be run in the background, at scheduled times. This lets you choose a time for these tasks to be run when it will be least disruptive to your system. You can also define the rate at which background tasks are performed, specifying whether I/O tasks should be given more processing time, or background rebuild and verify tasks should be given more processing time. (For more information, see “Scheduling Background Tasks” on page 76.)
- **Write Cache.** Write cache can be enabled or disabled using 3DM 2 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 occurs. With a Battery Backup Unit (BBU) installed, the cache stored on the 3ware controller can be restored. A UPS (uninterruptable power supply) is recommended when using write cache. (For more information, see “Enabling and Disabling the Unit Write Cache” on page 43.)

- **StorSave™ Profiles** allow you to set the level of protection versus performance that is desired for a unit when write cache is enabled. (For more information, see “Setting the StorSave Profile for a Unit” on page 46.)
- **Drive and Unit Identification.** Units or drives in enclosures can be identified by flashing LEDs. When the I²C port on the controller has been connected to a chassis with a Chassis Control Unit (CCU), such as the 3ware Sidecar, you can issue drive Locate commands that blink the LEDs for particular drives, so that you can quickly identify which drive needs to be checked or replaced. For more information, see “Locating a Drive by Blinking Its LED” on page 81.
- **Auto Rebuild.** For times when you do not have a spare available, setting the Auto Rebuild policy allows rebuilds to occur with an available drive or with a failed drive. (For more information, see “Setting the Auto Rebuild Policy” on page 30.)

3

3DM 2 (3ware Disk Manager) Introduction



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

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

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

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

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

- Browser Requirements for 3DM
- 3DM 2 can be installed from the 3ware CD that came with your 3ware RAID controller. You can also download the current version from the website at <http://www.3ware.com/support/download.asp>. Details about the installation are described in “Driver and Software Installation” on page 165.
- Starting 3DM and Logging In
- Working with the 3DM Screens
- Setting Up 3DM Preferences

For details about the settings and fields on each of the 3DM 2 screens, see “3DM 2 Reference” on page 88.

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

Browser Requirements for 3DM

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

- Safari 2.0.4 or newer
- Firefox 1.5.0.4 or newer

Additional requirements:

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



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

3DM 2 can be installed from the 3ware CD that came with your 3ware RAID controller. You can also download the current version from the website at <http://www.3ware.com/support/download.asp>. Details about the installation are described in “Driver and Software Installation” on page 165.

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

Starting 3DM and Logging In

Normally after installation, the 3DM process starts automatically when you start your system.

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

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

If the 3DM process does not start automatically, you can start it manually, as described under “Starting and Stopping the 3DM Process Manually on the Macintosh” on page 17. You will know if the process is not running, because

when you try to use the 3DM web application, you will get a page not found error.

If you want to check the status of a controller from a different computer, see “Viewing 3DM Remotely Using a Web Browser” on page 18.

Logging In to the 3DM Web Application

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

Two levels of access are provided:

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



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

To log in to the 3DM web application

- 1 You can start the 3DM 2 web application in one of the following ways:
 - In the Finder, choose **Applications > AMCC**, and then double-click **Connect to 3DM2.webarchive**.

Your browser will open and go to the URL for 3DM 2.

OR

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

The default URL is `http://localhost:888/`

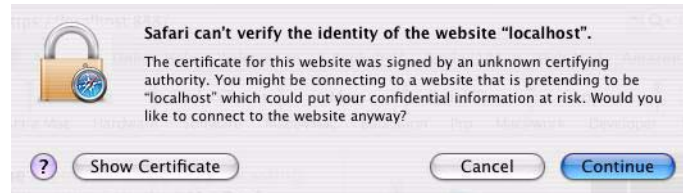
You can also replace “localhost” with the IP address of the computer that contains the 3ware controller. For example:

`http://<IP address>:888/`



Note: If you receive a page not found message, make sure you entered the URL correctly. If you did, 3DM may not be running in the background. You can start it manually, as described under “Starting 3DM on the Macintosh” on page 75.

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

Figure 6. Security Certificate Message from Browser

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

- 3 When the 3DM logon screen appears, select whether you are a **User** or **Administrator**.
- 4 Enter your password and click **Login**.

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



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

Starting and Stopping the 3DM Process Manually on the Macintosh

The 3DM process should start automatically after it has been installed. If it does not, you can start it manually.

To see if the 3DM process is already running

- Open a Terminal window and type:

```
ps -ax | grep 3dm2 | grep -v grep
```

If 3DM is running, you will see it included on the output line that displays.

To stop the 3DM process so you can restart it

- 1 In a Terminal window, type:

```
sudo killall 3dm2
```

- 2 When prompted for it, enter your administrator password.
- 3 Wait for a minute or so before verifying that the process has been terminated. (It can take a couple of minutes for the process to be stopped.)

- 4 Verify that the process has been terminated by typing

```
ps -ax | grep 3dm2 | grep -v grep
```

The output line should not include 3DM.
- 5 If the process is still running, contact AMCC/3ware Technical Support for assistance.

To start the 3DM process manually

- 1 Open a Terminal window and type:

```
sudo /usr/sbin/3dm2
```
- 2 Enter your administrator password, when prompted for it.
The 3DM process starts.
- 3 Open your browser and enter the URL for your system.
The default URL is `http://localhost:888/`
You can also replace “localhost” with the IP address of the computer that contains the 3ware controller. For example: `http://<IP address>:888/`

Viewing 3DM Remotely Using a Web Browser

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

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

To connect to 3DM2 through your web browser

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

If you do not know the URL or IP for the system, you can contact your network administrator, or open a Terminal window and type `ifconfig`.

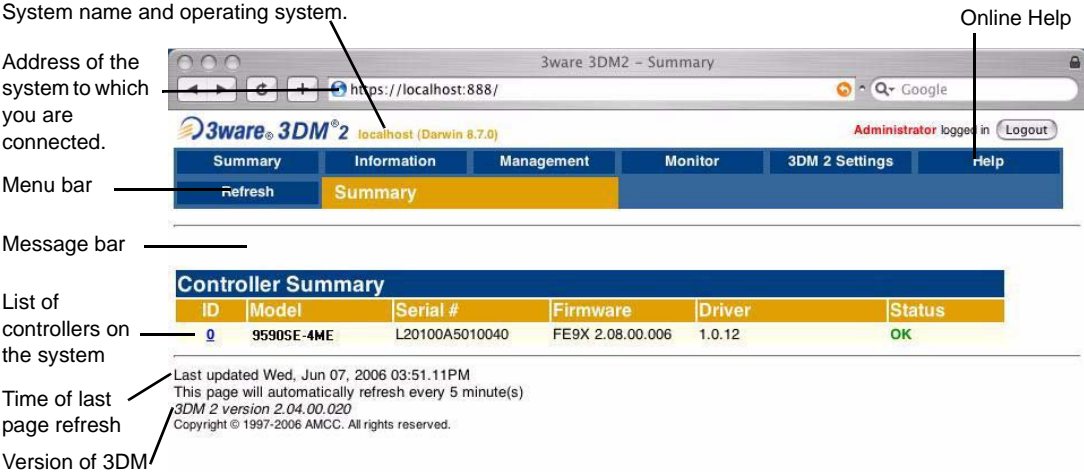


Note: When using 3DM to access a remote system, the time on the local system must match the time on the file server. If the time varies by more than 30 minutes, it will not be possible to remotely monitor the system (you will not be able to log in). If you are in a different time zone, you must first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

Working with the 3DM Screens

3DM's features are organized on a series of pages you view in your browser. After you log in to 3DM, the Summary page shows a list of controllers installed in the computer at the URL you specified.

Figure 7. 3DM Main Screen



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

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

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

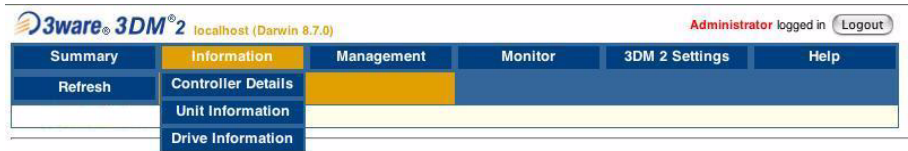


Tip: If you have a question about something you see on the screen, just click the Help button in the menu bar.

3DM Menus

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

Figure 8. 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 policies such as enabling of unit write cache, and controller settings that affect all units managed by the controller), tasks that can be scheduled (rebuild, verify, and self-test), and maintenance of individual units. Unit configuration can also be done through the **Management > Maintenance** page.

The **Monitor menu** gives you access to the Alarms page, the BBU page, and the Enclosure Summary page. The **Alarms** page shows a list of alarms, including the specific alarm message, and the exact date and time it occurred. The **BBU** page shows the status of a Battery Backup Unit (BBU), if one is installed, and allows you to test the battery. (BBU is not supported on the 9590SE-4ME.) The **Enclosure Summary** page provides lists the enclosures connected to the controller and lets you drill down for more detailed status information about each.

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

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

Viewing Information About Different Controllers

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

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

Figure 9. 3DM Controller Selection Drop-down



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

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 26.



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

3DM Screens and What They're Used For

The table below shows a list of the pages you work with in 3DM and describes what they are used for. Details about each page and the fields and features on it are provided in Chapter 8, “3DM 2 Reference”. The page names in the table provide links to details about that page.

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

Table 5: List of 3DM Pages

3DM Page	Description
Controller Summary page	<p>Provides basic information about each 3ware RAID controller in your system.</p> <p>To see this page, click Summary in the menu bar.</p>
Controller Details page	<p>Provides detailed information about the current controller.</p> <p>To see this page, choose Information > Controller Details from the menu bar.</p>
Unit Information page	<p>Shows a list of the units on the current controller and provides summary information about each unit.</p> <p>To see this page, choose Information > Unit Information from the menu bar or click an ID number on the Controller Summary.</p>
Unit Details page	<p>Shows details about a particular unit.</p> <p>To see this page, click an ID number on the Unit Information page.</p>
Drive Information page	<p>Shows a list of drives on the current controller and provides summary information about each drive.</p> <p>To see this page, choose Information > Drive Information from the menu bar.</p>
Drive Details window	<p>Shows the SMART data for a specific drive, and shows additional detail information for the drive.</p> <p>To see this page, click the Port # for a drive on the Drive Information page.</p>
Controller Settings page	<p>Lets you view settings that affect the units on the current controller and change some of those settings.</p> <p>Controller-level settings that can be changed include background task rate, Auto Rebuild, Auto-Carving, and Carve Size. Some additional policies are shown that can only be changed in the CLI.</p> <p>Unit-level settings include specifying the StorSave Profile and enabling or disabling the Write Cache, Auto-Verify, Continue on Error During Rebuild, and Queuing.</p> <p>To see this page, choose Management > Controller Settings from the menu bar.</p>
Scheduling page	<p>Lets you view and change the schedule for tasks that affect all units on the current controller.</p> <p>To see this page, choose Management > Scheduling from the menu bar.</p>

Table 5: List of 3DM Pages

3DM Page	Description
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. (BBUs are not supported on the 9590SE-4ME.)
Enclosure Summary page	Lists the enclosures attached to your 3ware controller. To view this page, choose Monitor > Enclosure Support on the menu bar.
Enclosure Details page	Shows details about a particular enclosure, including status information. You can also use this page to blink the LED for a particular drive. To view this page, click the ID number of the Enclosure on the Enclosure Summary page.
3DM 2 Settings page	Lets you set preferences, including email notification for alarms, passwords, page refresh frequency, whether remote access is permitted, and the incoming port which 3DM will use for listening. To view this page, click 3DM 2 Settings on the menu bar.

Setting Up 3DM Preferences

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

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

- Setting and Changing 3DM Passwords
- Managing E-mail Event Notification
- Enabling and Disabling Remote Access
- Setting the 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.

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

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

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

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

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

To set up event notification

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

To send a test message

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

- Click **Send Test Message**.

Enabling and Disabling Remote Access

When remote access is enabled, a user can connect to 3DM over the internet or an intranet, to check status or administer the controller and associated drives. (See “Viewing 3DM Remotely Using a Web Browser” on page 18.)

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 is important to refresh the page information regularly. That way you can be assured that the information you see in 3DM is current.

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

To set the frequency of page refreshes

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



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

Configuring Your Controller

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

- Viewing Information About a Controller
- Viewing Controller Policies
- Setting the Auto Rebuild Policy
- Using Auto-Carving for Multi LUN Support
- Setting the Size of Volumes Created with Auto-Carving



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 75.

Viewing Information About a Controller

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

If you have more than one controller in your system, you can easily view information about each one using 3DM. For example, if you have two 3ware Sidecars attached to your Mac Pro or Power Mac G5, you will have a different 3ware controller for each one.

To see details about a controller in 3DM

- 1 Start 3DM and log in as an administrator.

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.

Figure 10. Controller Summary Page

ID	Model	Serial #	Firmware	Driver	Status
0	9590SE-4ME	L20100A5010040	FE9X 2.08.00.006	1.0.12	OK
1	9590SE-4ME	L20100A5010045	FE9X 2.08.00.006	1.0.12	OK



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

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

Figure 11. Controller Details Page

Model	9590SE-4ME
Serial #	L20100A5010040
Firmware	FE9X 2.08.00.006
Driver	1.0.12
BIOS	BE9X 2.03.01.052
Boot Loader	BL9X 2.02.00.001
Memory Installed	224 MB
Bus Type	PCIe
Bus Width	4 lanes
Bus Speed	2.5 GHz
# of Ports	4
# of Drives	4
# of Units	1
Error Log	Download Error Log

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

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

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



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

About Controller Policies

The following policies affect all units and drives on a controller and can be adjusted as appropriate for your equipment. Controller policies are shown at the bottom of the Controller Settings page in 3DM (Figure 12).

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

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

- **Carve Size.** Sets the size for dividing up units into volumes when Auto-Carving is enabled. This setting can be between 1024 GB and 2048 GB.

Some additional policies can be set at the unit level. For more information, see “Setting Unit Policies” on page 42.

Viewing Controller Policies

You can view the current state of controller policies in 3DM, in the **Other Controller Settings** section at the bottom of the Controller Settings page (see Figure 12). Only the Auto Rebuild, Auto-Carving, and Carve Size policies can be changed on this page. The other policies do not apply to the Macintosh. For a summary of the initial default settings, see Table 2, “Default Settings for Policies and Background Tasks,” on page 2.

To view controller policies in 3DM

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

Figure 12. 3DM Controller Settings Page

The screenshot displays the 3DM Controller Settings page. At the top, there is a navigation bar with tabs for Summary, Information, Management, Monitor, 3DM 2 Settings, and Help. The 'Controller Settings' tab is selected. Below the navigation bar, there are several sections for configuring the controller (Controller ID 0):

- Background Task Rate (Controller ID 0):** Includes 'Rebuild/Migrate Rate' and 'Verify Rate', both set to 'Faster' with radio buttons for 'Faster I/O'.
- Unit Policies (Controller ID 0):** Includes 'Write Cache', 'Auto Verify' (checked), 'Continue on Source Error during Rebuild', 'Queuing' (checked), and 'StorSave' (Performance).
- Unit Names (Controller ID 0):** Includes 'Unit 0 [RAID 1]' with a text field containing 'PrimaryMirror' and buttons for 'Save Names' and 'Reset Names'.
- Other Controller Settings (Controller ID 0):** Includes 'Auto Rebuild' (Enabled), 'Auto-Carving' (Enabled), 'Carve Size' (1024), 'Number of Drives per Spin-up' (1), 'Delay between Spin-up' (2 second(s)), and 'Export Unconfigured Disk' (No).
- Update Firmware:** Includes an 'Image File' field with a 'Browse...' button and a 'Begin Update' button.

Setting the Auto Rebuild Policy

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

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

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

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

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

To enable Auto Rebuild through 3DM

- 1 Choose **Management > Controller Settings** from the menu bar in 3DM.
- 2 In the Other Controller Settings section at the bottom of the screen, select the **Enabled** option for **Auto Rebuild**.

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

Using Auto-Carving for Multi LUN Support

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

For example, using the default carve size of 2 TB, if the unit is 2.5 TB then it will contain two volumes, with the first volume containing 2TB and the second volume containing 0.5 TB. If the unit is 5.0 TB then it will contain 3 volumes, with the first two volumes containing 2 TB each and the last volume containing 1 TB.

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

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



Note: Using auto-carving can have an impact on performance.

32-bit and 64-bit You must turn on the Auto-Carving policy before creating the unit. Units created with this policy turned off will not be affected by a change to the policy. If the policy is turned off later, units that have been carved into volumes will retain their individual volumes; existing data is not affected.

To use auto-carving

- 1 Enable the auto-carving feature.
In 3DM, enable Auto-Carving at the bottom of the **Management > Controller Settings** page.
- 2 Create a new unit or migrate an existing unit to include the drives you want to use.
If the combined capacity of the drives exceeds the carve size, a number of volumes will be created.
- 3 Verify the creation of the volumes.
In 3DM 2, the number of volumes is shown on the Unit Details page.
- 4 Verify that the volumes appear in the operating system. They will appear as additional drives.



Notes:

- When volumes have been created through auto-carving, they cannot be deleted except by deleting the unit.
- Changing the auto-carve policy does not affect existing units.

Setting the Size of Volumes Created with Auto-Carving

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

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

To set the carve size in 3DM

- 1 Choose **Management > Controller Settings** from the menu bar in 3DM.
- 2 In the Other Controller Settings section at the bottom of the screen, in the **Carve Size** field, enter the size you want (between 1024 GB and 2048 GB) to use and click **Submit**.

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

Configuring Units

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

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

Configuring a New Unit

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

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

Configuration Options When Creating a Unit

This section provides an overview of the choices you have when configuring a new unit. For step-by-step instructions, see “Creating a Unit” on page 35.

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

- Drives to be included in the unit
- Type of configuration (RAID Level)

- Name of the unit (optional)
- Stripe size, if appropriate for the RAID level
- Unit policies that affect how the unit will be handled

You can make some types of changes to the RAID configuration later, and you can change the unit name and the unit policies. For details, see “Changing An Existing Configuration by Migrating” on page 48 and “Setting Unit Policies” on page 42.

Drives to be included in the unit

You may include from one to four drives in the unit, depending on the number of drives available. (For information about how many drives to select for a given RAID level, see “Determining What RAID Level to Use” on page 10.)

Available drives are those that are not currently part of a unit. If you want to use drives that are currently part of a different unit, you must first delete that unit to make the drives available. (For details, see “Deleting a Unit” on page 53.) If drives are listed under “Incomplete Drives and Others,” they must be deleted before they can be used.

If you want to add drives to be used in the unit, see “Adding a Drive” on page 56.

Type of configuration (RAID Level)

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



Note: Creating a unit erases all data on all drives. Although creating a RAID 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.

Stripe size, if appropriate for the RAID level

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

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

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

Unit policies

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

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

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

For a summary of what these policies do, see the discussion under “Setting Unit Policies” on page 42. For how to adjust each one, see the procedures later in this chapter.

Creating a Unit

In 3DM, creating a unit starts from the **Management > Maintenance** page (Figure 13).

Figure 13. 3DM Maintenance Page

The screenshot shows the 3DM Maintenance Page interface. At the top, there is a navigation bar with tabs for Summary, Information, Management, Monitor, 3DM 2 Settings, and Help. The 'Maintenance' tab is active. Below the navigation bar, there is a 'Rescan Controller' button with a tooltip that says '(This will scan all ports for newly inserted drives/units)'. The main content area is titled 'Unit Maintenance (Controller ID 0)' and shows 'NO UNITS'. Below this, there are buttons for 'Verify Unit', 'Rebuild Unit', 'Migrate Unit', 'Remove Unit', and 'Delete Unit'. A note below these buttons states: '*Before removing or deleting a unit, make sure there is no I/O on the unit and unmount it'. The 'Available Drives (Controller ID 0)' section contains a table with four rows, each representing a port and its associated drive information.

Port	Model	Capacity	Status	Action
<input type="checkbox"/> Port 0	ST3500641NS	465.76 GB	OK	[Remove Drive]
<input type="checkbox"/> Port 1	ST3500641NS	465.76 GB	OK	[Remove Drive]
<input type="checkbox"/> Port 2	ST3500641NS	465.76 GB	OK	[Remove Drive]
<input type="checkbox"/> Port 3	ST3500641AS	465.76 GB	OK	[Remove Drive]

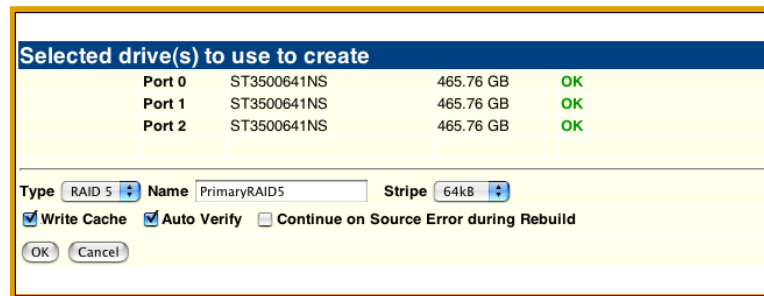
At the bottom of the 'Available Drives' section, there is a 'Select All Drives' link and a 'Create Unit' button.

To create a unit

- 1 In 3DM, choose **Management > Maintenance**.
- 2 In the Available Drives list, select the drives you want to include in the unit by marking the checkbox in front of the Port number for each one.
If you are creating single drive units (single disks or hot spares), you can configure multiple drives at once.
- 3 Click **Create Unit**.

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

Figure 14. Configuring a Unit in 3DM



- 4 In the **Type** field, select the RAID configuration you want.
- 5 If stripe size applies to the RAID type you select, select a **Stripe Size**. (Stripe size does not apply to RAID 1.)
- 6 Optional: In the **Name** box, enter a name for the unit (up to 21 characters, including dashes and underscores).
- 7 Make changes to the unit policies, as desired. You can enable or disable the **Write Cache**, **Auto Verify**, and **Continue on Source Error During Rebuild**. You can also set the **StorSave** policy.

For details about these settings, see “Setting Unit Policies” on page 42.

- 8 Click **OK**.

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

If you have auto-carving enabled and the size of your unit exceeds the carve size, you may see multiple unit volumes in your operating system. For details, see “Using Auto-Carving for Multi LUN Support” on page 31.

- 9 When the Mac OS displays a “Disk Insertion” message, go on to “Initializing (Formatting) and Partitioning Units”, below.

Initializing (Formatting) and Partitioning Units

After you create a unit, it needs to be formatted, partitioned, and mounted by the operating system before it can be used.



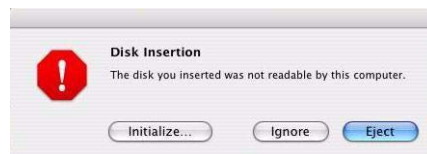
Note: “Initialization” of the unit by your operating system is different from “initialization” of a unit by 3ware. Initialization under your operating system will format your disk, erasing any existing data in the process. Initialization under 3ware does not erase data; it puts redundant data on the drives of redundant units into a known state so that data can be recovered in the event of a disk failure. For more information, see “About Initialization” in the *3ware Serial ATA RAID Controller User Guide for Mac OS X*.

When you create a unit through 3DM 2, the Mac OS X recognizes that a new disk is available, and displays a message asking what you want to do. (If this message does not appear, you can start the Disk Utility manually from the Finder and skip to step 2.)

To initialize and partition your unit

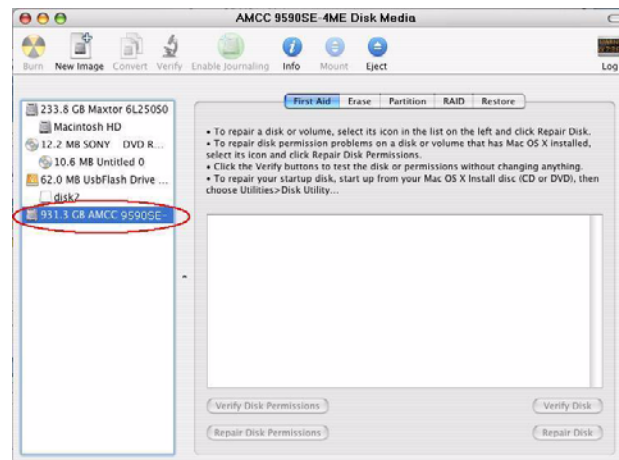
- 1 In the Mac OS message, click **Initialize**.

Figure 15. Disk Insertion Message from the Mac OS



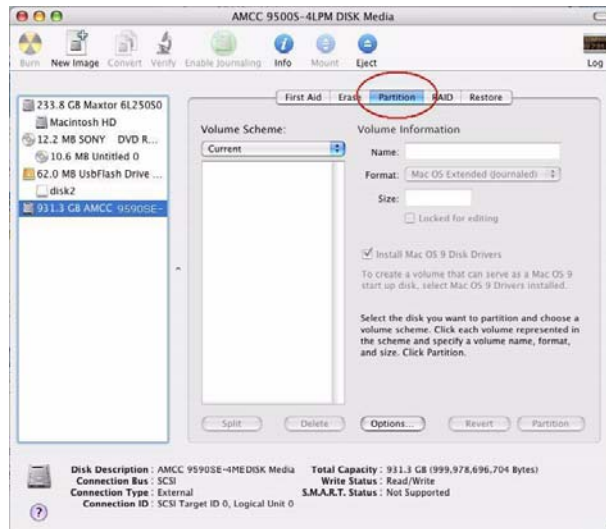
- 2 When the Macintosh Disk Utility window opens, find and select the drive that represents your RAID unit.

Figure 16. Macintosh Disk Utility Window with New RAID Unit



- 3 In the Disk Utility Window, select the **Partition** tab.

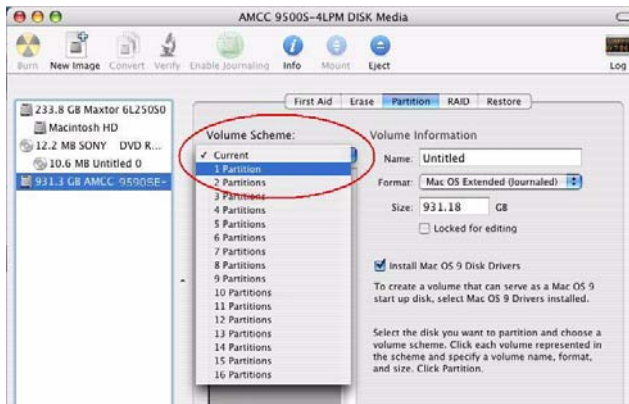
Figure 17. Macintosh Disk Utility Window, Partition Tab



- 4 In the Volume Scheme column, click **Current** to show the drop-down menu and select the number of partitions that you want your RAID unit to have.

Tip: If you only want one volume, select **1 Partition**. (Each partition will appear as a separate drive on your computer.)

Figure 18. Selecting the Number of Volumes in Disk Utility

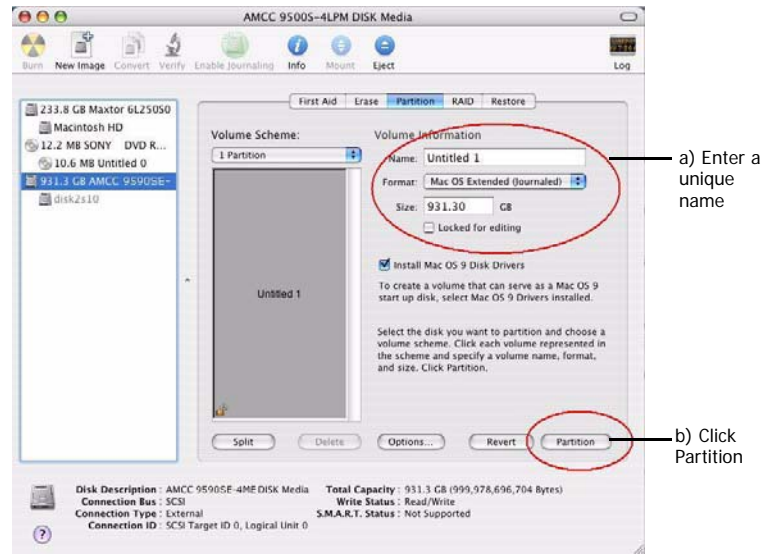


- 5 On the right, specify a volume name and then click **Partition**.

It is a good idea to use a unique name, although Mac OS X will allow you to give the same name to more than one partition.

If you have questions about what Format to select, see the Apple documentation.

Figure 19. Defining the Volume in the Macintosh Disk Utility



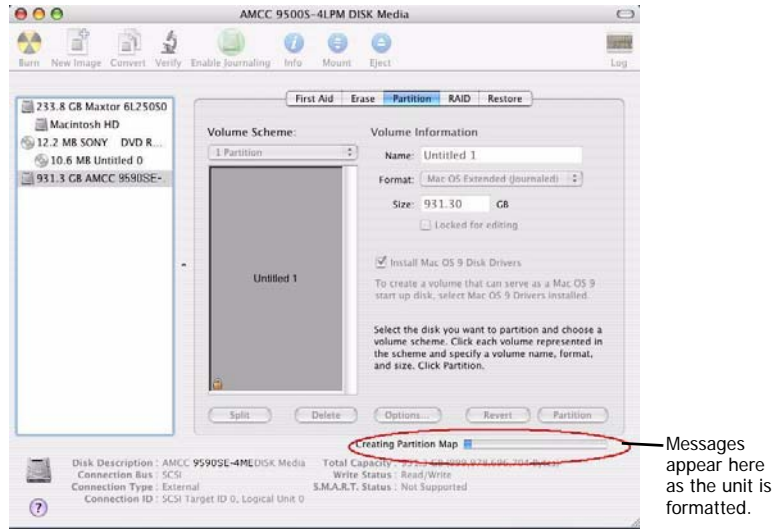
- 6 When a message asks you to confirm you want to partition the disk, click **Partition**.

Figure 20. Confirmation Message to Create the Partition



You will see a series of messages appear toward the bottom of the Disk Utility window as the RAID unit is first partitioned and then formatted. This may take a couple of minutes, depending on the size of the drives in your RAID unit.

Figure 21. Macintosh Disk Utility Showing Partitioning Progress



When the partitioning is complete, icons for each new volume appear on your desktop. They are now ready for use.

You can now close the Macintosh Disk Utility window. Your RAID unit is ready for use.

Creating a Hot Spare

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



Note: When a hot spare replaces a failed drive, an event notification is generated and appears in the list of alarms in 3DM. You can also have 3DM send you an email about this. See “Managing E-mail Event Notification” on page 24.

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

In order to replace a failed drive, a hot spare must have the same or larger storage capacity than the drive it is replacing.

The Auto Rebuild policy allows automatic rebuilding to occur with available drives that are not designated as spares. For more information, see “Setting the Auto Rebuild Policy” on page 30.



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

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

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

If you need to add a drive to be used as the hot spare, follow the instructions under "Adding a Drive" on page 56.

To specify a hot spare

- 1 In 3DM, choose **Management > Maintenance**.
- 2 In the Available Drives list, select the drive you want as a hot spare by marking the checkbox in front of it's Port number.
- 3 Click **Create Unit**.
- 4 In the dialog box that appears, select the configuration type **Spare**.
- 5 Click **Ok**.

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

Naming a Unit

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

To name or rename a unit through 3DM

- 1 Make sure the appropriate controller is selected in the drop-down list at the right of the menu bar.
- 2 Choose **Management > Controller Settings** from the menu bar in 3DM.
- 3 In the **Unit Names** section of the Controller Settings page, locate the unit for which you want to change the name.

- 4 In the text box, enter or type over the name shown. A name can be up to 21 characters, and can include dashes and underscores.
- 5 Click the **Save Names** button.



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

Setting Unit Policies

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

- **Unit Write Cache.** Determines whether write cache is enabled for the unit. When the write cache is enabled, data is stored locally on the drive before it is written to disk, allowing the computer to continue with its next task. This provides the most efficient access times for your computer system. When disabled, the computer will wait for the drive to write all the data to disk before going on to its next task. For details, see “Enabling and Disabling the Unit Write Cache” on page 43.

This feature interacts with functionality of the BBU, if you have one, and with the unit’s StorSave profile. For details, see “Enabling and Disabling the Unit Write Cache” on page 43.

- **Auto Verify.** Determines whether Auto Verify is enabled for the unit. When enabled, the Auto Verify policy causes a verify task to be performed automatically once every 24 hours. This feature is designed to make it easier to insure regular verification of units. If verify schedules have been enabled, then Auto Verify will run only in the scheduled verify time slots. When Auto Verify is disabled, you must manually specify when you want to verify a unit, even if you have set a verify schedule. For details, see “Setting Auto Verify for a Unit” on page 44.
- **Continue on Source Error During Rebuild.** Determines whether ECC errors are ignored when they are encountered during a rebuild. (ECC errors are an indication of errors that have occurred on a particular drive since it was last read.) When not enabled, a rebuild will abort upon encountering an ECC error and the unit will be set to Degraded. For details, see “Setting Continue on Source Error During Rebuild” on page 45.
- **Queuing.** Determines whether NCQ (Native Command Queuing) is enabled for the unit. When enabled for drives that support it, this policy can improve performance. For details, see “Enabling and Disabling Queuing for a Unit” on page 46.

- **StorSave Profile.** Determines what StorSave profile is used for the unit. Three profiles are available: Protection, Balanced, and Performance. For details, see “Setting the StorSave Profile for a Unit” on page 46.

Figure 22. Unit Policies on Controller Settings Page in 3DM

The screenshot shows the 3DM web interface for Controller ID 0. The 'Unit Policies' section is highlighted, showing the following settings for Unit 0 [RAID 5]:

Unit	Write Cache	Auto Verify	Continue on Source Error during Rebuild	Queuing	StorSave
Unit 0 [RAID 5]	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Performance

Other settings visible in the 'Unit Policies' section include:

- Background Task Rate (Controller ID 0):
 - Rebuild/Migrate Rate: Faster Rebuild (radio buttons) or **Faster I/O** (radio button selected)
 - Verify Rate: Faster Verify (radio buttons) or **Faster I/O** (radio button selected)
- Unit Names (Controller ID 0):
 - Unit 0 [RAID 5]: PrimaryRAID5
 - Buttons: Save Names, Reset Names
- Other Controller Settings (Controller ID 0):
 - Auto Rebuild: Enabled Disabled
 - Auto-Carving: Enabled Disabled
 - Carve Size: 1024 (text input) [Submit]
 - Number of Drives per Spin-up: 1
 - Delay between Spin-up: 2 second(s)
 - Export Unconfigured Disk: No

Enabling and Disabling the Unit Write Cache

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



Note: If write cache is enabled, in the event of a power failure, the data in the write cache will be lost if you do not have a Battery Backup Unit (BBU). To avoid a sudden power failure if you do not have a BBU, it is advisable to have an Uninterruptible Power Supply (UPS). (BBU is not supported on the 9590SE-4ME.)

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

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

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



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

To enable or disable unit write cache through 3DM

- 1 Choose **Management > Controller Settings** from the menu bar in 3DM.
- 2 In the **Unit Policies** section of the Controller Settings page, check the Write Cache box to enable it for the designated unit.

Unit Policies (Controller ID 0)	
	Write Cache
Unit 0 [RAID 0]	<input checked="" type="checkbox"/>
Unit 1 [RAID 1]	<input checked="" type="checkbox"/>

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

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

Setting Auto Verify for a Unit

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

If Auto Verify is set and there is no schedule set up for verify tasks, then the controller firmware can initiate a verify task once every 24 hours. If verify time windows are scheduled, then the controller will only start an automatic verify task during the scheduled time windows. (For information about schedules, see "Scheduling Background Tasks" on page 76.)

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

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

To set the Auto Verify policy for an existing unit

- 1 Choose **Management > Controller Settings** from the menu bar in 3DM.
- 2 In the **Unit Policies** section of the Controller Settings page, check the **Auto Verify** box for the appropriate unit. (To disable this policy, uncheck the box.)

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

Setting Continue on Source Error During Rebuild

The **Continue on Source Error During Rebuild** policy is available for units which are redundant. (For units which are not redundant, this option is not shown on the screen.) When this policy is set, ECC (Error Correcting Code) errors are ignored when they are encountered during a rebuild. (ECC errors are typically defects that have been detected in the drive since initialization.) When this policy is not set, if a unit is rebuilding, the rebuild will abort when it encounters an ECC error and the unit will be set back to Degraded.

Since enabling this policy could result in the loss of some source data in the event of source errors, the default is to not enable this policy. Select this option only if you want to ensure that a rebuild will complete successfully without manual intervention. If the rebuild fails and **Continue on Source Error During Rebuild** is not selected, then you have the option to start another rebuild manually. After completing a rebuild with this policy enabled, it is recommended that you execute a file system check when the rebuild completes. On Mac OS X, you can do this using the First Aid tab in the Disk Utility—select the disk on the left and then click **Verify Disk**. If verification encounters problems, you can then use the **Repair Disk** option on the same screen.

To set the Continue on Source Error During Rebuild policy in 3DM

- 1 Choose **Management > Controller Settings** from the menu bar in 3DM.
- 2 In the **Unit Policies** section of the Controller Settings page, check the boxes to select the policies you want to be in effect for each unit

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

Enabling and Disabling Queuing for a Unit

Some drives support NCQ (Native Command Queuing), a feature that can result in increased performance for applications that require a lot of random access of data (usually server-type applications). This is accomplished by causing command reordering to be done on the drive.

In order to make use of NCQ, the feature must be enabled at both the drive and the controller.

You can see whether NCQ is supported and enabled for a particular drive in the Drive Details window. For details, see “Drive Details window” on page 95.



Note: Not all drives support NCQ. If a drive does not support NCQ, the policy setting for the controller is ignored.

To enable or disable queuing for a unit through 3DM

- 1 Choose **Management > Controller Settings** from the menu bar in 3DM.
- 2 In the **Unit Policies** section of the Controller Settings page, enable queuing by checking the box under “Queuing” for the designated unit; disable it by unchecking the box.

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

Setting the StorSave Profile for a Unit

You can set the desired level of data protection versus performance for a unit by selecting the StorSave Profile. Three profiles are provided: *Protection* (maximum data protection), *Performance* (maximum performance, less data protection), and *Balanced* (a middle ground). The default is Protection.

About StorSave Profile Levels

The three profiles automatically adjust several different factors that affect protection and performance on a per unit basis. These are summarized in the table below and further explained after the table.

Table 6: StorSave Profile Definitions

	Protection (Default)	Balanced	Performance
Definition	Maximum data protection, but slower performance.	More data protection than <i>Performance</i> but less data protection than <i>Protection</i> .	Maximum performance for the unit, but less data protection.
FUA (Force Unit Access)	Honor FUA (If no BBU is present) Ignore FUA (If BBU is present)	Honor FUA (If no BBU is present) Ignore FUA (If BBU is present)	Ignore FUA
Write Journaling	Enabled	Disabled, if no BBU present. (Enabled, if BBU is present.)	Disabled (If BBU is present, this essentially disables the BBU for this unit.)
Disable Cache on Degrade	Enabled	Disabled	Disabled

- FUA (Force Unit Access).** FUA commands are a way that the RAID controller or a program (such as a database program) can ensure that data is actually written to the disk drive media, and is not stored in cache. When a write command is followed with a FUA command, then the disk drive will only issue “command complete” to the controller once the data is written to media. When performance is considered more important than protection, it may be desirable to ignore FUA commands.

The Protection and Balanced profiles honor FUA commands if no BBU is present; the Performance profile ignores them regardless of whether a BBU is present.

If you use a battery backup unit (BBU), FUA is ignored, because the BBU preserves the contents of the controller cache memory for a limited period of time (up to 72 hours), in the event of a power failure.

- Write Journaling.** Write journaling tracks the writing of data to disk and preserves a copy of data that has not yet been written to the disk media. Following a power failure or in the event of accidental drive removal and reinsertion, the firmware can recover the unit without data loss. All pending writes sitting in the controller cache are replayed after power is restored or the drive is reinserted and are flushed from the controller to the drive.

Using write journaling helps protect your data, however it can have an impact on performance.

The Protection profile enables write journaling; the Performance and Balanced Profile disables it. The Balanced profile disables it only if no BBU is present.

If write journaling is disabled and a BBU is present, then it is as if the BBU was disabled for that unit.

- **Write cache disabled on degrade.** In the event that a unit degrades, the use of write cache can be disabled until the unit is rebuilt. Once the unit is rebuilt, you must enable the write cache manually. The write cache will not automatically reenable when the unit is rebuilt.

The Protection profile enables this feature, so that write cache is disabled in the event a unit degrades; the Performance and Balanced profiles disable this feature, so that write cache continues to be enabled.

Setting the StorSave Profile through 3DM

In 3DM, the StorSave Profile is a unit policy that can be set on the **Controller Settings** page.

To set the StorSave profile through 3DM

- 1 Choose **Management > Controller Settings** from the menu bar in 3DM.
- 2 In the **Unit Policies** section of the Controller Settings page, select the profile you want to use from the drop-down list in the StorSave column.

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

Changing An Existing Configuration by Migrating

You can convert one RAID configuration into another while the unit is online. This process is known as RAID Level Migration (RLM).

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

- RAID Level (for example, a RAID 1 to a RAID 5)
- Unit Capacity Expansion (for example, adding a 4th drive to a 3-drive RAID 5)

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



Note: A unit being migrated can still be used (I/O still continues), however the performance will be affected while the migrating task is active. You can control how much effect this has on performance by setting the background task rate. For more information, see “Setting Background Task Rate” on page 112.

This section includes the following topics about changing existing configurations:

- RAID Level Migration (RLM) Overview
- Changing RAID Level
- Expanding Unit Capacity
- Informing the Operating System of Changed Configuration

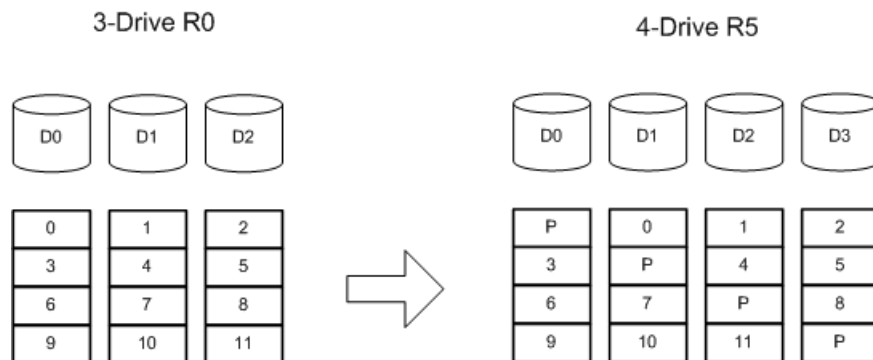
If you want to change the policy settings for an existing unit, there is no need to change the configuration. See “Setting Unit Policies” on page 42.

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 23 shows an example of how data is reconfigured during a migration. In this example, the migration is from a 3-drive RAID 0 to a 4-drive RAID 5, with both having the same stripe size. As can be seen, every piece of user data is moved from its original physical location.

Figure 23. RAID Level Migration Example



Typically, a unit is reconfigured with the same or more storage capacity. Sometimes additional drives are added. The following table shows valid reconfigurations, some of which will require the addition of more drives.

Table 7: Valid Migration Paths

Source	Destination					
	R0	R1	R5	R10	Single	Spare
R0	Yes	No	Yes	Yes	No	No
R1	Yes	No	Yes	Yes	Yes	No
R5	Yes	No	Yes	Yes	No	No
R10	Yes	No	Yes	Yes ^a	No	No
Single	Yes	Yes	Yes	Yes	No	No
Spare	No	No	No	No	No	No

- a. When migrating a RAID 10 to a RAID 10, the only change you can make is the stripe size.



Note: You can only migrate a unit to a RAID level that has the same or more capacity as the existing one. A four-drive RAID 5 unit can migrate to a four-drive RAID 0, but a three-drive RAID 0 unit cannot migrate to a three-drive RAID 5, without adding another drive, due to the need for additional storage capacity for parity bits.

Changing RAID Level

You can use migrate to change the RAID level of an existing unit while the unit is online, without experiencing any data loss. When you change a RAID level, you may also add one or more drives to the unit. You can also migrate to change the unit's stripe size. For example, a four-drive RAID 5 with a 64KB stripe size can be migrated to a four-drive RAID 5 with 256KB stripe size. The steps below describe how to change a RAID level in 3DM2.



Note: Once migration starts, the unit stays in the migrating state until the migration process is complete. The migration process cannot be aborted, and must be allowed to finish before a rebuild or verify to the unit is permitted.



Warning: It is important that you allow migration to complete before removing any drives that are involved in the migration. Removing drives from the unit during migration may cause the migration process to stop, and can jeopardize the safety of your data.

To change the RAID level of a unit

- 1 In 3DM 2, choose **Management > Maintenance**.
- 2 In the Unit Maintenance table on the Maintenance Page, select the unit for which you wish to change the RAID level, by checking the box next to the Unit ID.



The unit to be migrated must be in a normal state (not degraded, initializing, or rebuilding) before starting the migration.

- 3 Click the **Migrate Unit** button.
The Migrate dialog box appears.
- 4 Select any drives to be added to the unit.
- 5 Select the new RAID level.
- 6 Optionally, select a new Stripe size.
- 7 Click **OK**.
The Maintenance page updates to show the new unit and the Migration progress.
- 8 Inform the operating system of the change, as described below under “Informing the Operating System of Changed Configuration”.

Expanding Unit Capacity

You can expand a unit's capacity by adding one or more drives to it without changing the RAID level, except for singles and RAID 1 units. (Since a single can only have one drive, and a RAID 1 can only have two drives, if you add a drive to either, the RAID level must be changed.)

For a RAID 5 with 3 drives, you can change the capacity by adding a fourth drive.

Expanding unit capacity can be accomplished while the unit is online, without experiencing any data loss. This process is also referred to as Online Capacity Expansion (OCE).

To expand a unit's capacity

- 1 In 3DM 2, choose **Management > Maintenance**.
- 2 In the Unit Maintenance table on the Maintenance Page, select the unit you wish to expand by checking the box next to the Unit ID.

- 3 Click the **Migrate Unit** button.

The Migrate dialog box appears, listing the drives which can be added to the unit.

- 4 Select the drives(s) you wish to add to the unit by checking the Port ID box next to each one.
- 5 If desired or necessary, select the appropriate RAID level.
- 6 Click **OK**.

The Maintenance page updates to show the newly reconfigured unit. The Status column title indicates that Migration is in progress.

- 7 After the migration is complete, inform the operating system of the change, as described below.

You can check the status of the migration on the Maintenance page.

Informing the Operating System of Changed Configuration

After you change the configuration of a unit, you must inform the operating system of the change, and you may need to re-partition the unit.

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

To inform the operating system that a unit has been changed

- 1 Unmount the file system from the unit.

Launch the Macintosh Disk Utility, select the unit, and click the Unmount button the toolbar, or select the icon for the unit on the desktop and drag it to the trash.

- 2 In the software, remove and rescan the controller, in order to update unit information.
 - a In 3DM2 choose **Management > Maintenance** and select the appropriate unit.
 - a Click the **Remove Unit** button.
 - b After the unit has been removed, click the **Rescan** button. The new unit capacity displays.
- 3 Resize the partition and file system or create a new partition.

Deleting a Unit

You delete a unit—either an array of disks, or a Single Disk—when you want to reconfigure the unit or use the drives for other purposes.

After you delete a unit, the drives appear in the list of Available Drives.



Warning: When a unit is deleted, all of the data on that unit will be lost. The drives cannot be reassembled into the same unit because the data on it is erased. If you want to reassemble the drives into the same unit on another controller, use the **Remove Unit** button in 3DM instead of the **Delete Unit** button. Or, you can shut down the computer and physically move the drives (or the 3ware Sidecar containing the drives) to another 3ware 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 56.

To delete a unit through 3DM

- 1 Make sure the operating system is not accessing the unit you want to remove.

For example, make sure you are not copying files to the unit, and make sure that there are no applications with open files on that unit.

- 2 Backup any data you want to keep.
- 3 Unmount the unit.

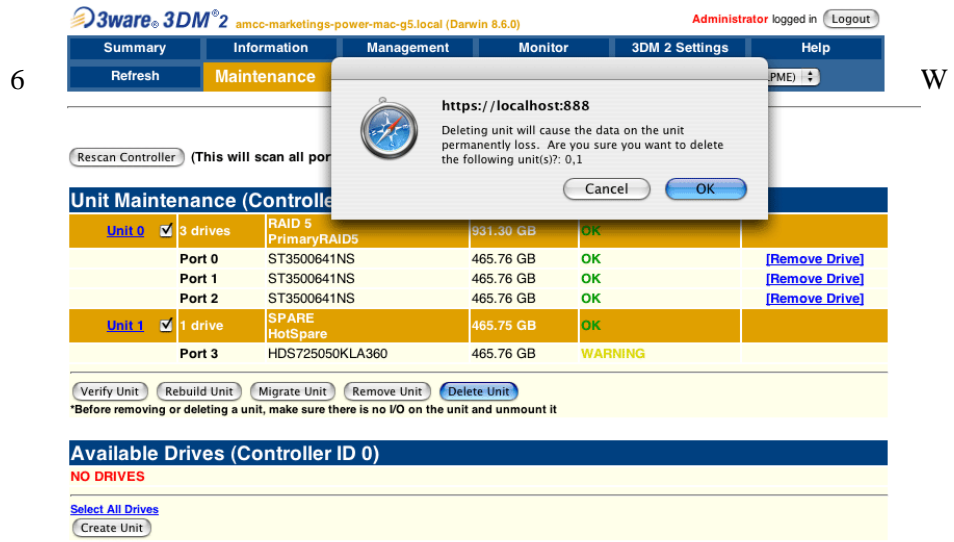
Launch the Macintosh Disk Utility, select the unit, and click the Unmount button the toolbar, or select the icon for the unit on the desktop and drag it to the trash.

This step is very important. If a unit is not unmounted and you delete it, it is the equivalent of physically yanking a hard drive out from under the operating system. You could lose data, the system could hang, or the controller could reset.

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

- In the Unit Maintenance section of the Maintenance page, select the unit you want to remove and click **Delete Unit** (Figure 24).

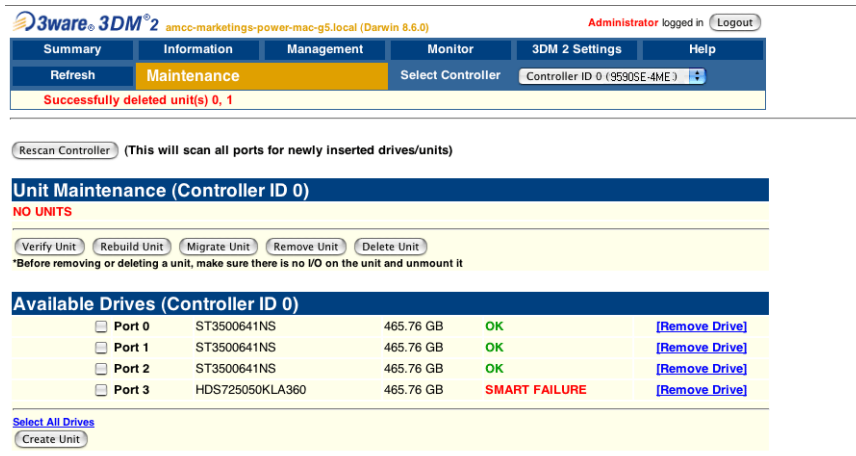
Figure 24. Deleting a Unit Through 3DM



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

Figure 25. Unit Successfully Deleted through 3DM



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.”

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 57.

To remove a unit through 3DM

- 1 Make sure the operating system is not accessing the unit you want to remove.

For example, make sure you are not copying files to the unit, and make sure that there are no applications with open files on that unit.

- 2 Unmount the unit.

Launch the Macintosh Disk Utility, select the unit, and click the **Unmount** button the toolbar, or select the icon for the unit on the desktop and drag it to the trash.

This step is very important. If a unit is not unmounted and you remove it, it is the equivalent of physically yanking a hard drive out from under the operating system. You could lose data, the system could hang, or the controller could reset.

- 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.

You can now physically remove the drives and move them to another controller.

If you change your mind before physically removing the drives and want to reuse the drives and unit on the current controller, just click **Rescan Controller**.

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 move a unit without powering down the system, allowing you to hot-swap the unit. The Remove Unit feature lets you prepare a unit to be disconnected from the controller, and the Rescan feature checks the controller for drives that are now connected, and updates the 3DM screens with current information. For details, see “Removing a Unit” on page 55 and “Rescanning the Controller” on page 58.



Note: Moving a unit to another controller while the unit is in the migration state is supported with one restriction. If the unit was in the middle of the migration process and the controller was shutdown uncleanly, the unit cannot be moved to another controller until the unit has recovered from the unclean shutdown. This may require initializing, verifying, or rebuilding the unit.

Adding a Drive

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

To add a drive

- 1 Insert the drive into the hot-swap carrier or into your 3ware Sidecar.
(For details about using the 3ware Sidecar, see *3ware Sidecar Kit with the 9650SE-4LPME: Installation Guide*.)
- 2 In 3DM, choose **Management > Maintenance**.
- 3 On the Maintenance page, click **Rescan Controller**.

The drive will appear in the list of available drives. You can now use it in a new RAID configuration, as part of an existing configuration, or as a replacement drive in the event that another drive degrades.

If you want to use this drive as a spare, see “Creating a Hot Spare” on page 40.

Removing a Drive

If you have a hot-swap carrier or 3ware Sidecar and want to physically remove a drive from your system without powering it down, you should 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.



Notes:

If you want to remove a unit from your system and reassemble it in another system, do not follow these steps. Instead, turn to “Removing a Unit” on page 55.

If you physically remove a drive on a controller without first removing it in 3DM, it will be listed as removed, however it will not be completely removed unless you Rescan the controller.

Drives that are part of a non-redundant or degraded unit cannot be removed.

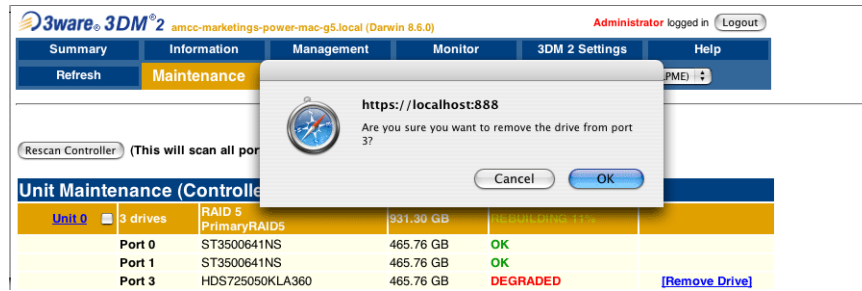
To remove a drive

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

On the Maintenance page, **Remove Drive** links appear next to all drives that can be removed from units, and next to drives in the Available Drives list.

- 2 Locate the drive you want to remove and click the **Remove Drive** link (Figure 26).
- 3 When 3DM asks you to confirm that you want to remove the drive, click **OK**.

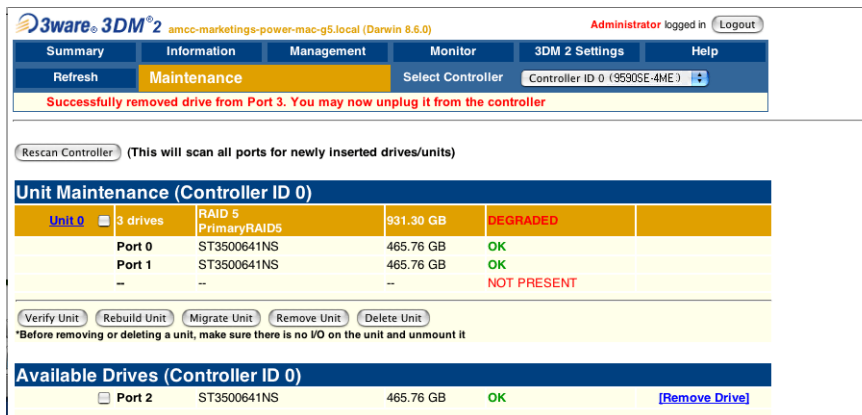
Figure 26. Removing a Drive in 3DM



You can now remove the drive from your system.

If you removed a drive that was part of a unit, the unit will become degraded, as shown in (Figure 27).

Figure 27. Result of Removing Drive from Unit in 3DM



Rescanning the Controller

When you make a change by physically adding or removing drives or units, you can have 3DM rescan the controller to update the list of units and available drives shown on the **Maintenance** page.

This is useful in a variety of circumstances. For example, if you add new drives to the controller, you can make them available by rescanning the controller. Or if you turn on the 3ware Sidecar after turning on your computer, you can use rescan to make the controller see the drives.

Rescanning checks all ports on the controller. It then updates the status of all ports, so if error conditions have been fixed, the status is updated to reflect that. For more details about how the Rescan feature works, see the information in the 3DM Reference section, under “Maintenance page” on page 102.

To rescan the controller

- 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.

6

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 Disk Manager (3DM) provide tools to let you check unit and drive status, and manually start background maintenance tasks. 3DM also lets you review alarms and errors and schedule background maintenance tasks. On Windows systems, the WinAVAlarm utility monitors the controller and will display a message window and give an audible alarm when events occur at or above the threshold you select for it.

Details about these features are described in this section, which is organized into the following topics:

- Checking Unit and Drive Status
 - Enclosure LED Status Indicators
 - Unit Statuses
 - Drive Statuses
- About Degraded Units
- About Inoperable Units
- Alarms, Errors, and Other Events
- Background Tasks
- Scheduling Background Tasks
- Locating a Drive by Blinking Its LED

Checking Unit and Drive Status

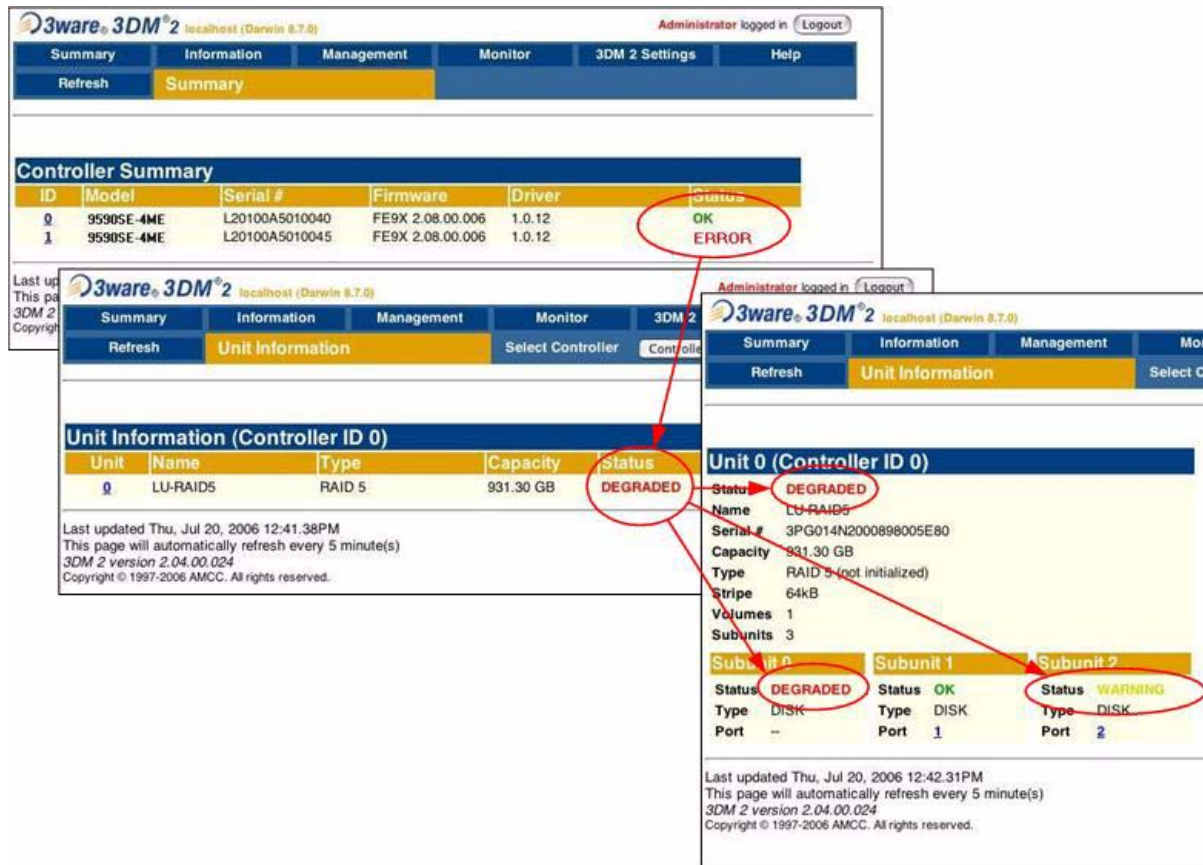
The information screens in 3DM let you see both summary and detailed information about your 3ware RAID controller, configured units, and available drives. You can quickly see the status of your controller and drives, and drill down to find details about any units or drives that have problems.

A status column on the controller, unit, and drive information pages lets you quickly see whether everything is working (OK), performing a task (such as initializing, verifying, or rebuilding), or has a problem (error, degraded, warning).

The next figure illustrates how you can drill down to get additional detail about units and drives in your system.

Figure 28. Drilling Down to Check Status Information

The screenshot shows the 3ware 3DM 2 interface. At the top, there are navigation tabs: Summary, Information, Management, Monitor, 3DM 2 Settings, and Help. Below these is a 'Controller Summary' table with columns for ID, Model, Serial #, Firmware, Driver, and Status. The Status for Controller ID 0 is 'ERROR'. A red circle highlights this 'ERROR' status, with an arrow pointing to the 'Unit Information (Controller ID 0)' section. This section contains a table with columns for Unit, Name, Type, Capacity, and Status. The Status for Unit 0 is 'DEGRADED REBUILDING 10% (paused)'. Another red circle highlights this status, with an arrow pointing to the 'Unit 0 (Controller ID 0)' details section. This section shows various parameters like Name, Serial #, Capacity, Type, Stripe, Parities, Volumes, and Subunits. Below this is a table for Subunits with columns for Subunit #, Status, Type, and Port. The status for Subunit 2 is 'DEGRADED'. A red circle highlights this status, with an arrow pointing to the 'Subunit 0' row, which has a status of 'REBUILD 16%'. A final red circle highlights the 'REBUILD 16%' status, with an arrow pointing back to the 'Unit Information' section.



For RAID 10, a single RAID unit may have more than one status. For example, part of the unit could be rebuilding, while another part is degraded or initializing. When this is the case, you will see both statuses listed at the top unit level. When you drill in to see details, you will be able to see which the specific subunits or drives to which the status applies.

For an explanation of unit and drive status, see:

- “Unit Statuses” on page 63
- “Drive Statuses” on page 64

For information about what the LEDs on your enclosure mean, see “Enclosure LED Status Indicators” on page 63.

Enclosure LED Status Indicators

The LEDs on your enclosure also provide status information about your drives and units.

Table 8: Meaning of LED Colors and Behavior

Color	Drive Status
Solid green	OK
Blinking green	Identify This occurs when you have used the Identify command in 3DM to locate a particular drive or unit. (See “Locating a Drive by Blinking Its LED” on page 81.)
Black	No drive
Solid Amber	Hot spare
Blinking amber	Rebuilding The drive in this slot is part of a RAID unit that is currently rebuilding. You can continue to use the unit. For more information, see “Rebuilding Units” on page 73.
Solid red	Drive fault This drive has failed. You should replace it and rebuild the unit.
Blinking red	Predicted drive fault 3ware software predicts that this drive will fail soon. You may want to replace it.

Unit Statuses

The following is a list of unit statuses you may see in 3DM:

- **OK.** The unit is optimal and is functioning normally.
- **Rebuilding.** The unit is in the process of writing data to a newly added disk in a redundant unit, in order to restore the unit to an optimal state. The unit is not fully fault tolerant until the rebuilding is complete. For more information, see “Rebuilding Units” on page 73.
- **Rebuild-Paused.** The unit is set to rebuild, however scheduling is enabled, and the present time is not during a scheduled timeslot. Rebuilding will start at the next scheduled time slot. Rebuilds are also paused for up to ten minutes after a reboot, even during a scheduled timeslot.
- **Initializing.** The unit is in the process of writing to all of the disks in the unit in order to make the array fault tolerant. For more information, see “About Initialization” on page 69.

- **Initializing-Paused.** The unit is set to initialize, however scheduling is enabled and the present time is not during a scheduled timeslot. Initializing will start at the next scheduled time slot. Initialization is also paused for up to ten minutes after a reboot, even during a scheduled timeslot.
- **Verifying.** The unit is in the process of ensuring that the parity data of a redundant unit is valid. For more information, see “About Verification” on page 70.
- **Verify-Paused.** The unit is set to verify, however, scheduling is enabled, and the present time is not during a scheduled timeslot. Verification will start at the next scheduled time slot.
- **Migrating.** The unit is in the process of being reconfigured while it is online. Migration can be used to change the RAID level, to expand the capacity by adding additional drives, or to change the stripe size. For more information, see “Changing An Existing Configuration by Migrating” on page 48.
- **Migrate-Paused.** The unit is in the process of migrating, however scheduling is enabled, and the present time is not during a scheduled timeslot. Migrating will start at the next scheduled time slot. Migration is also paused for up to ten minutes after a reboot, even during a scheduled timeslot.
- **Degraded.** One or more drives in the redundant unit is no longer being used by the controller. For more information, see “About Degraded Units” on page 65.
- **Inoperable.** This is a condition where one or more drives are missing from a unit, causing the unit to no longer be available to the operating system. Data on an inoperable unit cannot be accessed. For more information, see “About Inoperable Units” on page 65.

Drive Statuses

The following is a list of drive statuses you may see in 3DM:

- **OK.** The drive is fine and is functioning normally.
- **Not Present.** No drive is present in this slot.
- **Drive Removed.** The drive has been removed.
- **Other.** A number of other drive statuses may appear in the event of a problem. If you have a question about a status shown, contact AMCC customer support. knowing the exact drive status can help trouble-shoot the problem.

About Degraded Units

Fault tolerant RAID units provide data redundancy by duplicating information on multiple drives. These RAID units make it possible to continue use even if one of the drives in the unit has failed.

- RAID 1 and RAID 10 units each use mirroring to achieve fault tolerance. Identical data is stored on two or more drives to protect against drive failure.
- RAID 5 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 fails or is removed or unplugged, the unit is said to be *degraded*.

You can still read and write data from a degraded unit, but the unit will not be fault tolerant until it is rebuilt using the Rebuild feature.

When a RAID unit becomes degraded, it is marked as such, and the drive(s) that failed are marked as **Degraded** in the 3DM pages. On the 3ware Sidecar, the LED for failed drives turns red.

You should replace the failed drive and rebuild the unit as soon as it is convenient to do so. The unit will not be fault tolerant until it has been rebuilt. Rebuilding can occur automatically, depending on your settings. For more information, see “Rebuilding Units” on page 73.

About Inoperable Units

Units become inoperable when there are no longer enough drives in the unit for it to function. For example, a RAID 5 unit created from four drives becomes degraded if one drive fails or is removed, but becomes inoperable if two drives fail or are removed.

Data on an inoperable unit cannot be accessed unless the missing drives are reconnected.

If you have data on a unit that is currently “inoperable,” contact technical support.

Alarms, Errors, and Other Events

3ware provides several levels of detail about alarms, errors, and other events. This information is available through the 3DM web application and the CLI.

The next few pages describe these capabilities.

- “Viewing Alarms, Errors, and Other Events” on page 66
- “Downloading an Error Log” on page 67
- “Viewing SMART Data About a Drive” on page 67

CLI capabilities are described in the “3ware® CLI Guide” *3ware Serial ATA RAID Controller CLI Guide*.

Viewing Alarms, Errors, and Other Events

The **Alarms** page in 3DM shows a log of all events (also called Asynchronous Event Notifications, or AENs) that have occurred on units. These events include alarms that occur when the 3ware RAID controller requires attention, such as when a disk unit becomes degraded and is no longer fault tolerant. They also include SMART notifications and informational notification, such as when sectors have been repaired during verification.

Event messages are categorized into the following levels of severity:

- **Errors** (high severity events), shown next to a red box
- **Warnings**, shown next to a yellow box
- **Information**, shown next to a blue box

Examples of event messages:

- **Error:** Unclean shutdown
- **Warning:** Degraded unit
- **Information:** Start and completion of rebuilding, verifying, initializing, migrating, and so forth.

3DM can e-mail notifications of these events to one or more recipients. For more information, see “Managing E-mail Event Notification” on page 24.

A list of the possible error and other event messages is provided under “Error and Notification Messages” on page 119.

To view alarms, errors and other events in 3DM

- 1 Choose **Monitor > Alarms**.

The Alarms page displays, listing all event notifications.

- 2 For details about a particular alarm, click it.
A Help window opens with additional information about the alarm.

To see an explanation of a specific item in 3DM

- Click on the message you are interested in, on the 3DM Alarms page.
A help topic opens with additional information.

Downloading an Error Log

You can download an error log containing information from the firmware log. This can be useful when troubleshooting certain types of problems. For example, you might want to send the saved file to 3ware Customer Support for assistance when troubleshooting.

To download the error log

- 1 In 3DM, choose **Information > Controller Details** from the menu bar.
- 2 Make sure the correct controller is displayed in the **Select Controller** field in the menu bar.
- 3 On the Controller Details page, click the **Download Error Log** link.
- 4 When the Save or Open dialog box appears, navigate to where you want to save the log and click **OK**.

Viewing SMART Data About a Drive

You can view SMART (Self-Monitoring, Analysis, and Reporting Technology) data about a 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 80.

To view SMART data

- 1 Choose **Information > Drive Information** from the menu bar.
- 2 On the Drive Information page, click the port number for the drive you are interested in.

A window showing details of the SMART data opens. The data is shown as hex values.

Background Tasks

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

- Initialization of units
- Verification of units
- Rebuilds when units have become degraded
- Migration of an on-line RAID from one RAID configuration to another
- Self-tests

You can set up your system so that these tasks occur as they are needed, or you can create schedules so that they occur during non-peak times.

Background tasks can have an effect on performance, so using a schedule can minimize the impact.

This section includes the following topics related to background tasks:

- About Initialization
- About Verification
- Starting a Verify Manually
- Rebuilding Units
- Cancelling a Rebuild and Restarting It with a Different Drive
- Setting Background Task Rate
- Background Task Prioritization
- Scheduling Background Tasks
- Viewing Current Task Schedules
- Turning On or Off Use of a Task Schedule
- Removing a Task Schedule
- Adding a New Task Schedule Slot
- Selecting Self-tests to be Performed

Although the migration of a unit is handled as a background task, initiating it is similar to creating a new unit. For details, see “Changing An Existing Configuration by Migrating” on page 48.

About Initialization

For 3ware SATA RAID controllers, *initialize* means to put the redundant data on the drives of redundant units into a known state so that data can be recovered in the event of a disk drive failure. For RAID 1 and RAID 10, initialization copies the data from the lower port to the higher port. For RAID 5, initialization calculates the RAID 5 parity and writes it to disk. This is sometimes referred to as *background initialization* or *resynching*, and does not erase user data.

You can partition, format, and use the unit safely while it is initializing. The unit is fully fault-tolerant while the initialization takes place. That is, if the unit degrades before the initialization is complete, the data will remain intact.

Although you can use the unit while it is being initialized in the background, initialization does slow I/O performance until completed. You can adjust how much initialization will slow performance by setting the rate at which it occurs. (See “Setting Background Task Rate” on page 75.) You can also postpone initialization until a scheduled time. (See “Scheduling Background Tasks” on page 76).



Note: Units will be automatically initialized using background initialization when they are verified for the first time. (Verification requires that the units have been previously initialized.) This will not affect the data on the drives, and the units will perform normally, although performance will be slowed until the initialization and verification are completed.

Initialization of Different RAID Types

Information about initialization for each of the different RAID types is described below .

Initialization of RAID 0 Units

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

Initialization of RAID 5 Units

RAID 5 units with three or four drives will be automatically initialized the first time they are verified.

Regardless of the size, all RAID 5 units are fully fault tolerant upon creation. These configurations use a specialized scheme for writing to the unit, which does not have to be valid to provide fault tolerance.

RAID 5 units with 3 or 4 disks do not need to be initialized to have full performance upon creation. It is okay that 3 or 4 disk RAID 5 units are not initialized. These RAID types are fully redundant, regardless of whether or not they are initialized.



Notes:

For RAID 5 with more 5 or more drives, it is strongly recommended that you initialize the unit before using it. Initializing such a unit is critical to insuring data integrity on the unit.

For RAID 5 with 3 or 4 drives, initialization before use is not required. However, initialization is required before a unit can be verified. Consequently, if you attempt to verify a RAID 5 with 3 or 4 drives that has not yet been initialized, you will see a message that the array has not been initialized, and initialization will begin. This is considered part of normal operation of the unit.

Initialization of RAID 1 and RAID 10 Units

RAID 1 and RAID 10 units do not need to be initialized when they are created to be fault tolerant and are immediately available for use with full performance when created.

Initialization of RAID 1 or RAID 10 units will take place automatically the first time the unit is verified.

Initialization of a RAID 1 unit results in data from one disk (the disk on the lower port number) being copied to the other disk. In RAID 10 units, data from one half of the unit is copied to the other half.

After the initialization, subsequent verifies to a RAID 1 or RAID 10 unit check for data consistency by comparing the data from one drive (or set of drives) to the other drive (or set of drives).

Background Initialization After Power Failure

The 3ware controller detects and handles power failures, using a mechanism that ensures that redundant units have consistent data and parity. When a redundant unit is unexpectedly shutdown, there is a possibility some data and parity may be inconsistent. If a unit or sub-unit of a redundant unit is detected to have been shutdown uncleanly, the unit or sub-unit will change its mode to either ‘Initializing’ or ‘Verifying.’

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

About Verification

Verification can provide early warning of a disk drive problem or failure. This allows you to replace drives before they fail.

You can manually request a verify, or you can enable the Auto Verify policy, and the controller will automatically start verification once every 24 hours. (See “Starting a Verify Manually” on page 73 and “Setting Auto Verify for a Unit” on page 44.)

During verification, I/O continues normally, but with a slight performance loss, depending on your verify rate setting. You can adjust how much verification will slow performance by setting a rate at which it occurs. (See “Setting Background Task Rate” on page 75.) You can also postpone verification until a scheduled time. (See “Scheduling Background Tasks” on page 76.)



Note: Not verifying the unit periodically can lead to an unstable array unit and may cause data loss.

It is strongly recommended that you schedule a verify at least 1 time per week.

What Verification Does

For a RAID 1 or RAID 10 unit, a verify compares the data of one mirror with the other. For RAID 5, RAID 6, , a verify calculates parity and compares it to what is written on the disk drive.

Verification checks each sector on a drive. This is important, because day-to-day use of the media may leave many sectors on a drive unused or unchecked for long periods of time. This can result in errors occurring during user operation. Periodic verification of the media allows the disk drive firmware to take corrective actions on problem areas on the disk, minimizing the occurrence of uncorrectable read and write errors.

Verifies can be scheduled to run at preferred times or can be run automatically during the Verify schedule window, if scheduling and the Auto Verify feature are enabled.

Verification of Non-Redundant Units

Verification of non-redundant units (single disks, spares, and RAID 0 units) read each sector of a drive, sequentially. If a sector can't be read, it is flagged as unreadable, and the next time the controller writes to that location, the drive reallocates the data to a different sector.

Verification of Redundant Units

Verification of redundant units also reads each sector, working from lowest block to highest block. If verification cannot read data in a sector, dynamic sector repair is used to recover the lost data from the redundant drive or drives; this recovered data is written to the problem sector. This forces the drive to reallocate the defective sector with a good spare sector.

If the verify unit process determines that the mirrored drives are not identical or the parity is not correct, the error is corrected. For RAID 1 and 10, this involves copying the miscompared data from the lower port(s) to the higher port(s) of the mirror. For RAID 5 and RAID 50, this involves recalculating

and rewriting the parity that was incorrect. AEN 36 (“Verify detected and fixed data/parity mismatch”) is posted to the Alarms page.

For RAID 1 and 10, verification involves copying the data from the lower port(s) to the higher port(s) of the mirror. For RAID 5 this involves recalculating and rewriting the parity for the entire unit. If the unit is not redundant, a file-system check is recommended to correct the issue. If the errors persist and cannot be overwritten from a backup copy, perform a final incremental backup. You will need to replace the defective drive, recreate the unit, and reinstall the data.

How Errors Are Handled

Verification makes use of the same error checking and error repair techniques used during ordinary use of drives configured through 3ware RAID controllers.

When verification encounters an error, the controller typically retries the command. If there are cable CRC errors, there may be multiple retries including downgrade of the UDMA mode. If the error persists and is unreparable (e.g., ECC errors), an error notification is issued to indicate the problem. (See AEN “0026 Drive ECC error reported” on page 134.)

If the disk drive is part of a redundant unit that is in a redundant state (not degraded or rebuilding), then Dynamic Sector Repair automatically rewrites the redundant data to the error location to force the drive to reallocate the error location. A notification of repair is posted to the alarms list. The result is a restoration of drive and data integrity; the primary and redundant data are again both valid.

If the unit is not redundant, it is recommended that you perform a file-system check to correct the issue. On Mac OS X, you can do this using the First Aid tab in the Disk Utility—select the disk on the left and then click **Verify Disk**. If verification encounters problems, you can then use the **Repair Disk** option on the same screen. If the errors persist and cannot be overwritten from a backup copy, perform a final backup of files that have changed since your last backup. You will need to replace the defective drive, recreate the array, and reinstall the data.

Starting a Verify Manually

Verification of units can be done automatically, on a schedule, or can be started manually, as described below. (See “Setting Auto Verify for a Unit” on page 44 and “Scheduling Background Tasks” on page 76.)



Note: If the unit has not previously been initialized and you manually select **Verify Unit** the initialization process starts.

To verify a unit through 3DM

- 1 In 3DM, choose **Management > Maintenance**.
- 2 In the **Unit Maintenance** section of the Maintenance page, select the unit you want to verify and click **Verify Unit**.

3DM puts the selected unit in verifying mode. If verify scheduling is not enabled on the Scheduling page, the verification process begins almost immediately. If verify scheduling is enabled, the unit will not start actively verifying until the next scheduled time.

A **Stop Verify** link appears next to the unit on the Maintenance page. If you need to stop the verify process, use this link. (If initialization starts because the unit had not previously been initialized, it cannot be halted, so no **Stop Verify** link appears.)

Rebuilding Units

Rebuilding is the process of generating data on a new drive after it is put into service to replace a failed drive in a fault tolerant unit.

If a hot spare is specified and a redundant unit degrades, it will be used to automatically replace the failed drive in the redundant unit without intervention on your part. The rebuild process will automatically be launched as a background process at the next scheduled time. If scheduling is turned off, the rebuild process will start almost immediately (within a couple of minutes). If 3DM is running and E-mail notification is enabled, an event notification will be sent to specified users when the unit degrades and again when the rebuild process is complete.

If the Auto Rebuild policy is enabled (see “Setting the Auto Rebuild Policy” on page 30), the firmware will attempt to rebuild a degraded unit with an available drive or a failed drive.

If desired, you can manually replace the drive, rescan the controller, and start the rebuild process. Rebuilds on multiple units can take place simultaneously.

If multiple drives are faulted in a RAID 10 configuration, the drives are rebuilt simultaneously. In a 4-drive RAID 10 configuration, up to two drives can be rebuilt.



Note: If both drives in a RAID 10 mirrored set are faulted, the data is not recoverable. Up to half of the drives in a RAID 10 unit can become defective and still have the user data retained, as long as the failed drives are only half of each mirrored pair.

When a RAID 5 is running in Degraded mode and you rebuild it, the missing data is reconstructed from all functioning drives.

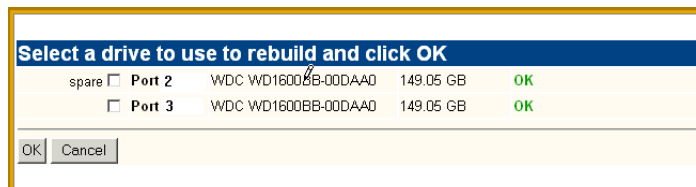


Note: If a rebuild fails, check the Alarms page for the reason. If there was an ECC error on the source disk, you can force the rebuild to continue by checking the Overwrite ECC Error policy on the Controller Settings page in 3DM and then running Rebuild again. This will cause uncorrectable blocks to be rewritten, but the data may be incorrect. It is recommended that you execute a file system check when the rebuild completes. On Mac OS X, you can do this using the First Aid tab in the Disk Utility—select the disk on the left and then click **Verify Disk**. If verification encounters problems, you can then use the **Repair Disk** option on the same screen.

To rebuild a unit through 3DM

- 1 If necessary, add a new drive to replace the failed drive. (For details, see “Adding a Drive” on page 56.)
- 2 In 3DM, choose **Management > Maintenance**.
- 3 In the **Unit Maintenance** section of the Maintenance page, select the degraded unit and click the **Rebuild Unit** button.
- 4 When a dialog box displays available drives, select the drive you want to replace the failed drive and click **OK**.

Figure 29. Selecting a Drive when Rebuilding



- 5 If the degraded unit has more than one failed drive (for example, a RAID 10 where both mirrored pairs each have a failed drive), repeat step 3 and step 4 to select another drive.

If rebuild scheduling is not enabled on the **Scheduling** page, the rebuild process begins almost immediately in the background. If rebuild

scheduling is enabled, the unit will not start actively rebuilding until the next scheduled time.



Note: If you need to cancel a rebuild, you can do so by using the **Remove Drive** link on the Maintenance page to remove the drive from the unit.

Cancelling a Rebuild and Restarting It with a Different Drive

You can cancel a rebuild by using the **Remove Drive** link on the Maintenance page.



Note: If you want to pause the rebuild process through 3DM, you can do so by setting or changing the rebuild schedule on the Scheduling page. If you set a schedule for rebuilds that does not include the current time, the rebuild process will pause.

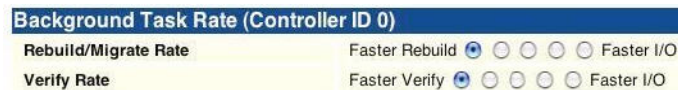
Setting Background Task Rate

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

Controllers can have separate settings for Rebuild/Migrate Rate and Verify Rate. (Initialization occurs at the Rebuild rate.)

To change the background task rate

- 1 Choose **Management > Controller Settings** from the menu bar.
- 2 In the **Background Task Rate** section of the Controller Settings page, select one of the five radio buttons to indicate the relative task rate for Rebuild and Verify Tasks.



The furthest left buttons set the firmware to the fastest rebuild and verify settings. This means that maximum processing time will be given to rebuilds or verifies rather than I/O. The furthest right buttons set the firmware to the slowest rebuild and verify settings, giving maximum processing time to I/O.

After you select one of the radio buttons, the page refreshes, and a message at the top confirms the change you have made.

Background Task Prioritization

Although migration tasks follow the same schedule as rebuild and initialization tasks, they are always given the highest priority because of the controller and disk resources required during migration.

Once a unit is put into the migration state, it must be allowed to complete the process. While migrating, rebuilds or verifies to the unit are not permitted.

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

Controllers can work on multiple units at the same time. This means that if you have both a redundant unit and a non-redundant unit, the verification of the redundant unit and the media scan of the non-redundant unit will occur at the same time.

Scheduling Background Tasks

You can set up scheduling windows for when background tasks occur so that routine maintenance of storage media occurs when it will be least likely to interfere with day-to-day work on the system (peak I/O times). By creating and using schedules, you can specify when active rebuilding, migrating, verifying, and testing of units should occur. For example, you might these tasks to occur at 2AM each day, or on weekends.

The initial schedule setting is to “Ignore Schedule.” This allows the controller firmware to automatically initiate background tasks.



Note: Initialization follows the rebuild/migrate schedule.

Rebuild/migrate, verify, and self-test tasks are scheduled separately, but in a very similar way. You can perform the following scheduling tasks:

- Viewing Current Task Schedules
- Turning On or Off Use of a Task Schedule
- Removing a Task Schedule
- Adding a New Task Schedule Slot
- Selecting Self-tests to be Performed



Tip: If you want to change a task schedule window, you first remove the schedule item and then add it back with the desired day, time, and duration.



Note: Setting up the scheduling window does not actually request background tasks. It simply specifies when they can run. For more information about the background tasks themselves, see “Background Tasks” on page 68.

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 75.

Scheduled Task Duration

If a rebuild completes within a scheduling window, it will not start over at the next scheduled time block, unless another rebuild is required.

If a rebuild does not complete in the scheduled time block, it will continue where it left off at the next scheduled time block.

Similarly, if a verify operation does not complete in the scheduled time block, it will continue where it left off at the next scheduled time block.

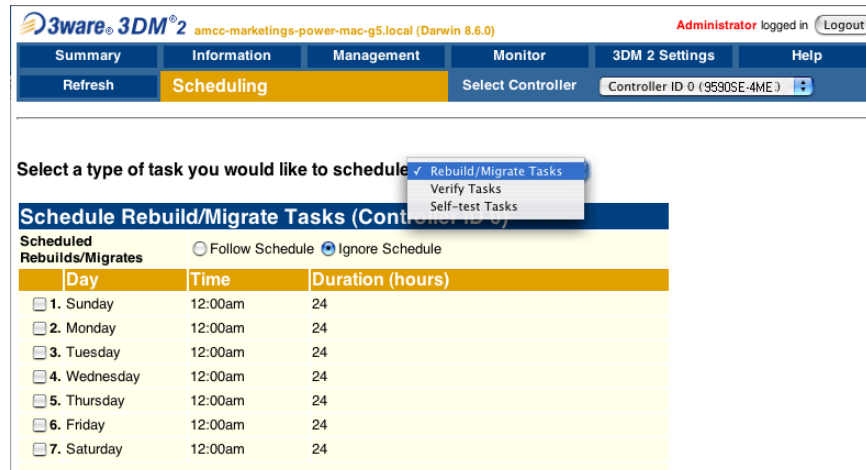
Viewing Current Task Schedules

You can see the current schedules for background tasks on the **Scheduling** page.

To view the current task schedule

- 1 Choose **Management > Schedule** from the menu bar.
The Scheduling page appears, showing the schedule for Rebuild Tasks. (Migration and initialization tasks follow the Rebuild Task schedule.)
- 2 To view Verify Tasks or Self-test Tasks, select it from the drop-down list at the top of the page.

Figure 30. Selecting Task Schedules to View



Select a type of task you would like to schedule

- ✓ Rebuild/Migrate Tasks
- Verify Tasks
- Self-test Tasks

Schedule Rebuild/Migrate Tasks (Controller ID 0 (95905E-4ME))

Scheduled Rebuilds/Migrates Follow Schedule Ignore Schedule

	Day	Time	Duration (hours)
<input type="checkbox"/>	1. Sunday	12:00am	24
<input type="checkbox"/>	2. Monday	12:00am	24
<input type="checkbox"/>	3. Tuesday	12:00am	24
<input type="checkbox"/>	4. Wednesday	12:00am	24
<input type="checkbox"/>	5. Thursday	12:00am	24
<input type="checkbox"/>	6. Friday	12:00am	24
<input type="checkbox"/>	7. Saturday	12:00am	24

Turning On or Off Use of a Task Schedule

Turning on the schedule for Rebuild/Migrate and Verify tasks forces rebuilds, migrates, and verifies to be performed only during the time specified by the schedule. If the schedule is not turned on, rebuilds, migration, initialization, and verify can happen whenever they are required or are manually started.

There may be times when you want to disable scheduled rebuild/migrate or verify tasks, so that you can rebuild, migrate, or verify a unit right away, without waiting for the next scheduled time. In this case, you can disable the schedule, as described below.



Note: When you first use 3DM, daily schedules exist with 24 hour duration—that is, the schedule is for “all the time.” Until you change these 24-hour daily schedule, enabling the schedule will not have any direct effect.

You can easily disable a current Verify or Rebuild/Migrate schedule without deleting the schedule itself.

To turn on or off use of the current Verify or Rebuild task schedule

- 1 Choose **Management > Schedule** from the menu bar.
The Scheduling page appears, showing the schedule for Rebuild/Migrate Tasks.
- 2 To view Verify Tasks, select it from the drop-down list at the top of the page.

- 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.

Schedule Rebuild Tasks (Controller ID 2)		
Scheduled Rebuilds <input type="radio"/> Follow Schedule <input checked="" type="radio"/> Ignore Schedule		
Day	Time	Duration (hours)
<input type="checkbox"/> 1. Sunday	12:00am	24
<input type="checkbox"/> 2. Monday	12:00am	24



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 80.

Removing a Task Schedule

By default, daily task schedules are defined, each starting at 12:00 am and running for 24 hours.

A maximum of seven schedules can be defined. When seven schedules are shown for any of the tasks, you must remove a schedule before you can add another.

To remove a task schedule

- Choose **Management > Schedule** from the menu bar.
The Scheduling page appears, showing the schedule for Rebuild/Migrate Tasks.
- To view Verify Tasks or Self-test Tasks, select it from the drop-down list at the top of the page.
- Select the checkbox next to the schedule(s) you want to remove.
- 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.



The screenshot shows a section of the Scheduling page with a yellow background. It contains a 'Remove Checked' button, an 'Add New Schedule' button, and three dropdown menus: 'Day' set to 'Sunday', 'Time' set to '12:00am', and 'Duration' set to '1'.

- 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: one to check whether UDMA Mode can be upgraded, and another to check whether SMART thresholds have been exceeded. (For more information about these self-tests, see the 3DM Reference section, “Scheduling page” on page 100.)

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.

Schedule Self-tests (Controller ID 2)		
Day	Time	Tasks (applies to all schedule items)
<input type="checkbox"/> 1, Sunday	12:00am	<input checked="" type="checkbox"/> Upgrade UDMA mode
<input type="checkbox"/> 2, Monday	12:00am	<input checked="" type="checkbox"/> Check S.M.A.R.T. Thresholds

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.

Locating a Drive by Blinking Its LED

You can easily identify the drives in a unit, or an individual drive, by causing the LEDs associated with the drives to blink.

You can issue the command to blink the LED through 3DM.

(For details about what the different LED patterns on the enclosure mean, see “Enclosure LED Status Indicators” on page 63.)

To blink the LED for a drive

- 1 Do one of the following:
 - Choose **Information > Drive Information** from the main menu in 3DM. On the Drive Information page, identify the drive you want to physically locate.
 - Choose **Monitor > Enclosure** from the main menu in 3DM. On the list of enclosures, click the ID number of the enclosure. On the Enclosure Detail page, identify the drive you want to physically locate.
- 2 Check the box in the **Identify** column.
The LED on the enclosure begins blinking.
- 3 When you are finished working with the drive and no longer need to see the LED, return to this page and uncheck the **Identify** box.

To blink the LEDs for all drives in a unit

- 1 Choose from the main menu in 3DM.
- 2 On the list of units, locate the unit you want to identify.
- 3 Check the box in the **Identify** column.

The LEDs associated with each drive in the unit begin blinking on the enclosure.

Maintaining Your Controller

This section contains instructions for how to perform tasks that help you maintain your controller, including:

- Determining the Current Version of Your 3ware Driver
- Updating the Firmware and Driver
- Updating the Firmware Through 3DM 2

Determining the Current Version of Your 3ware Driver

Figure 31. Controller Summary Page

The screenshot shows a web browser window titled "3ware 3DM2 - Summary" with the URL "https://localhost:888/". The page header includes the 3ware logo and "3DM² localhost (Darwin 8.7.0)". A navigation bar contains tabs for Summary, Information, Management, Monitor, 3DM 2 Settings, and Help. The "Summary" tab is active, and a "Refresh" button is visible. Below the navigation bar, the "Controller Summary" section contains a table with the following data:

ID	Model	Serial #	Firmware	Driver	Status
0	9590SE-4ME	L20100A5010040	FE9X 2.08.00.006	1.0.12	OK

Below the table, the page indicates it was last updated on Wed, Jun 07, 2006 03:51.11PM, will refresh every 5 minutes, and is version 2.04.00.020. Copyright © 1997-2006 AMCC. All rights reserved.

You can view controller and driver information in several different ways:

- Using 3DM 2 you can see both the driver and firmware versions (see the “Controller Summary page” on page 89)
- Using the CLI you can see both the driver and firmware versions (see *3ware Serial ATA RAID Controller CLI Guide*)

Updating the Firmware and Driver



Note: It is a good idea to back up your data before updating the firmware. Updating the firmware can render the device driver and/or management tools incompatible. It is also recommended to have a copy of the current firmware image for rollbacks.

You can download the latest drivers and firmware from the 3ware website, at <http://www.3ware.com/support>.

Tip: If you only want to update the firmware, you can do so through 3DM, after downloading it. For more information, see “Updating the Firmware Through 3DM 2” on page 85.

To download the driver or firmware

- 1 On the 3ware website (www.3ware.com), navigate to **Service and Support > Software Downloads**.
- 2 Click **Download Released Software**.
- 3 Select the product and release desired.
- 4 Select Driver or Firmware (as appropriate) as the item to download.
- 5 Select the Operating System you are using.
- 6 Click **Next**.
- 7 When details about the download you requested appear, click the link for the item you want to download.
- 8 Read and agree to the license agreement that appears.
- 9 Click **Save** to save the file to disk.
- 10 Uncompress the file to extract the driver or firmware files to a local directory.
(Make note of the absolute path to the local directory.)

To update the driver and firmware under Mac OS X

- 1 Open a Terminal window.
- 2 Type `sudo tw_update` and press Enter.
- 3 When prompted, enter your administrator password.
The usage for the `tw_update` command displays.

4 Type:

```
./tw_update fw=[absolute path to the firmware image]
```

And press Enter.

After the “fw=”, be sure to enter the absolute path to the location of the firmware image. Do not type the brackets shown in the example above.

5 After the update has completed, power cycle your computer (that is, turn it off and then turn it on again).

Updating the Firmware Through 3DM 2

You can use 3DM 2 to update the 3ware RAID controller firmware.

To update the firmware through 3DM

- 1 Download the firmware update from the 3ware website. For details, see “To download the driver or firmware” on page 84.
- 2 In 3DM 2, navigate to **Management > Controller Settings**.
- 3 In the **Update Firmware** section of Controller Settings page, browse to the location where you have saved the downloaded firmware update.
- 4 Click **Begin Update**.
The 3ware RAID controller firmware is updated.
- 5 Power cycle your system for the firmware update to take effect.

Viewing Battery Information

The Battery Backup Unit (BBU) is an add-on card that can be attached to most 3ware 9000 RAID controllers to supply power from a battery pack in the event of a system power loss. (The BBU is not supported on the 9590SE-4ME.) This allows the controller to use write-caching for optimal performance and to preserve data in the event of a system power failure. When fully charged, the battery preserves the contents of the cache memory for up to 72 hours. When power is restored, the cached write data is written to the disks.

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



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

To view information about a BBU in 3DM 2

- On the menu bar, choose **Monitor > Battery Backup**.

The Battery Backup page appears, on which you can see details and status about the unit. This page is refreshed every 30 seconds.

For details about the fields on this page, see “Battery Backup page” on page 110.

Testing Battery Capacity

Batteries in the BBU need to be replaced periodically. A battery test should be run every four weeks in order to get a reliable estimate of battery capacity, and to determine when it needs to be replaced.

The battery test is used to measure the battery’s capacity to back up write data. In order to make a reliable estimate of battery capacity, the BBU pre-charges the battery before it proceeds with a full discharge cycle. The battery is automatically charged again after the test completes. The whole process usually takes between 8 and 12 hours.

While running the battery test and until charging is completed, write cache is temporarily disabled.

For how to replace the battery, see the installation guide that came with your controller.

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 32. Battery Backup Information Screen in 3DM

The screenshot shows the 3DM web interface with the following details:

- Header: 3ware 3DM[®]2 AUTHORIZ:H8YA15 (Windows 2000 Service Pack 4) Administrator logged in Logout
- Navigation: Summary, Information, Management, Monitor, 3DM 2 Settings, Help
- Buttons: Refresh, Battery Backup, Select Controller, Controller ID 0 (9550SX-16ML)
- Section: **Battery Backup Information (Controller ID 0)**
- Table:

Battery Backup Unit	PRESENT
Firmware	BBU: 1.01.01.000
Serial #	M21900A5390019
BBU Ready	Ready
BBU Status	OK
Battery Voltage	OK
Battery Temperature	OK
Estimated Backup Capacity	0 hours
Last Capacity Test	XX-XXX-XXXX [Test Battery Capacity]
Battery Installation Date	26-Oct-2005
- Footer: Last updated Fri, Oct 28, 2005 08:35:32PM. This page will automatically refresh every 5 minute(s). 3DM 2 version 2.04.00.011. Copyright © 1997-2005 AMCC. All rights reserved.

- 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 33. BBU Information Screen While Battery is Testing

The screenshot shows the 3DM web interface with the following details:

- Header: 3ware 3DM[®]2 ALANTEST (Microsoft Windows 2000 build 2195 Service Pack 4) Administrator logged in Logout
- Navigation: Summary, Information, Management, Monitor, 3DM 2 Settings, Help
- Buttons: Refresh, Battery Backup, Select Controller, Controller ID 0 (9550SX-16ML)
- Message: Successfully started battery capacity test
- Section: **Battery Backup Information (Controller ID 2)**
- Table:

Battery Backup Unit	PRESENT
Firmware	BBU: 1.01.01.000
Serial #	M21900A5390019
BBU Ready	Not Ready
BBU Status	TESTING
Battery Voltage	OK
Battery Temperature	OK
Estimated Backup Capacity	0 hours
Last Capacity Test	XX-XXX-XXXX [Test Battery Capacity]
Battery Installation Date	26-Oct-2005
- Footer: Last updated Fri, Oct 28, 2005 08:35:32PM. This page will automatically refresh every 5 minute(s). 3DM 2 version 2.04.00.011. Copyright © 1997-2005 AMCC. All rights reserved.

8

3DM 2 Reference

This section includes details about the fields and features available on the pages you work with throughout 3DM 2. It is organized by 3DM page, as the pages are organized on the 3DM menu bar.

- Controller Summary page
- Controller Details page
- Unit Information page
- Unit Details page
- Drive Information page
- Drive Details window
- Controller Settings page
- Scheduling page
- Maintenance page
- Alarms page
- Battery Backup page
- Enclosure Summary page
- Enclosure Details page
- 3DM 2 Settings page

Controller Summary page

Figure 34. Controller Summary Page

3ware® 3DM® 2 Server3 (Darwin 8.6.0) Administrator logged in Logout						
Summary		Information	Management	Monitor	3DM 2 Settings	Help
Refresh		Summary				
Controller Summary						
ID	Model	Serial #	Firmware	Driver	Status	
0	9590SE-4ME	L20100A5010040	FE9X 2.08.00.006	1.0.12	OK	
1	9590SE-4ME	L20100A5010045	FE9X 2.08.00.006	1.0.12	OK	
<small>Last updated Wed, Jun 07, 2006 03:51:11PM This page will automatically refresh every 5 minute(s) 3DM 2 version 2.04.00.020 Copyright © 1997-2006 AMCC. All rights reserved.</small>						

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

This page provides basic information about each 3ware RAID controller in your system. To see details about the units in a controller, click the link in the ID column.

ID. The ID that the operating system assigns to the controller.

Model. The model name of the controller. (The model number is also printed



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.

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 backside of the controller.)

Firmware. The firmware version running on the controller.

Driver. The driver version being used to interact with the controller.

Status. The overall status of the controller. Possible statuses include OK, Warning, Error, and No Units. **Warning** indicates that a background task is currently being performed (rebuilding, migrating, or initializing). **Error** indicates that a unit is degraded or inoperable. If both Error and Warning conditions exist, the status will appear as Error. For more information, see “Checking Unit and Drive Status” on page 60.

Controller Details page

Figure 35. Controller Details Page

The screenshot shows the 3DM 2 web interface. At the top, there is a navigation bar with tabs: Summary, Information, Management, Monitor, 3DM 2 Settings, and Help. The 'Controller Details' tab is active. Below the navigation bar, there is a 'Refresh' button and a 'Select Controller' dropdown menu showing 'Controller ID 0 (9590SE-4ME)'. The main content area is titled 'Controller Details (Controller ID 0)' and contains a table with the following information:

Model	9590SE-4ME
Serial #	L20100A5010040
Firmware	FE9X 2.08.00.006
Driver	1.0.12
BIOS	BE9X 2.03.01.052
Boot Loader	BL9X 2.02.00.001
Memory Installed	224 MB
Bus Type	PCIE
Bus Width	4 lanes
Bus Speed	2.5 GHz
# of Ports	4
# of Drives	4
# of Units	1
Error Log	Download Error Log

Below the table, there is a footer section with the following text:

Last updated Thu, Jul 20, 2006 11:39:18AM
 This page will automatically refresh every 5 minute(s)
 3DM 2 version 2.04.00.023
 Copyright © 1997-2006 AMCC. All rights reserved.

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

This page provides detailed information about the controller specified in the drop-down list on the menu bar.

You can also open or download an error log from this screen.

Model. The model name of the controller.

Serial #. The serial number of the controller.

Firmware. The firmware version running on the controller.

Driver. The driver version being used to interact with the controller.

BIOS. The BIOS version on the controller.

Boot Loader. Boot Loader version on the controller.

Memory Installed. The amount of memory installed on the controller.

Bus Type. The bus type used on the controller is shown: PCI, PCIX, or PCIE.

Bus Width. The bus width used on the controller: 4 lanes, 8 lanes, or 16 lanes for PCIE slots.

Bus Speed. The speed of the bus used on the controller is shown.

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 36. Unit Information Page

3ware 3DM[®] 2 Server3 (Darwin 8.6.0) Administrator logged in Logout

Summary Information Management Monitor 3DM 2 Settings Help

Refresh Unit Information Select Controller Controller ID 0 (95305E-4ME)

Unit Information (Controller ID 0)

Unit	Name	Type	Capacity	Status	Identify
0	PrimaryMirror	RAID 1	465.65 GB	VERIFYING 55% (active)	<input checked="" type="checkbox"/>

Last updated Wed, Jun 07, 2006 03:53:27PM
 This page will automatically refresh every 5 minute(s)
 3DM 2 version 2.04.00.020
 Copyright © 1997-2006 AMCC. All rights reserved.

The Unit Information page appears when you choose **Information > Unit Information** from the menu bar, or when you click an ID number on the Controller Summary page.

This page shows a list of the units on the current controller and provides summary information about each unit.

To see details about a particular unit, click the link in the Unit # column.

Unit #. The unit number assigned to the unit by the firmware.

Name. If a name has been given to this unit, it shows here. If it is empty, no name has been assigned. You can name your unit in the **Unit Names** section of the **Management > Controller Settings** page.

Type. The type of unit, specified during configuration: RAID 0, RAID 1, RAID 5, RAID 10, Single Disk, or Spare. For details about each of the RAID levels, see “Available RAID Configurations” on page 7.

Capacity. The logical capacity (size) of the unit. 1KB = 1024 bytes.

Status. The operational status of the unit: OK, Rebuilding, Initializing, Migrating, Verifying, Degraded, or Inoperable (missing drives). When a unit is Rebuilding, Initializing, Migrating, or Verifying, the percentage (%) complete is also shown. For an explanation of the statuses, see “Unit Statuses” on page 63.



Note: If an asterisk (*) appears next to the status of a unit, there is an error on one of the drives in the unit. This feature provides a diagnostic capability for potential problem drives. The error may not be a repeated error, and may be caused by an ECC error, SMART failure, or a device error. To see if this error condition still exists, rescan the controller; rescanning will clear the drive error status if the condition no longer exists.

Identify. Check this box to cause the LED for the drives associated with this unit to blink in the enclosure. .

Unit Details page

Figure 37. Unit Details Page

The screenshot shows the 3ware 3DM 2 web interface. At the top, it says "3ware 3DM 2 Server3 (Darwin 8.6.0)" and "Administrator logged in" with a "Logout" button. Below this is a navigation bar with tabs: "Summary", "Information", "Management", "Monitor", "3DM 2 Settings", and "Help". Under "Information", there is a "Unit Information" tab selected, and a "Select Controller" dropdown menu showing "Controller ID 0 (9590SE-4ME)".

The main content area is titled "Unit 0 (Controller ID 0)". It displays the following information:

- Status: **DEGRADED**
- Name: LU-RAID5
- Serial #: 3PG014N2000898005E80
- Capacity: 931.30 GB
- Type: RAID 5 (not initialized)
- Stripe: 64kB
- Volumes: 1
- Subunits: 3

Below this, there is a table showing details for each subunit:

Subunit 0	Subunit 1	Subunit 2
Status: DEGRADED	Status: OK	Status: WARNING
Type: DISK	Type: DISK	Type: DISK
Port: --	Port: 1	Port: 2

At the bottom of the page, it says: "Last updated Thu, Jul 20, 2006 12:42:31PM", "This page will automatically refresh every 5 minute(s)", "3DM 2 version 2.04.00.024", and "Copyright © 1997-2006 AMCC. All rights reserved."

The Unit Details page appears when you click an ID number on the Unit Information page. Because it is a sub-page of Unit Information, the page title in the menu bar continues to display “Unit Information” even when you view details of a unit.

The Unit Details page shows details about a particular unit. The specific information shown depends on what type of unit it is. For example, details about a RAID 5 unit made up of three subunits, each of which contains one drive, will include details about the unit and each subunit, as shown in Figure 37. 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. For status definitions, see "Unit Statuses" on page 63.

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, Single Disk, Spare, or Disk

Volumes. Displays the number of volumes in a unit. This is usually 1. If you have a unit on which you have enabled the auto-carving policy, you will see the number of volumes into which the unit has been divided. For more information, see "Using Auto-Carving for Multi LUN Support" on page 31.

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

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



Note: If an asterisk (*) appears next to the status of a subunit, there is an error on one of the drives in the subunit. This feature provides a diagnostic capability for potential problem drives. The error may not be a repeated error, and may be caused by an ECC error, SMART failure, or a device error. Rescanning the controller will clear the drive error status if the condition no longer exists.

Port #. If the Type is Disk, Single Disk, 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 38. Drive Information Page

3ware® 3DM® 2 Server3 (Darwin 8.6.0)		Administrator logged in Logout					
Summary	Information	Management	Monitor				
Refresh	Drive Information	Select Controller	Controller ID 0 (9590SE-4ME)				
Drive Information (Controller ID 0)							
Port	Model	Capacity	Serial #	Firmware	Unit	Status	Identify
0	ST3500641NS	465.76 GB	3PG014N2	2.AEA	0	OK	<input type="checkbox"/>
1	ST3500641NS	465.76 GB	3PG00WYE	2.AEA	0	OK	<input type="checkbox"/>
2	ST3500641NS	465.76 GB	3PG00WW1	2.AEA	--	OK	<input type="checkbox"/>
3	ST3500641AS	465.76 GB	3PG01PFW	3.AAG	--	OK	<input type="checkbox"/>

Last updated Wed, Jun 07, 2006 03:54:54PM
 This page will automatically refresh every 5 minute(s)
 3DM 2 version 2.04.00.020
 Copyright © 1997-2006 AMCC. All rights reserved.

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.

This page shows a list of drives on the current controller and a summary of each one.

To see additional detail about a particular drive in the Drive Details window, including the SMART data, whether NCQ is supported and enabled, and the SATA Link speed, 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, Not Present, and so forth. If you need help regarding a status displayed here, please contact Technical Support. For more information, see “Drive Statuses” on page 64.

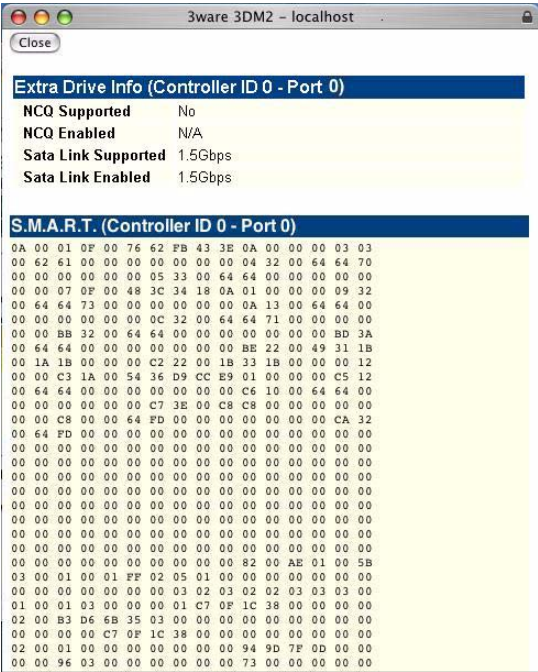


Note: In most cases, the status of the drive will not correspond to the status of the unit, shown on the Unit Information page. Different status information is provided for drives and for units.

Identify. Check this box to cause the LED for this drive to blink in the enclosure.

Drive Details window

Figure 39. S.M.A.R.T. Data Page



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

This Drive Details window shows some Extra Drive Information, including NCQ and SATA Link Speed support, and the SMART data for the drive.

Extra Drive Information

NCQ Supported and **NCQ Enabled.** Some drives support NCQ (Native Command Queuing), which can result in increased performance for some applications, usually server-type applications. In order to make use of Native Command Queuing, the feature must be enabled at both the drive and the controller. Not all drives support NCQ.

The NCQ values in this window indicate whether the feature is supported and enabled at the drive. At the controller level, queuing is enabled or disabled for all drives in a unit on the Controller Settings page.

SATA Link Supported and **SATA Link Enabled.** These fields show the fastest link speed that the disk drive supports and the current speed that the drive is running.

SMART Data

SMART data is displayed as hex values.

Consult your disk drive manufacturer for information on how to interpret the SMART data. The SMART data meaning varies by disk drive manufacturer and model.

Controller Settings page

Figure 40. Controller Settings Page

The screenshot displays the 3ware 3DM 2 web interface. At the top, there is a navigation bar with tabs for Summary, Information, Management, Monitor, 3DM 2 Settings, and Help. The '3DM 2 Settings' tab is active, and the 'Controller Settings' sub-tab is selected. The page is for Controller ID 0 (9590SE-4ME). The settings are organized into several sections:

- Background Task Rate (Controller ID 0):** Includes 'Rebuild/Migrate Rate' and 'Verify Rate', each with radio buttons for 'Faster Rebuild' and 'Faster I/O'.
- Unit Policies (Controller ID 0):** A table with columns for 'Write Cache', 'Auto Verify', 'Continue on Source Error during Rebuild', 'Queuing', and 'StorSave'. The 'Unit 0 [RAID 1]' row shows 'Auto Verify' checked and 'Queuing' checked.
- Unit Names (Controller ID 0):** A text input field for 'Unit 0 [RAID 1]' containing 'PrimaryMirror', with 'Save Names' and 'Reset Names' buttons.
- Other Controller Settings (Controller ID 0):** Includes 'Auto Rebuild' and 'Auto-Carving' (both enabled), 'Carve Size' (1024), 'Number of Drives per Spin-up' (1), 'Delay between Spin-up' (2 second(s)), and 'Export Unconfigured Disk' (No).
- Update Firmware:** An 'Image File' input field with a 'Browse...' button and a 'Begin Update' button.

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

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

There are four main sections on this page:

- Background Task Rate
- Unit Policies
- Unit Names
- Other Controller Settings
- Update Firmware

Background Task Rate

The Background Task Rate fields let you change the balance of background tasks and I/O (reading and writing to disk) performed by the controller.

There are separate settings for Rebuild/Migrate Rate and Verify Rate, Figure 40. The Rebuild/Migrate Rate also applies to initialization. Although the same rate is used for rebuilding, migrating, and initializing, migrating has the highest priority.

The five radio buttons let you set the ratio at which background tasks are performed in comparison to I/O. For additional information, see “Setting Background Task Rate” on page 75.

Unit Policies

3DM lists each unit on the current controller, and shows you whether the policies are currently enabled or disabled for each unit.

Write Cache. When write cache is enabled, data is stored locally in memory on the drive before it is written to the disk drive media, allowing the computer to continue with its next task. This improves performance. However, in the event of a power failure, the data in the write cache will be lost if you do not have a battery backup unit (BBU) or an uninterruptable power supply (UPS).

For additional information, see “Enabling and Disabling the Unit Write Cache” on page 43.

Auto Verify. When the Auto Verify policy is enabled, a verify task is performed automatically once every 24 hours. This feature is designed to make regular verification of units easier.

If a verify scheduling window has been set up and enabled, then Auto Verify will wait until the scheduled time window to start the automatic verify process.

When Auto Verify is not enabled, verify tasks are only run if you manually request one on the 3DM **Management** page. If a verify scheduling window is set and enabled, then manual verifies will wait until the scheduled time to start.

Continue on Source Error During Rebuild. This policy applies only to units which are redundant. (For units which are not redundant, a check box is not available.) When this policy is set, ECC errors are ignored when they are encountered during a rebuild. When this policy is not set, a rebuild will abort upon encountering an ECC error and the unit will be set back to Degraded.

Since this option could result in the loss of some source data in the event of source errors, select this option only if you want to ensure that a rebuild will complete successfully without manual intervention. If the rebuild fails and **Continue on Source Error During Rebuild** is not selected, then you have the

option to start a rebuild manually. It is recommended that you execute a file system check when the rebuild completes. On Mac OS X, you can do this using the First Aid tab in the Disk Utility—select the disk on the left and then click **Verify Disk**. If verification encounters problems, you can then use the **Repair Disk** option on the same screen.

Queuing. This policy enables or disables Native Command Queuing (NCQ) for drives in the unit. By default, queuing is disabled. You can enable it, if desired.

NCQ only operates when the feature is enabled at both the drive and the controller. If a drive does not support NCQ, the policy setting for the controller is ignored.

Enabling NCQ can improve performance in many applications; it causes command reordering to be done on the drive itself.

StorSave Profile. The StorSave feature includes an option that lets you change the StorSave Profile used for a unit. Three profiles are available: Protection, Balanced, and Performance. These profiles automatically adjust several different factors that affect protection and performance, including whether FUA (Forced Unit Access) is honored, whether Write Journaling is enabled, and whether Disable Cache on Degrade is enabled. For additional information, see “Setting the StorSave Profile for a Unit” on page 46.



Note: If the write cache setting is disabled for a unit, the StorSave Profile capability does not apply and is automatically disabled.

Unit Names

Units can be assigned names. A name can be assigned when the unit is created and can be changed from this screen. For additional information, see “Naming a Unit” on page 41.

Other Controller Settings

The Other Controller settings displays information about additional settings, some of which do not apply for the Macintosh.

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

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

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

For additional information, see “Setting the Auto Rebuild Policy” on page 30.

Auto-Carving. Auto-carving can be enabled or disabled by selecting the appropriate radio button.

When this feature is enabled, any unit that is over a specified size (known as the *carve size*) will be broken down into multiple volumes of that size, plus a remainder volume. The default carve size is 2048 GB (2 TB). For example, using the default carve size, if the unit is 2.5 TB then it will contain two volumes, with the first volume containing 2 TB and the second volume containing 0.5 TB. If the unit is 5.0 TB then it will contain 3 volumes, with the first two volumes containing 2 TB each and the last volume containing 1 TB.

Carve Size. Sets a size for dividing up units into volumes when Auto-Carving is enabled. This setting can be between 1024 and 2048 GB.

Number of Drives Per Spin-up. Number of drives that will spin up at the same time when the controller is powered up. (This setting only applies when the feature is supported by the disk drives.) This setting can only be changed in the CLI.

Delay between Spin-ups. The delay time (in seconds) between drive groups that spin up at one time on this particular controller. This setting can only be changed in the CLI.

Export JBOD (Unconfigured) Disks. This feature is not relevant for the Macintosh.

For additional information, see “Setting the Auto Rebuild Policy” on page 30.

Update Firmware

The Update Firmware function allows you to update the firmware of your 3ware RAID controller to the latest version. This keeps the firmware compatible with updates to your operating system and allows you to take advantage of new features 3ware may have added to your controller’s functionality.

For additional information, see “Updating the Firmware Through 3DM 2” on page 85.

Scheduling page

Figure 41. Scheduling Page

3DM 2 Server3 (Darwin 8.6.0) Administrator logged in Logout

Summary Information Management Monitor 3DM 2 Settings Help

Refresh Scheduling Select Controller Controller ID 0 (95905E-4ME)

Select a type of task you would like to schedule: Rebuild/Migrate Tasks

Schedule Rebuild/Migrate Tasks (Controller ID 0)

Scheduled Rebuilds/Migrates Follow Schedule Ignore Schedule

Day	Time	Duration (hours)
<input type="checkbox"/> 1. Sunday	12:00am	24
<input type="checkbox"/> 2. Monday	12:00am	24
<input type="checkbox"/> 3. Tuesday	12:00am	24
<input type="checkbox"/> 4. Wednesday	12:00am	24
<input type="checkbox"/> 5. Thursday	12:00am	24
<input type="checkbox"/> 6. Friday	12:00am	24
<input type="checkbox"/> 7. Saturday	12:00am	24

Remove Checked

Add New Slot Day Sunday Time 12:00am Duration 1

Last updated Wed, Jun 07, 2006 04:00:06PM
 This page will automatically refresh every 5 minute(s)
 3DM 2 version 2.04.00.020
 Copyright © 1997-2006 AMCC. All rights reserved.

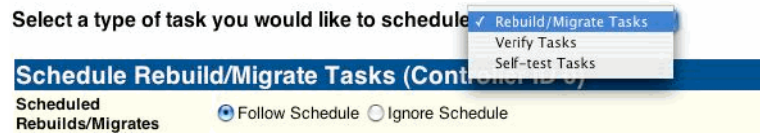
The Scheduling page appears when you choose **Management > Scheduling** from the menu bar.

The Scheduling page lets you set up a schedule for when background tasks (rebuild, migrate, initialize, verify, and self-test) should occur. Background tasks can have impact on the performance of your system, so you may prefer to schedule them at times when they will be least disruptive, such as in the middle of the night or on a weekend.

Select a type of task you would like to schedule. You start by selecting the type of task for which you want to set the schedule from the drop-down list at the top of the page.

- Rebuild/migrate tasks (also applies to initialization)
- Verify tasks (also applies to media scans)
- Self-tests

3DM then updates the page to show you schedule details for that type of task.



Follow Schedule/Ignore Schedule. You can enable or disable the schedule for the Rebuild/Migrate and Verify tasks by selecting either **Follow Schedule** or **Ignore Schedule**. When schedules are set to be ignored, these tasks can be performed at any time, and are not restricted to the scheduled times.

For details about the different background tasks, see “Background Tasks” on page 68.

Task Schedules

Initially, 7 schedule slots are defined, for 24 hours each. Even if **Follow Schedule** is enabled, this schedule is equivalent to **Ignore Schedule**, because tasks can run at any time, round the clock.

A maximum of 7 slots can be created, so to set a different schedule, start by deleting one or more of the existing scheduled slots, and then add new slots.

For step-by-step instructions for adding and removing schedules, and setting schedules to be followed or ignored, see “Scheduling Background Tasks” on page 76.

Self-test Schedules

Unlike scheduling of rebuilds and verifies, scheduling of self-tests is always followed. To disable self-tests you either remove all schedule times, or uncheck the tests listed in the Tasks column.



Note: Only the checked tasks will be run during the scheduled times. If none of the tasks are checked, self-tests will never run, even if you have scheduled time slots set.

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 42. Maintenance Page

3ware 3DM² localhost (Darwin 8.7.0) Administrator logged in Logout

Summary Information Management Monitor 3DM 2 Settings Help

Refresh Maintenance Select Controller Controller ID 0 (S590SE-4ME)

Rescan Controller (This will scan all ports for newly inserted drives/units)

Unit Maintenance (Controller ID 0)

Unit 0	2 drives	RAID 1 PrimaryMirror	465.65 GB	VERIFYING 60%	[Stop Verify]
Port 0	ST3500641NS	465.76 GB	OK	[Remove Drive]	
Port 1	ST3500641NS	465.76 GB	OK	[Remove Drive]	

Verify Unit Rebuild Unit Migrate Unit Remove Unit Delete Unit

*Before removing or deleting a unit, make sure there is no I/O on the unit and unmount it

Available Drives (Controller ID 0)

<input type="checkbox"/> Port 2	ST3500641NS	465.76 GB	OK	[Remove Drive]
<input type="checkbox"/> Port 3	ST3500641AS	465.76 GB	OK	[Remove Drive]

Select All Drives
Create Unit

Last updated Wed, Jun 07, 2006 04:01:37PM
This page will automatically refresh every 5 minute(s)
3DM 2 version 2.04.00.020
Copyright © 1997-2006 AMCC. All rights reserved.

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

The Maintenance page lets you perform maintenance tasks on existing units on the current controller and lets you create new units by configuring available drives.

Information about the Maintenance page is organized under these headings:

- Rescan Controller
- Unit Maintenance
- Maintenance Task Buttons
- Available Drives (to Create Units)

Rescan Controller

The **Rescan Controller** button scans the ports on the controller. Rescanning updates the list of available drives shown and updates the status of all ports. If error conditions have been fixed, the status is updated to reflect that.

Rescanning 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, Rescan will find it.



Note: If you unplug a drive without first removing it through 3DM, Rescan may not recognize it as gone unless the drive was in use or until it is required by the system. Always use the **Remove** link to remove a drive before unplugging it.

Rescan checks all ports. It checks empty ports for newly plugged-in drives. If those drives were previously part of a 3ware RAID configuration and they still have valid DCB (Disk Configuration Block) information on them, the controller tries to piece them back together into a working unit. If a working unit can be formed, it will appear in the Unit Maintenance list when the scan is complete, and the operating system will be notified of the unit. This process is known as importing drives.

If new drives do not have any data indicating they were previously part of a 3ware RAID configuration, they will appear in the Available Drives list.

In addition, if there is a unit with the status Inoperable before a rescan (for example, a RAID 5 unit missing 2 or more drives), and a rescan finds drives that complete the unit, the inoperable unit will become a valid unit.

Unit Maintenance

The Unit Maintenance section of the page lists all existing units on the current controller, and displays summary information about them.

The top row shows information about the unit, while subsequent rows show summary information about each drive in the unit.

Unit Information

Unit Maintenance (Controller ID 0)					
Unit Information	<input type="checkbox"/> Unit 0	2 drives	RAID 1 Primary Mirror	465.65 GB	VERIFYING 80% [Stop Verify]
Drive Information	Port 0		ST3500641NS	465.76 GB	OK [Remove Drive]
	Port 1		ST3500641NS	465.76 GB	OK [Remove Drive]
Verify Unit Rebuild Unit Migrate Unit Remove Unit Delete Unit <small>*Before removing or deleting a unit, make sure there is no VD on the unit and unmount it</small>					

Unit Number. The unit number assigned to the unit by the firmware. Use the checkbox next to the unit to select a unit before clicking one of the task buttons.

Drives. Number of drives in the unit.

Type of Unit. Type of unit: RAID 0, RAID 1, RAID 5, RAID 10, Single Disk, or Spare. If the unit has been given a unique name, it shows beneath the RAID type.

Name of Unit. User-assigned unique name of the unit. The default setting is blank.

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

Status. Operational status of the unit: Ok, Rebuilding, Initializing, Verifying, Migrating, Degraded, or Inoperable (missing drives). When Rebuilding, Initializing, Migrating, or Verifying, the percentage (%) complete is also shown. The percentage complete can be active or paused. To see whether this task is currently active or paused, click on the unit number to display the Unit Details page, which has that information. For an explanation of the statuses, see “Unit Statuses” on page 63.

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. For more information, see “Drive Statuses” on page 64.

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.

Maintenance Task Buttons

Below the list of units, a row of task buttons lets you perform maintenance and configuration tasks related to the unit. Before clicking one of these buttons, select the appropriate unit.



Verify Unit. Puts the selected unit in verifying mode. If verify scheduling is enabled on the Scheduling page, the unit will not start actively verifying until the scheduled time, and the status will indicate “Verify-Paused.” (The Unit Details page will indicate whether a unit is actively verifying.) If verify scheduling is not enabled, clicking Verify Unit begins the verification process.

If the unit you selected to verify is a redundant unit, the redundancy of the unit will be verified. For example it will check parity for a RAID 5 or check data consistency for a RAID 1. If the unit you checked is not a redundant unit, verify will do a surface scan of the media. During verification, I/O continues normally. For RAID 0, single disks, and spares, there is only a slight performance loss. For redundant units, you can set the background task rate on the Controller Settings page to specify whether more processing time should be given to verifying or to I/O. For more information, see “About Verification” on page 70 and “Setting Background Task Rate” on page 75.

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 69.

Rebuild Unit. Replaces a failed drive in a degraded unit with an available drive and begins rebuilding the RAID. When you select a degraded unit and click **Rebuild Unit**, a dialog box listing available drives appears, so that you can select the drive you want to use. If the degraded unit has more than one failed drive (for example, a RAID 10 where both mirrored pairs each have a failed drive), you will repeat this process a second time.

If rebuild scheduling is enabled on the Scheduling page, the unit will not start actively rebuilding until the scheduled time, and the status will change to say “Rebuild-Paused.” (The Unit Details page indicates whether a unit is actively rebuilding.) If rebuild scheduling is not enabled, the rebuild process will begin right away.

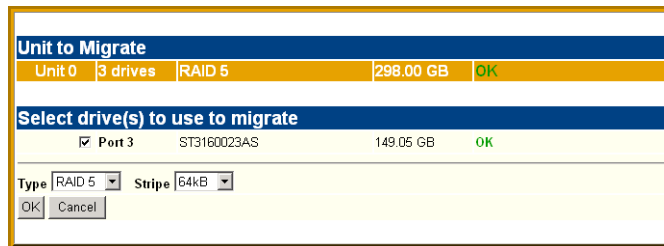
For more information about rebuilds, see “Rebuilding Units” on page 73.

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



Warning: Once migration of a unit is started, it cannot be cancelled.

When you select a unit and click **Migrate Unit**, a dialog box appears which lists the drives in the unit and any additional available drives. In the dialog box are two drop-down menus, one for choosing the RAID level and one for choosing stripe size.



You can only migrate a unit to a RAID level that will be larger than the original unit. For example, you can migrate from a RAID 5 array with 4 drives to a RAID 0 with four drives but you cannot migrate from a RAID 5 with four drives to a RAID 10 with four drives.

After you have specified changes to the unit, the Unit Maintenance screen reflects your changes and shows the percentage of migration completed.

While the unit is migrating, you can still access the unit as normal but the performance will be lower. You can adjust the I/O rate with the radio buttons on the Controller Settings page. (See “Setting Background Task Rate” on page 75.)

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 the system is not accessing it. (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.) You can unmount the unit by selecting the icon for it on the desktop and dragging it to the Trash.

If a unit is not unmounted and you remove it, it is the equivalent of physically yanking a hard drive out from under the operating system. You could lose data, the system could hang, or the controller could reset.

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.

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.

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 the system is not accessing it. (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.) You can unmount the unit by selecting the icon for it on the desktop and dragging it to the trash.

If a unit is not unmounted and you remove it, it is the equivalent of physically yanking a hard drive out from under the operating system. You could lose data, the system could hang, or the controller could reset.



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.

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.

Create Unit

Use the **Create Unit** button to create a unit for use on the current controller. Begin by selecting the drives you want to use in the list of Available Drives, and then click **Create Unit**. You will be prompted to select the unit Type, Name, Stripe size (if applicable), and unit policy settings.

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

Figure 43. Configuration Window in 3DM

The screenshot shows a configuration window titled "Selected drive(s) to use to create". It contains a table with three rows of drive information, followed by configuration options for RAID type, name, stripe size, and various checkboxes. At the bottom, there are "OK" and "Cancel" buttons.

Selected drive(s) to use to create				
Port 0	WDC WD360GD-00FNAD	149.05 GB	OK	
Port 1	HDS722525VLSA80	149.05 GB	OK	
Port 2	WDC WD360GD-00FNAD	149.05 GB	OK	

Type: RAID 5 Name: Stripe: 64KB

Write Cache Auto Verify Continue on Source Error during Rebuild

StorSave: Protection

OK Cancel

For more detailed instructions, see “Configuring a New Unit” on page 33.

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, Single Disk, and Spare Disk. For information about these configurations, see “Available RAID Configurations” on page 7.

Name. You can enter a name for the unit.

Stripe. The drop-down list of stripe sizes lists the possible stripe sizes for the configuration you selected in the RAID level drop-down.

The default stripe size of 64KB will give the best performance with applications that have many sequential reads and writes. A larger stripe size will give better performance with applications that have a lot of random reads and writes. In general, the smaller the stripe size, the better the sequential I/O and the worse the random I/O. The larger the stripe size, the worse the sequential I/O and the better the random I/O.

Write Cache, Auto Verify, and Continue on Source Error during Rebuild. These check boxes let you set the policies for the unit. These policies can also be set and changed on the Controller Settings page. For details about these policies, see “Unit Policies” on page 97.



Note: If the configuration window disappears while you are selecting drives, 3DM 2 may have refreshed. Click **Create Unit** again. If desired, you can reduce the frequency with which information refreshes in 3DM 2, or disable refresh temporarily, on the 3DM 2 Settings page.

StorSave. You can specify the StorSave Profile to be used for the unit. Three profiles are available: Protection, Balanced, and Performance. For more information, see “Setting the StorSave Profile for a Unit” on page 46.

Alarms page

Figure 44. Alarms Page

The screenshot shows the 3ware 3DM2 Alarms Page. At the top, there is a navigation bar with tabs for Summary, Information, Management, Monitor, 3DM 2 Settings, and Help. The 'Alarms' tab is selected. Below the navigation bar, there is a 'Clear Alarms' button and a legend for severity levels: INFO (blue), WARNING (yellow), and ERROR (red). The main content is a table with three columns: Sev, Time, and Message. The table contains seven rows of alarm events.

Sev	Time	Message
ERROR	Jun 02, 2006 07:48.35PM	{0x04:0x3A00}: Drive power on reset detected: port=1
ERROR	Jun 02, 2006 07:48.31PM	{0x04:0x3A00}: Drive power on reset detected: port=0
INFO	Jun 02, 2006 07:12.51PM	{0x04:0x2900}: Verify started: unit=0
INFO	Jun 02, 2006 07:04.22PM	{0x04:0x0700}: Initialize completed: unit=0
WARNING	Jun 02, 2006 05:01.39PM	{0x04:0x4200}: Primary DCB read error occurred: port=2, error=0x208
WARNING	Jun 02, 2006 04:57.45PM	{0x04:0x4200}: Primary DCB read error occurred: port=2, error=0x208
INFO	Jun 02, 2006 04:14.15PM	{0x04:0x0C00}: Initialize started: unit=0

The Alarms page appears when you click **Monitor > Alarms** on the menu bar.

This page displays a list of AENs (asynchronous event notifications) received from the controller displayed in the drop-down list in the menu bar.

Up to 1000 events can be listed. After the 1000-limit is reached, the oldest events are deleted, as new ones occur.

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

For information about a particular event, click it on the Alarms page; the 3DM Help will open with information about the event. For a complete listing of the alarms that appear on the Alarms page, see “Error and Notification Messages” on page 119.

Clear Alarms. The **Clear Alarms** button removes all alarms shown in the list.

Sev. Shows the severity of the event. Three levels are provided:

- Errors are shown next to a red box
- Warnings are shown next to a yellow box
- Information is shown next to a blue box

Time. The time shown for alarms is the time the alarm was received by the driver from firmware.

Message. The specific text relating to the alarm condition.

Battery Backup page

The Battery Backup feature is not supported for the 9590SE-4ME.

Figure 45. Battery Backup Page

Battery Backup Information (Controller ID 0)	
Battery Backup Unit	PRESENT
Firmware	BBU: 1.01.01.000
Serial #	M21900A5390019
BBU Ready	Ready
BBU Status	OK
Battery Voltage	OK
Battery Temperature	OK
Estimated Backup Capacity	0 hours
Last Capacity Test	XX-XX-XXXX [Test Battery Capacity]
Battery Installation Date	26-Oct-2005

Last updated Fri, Oct 28, 2005 08:35:32PM
 This page will automatically refresh every 5 minute(s)
 3DM 2 version 2.04.00.011
 Copyright © 1997-2005 AMCC. All rights reserved.

The Battery Backup page appears when you choose **Monitor > Battery Backup** on the menu bar. Use this page to determine whether a backup battery is present, see details about it, and perform a battery test.

Battery Backup Unit. Indicates whether the BBU is present.

Firmware. Indicates the BBU firmware version.

Serial Number. Indicates the BBU serial number.

BBU Ready. Indicates if the BBU is able to backup the 3ware RAID controller or not. If the BBU is “Ready”, write cache can be enabled on the 3ware RAID controller. When the status is not “Ready,” write caching is automatically disabled on all units attached to the controller.

BBU Status. Indicates the status of the BBU. Possibly BBU statuses include the following:

- **OK.** The BBU is functioning normally.
- **Not Present.** The BBU was not detected or is disabled. (The BBU can be disabled using CLI.)
- **No Battery.** No battery pack is installed in the BBU.
- **Testing.** A battery capacity test is in process.
- **Charging.** The battery is being charged. Charging of the battery occurs automatically if the battery voltage falls too low. This normally occurs

about once a week to top off the charge level; the process does not change the BBU readiness state.

If the battery is ever discharged through a backup cycle or if the system power is off for more than two weeks, the battery status changes to “Charging” the next time the system is powered on. This indicates the BBU is not able to backup the 3ware RAID controller. When the BBU is in the charging state, write caching is disabled automatically on all units attached to the controller.

- **Fault.** The BBU detected a fault. This occurs if the voltage or temperature is outside the acceptable range.
- **Error.** Other BBU error. Please contact AMCC Technical Support.
- **Weak Battery.** The battery should be replaced soon. The results of a battery health test or capacity test indicate that the battery is below the warning threshold (48 hours).
- **Failed Battery.** The battery failed a test and must be replaced. A “Failed Battery” status is displayed if the battery failed the health test or the battery capacity is below the error threshold (24 hours). The battery must be replaced.

Battery Voltage. Indicates the voltage status of the battery. The BBU measures and evaluates the battery voltage continuously. If the voltage falls outside the normal range, warning or error level AENs are generated. In the case of a voltage error the BBU status will change to “Fault” and the battery will be disconnected electronically.

Battery Temperature. Indicates the temperature status of the battery. The BBU measures and evaluates the battery pack temperature continuously. If the temperature falls outside the normal range, warning or error level AENs are generated based on the measured temperature. In the case of a temperature error, the BBU status will change to “Fault” and the battery will be disconnected electronically.

Estimated Backup Capacity. Indicates the estimated backup capacity in hours. This is the amount of time that the battery backup unit can protect the data in the 3ware RAID controller's cache memory. This field is set to zero at the start of a new test and is updated after the test completes. A capacity of zero will also show if the BBU is disconnected and then reconnected.

Under optimal conditions, a battery can protect for up to 72 hours. However, with a fresh battery, you may see a higher number in this field. As the battery ages, the backup capacity diminishes.

Last Capacity Test. Indicates the date when the last battery test was completed. To test the battery click the **Test Battery Capacity** link. For details, see “Testing Battery Capacity” on page 86.

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

Enclosure Summary page

Figure 46. Enclosure Summary Page

3ware 3DM[®]2 localhost (Darwin 8.7.0) Administrator logged in Logout

Summary Information Management Monitor 3DM 2 Settings Help

Refresh Enclosure Support Select Controller Controller ID 0 (9590SE-4ME)

Enclosure Summary				
ID	Slots	Drives	Fans	Temp Sensor
0	4	2	1	1

Last updated Wed, Jun 07, 2006 04:03:08PM
 This page will automatically refresh every 5 minute(s)
 3DM 2 version 2.04.00.020
 Copyright © 1997-2006 AMCC. All rights reserved.

The Enclosure Summary page appears when you choose **Enclosure > Enclosure Summary** from the menu bar.

The Enclosure Summary page provides basic information about any enclosures attached to your system.

ID. The ID that the 3ware firmware assigns to the enclosure.

Slots. The number of slots in the enclosure.

Drives. The number of drives in the enclosure.

Fans. The number of fans in the enclosure.

Temp Sensor. The number of the temperature sensor in the enclosure.

Enclosure Details page

Figure 47. Enclosure Details Page

The screenshot shows the 3ware 3DM 2 web interface. The top navigation bar includes Summary, Information, Management, Monitor, 3DM 2 Settings, and Help. The 'Enclosure Details' tab is selected. The page displays the following information:

- Enclosure ID 0**: Controller ID 0
- Fan Summary**: Fan 0 is OK.
- Temp Sensor Summary**: Temp Sensor 0 is 25°C (77°F).
- Slot Summary**:

Slot	Status	Port	Identify
0	OK	0	<input checked="" type="checkbox"/>
1	OK	1	<input checked="" type="checkbox"/>
2	NO DEVICE	--	<input type="checkbox"/>
3	NO DEVICE	--	<input type="checkbox"/>

The Enclosure Details page appears when you click the ID of the enclosure on the Enclosure Summary page.

Enclosure ID. The ID of the controller to which the enclosure is attached.

Fan Summary. Shows the ID of the enclosure and the status of the fan—either OK or Unknown.

Temp Sensor Summary. Shows the ID of the enclosure and the temperature in the enclosure.

The maximum temperature for successful use of a drive should be noted in the documentation for the drive.

Slot Summary. Lists the enclosure slots and indicates which ones contain drives, and the status of each drive. The Identify checkbox can be used to blink the LED associated with that slot.

Identify. Check the box for a slot to cause the LED for it to blink in the enclosure.

3DM 2 Settings page

Figure 48. 3DM 2 Settings Page

The screenshot shows the 3DM 2 Settings page with the following sections and fields:

- Navigation:** Summary, Information, Management, Monitor, 3DM 2 Settings (selected), Help. A "Refresh" button is also present.
- E-mail notification:**
 - Send E-mail: Enabled Disabled
 - Notify on: INFO (dropdown)
 - Sender: None (text field)
 - Recipient(s): mwname@pacbell.net (text field)
 - Mail Server(name or IP): mail.pacbell.net (text field)
 - Mail Server Login: (text field)
 - Mail Server Password: (text field)
 - Buttons: Save E-mail Settings, Send Test Message
- Password:**
 - Change Password For: User (dropdown)
 - Current Password: (text field)
 - New Password: (text field)
 - Confirm New Password: (text field)
 - Button: Change Password
- Page Refresh:**
 - Minutes Between Refresh: 5 (dropdown)
- Remote Access:**
 - Allow Remote Access: Enabled Disabled

The 3DM 2 Settings page appears when you click **3DM 2 Settings** on the menu bar. Use this page to set preferences, including email notification for alarms, passwords, page refresh frequency, whether remote access is permitted, and the incoming port for 3DM to listen for requests.

The initial settings for most of these preferences are specified during installation of 3DM.

Information about the 3DM 2 Settings page is organized under these headings:

- E-mail Notification
- Password
- Page Refresh
- Remote Access
- HTTP Settings

E-mail Notification

Use the fields in this section to set up and manage notifications of events by e-mail.

Send E-mail. This field determines whether e-mail notification is **Enabled** or **Disabled**. It is a good idea to enable this feature, so that you receive email when your units or drives have problems.

Notify On. Specifies the type of events for which notifications should be sent. A severity of **Information** will send e-mails for all alarms, a severity of **Warning** will send e-mail for alarms with severity of Warning and Error. A severity of **Error** will send e-mail for alarms with severity of Error.

Sender. Enter the email address which will appear in the “From” field.

Recipient. The e-mail address to which notifications should be sent. You can enter multiple addresses, separated by commas (,).

Mail Server (name or IP). If the machine on which you are running 3DM has access to a name server, you may enter the machine name of the mail server in the Server field. Otherwise, use the IP address.

Mail Server Login. If your email server requires authentication, enter the login for the server. If you are uncertain of the login, contact the administrator of the email server.

Mail Server Password. If your email server requires authentication, enter the password for the Mail Server login.

Save E-mail Settings button. Saves the e-mail notification settings.

Send Test Message button. Sends a test message using the saved e-mail settings.

Password

Use the fields in this section to set the passwords for the User and Administrator. When 3DM is first installed, the default password for both is 3ware.

Change Password For. Select the access level for which you are setting the password: **User** or **Administrator**. Users can only view status information in 3DM, while Administrators can make changes and administer the controller and associated drives.

Current Password. Enter the current password.

New Password. Enter the new password.

Confirm New Password. Enter the new password a second time, to be sure you have entered it correctly.

Change Password button. Saves password changes.

Page Refresh

Minutes Between Refresh. Displays how frequently pages in 3DM will be refreshed with new data from the controller. To change this setting, select another option from the drop-down. If you prefer 3DM to only refresh when you click **Refresh Page**, select **Never**.

The Login, Help and Drive SMART data pages do not automatically refresh. All other 3DM pages do.

Remote Access

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

HTTP Settings

Listening Port. This field specifies the HTTP: port to be used by 3DM when listening for communications. The default port setting is 888.

If you change this port, make sure the port you specify is not being used. Failure to do so will cause 3DM to stop responding and you will have to restart it by hand.

Change Port button. Saves a new port number.

Troubleshooting

This troubleshooting section includes the following sections:

- Web Resources
- Before Contacting Customer Support
- Basic Troubleshooting: Check This First
- Command Logging
- Enclosure-Related Problems
- Error and Notification Messages

Web Resources

For support, troubleshooting tips, frequently asked questions, software releases, and compatibility information related to 3ware RAID controllers, refer to:

- 3ware support page at:
<http://www.3ware.com/support/>
- 3ware knowledgebase:
<http://www.3ware.com/KB/kb.asp>
- 3ware software downloads:
<http://www.3ware.com/support/download.asp>
- 3ware documentation:
<http://www.3ware.com/support/userdocs.asp>
- 3ware Compatibility Lists:
http://www.3ware.com/support/sys_compatibility.asp

If you have a degraded unit or problem drive, see “Maintaining Units” on page 60.

Before Contacting Customer Support

Three screens in 3DM 2 provide controller version and status information that can be helpful when contacting 3ware Customer Support with questions or for troubleshooting: Controller Summary, Unit Details, and Unit Information.

You can copy and paste the information from these screens into an email using the system clipboard. When each page is displayed on the screen, highlight it using your mouse (or press Ctrl-A to select all text), copy it to the clipboard, and then paste it into an e-mail.

You may also want to take a screen capture of these pages so that you can respond to questions about your system configuration to the Customer Support representative.

Additional useful information can be gathered from the error logs. For instructions for collecting error logs, see knowledgebase article 12278: <http://www.3ware.com/KB/article.aspx?id=12278>.

Basic Troubleshooting: Check This First

Many error messages can be traced to improperly connected hardware. Hardware can appear to be connected, yet not be in full contact. This can cause intermittent errors that are hard to identify.

Reseat the following items to make sure they are in full contact and are not loose:

- Cables
- Power cords and power connectors
- BBU connectors
- RAID controller
- Hard drives

If you have insured that all connections are secure and the errors still occur, one strategy to confirm or rule out hardware problems is to swap suspected bad drives, cables or power cords with known good ones. You can also:

- Move the drive to a different port on the controller.
- In the case of a controller, try a different slot (being sure to use a slot of the correct type for your controller), or even a different computer.

Command Logging

All changes that are made to RAID configurations using 3DM or CLI are automatically stored in a special log file, `tw_mgmt.log`. This log can be helpful to AMCC technical support for troubleshooting problems with your RAID controller and units.

In Linux, FreeBSD and Mac OS X, `tw_mgmt.log` is in the `/var/log` directory.

In Windows, `tw_mgmt.log` is in the 3DM2 installation directory if 3DM2 is installed on your system. If 3DM2 is not installed, the log file is in the home directory of the current user.

When you install 3DM, you are given the option of turning Command logging on or off. If you later want to disable it, you can do so through the CLI. (For details see the *3ware Serial ATA RAID Controller CLI Guide*.)

There are other logs that may be useful to technical support. For instructions in how to collect the system logs, see <http://www.3ware.com/kb/article.aspx?id=12278>.

Enclosure-Related Problems

An LED is blinking red on the 3ware Sidecar.

A blinking red LED on the 3ware Sidecar indicates that there is a “predicted fault” on the drive in that slot.

This can result from a number of different factors, include a SMART error, read error, or cable error. The drive has not failed yet, but may fail soon.

For additional information about the LED indicators on the 3ware Sidecar, see “Enclosure LED Status Indicators” on page 63.

Error and Notification Messages

Error and notification messages are issued by the 3ware RAID controller when an error is detected or when an action is completed. These messages are sometimes referred to as AENs (asynchronous event notifications).

AEN messages are displayed on the 3DM 2 Alarms page and CLI Show Alarms page.

On the 3DM 2 Alarms page, you can click on the message to jump to help text about that message. You can also look the message up in the list below. In 3DM 2, the message number is the last few digits within the parentheses at the

beginning of the message description. For example, in the string (0x04:0x002B), “002B” is the message number. To find additional information about the message 2B, you would look up 002B in the list below.

Note that the messages are listed below in hex order, since the message numbers are in hex.

Error and notification messages are listed in Table 9. Descriptions of each are provided after the table.

Sev	Time	Message
	Mon, Jan 19, 2004 01:12.54AM	(0x04:0x002B): Background verify done: unit=0
	Sun, Jan 18, 2004 11:57.02PM	(0x04:0x0029): Background verify started: unit=0
	Sun, Jan 18, 2004 01:16.35AM	(0x04:0x002B): Background verify done: unit=0
	Sun, Jan 18, 2004 12:00.48AM	(0x04:0x0029): Background verify started: unit=0

Table 9: Error and Notification Message List

Value	Message
0001	Controller reset occurred
0002	Degraded unit
0003	Controller error occurred
0004	Rebuild failed
0005	Rebuild completed
0006	Incomplete unit detected
0007	Initialize completed
0008	Unclean shutdown detected
0009	Drive timeout detected
000A	Drive error detected
000B	Rebuild started
000C	Initialize started
000E	Initialize failed
000F	SMART threshold exceeded
0019	Drive removed
001A	Drive inserted
001E	Unit inoperable
001F	Unit Operational
0021	Downgrade UDMA mode

Table 9: Error and Notification Message List

Value	Message
0022	Upgrade UDMA mode
0023	Sector repair completed
0024	Buffer integrity test failed
0025	Cache flush failed; some data lost
0026	Drive ECC error reported
0027	DCB checksum error detected
0028	DCB version unsupported
0029	Verify started
002A	Verify failed
002B	Verify completed
002C	Source drive ECC error overwritten
002D	Source drive error occurred
002E	Replacement drive capacity too small
002F	Verify not started; unit never initialized
0030	Drive not supported
0032	Spare capacity too small
0033	Migration started
0034	Migration failed
0035	Migration completed
0036	Verify fixed data/parity mismatch
0037	SO-DIMM not compatible
0038	SO-DIMM not detected
0039	Buffer ECC error corrected
003A	Drive power on reset detected
003B	Rebuild paused
003C	Initialize paused
003D	Verify paused
003E	Migration paused
003F	Flash file system error detected
0040	Flash file system repaired

Table 9: Error and Notification Message List

Value	Message
0041	Unit number assignments lost
0042	Primary DCB read error occurred
0043	Backup DCB read error detected
0044	Battery voltage is normal
0045	Battery voltage is low
0046	Battery voltage is high
0047	Battery voltage is too low
0048	Battery voltage is too high
0049	Battery temperature is normal
004A	Battery temperature is low
004B	Battery temperature is high
004C	Battery temperature is too low
004D	Battery temperature is too high
004E	Battery capacity test started
004F	Cache synchronization skipped
0050	Battery capacity test completed
0051	Battery health check started
0052	Battery health check completed
0053	Battery capacity test is overdue
0055	Battery charging started
0056	Battery charging completed
0057	Battery charging fault
0058	Battery capacity is below warning level
0059	Battery capacity is below error level
005A	Battery is present
005B	Battery is not present
005C	Battery is weak
005D	Battery health check failed
005E	Cache synchronization completed
005F	Cache synchronization failed; some data lost

Error and Notification Message Details

0001 Controller reset occurred

Event Type

Information

Cause

The device driver has sent a soft reset to the 3ware RAID controller. The driver does this when the controller has not responded to a command within the allowed time limit (30 sec.). After the soft reset command has been sent, the driver will resend the command.

Action

If this message occurs more than three times a day, collect the system logs and contact Technical Support.

If this message is seen while installing a 9550SX controller card under FreeBSD, it is due to the APIC (Advanced Programmable Interrupt Controller) being enabled. To complete the installation you must disable APIC. See Knowledge Base 14853: <http://www.3ware.com/kb/article.aspx?id=14853>.

See Also

For how to collect the system logs, see <http://www.3ware.com/kb/article.aspx?id=12278>

For more information regarding FreeBSD installation, see KB articles 14850: <http://www.3ware.com/kb/article.aspx?id=14850>

0002 Degraded unit

Event Type

Error

Cause

An error was encountered and the unit is now operating in degraded (non-redundant) mode. This is usually due to a drive failure or the physical removal of a drive from a redundant unit.

Action

Check hardware connections and reseal the drive or drives. Rescan the controller from 3DM or CLI to see if the unit has been restored. If you are

able to restore the unit before any data has been written to the unit, a rebuild will not be necessary. If the unit remains degraded, replace the missing or dead drives and initiate a rebuild.

See Also

“About Degraded Units” on page 65

“Rebuilding Units” on page 73

0003 Controller error occurred

Event Type

Error

Cause

The 3ware RAID controller has encountered an internal error.

Action

Please collect log files and contact AMCC Customer Support, as a replacement board may be required. Technical support is at <http://www.3ware.com/support/index.asp>. Information on collecting logs is at <http://www.3ware.com/KB/article.aspx?id=12278>.

0004 Rebuild failed

Event Type

Error

Cause

The 3ware RAID controller was unable to complete a rebuild operation. This error can be caused by drive errors on either the source or the destination of the rebuild. However, because ATA drives can reallocate sectors on write errors, the rebuild failure is most likely caused by the source drive of the rebuild detecting a read error.

Action

The default operation of the 3ware RAID controller is to abort a rebuild if an error is encountered. If you want rebuilds to continue when there is a source error, you can set a unit policy to Continue on Source Error During Rebuild in 3DM or CLI.

The consequence of continuing a rebuild when there is a source error is that there may be corrupt data in your rebuilt unit. In some cases, however, this

may be your only alternative for recovering as much data as possible from a unit that has become degraded.

To lower the likelihood of getting this error, schedule regular verifications.

See Also

“Setting Continue on Source Error During Rebuild” on page 45.

“Scheduling Background Tasks” on page 76

0005 Rebuild completed**Event Type**

Information

Cause

The 3ware RAID controller has successfully completed a rebuild. The data is now redundant.

Action

None required.

0006 Incomplete unit detected**Event Type**

Warning

Cause

The 3ware RAID controller has detected an incomplete unit.

An incomplete unit is a unit in which the 3ware RAID controller is unable to detect one or more drives. The drives may be missing, dead, or improperly connected. A unit that is incomplete is also degraded (although a degraded unit can be complete if all drives are still detected, including the failed drive).

Action

Check hardware connections and reseal the drives. Rescan the controller from 3DM to see if the unit has been restored. If you are able to restore the unit before any data has been written to the unit, a rebuild will not be necessary. If the unit remains incomplete, replace the missing or dead drives and initiate a rebuild.

0007 Initialize completed

Event Type

Information

Cause

The 3ware RAID controller completed the “synching” background initialization sequence of RAID levels 1, 10, or 5. For RAID 5, the data on the unit was read and the resultant new parity was written. For RAID 1 and 10, one half of the mirror was copied to the other half (mirrors are synchronized).

This message will not appear for a foreground initialization.

0008 Unclean shutdown detected

Event Type

Warning

Cause

The 3ware RAID controller detected an unclean shutdown of the operating system, either from a power failure or improper shutdown procedure. The controller will force the unit to begin verifying, due to the possibility that data on a redundant unit could be out of synchronization.

Action

Allow the verification to complete. Verifications have little overhead in terms of system performance and keep your units in optimum condition.

To prevent unclean shutdowns, always go through the normal shutdown procedure. It is also recommended to use an uninterruptible power supply (UPS) to prevent unclean shutdowns due to sudden power loss.

See Also

“About Verification” on page 70

0009 Drive timeout detected

Event Type

Error

Cause

A drive has failed to respond to a command from a 3ware RAID controller within the allowed time limit (20 secs.). After sending this error message, the

controller will attempt to recover the drive by sending a reset to that drive and retrying the failed command.

Possible causes of drive time-outs (also known as ATA-Port time-outs) include a bad or intermittent disk drive, power cable or interface cable.

Action

If you have checked hardware connections and no cause other than the drive can be found, replace the drive.

You may also want to use the drive manufacturer's diagnostic and repair utilities on the drive.

See Also

For links to drive manufacturer diagnostic utilities and troubleshooting advice, see <http://www.3ware.com/KB/article.aspx?id=14924>.

“Basic Troubleshooting: Check This First” on page 118

000A Drive error detected**Event Type**

Error

Cause

A drive has returned an error to the 3ware RAID controller that it is unable to complete a command. The error type is not a time-out (000A) or uncorrected ECC (0026).

This message may be seen as part of a recovery operation initiated by the 3ware RAID controller on the drive. One possible cause is multiple write commands to a sector forcing the drive to remap a defective sector. This message may be seen if error recovery operations initiated by the 3ware RAID controller are unsuccessful.

Action

If you see this message, the drive repairs may lie outside of the 3ware RAID controller's abilities. Try running the drive manufacturer's diagnostic and repair utilities on the drive.

If necessary, replace the drive.

See Also

For links to drive manufacturer diagnostic utilities and troubleshooting advice, see <http://www.3ware.com/KB/article.aspx?id=10894>.

000B Rebuild started

Event Type

Information

Cause

The 3ware RAID controller started to rebuild a degraded unit. The rebuild may have been initiated by you, may have started automatically on a hot spare or may have started after drive removal or insertion (due to the Auto Rebuild policy).

Action

Allow the rebuild to complete. This will return the unit to its normal redundant state.

See Also

“Scheduling Background Tasks” on page 76.

“Rebuilding Units” on page 73.

“Background Task Prioritization” on page 76.

000C Initialize started

Event Type

Information

Cause

The 3ware RAID controller started an initialization. This is always a “synching” background initialization and does not erase user data. Initialization either occurs at unit creation time or later during the initial verification of redundant units.

Action

Allow the initialization to complete. This will return the unit to its normal redundant state.

See Also

For more information, see “About Initialization” on page 69

000E Initialize failed

Event Type

Error

Cause

The 3ware RAID controller was unable to complete the initialization. This error can be caused by unrecoverable drive errors.

If this unit was a redundant unit, and the initialization failed because of a problem on a particular disk drive, then the unit will be degraded.

Action

If the unit was degraded, then rebuild the unit. This may necessitate replacing the drive.

Check physical cable and power connections. You can also run the drive manufacturer's diagnostic and repair utilities on the drive.

See Also

For links to drive manufacturer diagnostic utilities and troubleshooting advice, see <http://www.3ware.com/KB/article.aspx?id=10894>.

“Basic Troubleshooting: Check This First” on page 118

000F SMART threshold exceeded**Event Type**

Warning

Cause

SMART monitoring is predicting a potential drive failure.

The 3ware RAID controller supports SMART monitoring, whereby the individual drives automatically monitor certain parametric information such as error rates and retry counts. This type of monitoring may be able to predict a drive failure before it happens, allowing you to schedule service of the unit before it becomes degraded. The SMART status of each drive attached to the 3ware RAID controller is monitored daily.

Action

AMCC recommends that you replace any drive that has exceeded the SMART threshold.

If the drive is part of a redundant unit, remove the drive through 3DM2 or CLI. Replace the drive and start a rebuild.

If the drive is not part of a redundant unit, then you will need to backup your data before replacing the drive.

See Also

“Viewing SMART Data About a Drive” on page 67

“Rebuilding Units” on page 73.

0019 Drive removed

Event Type

Warning

Cause

A drive was physically removed from the controller while the controller was powered on.

Action

If the drive is not part of a redundant unit, return the drive as soon as possible. You may need to rescan the controller to have the drive recognized. If at all possible, do not remove a drive from a non-redundant unit as this may cause data loss or a system hang.

001A Drive inserted

Event Type

Information

Cause

A drive was connected to the controller while the controller was powered on.

Action

The drive is now available for use. If the drive is part of a unit add the remaining drives and rescan the controller, in 3DM or CLI, to bring the unit online.

001E Unit inoperable

Event Type

Error

Cause

The 3ware RAID controller is unable to detect sufficient drives for the unit to be operable. Some drives have failed or are missing.

Examples of inoperable units are as follows:

- RAID 0 missing any drives.

- A RAID 5 or 50 unit with two or more drives missing from the same RAID 5 unit or subunits.
- A RAID 10 unit with both drives missing from one of the RAID 1 subunits.

Note: The controller only generates this message if the unit is missing drives for more than 20 seconds. This allows a hot-swap of a drive to be completed without generating this error.

Action

The unit is no longer available for use. Return all missing drives to the unit. If the drives are physically present, check all data and power connections.

CAUTION: Do not delete the inoperable unit and recreate it as this will overwrite the data and make data recovery very difficult.

You may wish to contact technical support at <http://www.3ware.com/support>.

See Also

“About Inoperable Units” on page 65.

001F Unit Operational

Event Type

Information

Cause

Drive insertion caused a unit that was inoperable to become operational again. Any data that was on that unit will still be there. This message is only sent if the unit was inoperable for more than 20 seconds. That means that if the hot-swap of a drive occurred within 20 seconds, messages are not generated.

Action

None Required. The unit is available for use.

0021 Downgrade UDMA mode

Event Type

Warning

Cause

The 3ware RAID controller has downgraded the UDMA transfer rate between the controller and the ATA disk drives. This message only applies to parallel ATA and certain legacy serial ATA drives.

Background Information

The 3ware RAID controller communicates to the ATA disk drives through the Ultra DMA (UDMA) protocol. This protocol ensures data integrity across the ATA cable by appending a Cyclical Redundancy Check (CRC) for all ATA data that is transferred. If the data becomes corrupted between the drive and the 3ware RAID controller (because of an intermittent or poor quality cable connection) the 3ware RAID controller detects this as a UDMA CRC or cable error. The 3ware RAID controller then retries the failed command three times at the current UDMA transfer rate. If the error persists, it lowers the UDMA transfer rate (for example, from UDMA 100 to UDMA 66) and retries another three times.

Action

Check for possible causes of UDMA CRC errors such as defective or poor quality interface cables or cable routing problems through electrically noisy environments (for instance, cables are too close to the power supply). Also check for cables which are not standard or exceed the ATA specification. A list of cables for use with 3ware controllers is available at <http://3ware.com/products/cables.asp>.

0022 Upgrade UDMA mode

Event Type

Warning

Cause

During a self-test, the controller found that a drive was not in the optimal UDMA mode and upgraded its UDMA transfer rate.

Action

None required. The drive and cable are working in optimal mode.

0023 Sector repair completed

Event Type

Warning

Cause

The 3ware RAID controller moved data from a bad sector on the drive to a new location.

Background Information

The 3ware RAID controller supports a feature called dynamic sector repair that allows the unit to recover from certain drive errors that would normally result in a degraded unit situation. For redundant units such as RAID 1, 5, 10, and , the 3ware RAID controller essentially has two copies of your data available. If a read command to a sector on a disk drive results in an error, it reverts to the redundant copy in order to satisfy the host's request. At this point, the 3ware RAID controller has a good copy of the requested data in its cache memory. It will then use this data to force the failing drive to reallocate the bad sector, which essentially repairs the sector.

Action

Sector repairs are an indication of the presence of grown defects on a particular drive. While typical modern disk drives are designed to allow several hundred grown defects, special attention should be paid to any drive in a unit that begins to indicate sector repair messages. This may be an indication of a drive that is beginning to fail. You may wish to replace the drive, especially if the number of sector repair errors exceeds 3 per month.

0024 Buffer integrity test failed**Event Type**

Error.

Cause

The 3ware RAID controller performs diagnostics on its internal RAM devices as part of its data integrity features. Once a day, a non-destructive test is performed on the cache memory. Failure of the test indicates a failure of a hardware component on the 3ware RAID controller. This message is sent to notify you of the problem.

Action

You should replace the 3ware RAID controller.

If the controller is still under warranty, contact 3ware Technical Support for a replacement controller.

0025 Cache flush failed; some data lost

Event Type

Error

Cause

The 3ware RAID controller was not able to commit data to the drive(s) during a caching operation. This is due to a serious drive failure, possibly from a power outage.

Background Information

The 3ware RAID controller uses caching layer firmware to improve performance. For write commands this means that the controller acknowledges it has completed a write operation before the data is committed to disk. If the 3ware RAID controller cannot commit the data to the drive after it has acknowledged to the host, this message is posted.

Action

To troubleshoot the reasons for the failure, collect the logs for your system and contact 3ware technical support at <http://www.3ware.com/support/index.asp>. For information on what error logs are and how to collect them, see <http://www.3ware.com/KB/article.aspx?id=12278>.

0026 Drive ECC error reported

Event Type

Error

Cause

Drive ECC errors are an indication of grown defects on a particular drive. For redundant units, this typically means that dynamic sector repair has been invoked (see message “0023 Sector repair completed” on page 132). For non-redundant units (RAID 0 and degraded units), which do not have another copy of the data, drive ECC errors result in the 3ware RAID controller returning failed status to the associated host command.

Action

Schedule periodic verifications of all units so that drive ECC errors can be found and corrected. If the unit is non-redundant a unit file system check is recommended.

For Mac OS X, you can use the First Aid tab in the Disk Utility—select the disk on the left and then click Verify Disk. If verification encounters problems, you can then use the Repair Disk option on the same screen.

See Also

“Setting Auto Verify for a Unit” on page 44

“Scheduling Background Tasks” on page 76

0027 DCB checksum error detected**Event Type**

Error

Cause

The drive’s Drive Configuration Block (DCB) has been corrupted.

The 3ware RAID controller stores certain configuration parameters on a reserved area of each disk drive called the Drive Configuration Block. As part of power-on initialization, the 3ware RAID controller performs a checksum of the DCB area to ensure consistency.

Action

If this error occurs, please contact 3ware technical support at <http://www.3ware.com/support/index.asp> for assistance.

0028 DCB version unsupported**Event Type**

Error

Cause

The unit that is connected to your 3ware RAID controller was created on a legacy 3ware product that is incompatible with your new controller.

During the evolution of the 3ware product line, the format of the Drive Configuration Block (DCB) has been changed to accommodate new features. The DCB format expected by the 3ware RAID controller and the DCB that is written on the drive must be compatible. If they are not, this message is sent.

Action

Return the drives back to their original controller and contact 3ware technical support at <http://www.3ware.com/support/index.asp> for further assistance.

0029 Verify started

Event Type

Information

Cause

The 3ware RAID controller has started verifying the data integrity of a unit. The verification functions for different RAID levels are as follows:

- **Single and Spare.** Verify = Media scan
- **RAID 0.** Verify = Media scan
- **RAID 1 and 10.** Verify = Comparison of mirror sides
- **RAID 5.** Verify = Comparison of parity data with user data

Action

Allow verify to complete to identify any possible data integrity issues.

See Also

For information on scheduling a verify process, see “Scheduling Background Tasks” on page 76. For information on verification of a unit, see “About Verification” on page 70.

002A Verify failed

Event Type

Error

Cause

Verification of a unit has terminated with an error. For each RAID level being verified, this may mean:

- **Single and Spare.** A single drive returned an error, possibly because of a media defect.
- **RAID 0.** A single drive returned an error, possibly because of a media defect.
- **RAID 1 and 10.** One side of the mirror does not equal the other side.
- **RAID 5.** The parity data does not equal the user data.

For any RAID type, the most likely cause of the error is a grown defect in the drive. For out-of-synchronization mirrors or parity, the error could be caused by improper shutdown of the unit.

Action

When a verify fails, redundant units will automatically resynchronize user data through a background initialization. The initialize will not erase user data, but will recalculate and rewrite user parity data.

If the unit was non-redundant, any data in the error location is lost. (However, the error could be in a part of the drive that did not contain data.) A unit file system check is recommended.

For Mac OS X, you can use the First Aid tab in the Disk Utility—select the disk on the left and then click Verify Disk. If verification encounters problems, you can then use the Repair Disk option on the same screen.

The resynchronization of data that takes place during a background initialization can slow down access to the unit. Once initialization has begun, it cannot be canceled. You can pause it, however, by scheduling it to take place during off-hours. For more information, see “Scheduling Background Tasks” on page 166. You can also set the initialization process to go slower and use fewer system resources. For more information, see “Setting Background Task Rate” on page 165. (Initialization occurs at the Rebuild rate.)

See Also

“About Initialization” on page 69

002B Verify completed**Event Type**

Information

Cause

Verification of the data integrity of a unit was completed successfully.

See Also

“About Verification” on page 70

002C Source drive ECC error overwritten**Event Type**

Error

Cause

A read error was encountered during a rebuild and the controller is configured to ‘ignore ECC’ or to ‘Force continue on source errors’. The sector in error

was reallocated. This will cause uncorrectable blocks to be rewritten, but the data may be incorrect.

Action

It is recommended that you execute a file system check when the rebuild completes.

For Mac OS X, you can use the First Aid tab in the Disk Utility—select the disk on the left and then click Verify Disk. If verification encounters problems, you can then use the Repair Disk option on the same screen.

002D Source drive error occurred

Event Type

Error

Cause

An error on the source drive was detected during a rebuild operation. The rebuild has stopped as a result.

Action

The controller will report an error, even if the area of the source drive that had the error did not contain data. Scheduling regular verifies will lessen the chance of getting this error.

You can force the rebuild to continue by setting the Overwrite ECC Error policy through 3DM, CLI, or 3BM, and then rebuilding the unit again. This will cause uncorrectable blocks to be rewritten, but the data may be incorrect. It is recommended that you execute a file system check when the rebuild completes.

For Mac OS X, you can use the First Aid tab in the Disk Utility—select the disk on the left and then click Verify Disk. If verification encounters problems, you can then use the Repair Disk option on the same screen.

See Also

“Starting a Verify Manually” on page 73

“Setting Auto Verify for a Unit” on page 44

“Setting Continue on Source Error During Rebuild” on page 45

002E Replacement drive capacity too small**Event Type**

Error

Cause

The storage capacity of the drive you are using as a replacement drive is too small and cannot be used.

Action

Use a replacement drive equal to or larger than the drives already in use

002F Verify not started; unit never initialized**Event Type**

Warning

Cause

A verify operation has been attempted by the 3ware RAID controller, but the unit has never been initialized before. The unit will automatically transition to initializing mode and then start a verify.

Action

None required.

This is considered a normal part of operation. Not all types of RAID units need to be initialized in order to have full performance. The initialize will not erase user data, but will calculate and write parity data or mirror data to the drives in the unit.

See Also

“About Initialization” on page 69

0030 Drive not supported**Event Type**

Error

Cause

3ware 8000 and 9500S Serial ATA controllers only support UltraDMA-100/133 drives when using the parallel-to-serial ATA converter. This message indicates that an unsupported drive was detected during rollcall or a hot swap.

This message could also indicate that the parallel-to-serial converter was jumpered incorrectly.

Action

Use a parallel ATA drive which supports UDMA 100 or 133 and check that the parallel-to-serial converter was correctly jumpered to correspond to UDMA 100 or 133 drives.

See Also

Refer to the User Manual for your controller.

For a list of compatible drives, see

http://www.3ware.com/products/compatibility_sata.asp

0032 Spare capacity too small

Event Type

Warning

Cause

There is a valid hot spare but the capacity is not sufficient to use it for a drive replacement in existing units.

Action

Replace the spare with a drive of equal or larger capacity than the existing drives.

0033 Migration started

Event Type

Information

Cause

The 3ware RAID controller has started the migration of a unit.

Migration changes can include:

- Expanding capacity of a unit by adding drives
- Changing RAID levels, for example, from RAID 1 to RAID 5.

See Also

“RAID Level Migration (RLM) Overview” on page 49.

0034 Migration failed

Event Type

Error

Cause

The migration of a unit has failed.

Migration changes can include:

- Expanding capacity of a unit by adding drives.
- Changing RAID levels, for example, from RAID 1 to RAID 5.

Action

Review the list of events on the Alarms page for other entries that may give you an idea of why the migration failed (for example, a drive error on a specific port).

You may also wish to get the logs and contact technical support at <http://www.3ware.com/support/index.asp>. For information on what error logs are and how to collect them, see <http://www.3ware.com/KB/article.aspx?id=12278>.

See Also

“RAID Level Migration (RLM) Overview” on page 49

0035 Migration completed

Event Type

Information

Cause

The migrated unit is now ready to be used.

Migration changes can include:

- Expanding capacity of a unit by adding drives
- Changing RAID levels, for example, from RAID 1 to RAID 5.

Action

If the capacity of the unit did not change, then you do not need to do anything else. If the capacity of the migrated unit is larger, you will need to inform the operating system of the change. See “Informing the Operating System of Changed Configuration” on page 52.

0036 Verify fixed data/parity mismatch

Event Type

Warning

Cause

A verify error was found and fixed by the 3ware RAID controller.

Some examples of errors that can be fixed include:

- A parity inconsistency for a RAID 5.
- A data mismatch for a RAID 1 or RAID 10 unit.

Action

None required.

0037 SO-DIMM not compatible

Event Type

Error

Cause

There is incompatible SO-DIMM memory connected to the 9500S controller.

Note: This message only applies to the 3ware 9500S controller, which has removable memory. Other 3ware controller models do not have memory that can be removed.

Action

Replace the incompatible SO-DIMM with a compatible one.

See Also

For a list of SODIMMs compatible with the 9500S, see <http://www.3ware.com/KB/article.aspx?id=11748>.

0038 SO-DIMM not detected

Event Type

Error

Cause

The 3ware 9500S RAID controller is inoperable due to missing SO-DIMM memory.

Note: This message only applies to the 3ware 9500S controller, which has removable memory. Other 3ware controller models do not have memory that can be removed.

Action

Install a compatible SO-DIMM on the controller.

See Also

For a list of SODIMMs compatible with the 9500S, see <http://www.3ware.com/KB/article.aspx?id=11748>.

0039 Buffer ECC error corrected**Event Type**

Warning

Cause

The controller has detected and corrected a memory ECC error.

Action

None required.

If errors persist, contact technical support at <http://www.3ware.com/support/index.asp>.

003A Drive power on reset detected**Event Type**

Error

Cause

The controller has detected that a drive has lost power and then restarted. The controller may degrade the unit if it is a redundant unit (non-redundant units cannot be degraded).

Action

If this drive was the only one to lose power, check the cable connections. Also, check that your power supply is adequate for the type and number of devices attached to it.

See Also

For troubleshooting information and a link to drive manufacturer diagnostic utilities, see <http://www.3ware.com/KB/article.aspx?id=14927>.

003B Rebuild paused

Event Type

Information

Cause

The rebuild operation is paused.

Rebuilds are normally paused for two (formerly ten) minutes after a system first boots up and during non-scheduled times when scheduling is enabled.

Disabling or modifying the schedule with 3DM or CLI will allow the rebuild to resume.

See Also

“Scheduling Background Tasks” on page 76

003C Initialize paused

Event Type

Information

Cause

The initialization is paused.

Initializations are normally paused for two (formerly ten) minutes after a system first boots up. Initialization is also paused during non-scheduled times when scheduling is enabled. Initializations follow the rebuild schedule.

Action

If you want the initialize to resume, you can disable or modify the schedule through 3DM or CLI.

See Also

“Viewing Current Task Schedules” on page 77

“About Initialization” on page 69

003D Verify paused

Event Type

Information

Cause

The verify operation is paused.

Verifies are normally paused for 2 (formerly 10) minutes after a system first boots up. Verifies are also paused during non-scheduled times when scheduling is enabled.

Action

If you want the verification to resume, you can disable or modify the schedule through 3DM or CLI

See Also

“About Verification” on page 70

“Scheduling Background Tasks” on page 76

003E Migration paused

Event Type

Information

Cause

Migration is paused. Migration follows the rebuild schedule.

Action

If you want the migration to resume, you can disable or modify the schedule through 3DM or CLI

See Also

“RAID Level Migration (RLM) Overview” on page 49

“Scheduling Background Tasks” on page 76

003F Flash file system error detected

Event Type

Warning

Cause

A corrupted flash file system was found on the 3ware RAID controller during boot-up.

The 3ware RAID controller stores configuration parameters as files in its flash memory. These files can be corrupted when a flash operation is interrupted by events such as a power failure. The controller will attempt to restore the flash files from a backup copy.

Action

Update to the latest firmware, as earlier firmware resets corrupted files to default settings.

We recommend using 3DM, CLI or 3BM to check your settings, in case they were not able to be restored.

0040 Flash file system repaired

Event Type

Information

Cause

A corrupted flash file system has been successfully repaired.

Some of the flash files with insufficient data may have been lost in the operation. The configuration parameters which are lost will then return to their default values.

Action

We recommend using 3DM, CLI or 3BM to check your settings, in case they were not able to be restored.

0041 Unit number assignments lost

Event Type

Warning

Cause

The unit number assignments have been lost.

This may have occurred as a result of a soft reset.

Action

Please contact AMCC 3ware technical support at <http://www.3ware.com/support/index.asp>.

0042 Primary DCB read error occurred

Event Type

Warning

Cause

The controller found an error while reading the primary copy of the Disk Configuration Block (DCB).

The controller will attempt to correct the error by reading the back-up copy of the DCB. If a valid DCB is found, the primary DCB is re-written to rectify the errors.

Action

AMCC recommends verifying the unit. See “Starting a Verify Manually” on page 73.

0043 Backup DCB read error detected

Event Type

Warning

Cause

The controller has detected a latent error in the backup Disk Configuration Block (DCB).

The 3ware RAID controller checks the backup DCB, even when the primary DCB is OK. If an error is found, the controller will attempt to correct the error by reading the primary copy. If the primary copy is valid, the backup DCB will be rewritten to rectify the errors.

Action

AMCC recommends verifying the unit. See “Starting a Verify Manually” on page 73.

0044 Battery voltage is normal

Event Type

Information

Cause

The battery pack voltage being monitored by the Battery Backup Unit fell outside of the acceptable range and then came back within the acceptable range.

Action

None required

0045 Battery voltage is low

Event Type

Warning

Cause

The battery pack voltage being monitored by the Battery Backup Unit has fallen below the warning threshold.

Action

The Battery Backup Unit is presently still able to backup the 3ware RAID controller, but you should replace the battery pack if the warning continues.

0046 Battery voltage is high

Event Type

Warning

Cause

The battery pack voltage being monitored by the Battery Backup Unit has risen above the warning threshold.

Action

The Battery Backup Unit is presently still able to backup the 3ware RAID controller, but you should replace the battery pack if the warning continues.

0047 Battery voltage is too low**Event Type**

Error

Cause

The battery pack voltage being monitored by the Battery Backup Unit is too low to backup the 3ware RAID controller.

You may see this message during a battery capacity test. In this case, it is not a sign of battery failure.

You may also see this message if the battery pack is plugged in while the computer is on. This is not advised.

Action

Replace the battery pack if none of the above causes apply and the warning continues.

0048 Battery voltage is too high**Event Type**

Error

Cause

The battery pack voltage being monitored by the Battery Backup Unit is too high to backup the 3ware RAID controller.

Action

The battery pack must be replaced.

This may be a fault in the BBU control module. If you get this error, do the following:

- 1 Turn off the computer and remove the 3ware RAID controller.
- 2 Remove the BBU control module and battery module from the 3ware RAID controller.
- 3 Unplug the battery from the control module.
- 4 Return the BBU control module and battery module to 3ware.

For more details on removing the BBU, see the installation guide that came with your 3ware RAID controller.

0049 Battery temperature is normal

Event Type

Information

Cause

The battery pack temperature being monitored by the Battery Backup Unit fell outside of the acceptable range and then came back within the acceptable range.

Action

None required

004A Battery temperature is low

Event Type

Warning

Cause

The battery pack temperature being monitored by the Battery Backup Unit has fallen below the acceptable range. The most likely cause is ambient temperature.

Action

The Battery backup Unit is presently still able to backup the 3ware RAID controller, but you should replace the battery pack if the temperature warning persists and is not due to environmental reasons.

004B Battery temperature is high

Event Type

Error

Cause

The battery pack temperature being monitored by the Battery Backup Unit has risen above the acceptable range. However, the BBU is still able to backup the 3ware RAID controller.

Action

Check for sufficient airflow around the card. To increase airflow you can:

- Leave the PCI slots next to the controller empty
- Add fans to your computer case
- Move and bundle wiring that is blocking air circulation

The Battery Backup Unit is presently still able to backup the 3ware RAID controller, but you should replace the battery pack if the temperature warning persists.

Contact 3ware technical support at <http://www.3ware.com/support/index.asp> if this problem is not due to environmental reasons or improper case cooling.

004C Battery temperature is too low**Event Type**

Error

Cause

The battery pack temperature being monitored by the Battery Backup Unit is too low.

The BBU is unable to backup the 3ware RAID controller.

Action

Contact 3ware technical support at <http://www.3ware.com/support/index.asp>.

The battery pack must be replaced if the problem persists and is not due to environmental reasons.

004D Battery temperature is too high**Event Type**

Error

Cause

The battery pack temperature being monitored by the Battery Backup Unit is too high.

The BBU is unable to backup the 3ware RAID controller.

Action

Check for sufficient airflow around the card. To increase airflow you can:

- Leave the PCI slots next to the controller empty
- Add fans to your computer case
- Move and bundle wiring that is blocking air circulation

Contact 3ware technical support at <http://www.3ware.com/support/index.asp> if this problem is not due to environmental reasons or improper case cooling.

004E Battery capacity test started

Event Type

Information

Cause

A battery test was started through CLI or 3DM.

Background Information

The test estimates how many hours the Battery Backup Unit will be able to back up the 3ware RAID controller in case of a power failure.

This test performs a full battery charge/discharge/re-charge cycle and may take up to 20 hours to complete. During this test the Battery Backup Unit cannot backup the 3ware RAID controller. In addition, all units have their write cache disabled until the test completes.

Action

None required.

See Also

See the Install Guide for your controller.

004F Cache synchronization skipped

Event Type

Warning

Cause

The cache synchronization that is normally performed when power is restored after a power failure was skipped and write data is still being backed up in the controller cache. This can occur if a unit was physically removed or became inoperable during the power outage.

Action

Return missing drive(s) to the controller so that the missing write data can be saved.

0050 Battery capacity test completed

Event Type

Information

Cause

The Battery Backup Unit has completed a battery capacity test.

The BBU is again able to backup the 3ware RAID controller and write cache has been re-enabled for all units. (During the test, backup and write cache were disabled).

0051 Battery health check started

Event Type

Information

Cause

The Battery Backup Unit periodically evaluates the health of the battery and its ability to backup the 3ware RAID controller in case of a power failure. This health check has started.

0052 Battery health check completed

Event Type

Information

Cause

The Battery Backup Unit evaluates periodically the health of the battery and its ability to backup the 3ware RAID controller in case of a power failure. This message is posted to the host when this health check has completed.

0053 Battery capacity test is overdue

Event Type

Information

Cause

There has not been a battery capacity test run in the last 6 months, which is the maximum recommended interval. This message will be sent once every week until the test is run.

Action

AMCC recommends running the test at least once every 6 months, if the measured battery capacity is longer than 120 hours. If the measured battery capacity is less than 120 hours the recommended test interval is 4 weeks.

0055 Battery charging started

Event Type

Information

Cause

The Battery Backup Unit has started a battery charge cycle.

Action

None required

0056 Battery charging completed

Event Type

Information

Cause

The Battery Backup Unit has completed a battery charge cycle.

0057 Battery charging fault

Event Type

Error

Cause

The Battery Backup Unit has detected a battery fault during a charge cycle. The Battery Backup Unit is not ready and is unable to backup the 3ware RAID controller.

Action

Replace the battery pack.

See Also

See the Install Guide for your controller

0058 Battery capacity is below warning level

Event Type

Information

Cause

The measured capacity of the battery is below the warning level. The Battery Backup Unit is presently still able to backup the 3ware RAID controller, but it is weakening.

Action

Replace the battery pack if the warnings persist.

See Also

See the Install Guide for your controller.

0059 Battery capacity is below error level

Event Type

Error

Cause

The measured capacity of the battery is below the error level. The Battery Backup Unit is not ready and is unable to backup the 3ware RAID controller.

Action

Replace the battery pack.

See Also

See the Install Guide for your controller.

005A Battery is present

Event Type

Information

Cause

A battery pack is connected to the 3ware RAID controller.

005B Battery is not present

Event Type

Error

Cause

The battery pack has been removed from the 3ware RAID controller.

Action

Reinstall the battery pack

005C Battery is weak

Event Type

Warning

Cause

The Battery Backup Unit periodically evaluates the health of the battery and its ability to backup the 3ware RAID controller in case of a power failure. This message is posted when the result of the health test is below the warning threshold.

Action

Replace the battery pack if warnings persist.

005D Battery health check failed

Event Type

Error

Cause

The Battery Backup Unit is not able to backup the 3ware RAID controller.

The Battery Backup Unit periodically evaluates the health of the battery and its ability to backup the 3ware RAID controller in case of a power failure. This message is posted when the result of the health test is below the fault threshold.

Action

Replace the battery pack. The BBU cannot presently backup the controller.

005E Cache synchronization completed

Event Type

Information

Cause

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

You will also see this message if drive insertion causes a unit to become operational and retained write cache data was flushed.

005F Cache synchronization failed; some data lost

Event Type

Error

Cause

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

Appendices

The following information is available in the appendices:

- Appendix A, “Glossary” on page 159
- Appendix B, “Driver and Software Installation” on page 165
- Appendix C, “Compliance and Conformity Statements” on page 173
- Appendix D, “Warranty, Technical Support, and Service” on page 175

Glossary

- **3DM 2.** 3ware Disk Manager. The 3ware disk manager is a web-based graphical user interface that can be used to view, maintain, and manage 3ware controllers, disks, and units. It is available on the 3ware CD that came with your controller and can be downloaded from <http://www.3ware.com/support/download.asp>.
- **3ware.** Named after the 3 computer wares: hardware, software and firmware. A leading brand of high-performance, high-capacity Serial ATA (SATA) RAID storage solutions.
- **3ware Sidecar.** An external enclosure (or chassis) for use with a 3ware RAID controller. The 3ware Sidecar can hold up to 4 drives.
- **A-Chip.** AccerATA chip. Automated data port to handle asynchronous ATA disk drive interface.
- **AMCC.** Applied Micro Circuits Corporation provides the essential building blocks for the processing, moving and storing of information worldwide.
- **Array.** One or more disk drives that appear to the operating system as a single unit. Within 3ware software, arrays are typically referred to as units.
- **Background rebuild rate.** The rate at which a particular controller initializes, rebuilds, and verifies redundant units (RAID 1, RAID 5, RAID 10).
- **Carve size.** The size over which a unit will be divided into volumes, if auto-carving is enabled.
- **Chassis Control Unit (CCU).** A device within a chassis (or enclosure) used to identify a drive or display status of a RAID unit by flashing the appropriate LEDs.
- **CLI.** Command Line Interface. The 3ware CLI is a text program, rather than a GUI (graphical user interface). It has the same functionality as 3DM, and can be used to view, maintain, and manage 3ware controllers, disks, and units.
- **Configuration.** The RAID level set for a unit.

- **Controller.** The physical card from 3ware that you insert into a computer system and connect to your 3ware Sidecar. The controller contains firmware that provides RAID functionality. 3ware makes a number of different models of SATA RAID controllers.
- **Controller ID number.** Unique number assigned to every 3ware controller in a system, starting with zero.
- **Create an array.** The process of selecting individual disk drives and selecting a RAID level. The array will appear to the operating system as a single unit. Overwrites any existing unit configuration data on the drives. Note that in 3ware software tools, arrays are referred to as units.
- **DCB.** Disk configuration block. This is 3ware proprietary RAID table information that is written to disk drives that are in a RAID unit, single disk, or spare. The DCB includes information on the unit type, unit members, RAID level, and other important RAID information.
- **Delete an array.** Deleting an array (or unit) is the process of returning the drives in a unit to individual drives. This erases the DCB information from the drives and deletes any data that was on them. When a unit is deleted from a controller, it is sometimes referred to as being “destroyed.” If you want to remove a unit without deleting the data on it, do not delete it; instead use the Remove feature in 3DM, and then physically remove the drives.
- **Destroying.** Same as deleting a unit.
- **Degraded unit.** A redundant unit that contains a drive that has failed.
- **Disk roaming.** When moving a unit from one controller to another, refers to putting disks back in a different order than they initially occupied, without harm to the data.
- **Distributed parity.** Parity (error correction code) data is distributed across several drives in RAID 5, configurations. Distributing parity data across drives provides both protection of data and good performance.
- **Drive ID.** A unique identifier for a specific drive in a system. Also called a port ID.
- **Drive Number.** The SCSI number, or channel number, of a particular drive.
- **ECC.** Error correction code. ECC Errors are grown defects that have occurred on a drive since it was last read.
- **ECC Error policy.** Determines whether an error detected during a rebuild stops the rebuild or whether the rebuild can continue in spite of the error. Specified by the Continue on Source Error During Rebuild unit policy.
- **EMS (Enclosure Management Services).** Chassis-monitoring functions for environmental, power, mechanical monitoring, and control using the I²C (chassis control) 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.
 - **Fault tolerant.** A RAID unit which provides the ability to recover from a failed drive, either because the data is duplicated (as when drives are mirrored) or because of error checking (as in a RAID 5 unit).
 - **Firmware.** Computer programming instructions that are stored in a read-only memory on the controller rather than being implemented through software.
 - **Grown defect.** Defects that arise on a disk from daily use.
 - **Hot spare.** A drive that is available, online, and designated as a spare. When a drive fails in a redundant unit, causing the unit to become degraded, a hot spare can replace the failed drive automatically and the unit will be rebuilt.
 - **Hot swapping.** The process of removing a disk drive from the system while the power is on. Hot swapping can be used to remove units with data on them, when they are installed in hot-swap carriers. 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.** For 3ware SATA RAID controllers, initialize means to put the redundant data on the drives of redundant units into a known state so that data can be recovered in the event of a disk drive failure. For RAID 1 and 10, initialization copies the data from the lower port to the higher port. For RAID 5, initialization calculates the RAID 5 parity and writes it to disk (background initialization). This is sometimes referred to as *resynching*, and does not erase user data.
 - **Logical Units.** This term is used in the 3ware CLI. It is usually shortened to “units.” These are block devices presented to the operating system. A logical unit can be a one-tier, two-tier, or three-tier arrangement. Spare, and Single logical units are examples of one-tier units. RAID 1, RAID 5, and RAID 6 are examples of two-tier units and as such will have sub-units. RAID 10 is an example of a three-tier unit and as such will have sub-sub-units.

- **Migration.** The process of changing the characteristics of a unit. The change can be to expand the capacity of the unit (OCE), change the stripe size of the unit, change the unit from redundant to non-redundant, change the unit from non-redundant to redundant, and to change the unit from one type of redundant unit to another type of redundant unit (for example RAID 1 to RAID 5).
- **Mirrored disk array (unit).** A pair of drives on which the same data is written, so that each provides a backup for the other. If one drive fails, the data is preserved on the paired drive. Mirrored disk units include RAID 1 and RAID 10.
- **NCQ (Native Command Queuing).** A feature designed to improve performance of SATA hard disks in some applications that require a lot of random access of data, such as server-type applications. When NCQ is enabled, the commands are reordered on the drive itself.

NCQ must be supported by the drive. NCQ must be turned on in both the drive and the RAID controller. By default, the RAID unit's queue policy is disabled when creating a unit.
- **Non-redundant units.** A disk array (unit) 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 unit. See also *migration*.
- **Parity.** Information that the controller calculates using an exclusive OR (XOR) algorithm and writes to the disk drives in RAID 5, 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.** A controller has one or many ports. Each port can be attached to a single disk drive. On a controller with a Multi-lane serial port connector, one connector supports four ports.
- **Port ID.** A unique identifier for a specific port in a system. Also called a drive ID.
- **RAID.** Redundant array of inexpensive disks, combined into a unit (array), to increase your storage system's performance and provide fault tolerance (protection against data loss).
- **Rebuild task schedule.** The specification for when rebuilding, may occur, including start time and duration.

-
- **Rebuild a unit.** To generate data on a new drive after it is put into service to replace a failed drive in a fault tolerant unit (for example, RAID 1, 10, or 5).
 - **Redundancy.** Duplication of data on another drive or drives, so that it is protected in the event of a drive failure.
 - **Remove a drive.** The process of making a drive unavailable to the controller.
 - **Remove a unit.** The process of making a unit unavailable to the controller and the operating system. After a unit is removed it can be hot swapped out of the system. This is sometimes referred to as exporting a unit.
 - **RLM (RAID Level Migration).** The process of using an existing unit of one or more drives and converting it to a new RAID type without having to delete the original unit. For example, converting a single disk to a mirrored disk or converting a RAID 0 unit to a RAID 5 unit.
 - **Self-test.** A test that can be performed on a scheduled basis. Available self-tests include Upgrade UDMA mode and Check SMART Thresholds.
 - **Stagger time.** The delay between drive groups that will spin up, at one time, on a particular controller.
 - **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 stripe sizes are better for random I/O (such as databases). The stripe size is user-configurable at 64KB, 128KB, or 256KB.

This stripe size is sometimes referred as a “minor” stripe size. A major stripe size is equal to the minor stripe size times the number of disks in the unit.

- **Striping.** The process of breaking up files into smaller sizes and distributing the data amongst two or more drives. Since smaller amounts of data are written to multiple disk drives simultaneously, this results in an increase in performance. Striping occurs in RAID 0, 5, and 10.
- **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 1.5Gb/sec and 3.0 Gb/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, a verify will calculate RAID 5 parity and compare it to what is written on the disk drive.

Driver and Software Installation

This appendix provides detailed instructions for installing the 3ware driver and software for the 9650SE-4LPME and the 9590SE-4ME on your Apple Mac Pro or Power Mac G5.

You can install all software at once, or you can use the installer to install specific components.

If you install the disk management tool 3DM 2, you will be asked to specify some settings, such as email notifications and security settings. All of these settings can be modified later from the 3DM 2 software. You do not have to complete them at this time.

For help uninstalling the software, see “Uninstalling 3DM on the Macintosh” on page 172.

To install the driver and disk management tools

- 1 With your computer on, insert the 3ware CD that came in your 3ware Sidecar Kit.
- 2 When the 3wareCD window opens, double-click on the file `StartInstallMac` to launch the installer.

When prompted, enter your Macintosh Admin user name and password and click **OK** to start the installer.

Figure 49. Authenticate dialog requests user name and password



The installer will start and the welcome screen appears.

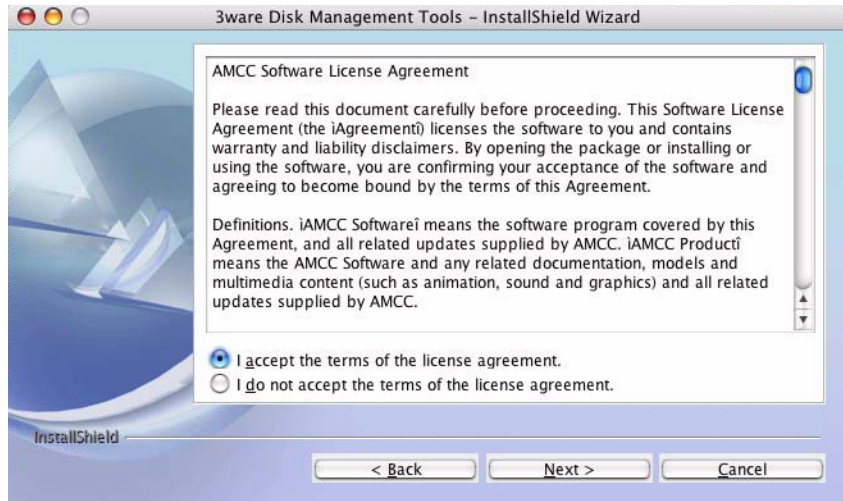
- 3 From the Welcome screen, click **Next** to start the installation process.

Figure 50. Welcome Installation Screen



- 4 On the License Agreement page, accept the agreement and click **Next**.

Figure 51. License Agreement Screen



- 5 If you want to change where the 3ware Disk Management tools 3DM and CLI will be installed, you can change the path and directory.

When you are ready, click **Next**.

Figure 52. Specify Directory Path Screen



- 6 Select what components you want to install and click **Next**.

3DM and CLI are applications that let you set up and manage RAID units. 3DM is browser-based; CLI is a command line interface.

The Firmware Upgrade Utility lets you update the firmware on your controller, if required.

The AMCC 3ware 9000 driver tells your operating system how to interact with the 3ware RAID controller. (Installing the driver will require that you restart your computer.)

The 3ware Documentation option installs the 3ware HTML Bookshelf on your computer. This is an HTML version of the User Guide and CLI Guide.

Figure 53. Select Components to Install Screen



- 7 To configure email notification, check the box and complete the 3DM 2 Email Configuration screen.

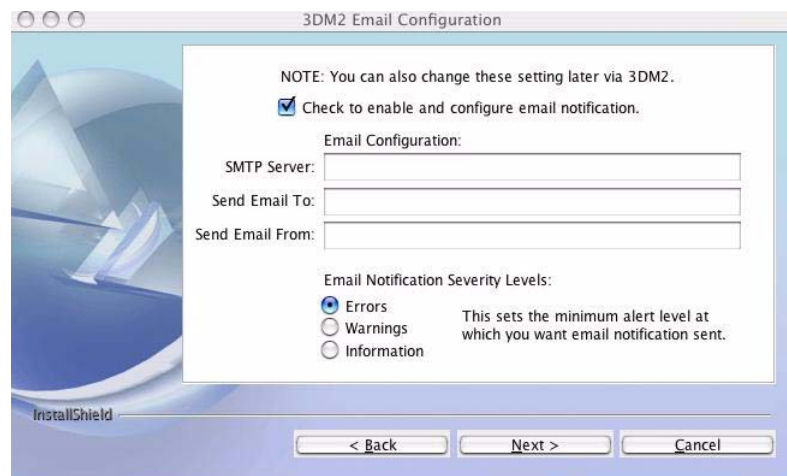
This features allows you to receive notification of problems with your 3ware RAID controller and units. For details about completing these fields, see “Managing E-mail Event Notification” on page 24.

You can select what level of notifications you want to be emailed about.

- **Errors.** You will be notified of Errors only.
- **Warnings.** You will be notified of Warnings and Errors.
- **Information.** You will be notified of Information, Warnings, and Errors.

When you are ready, click **Next** to continue.

Figure 54. 3DM2 Email Configuration Screen

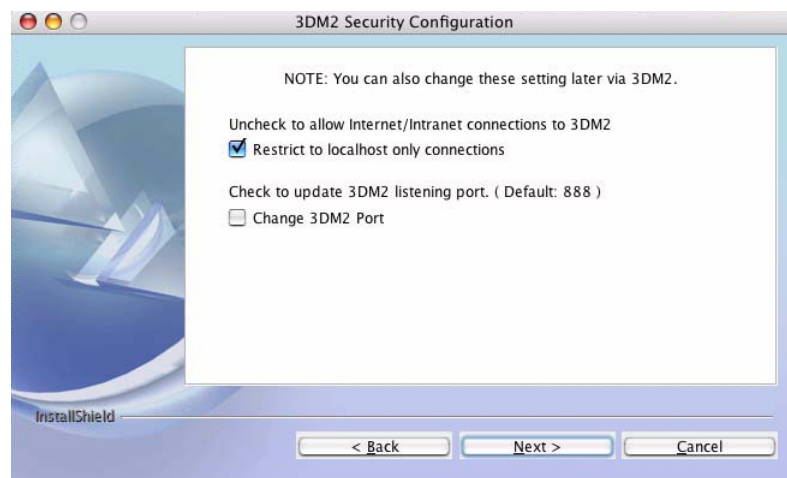


- 8 [Optional] On the 3DM 2 Security Configuration screen, specify whether you want to restrict access to localhost connections.

Enabling this feature prevents people from checking the status and administering the controller from across the internet or intranet.

If you want to allow people to remotely administer the controller, uncheck this box. For more information, see “Enabling and Disabling Remote Access” on page 25.

Figure 55. 3DM2 Security Configuration Screen

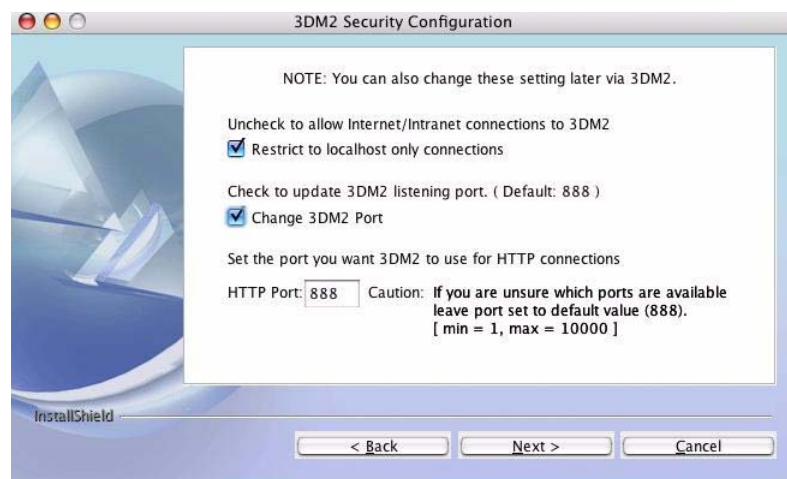


- 9 [Optional] On the same 3DM 2 Security Configuration screen, you can specify a different listening port than the default (888), if appropriate.

For more about this feature, see “Setting the Incoming Port #” on page 26.

When you are ready, click **Next** to continue.

Figure 56. 3DM2 Specify Listening Port



- 10 If you want the Installation Wizard to launch 3DM 2 after you finish the wizard, check the **Connect to 3DM2** box. This allows you to log into 3DM and configure a RAID unit right away.

If you do not want to launch 3DM 2 at this time, leave the box unchecked.

When you are ready, click **Next** to continue.

Figure 57. Final Installation Screen



- 11 On the summary screen, review the installation that is about to occur.

If you want to make changes, use the **Back** button to move back through the screens.

When you are ready, click **Install** to continue.

Figure 58. Installation Summary Screen



- 12 When the final installation screen lets you know that installation is complete, click **Finish**.

Figure 59. Final Installation Screen



You will be prompted to restart your computer in order for the driver to be used with your 3ware RAID controller.

- 13 Restart your Macintosh to load the driver.

Note: If you have not yet installed your 3ware controller and set up your 3ware Sidecar, you do not need to restart your computer at this time. Instead, power down your Macintosh and turn to the Installation Guide that came with your 3ware Sidecar Kit.

Uninstalling 3DM on the Macintosh

You can remove 3DM from your Macintosh by using the uninstall command located in the AMCC folder.



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

To uninstall 3DM

- 1 In the Finder, open **Applications > AMCC**.
- 2 Double-click **StartUninstall**.
- 3 If prompted, enter your administrator password.
- 4 When the uninstaller screen prompts you to select items to be uninstalled, select 3DM2 and click **Uninstall**.

The uninstaller will remove 3DM from your computer.

Compliance and Conformity Statements

This section is organized into the following topics:

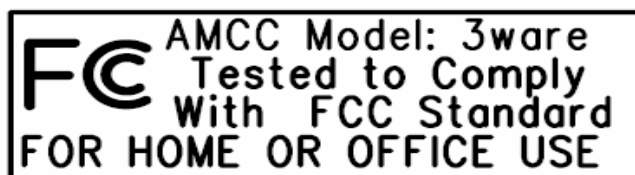
- FCC Radio Frequency Interference Statement
- European Community Conformity Statement

FCC Radio Frequency Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC (Federal Communications Commission) Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

To maintain compliance with FCC radio frequency emission limits, use shielded cables and connectors between all parts of the computer system.



European Community Conformity Statement

The Controller Models 9650SE-4LPME and 9590SE-4ME are in conformity with the following Common Technical Regulations and/or normative documents:

- EN 55022** Limits and methods of measurements of radio interference characteristics of information technology equipment
- EN 61000-4-2** Electromagnetic compatibility (EMC) Part 4: Testing and measurement techniques Section 2: Electrostatic discharge immunity test
- EN 61000-4-3** Electromagnetic compatibility (EMC) Part 4: Testing and measurement techniques Section 3: Radiated, Radio-Frequency, Electromagnetic Field Immunity Test
- EN 61000-4-4** Electromagnetic compatibility (EMC) Part 4: Testing and measurement techniques Section 4: Electrical fast transient/burst immunity test
- EN 60950** Safety of information technology equipment, including electrical business equipment following the provisions of the Electromagnetic Compatibility Directive 89/23/EEC Low Voltage Directive



Warranty, Technical Support, and Service

This section is organized into the following topics:

- Limited Warranty
- Warranty Service and RMA Process
- AMCC Technical Support and Services
- Sales and ordering information
- Feedback on this manual

Limited Warranty

RAID Controller Hardware. 3-Year Hardware Warranty: AMCC warrants this product against defects in material and workmanship for a period of thirty-six (36) months from the date of original purchase. AMCC, at no charge and at its option, will repair or replace any part of this product which proves defective by reason of improper workmanship or materials. Repair parts or replacement products will be provided by AMCC on an exchange basis and will be either new or refurbished to be functionally equivalent to new. Products or parts replaced under this provision shall become the property of AMCC.

3ware Sidecar Hardware. 1-Year Hardware Warranty: AMCC warrants this product against defects in material and workmanship for a period of twelve (12) months from the date of original purchase. AMCC, at no charge and at its option, will repair or replace any part of this product which proves defective by reason of improper workmanship or materials. Repair parts or replacement products will be provided by AMCC on an exchange basis and will be either new or refurbished to be functionally equivalent to new. Products or parts replaced under this provision shall become the property of AMCC.

Software Warranty: AMCC will replace a defective media purchased with this product for a period of up to 30 days from the date of purchase.

AMCC warranty service is provided by returning the defective product to AMCC.

Exclusions

This warranty does not cover any damage to this product which results from accident, abuse, misuse, natural or personal disaster, or any unauthorized disassembly, repair or modification. AMCC shall not be liable for any incidental or consequential damages, including but not limited to loss of profits, other loss, damage or expense directly or indirectly arising from the customer's misuse of or inability to use the product, either separately or in combination with other equipment, regardless of whether AMCC has been advised of the possibility of such damages. AMCC is not liable for and does not cover under warranty, any costs associated with servicing and/or the installation of AMCC products. This warranty sets for the entire liability and obligations of AMCC with respect to breach of warranty and the warranties set forth or limited herein are the sole warranties and are in lieu of all other warranties, expressed or implied, including warranties or fitness for particular purpose and merchantability.

State Law Provisions

This warranty gives you specific legal rights and you may have other rights which vary from state to state. Some states do not allow the exclusion of incidental or consequential damages or allow limitation of implied warranties or their duration, so that the above exclusions or limitations may not apply.

Warranty Service and RMA Process

To obtain warranty service during the warranty period, register at the 3ware website and submit an RMA request online at <https://www.3ware.com>.

You will be issued a return material authorization (RMA) number. AMCC will send a replacement in approximately two business days after receipt of the defective unit (transit time not included).

Advanced replacement is available with a credit card number with authorization in the amount equaling the then current list price of the 3ware Serial ATA RAID Controller, including shipping costs. As soon as practicable thereafter, AMCC will ship the advanced replacement to you at the address of your choosing. Upon receipt of the advanced replacement, we ask that you immediately ship the defective AMCC 3ware Serial ATA RAID Controller to AMCC, RAID Products RMA DEPT, 6290 Sequence Drive, San Diego, CA 92121. If AMCC receives the defective AMCC 3ware Serial ATA RAID Controller from you within thirty (30) days of the date of shipment of the advanced replacement, AMCC will destroy your credit card authorization and you will not be charged for the advanced replacement.

Please use the original packing material contents of the box when exchanging or returning a product.

For information about the status of a replacement, please contact AMCC Technical Support.

AMCC Technical Support and Services

Product information, Frequently Asked Questions, software upgrades, driver files and other support are available through the AMCC World Wide Web site at <http://www.3ware.com>. AMCC's 3ware software library is accessible at: <http://www.3ware.com/support/download.asp>

Web-based software downloads feature upgrading multiple switches simultaneously.

For specific answers to questions or to give feedback about the product, visit our Web site at <http://www.3ware.com/support> and use our convenient e-mail form. AMCC also offers toll-free 1 (800) 840-6055 or 1 (408) 542-8800 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 using the email form at <http://www.3ware.com/support>.

Index

Numerics

3DM

- 3DM menus 20
 - Alarms page 109
 - Battery Backup Information page 110
 - browser requirements 15
 - Controller Details page 90
 - Controller Settings page 96
 - Controller Summary page 89
 - Disk Management Utility Overview 14
 - Drive Details page 95
 - Drive Information page 93
 - enabling remote access 25
 - Enclosure Details page (3DM) 113
 - Enclosure Summary page (3DM) 112
 - installation 165
 - main 3DM screen 19
 - Maintenance page 102
 - managing email event notification 24
 - page refresh frequency 26
 - passwords 24
 - preferences 23
 - remote access, enabling 25
 - Scheduling page 100
 - setting incoming port number 26
 - Settings page 114
 - SMART Details page 95
 - starting 15
 - Unit Details page 92
 - Unit Information page 91
- 3ware HTML Bookshelf viii
- 3ware Sidecar LED status indicators 63

A

A-Chip

- definition 159

AEN

- Backup DCB read error detected (0043) 147
- Battery capacity is below error level (0059) 155
- Battery capacity is below warning level (0058) 155
- Battery capacity test completed (0050) 153
- Battery capacity test is overdue (0053) 154
- Battery capacity test started (004E) 152
- Battery charging completed (0056) 154
- Battery charging fault (0057) 155
- Battery charging started (0055) 154
- Battery health check completed (0052) 153

- Battery health check failed (005D) 157
- Battery health check started (0051) 153
- Battery is not present (005B) 156
- Battery is present (005A) 156
- Battery is weak (005C) 156
- Battery temperature is high (004B) 150
- Battery temperature is low (004A) 150
- Battery temperature is normal (0049) 150
- Battery temperature is too high (004D) 151
- Battery temperature is too low (004C) 151
- Battery voltage is high (0046) 148
- Battery voltage is low (0045) 148
- Battery voltage is normal (0044) 148
- Battery voltage is too high (0048) 149
- Battery voltage is too low (0047) 149
- Buffer ECC error corrected (0039) 143
- Buffer integrity test failed (0024) 133
- Cache flush failed, some data lost (0025) 134
- Cache synchronization completed (005E) 157
- Cache synchronization failed 157
- Cache synchronization skipped (004F) 152
- Controller error occurred (0003) 124
- Controller reset occurred (1001) 123
- DCB checksum error detected (0027) 135
- DCB version unsupported (0028) 135
- Degraded unit (0002) 123
- Downgrade UDMA (0021) 131
- Drive ECC error reported (0026) 134
- Drive error detected (000A) 127
- Drive inserted (001A) 130
- Drive not supported (0030) 139
- Drive power on reset detected (003A) 143
- Drive removed (0019) 130
- Drive timeout detected (0009) 126
- Flash file system error detected (003F) 146
- Flash file system repaired (0040) 146
- Incomplete unit detected (0006) 125
- Initialize completed (0007) 126
- Initialize failed (000E) 128
- Initialize paused (003C) 144
- Initialize started (000C) 128
- Migration completed (0035) 141
- Migration failed (0034) 141
- Migration paused (003E) 145
- Migration started (0033) 140
- Primary DCB read error occurred (0042) 147
- Rebuild completed (0005) 125
- Rebuild failed (0004) 124
- Rebuild paused (003B) 144
- Rebuild started (000B) 128

Replacement drive capacity too small (002E) 139
 Sector repair completed (0023) 132
 SO-DIMM not compatible (0037) 142
 SO-DIMM not detected (0038) 142
 Source drive ECC error overwritten(002C) 137
 Source drive error occurred(002D) 138
 Spare capacity too small for some units (0032) 140
 Unclean shutdown detected (0008) 126
 Unit inoperable (001E) 130
 Unit number assignments lost (0041) 147
 Unit Operational (001F) 131
 Upgrade UDMA mode (0022) 132
 Verify completed(002B) 137
 Verify failed (002A) 136
 Verify fixed data/parity mismatch (0036) 142
 Verify not started, unit never initialized (002F) 139
 Verify paused (003D) 145
 Verify started (0029) 136
 AEN messages 66, 109, 119
 alarms 66
 viewing 66
 Alarms page, 3DM 109
 arrays 6
 array roaming 55, 56
 definition 159
 moving from one controller to another 56
 removing in 3DM 55
 asterisk next to unit 92, 93
 Auto Rebuild policy 13, 29
 setting 30, 98
 Auto Verify policy for units 97
 setting (3DM) 44
 auto-carving 31
 auto-carving policy 29
 auto-carving policy
 setting 99
 available drives, 3DM 107

B

Back button in Safari 5
 background initialization after power failure 70
 background tasks
 background rebuild rate (definition) 159
 background task rate 97
 background task rate, setting 75
 definition 12
 initialization 69
 overview 68
 prioritizing 76
 rebuilding a unit 73
 scheduling 76
 verification 70
 Backup DCB read error detected (0043) 147
 Battery capacity is below error level (0059) 155
 Battery capacity is below warning level (0058) 155
 Battery capacity test completed (0050) 153
 Battery capacity test is overdue (0053) 154
 Battery capacity test started (004E) 152
 Battery charging completed (0056) 154
 Battery charging fault (0057) 155
 Battery charging started (0055) 154
 Battery health check completed (0052) 153
 Battery health check failed (005D) 157
 Battery health check started (0051) 153
 Battery is not present (005B) 156
 Battery is present (005A) 156
 Battery is weak (005C) 156
 Battery temperature is high (004B) 150
 Battery temperature is low (004A) 150
 Battery temperature is normal (0049) 150
 Battery temperature is too high (004D) 151
 Battery temperature is too low (004C) 151
 Battery voltage is high (0046) 148
 Battery voltage is low (0045) 148
 Battery voltage is normal (0044) 148
 Battery voltage is too high (0048) 149
 Battery voltage is too low (0047) 149
 BBU
 Battery Backup Information page 110
 testing battery capacity 86
 viewing battery information 85

BIOS
 showing version 90
 blinking LEDs (drive locate) 81, 92, 94, 113
 browser requirements, 3DM 15
 Buffer ECC error corrected (0039) 143
 Buffer integrity test failed (0024) 133

C

Cache flush failed, some data lost (0025) 134
 Cache synchronization completed (005E) 157
 Cache synchronization failed 157
 Cache synchronization skipped (004F) 152
 cancel rebuild 75
 carve size 29
 setting 32, 99
 certificate message when starting 3DM 16
CLI
 definition 159
 installation 165
 Compliance and Conformity 173
 configuration
 changing 48
 controller 27
 definition 159
 unit 33
 configuring
 a controller 27
 units 33
 Continue on Source Error During Rebuild 97

- setting as a unit policy 45
- controller
 - controller ID number (definition) 160
 - controller information, viewing 27
 - controller policies
 - overview 29
 - viewing 29
 - definition 160
 - moving unit to another 56
 - rescanning 58
 - status 89
 - updating firmware 85
- Controller Details page, 3DM 90
- Controller error occurred (0003) 124
- Controller reset occurred (0001) 123
- Controller Settings page, 3DM 96
- Controller Summary page, 3DM 89
- conventions
 - in the user guide vii
- creating a unit
 - configuration options 33
 - definition 160
 - in 3DM 35
 - introduction 33
- current controller (definition) 21
- customer support
 - contacting 118, 177

D

- DCB checksum error detected (0027) 135
- DCB version unsupported (0028) 135
- DCB, definition 160
- Degraded (unit status) 64
- degraded unit
 - about 65
 - definition 160
- Degraded unit (0002) 123
- delay between spin-up policy (viewing in 3DM) 99
- deleting a unit 53
 - 3DM 106
 - definition 160
- destroy unit (definition) 160
- Disk Manager, using 14
- distributed parity 6
- Downgrade UDMA mode (0021) 131
- drive
 - adding in 3DM 56
 - capacity considerations 10
 - checking status in 3DM 60
 - coercion 11
 - drive ID (definition) 160
 - drive number (definition) 160
 - locate by blinking 81
 - removing in 3DM 57
 - status, viewing (3DM) 60

- statuses 64
 - types 5
 - viewing SMART data 67
- Drive Details page, 3DM 95
- Drive ECC error reported (0026) 134
- Drive error detected (000A) 127
- Drive Information page, 3DM 93
- Drive inserted (001A) 130
- drive locate 13, 92, 94, 113
- Drive not supported (0030) 139
- Drive power on reset detected (003A) 143
- Drive removed (0019) 130
- Drive timeout detected (0009) 126
- driver
 - current version, determining 83
 - installation 165
- drives per spin-up policy 99
- dynamic sector repair 72, 133

E

- ECC
 - definition 160
 - ECC error policy (definition) 160
- e-mail event notification, managing in 3DM 24, 115
- enclosure
 - blinking LEDs 81
 - detail information 113
 - LED status indicators 63
 - summary information 112
- Enclosure Details page (3DM) 113
- Enclosure Management Services (EMS),
 - definition 160
- Enclosure Summary page (3DM) 112
- errors 66
 - error correction 12
 - error log, downloading 67
 - error messages 119
 - how handled by verification process 72
 - viewing 67
- European Community Conformity statement 174
- events (see also errors and alarms) 66
- export a unit
 - definition 161
- Export JBOD policy
 - viewing in 3DM 99

F

- fault tolerant
 - definition 161
- FCC Radio Frequency Interference Statement 173
- firmware
 - definition 161
 - showing version 89, 90
 - updating 85
- Flash file system error detected (003F) 146

Flash file system repaired (0040) 146
FUA (Force Unit Access) commands, part of
StorSave profile 47

G

grown defect, definition 161

H

hot spare 9
 creating 40
 hot spare (definition) 161
hot swap 6
hot swap (definition) 161
HTTP port number for 3DM 116

I

identify
 drive by blinking LED 92, 94
 identify checkbox in 3DM 92, 94
 slot by blinking LED 113
 unit by blinking (3DM) 82
identify checkbox in 3DM 113
import a unit
 definition 161
incoming port number, 3DM 26
Incomplete unit detected (0006) 125
initialization
 about 69
 background initialization after power failure 70
 definition 161
 RAID 0 units 69
 RAID 1 units 70
 RAID 10 units 70
 RAID 5 units 69
 RAID 50 units 69
Initialize completed (0007) 126
Initialize failed (000E) 128
Initialize paused (003C) 144
Initialize started (000C) 128
Initializing (unit status) 63, 64
Inoperable (unit status) 64
inoperable units (about) 65
installation
 driver and disk management tools (3DM2 and
 CLI) 165
 of controller 1
Inter-IC bus, definition 161

J

JBOD policy (viewing in 3DM) 99

L

LEDs
 colors and behavior 63
 indicators 63

listening port for 3DM 116
logging in to 3DM 16
logical unit
 definition 161

M

main screen, 3DM 19
maintaining units 60
Maintenance page, 3DM 102
media scans
 (verification of non-redundant units) 71
menus, 3DM 20
message url http
 //www.3ware.com/KB/article.aspx?id=12278 118,
 124
 //www.3ware.com/support/index.asp 124, 141, 143,
 147, 151, 152
messages, error 119
Migrate-Paused (unit status) 64
Migrating (unit status) 64
migrating a unit 49, 105
 definition 162
Migration completed (0035) 141
Migration failed (0034) 141
Migration paused (003E) 145
Migration started (0033) 140
mirrored disk array
 definition 6, 162
 RAID 1 7
Multi LUN support (auto-carving) 29, 31
multiple volumes in one unit 31

N

name of unit 34, 91
 assigning 41, 98
NCQ (native command queuing)
 definition 162
 NCQ policy 98
non-redundant units
 definition 162

O

Online Capacity Expansion (OCE), definition 162
operating systems
 informing of changed configuration 52
operating systems supported 5
Other Controller Settings, 3DM 98

P

page refresh
 3DM 116
 frequency, 3DM 26
parity
 definition 162
 distributed 6

- partitioning and formatting units 37
- passwords, 3DM 24, 115
- PCB (definition) 162
- P-Chip (definition) 162
- policies
 - controller 29
 - initial settings 2
 - unit 42
 - units 97
- port
 - definition 162
- port ID (definition) 162
- preferences, 3DM 23
- Primary DCB read error occurred (0042) 147

Q

- queuing
 - enabling and disabling for a unit 46
 - Queuing policy (setting in 3DM) 98

R

- RAID
 - concepts and levels 6
 - configurations 7
 - determining level to use 10
 - RAID 0 7
 - RAID 1 7
 - RAID 10 9
 - RAID 5 8
- RAID Level Migration (RLM)
 - changing level 50
 - definition 163
 - overview 49
- Rebuild completed (0005) 125
- Rebuild failed (0004) 124
- Rebuild paused (003B) 144
- Rebuild started (000B) 128
- rebuild task schedule
 - adding (3DM) 79
 - removing (3DM) 79
 - viewing (3DM) 77
- rebuild task schedule (definition) 162
- Rebuilding (unit status) 63
- rebuilding a unit
 - 3DM 74, 105
 - about 73
 - cancelling and restarting 75
 - definition 163
 - introduction 73
- Rebuild-Paused (unit status) 63, 105
- redundancy
 - definition 163
- redundant units, about 71
- remote access
 - 3DM 116

- enabling in 3DM 25
- remote viewing of controllers through 3DM 18

- removing a drive 57
 - 3DM 104
 - definition 163
- removing a unit 55, 106
 - definition 163
- Replacement drive capacity too small (002E) 139
- rescan controller 58, 103
- roaming, array 55, 56

S

- scheduled background tasks 12
- scheduling
 - background tasks 76
 - prioritizing background tasks 76
 - task duration 77
- Scheduling page, 3DM 100
- Sector repair completed (0023) 132
- security certificate when starting 3DM 16
- self-tests
 - about 80, 101
 - definition 163
 - schedule
 - viewing (3DM) 77
 - schedule, adding (3DM) 79
 - schedule, removing (3DM) 79
 - selecting 80
- serial number
 - showing 89, 90
- Settings page, 3DM 114
- single disk 9
- SMART 66
 - data, viewing 67
 - monitoring 12
- SMART Details page, 3DM 95
- SO-DIMM not compatible (0037) 142
- SO-DIMM not detected (0038) 142
- software installation 165
- some data lost (005F) 157
- Source drive ECC error overwritten (002C) 137
- Source drive error occurred (002D) 138
- Spare capacity is too small for some units (0032) 140
- spin-up policy
 - delay between spin-ups (viewing in 3DM) 99
 - number of drives 99
- stagger time (definition) 163
- starting 3DM 15
- status
 - controller, viewing (3DM) 89
 - definitions
 - controller 89
 - drive 64
 - unit 63
 - drive, viewing (3DM) 60

- status LEDs 63
- unit, viewing (3DM) 60
- StorSave profile 13
 - setting 46, 98
- stripe size
 - changing 48
 - definition 163
- striping 6
 - definition 163
- subunit
 - definition 163
- system requirements 5

T

- task schedules
 - about, 3DM 101
 - adding 79
 - rebuild/migrate 79
 - removing 79
 - self-test 79
 - task duration 77
 - turning on and off 77, 78
 - verify 79
 - viewing 77
- technical support 175
 - contacting 118, 177
- troubleshooting 117
- TwinStor 9

U

- UDMA mode, definition 163
- ultra DMA protocol 132
- Unclean shutdown detected (0008) 126
- uninstalling 3DM on the Macintosh 172
- unit
 - checking status in 3DM 60
 - configuring 33
 - creating a unit
 - in 3DM 36
 - introduction 33
 - definition 6, 164
 - deleting a unit 53
 - in 3DM 53
 - expanding capacity 51
 - maintaining 60
 - moving from one controller to another 56
 - name 91, 98
 - naming 34, 41
 - partitioning and formatting 37
 - policies, setting 42, 97
 - rebuilding a unit 73
 - in 3DM 74
 - removing in 3DM 55
 - removing vs. deleting 55
 - statuses 63

- Unit Maintenance in 3DM 103
- unit number (definition) 163
- unit statuses 63
- verifying a unit 73
 - in 3DM 73
- volumes 93
- write cache, 3DM 97
- write cache, enabling and disabling 43
- Unit Details page, 3DM 92
- unit ID
 - definition 163
- Unit Information page, 3DM 91
- Unit inoperable (001E) 130
- Unit number assignments lost (0041) 147
- Unit Operational (001F) 131
- unit policies
 - enabling and disabling queuing for a unit 46
 - enabling and disabling write cache 43
 - overview 42
 - setting Auto Verify 44
 - setting Continue on Source Error During Rebuild 45
 - setting the StorSave policy 46
- updating
 - firmware 85
- Upgrade UDMA mode (0022) 132

V

- verification 12
 - about 70
 - error handling 72
 - media scans 71
 - non-redundant units 71
 - redundant units 71
- Verify completed(002B) 137
- Verify failed (002A) 136
- Verify fixed data/parity mismatch (0036) 142
- Verify not started, unit never initialized (002F) 139
- Verify paused (003D) 145
- Verify started (0029) 136
- verify task schedule
 - adding (3DM) 79
 - removing (3DM) 79
 - viewing (3DM) 77
- verifying
 - definition 164
- Verifying (unit status) 64
- verifying a unit 73, 105
 - Auto Verify policy 44
 - manually 73
 - stopping (3DM) 73
- Verify-Paused (unit status) 64, 105
- viewing 3DM remotely 18
- volumes
 - in a unit 93

multiple from one unit 31
resulting from auto-carvings 93

W

Warranty 175
write cache 12, 97
 disable on degrade, part of Storsave profile 48
 enabling in 3DM 43
write journaling, part of StorSave profile 47