## Revision History

<table>
<thead>
<tr>
<th>Revision</th>
<th>Revision Date</th>
<th>Details of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>August 2019</td>
<td>maxView Storage Manager v3.02.00</td>
</tr>
<tr>
<td>9</td>
<td>March 2019</td>
<td>maxView Storage Manager v3.01.00</td>
</tr>
<tr>
<td>8</td>
<td>January 2019</td>
<td>maxView Storage Manager v3.0.0</td>
</tr>
<tr>
<td>7</td>
<td>May 2018</td>
<td>Removed &quot;Proprietary and Confidential&quot; markings in footer text.</td>
</tr>
<tr>
<td>6</td>
<td>April 2018</td>
<td>maxView Storage Manager v2.06</td>
</tr>
<tr>
<td>5</td>
<td>September 2017</td>
<td>maxView Storage Manager v2.04</td>
</tr>
<tr>
<td>4</td>
<td>May 2017</td>
<td>maxView Storage Manager v2.03</td>
</tr>
<tr>
<td>3</td>
<td>September 2016</td>
<td>V1.2.0 Maintenance Release. maxView Storage Manager v2.02</td>
</tr>
<tr>
<td>2</td>
<td>April 2016</td>
<td>V1.1.0 Maintenance Release. maxView Storage Manager v2.01</td>
</tr>
<tr>
<td>1</td>
<td>December 2015</td>
<td>First Production release. maxView Storage Manager v2.00</td>
</tr>
</tbody>
</table>
Microsemi Adaptec® Product Support

If you have questions about installing or using your Microsemi Adaptec® product, check this document first—you will find answers to most of your questions. If you need further assistance, use the support options listed below. To expedite your service, have your computer in front of you.

Note: Please visit our Support site at start.microsemi.com for the most up to date contact information.

Self Help and Support in English

- Search the Microsemi Support Knowledgebase (ASK) at ask.microsemi.com for articles, troubleshooting tips, and frequently asked questions for your product.
- For support through email, submit your question at ask.microsemi.com.
- To contact Technical Support, visit our product support site at start.microsemi.com.

Technische Informationen und Support in Deutsch

- Suchen Sie in der Adaptec Support Knowledgebase (ASK) unter ask-de.microsemi.com nach Artikeln, Tipps zur Fehlerbehebung und häufig gestellten Fragen zu Ihrem Produkt.
- Support per Email erhalten Sie unter ask-de.microsemi.com.
- Um den Technischen Support zu kontaktieren, besuchen Sie uns bitte unter start.microsemi.com und klicken Sie auf „Support kontaktieren“, für Auswahlmöglichkeiten.

Техническая поддержка и информация на русском языке

- База знаний Microsemi (ASK) на сайте ask-ru.microsemi.com ask-ru.adaptec.com – статьи, советы по устранению неисправностей и часто задаваемые вопросы о Вашем продукте.
- Для поддержки по электронной почте отправьте Ваш запрос на сайте ask-ru.microsemi.com
- Для обращения в службу Технической Поддержки, пожалуйста, посетите наш web сайт start.microsemi.com и используйте ссылку "Contact Support".

日本語での技術情報とサポート

- ask.microsemi.co.jpのMicrosemi Support Knowledgebase (ASK)で、お使いの製品の情報トラブルシューティングのヒント、よくある質問を検索してください。
- Eメールでのサポートには ask.microsemi.co.jpから質問を送ってください。
- テクニカルサポートへコンタクトするには、弊社ウェブサイトstart.microsemi.comをご覧になり、"Contact Support"をクリックして下さい。
PLEASE READ CAREFULLY: THE USE OF THIS SOFTWARE IS SUBJECT TO THE SOFTWARE LICENSE TERMS OF MICROSEMI CORPORATION, AND OTHER LICENSORS WHOSE SOFTWARE MAY BE BUNDLED WITH THIS PRODUCT.

BY YOUR USE OF THE SOFTWARE INCLUDED WITH THIS PRODUCT YOU AGREE TO THE LICENSE TERMS REQUIRED BY THE LICENSOR OF THAT SOFTWARE, AS SET FORTH DURING THE INSTALLATION PROCESS. IF YOU DO NOT AGREE TO THE LICENSE TERMS APPLICABLE TO THE SOFTWARE, YOU MAY RETURN THE ENTIRE UNUSED PRODUCT FOR A FULL REFUND.

In return for acquiring a license to use the Microsemi software, which may include software from third party licensors and patches made available by Microsemi (“Software”), and the related documentation, you agree to the following terms and conditions:

1. License. This Agreement grants you, the Licensee, a license to:
   a. Use the Software on a single computer system, which is not intended for use by more than five (5) users; and:
   b. Make one copy of the Software in machine readable form solely for back-up purposes, provided you reproduce Microsemi’s copyright proprietary legends. Notwithstanding the foregoing, the Software may be used on the home, laptop or other secondary computer of the principal user of the Software, and an additional copy of the Software may be made to support such use. As used in this license, the Software is “in use” when it is either loaded into RAM or installed on a hard disk or other permanent memory device. The Software may be “in use” on only one computer at any given time. (Different license terms and fees are applicable for networked or multiple user applications.) As a specific condition of this license, you agree to use the Software in compliance with all applicable laws, including copyright laws, and that you will not copy, transmit, perform or distribute any audio or other content using the Software without obtaining all necessary licenses or permissions from the owner of the content.

2. Restrictions. You may not distribute copies of the Software to others or electronically transfer the Software from one computer to another over a network. You may not post or otherwise make available the Software, or any portion thereof, in any form, on the Internet. You may not use the Software in a computer service business, including in time sharing applications. The Software contains trade secrets and, in order to protect them, you may not decompile, reverse engineer, disassemble, or otherwise reduce the Software to a human-perceivable form. YOU MAY NOT MODIFY, ADAPT, TRANSLATE, RENT, LEASE, LOAN, RESELL FOR PROFIT, DISTRIBUTE, NETWORK OR CREATE DERIVATIVE WORKS BASED UPON THE SOFTWARE OR ANY PART THEREOF.

3. Ownership of Software. As Licensee, you own the media upon which the software is recorded or fixed, but Microsemi and its licensors retain title and ownership of the Software recorded on the original media and all subsequent copies of the Software, regardless of the form or media in which or on which the original and other copies may exist. This license is not a sale of the Software or any copy.

4. Confidentiality. You agree to maintain the Software in confidence and that you will not disclose the Software to any third party without the express written consent of Microsemi. You further agree to take all reasonable precautions to preclude access of unauthorized persons to the Software.

5. Term. This license is effective until January 1, 2045, unless terminated earlier. You may terminate the license at any time by destroying the Software (including the related documentation) together with all copies or modifications in any form. Microsemi will have the right to terminate our license immediately if you fail to comply with any term or condition of this Agreement. Upon any termination, including termination by you, you must destroy the Software (including the related documentation), together with all copies or modifications in any form.
6. Special Terms Applicable to Databases. Where a database is included with the Software, you acknowledge that it is licensed only in connection with the use of the Software to perform disc creation, and that the database and all data derived therefrom must be maintained in confidence in accordance with the provisions of Section 4. This license does not grant you any rights to distribute or disclose such database or data.

7. Limited Warranty. Microsemi and its Licensor warrant only that the media upon which the Software is furnished will be free from defects in material or workmanship under normal use and service for a period of thirty (30) days from the date of delivery to you. MICROSEMI AND ITS LICENSORS DO NOT AND CANNOT WARRANT THE PERFORMANCE OR RESULTS YOU MAY OBTAIN BY USING THE SOFTWARE OR DOCUMENTATION. THE FOREGOING STATES THE SOLE AND EXCLUSIVE REMEDIES MICROSEMI AND ITS LICENSORS WILL PROVIDE FOR BREACH OF WARRANTY. EXCEPT FOR THE FOREGOING LIMITED WARRANTY, MICROSEMI AND ITS LICENSORS MAKE NO WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED, AS TO NON-INFRINGEMENT OF THIRD PARTY RIGHTS, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow the exclusion of implied warranties or limitations on how long an implied warranty may last, so the above limitations may not apply to you. This warranty gives you specific legal rights and you may also have other rights which vary from state to state.

8. The entire liability of Microsemi and its licensors, and your exclusive remedy for a breach of this warranty, shall be:
   a. The replacement of any media not meeting the above limited warranty which is returned to Microsemi; or:
   b. if Microsemi or its distributor is unable to deliver replacement media which is free from defects in materials or workmanship, you may terminate this Agreement by returning the Software and your money will be refunded.

9. Limitation of Liability. IN NO EVENT WILL MICROSEMI OR ITS LICENSORS BE LIABLE TO YOU FOR ANY INCIDENTAL, CONSEQUENTIAL OR INDIRECT DAMAGES, INCLUDING ANY LOST PROFITS, LOST SAVINGS, OR LOSS OF DATA, EVEN IF MICROSEMI OR A LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, OR FOR ANY CLAIM BY ANY OTHER PARTY. Some states do not allow the exclusion or limitation of special, incidental, or consequential damages, so the above limitation or exclusion may not apply to you.

10. Export. You acknowledge that the laws and regulations of the United States and other countries may restrict the export and re-export of the Software. You agree that you will not export or re-export the Software or documentation in any form in violation of applicable United States and foreign law.

11. Government Restricted Rights. The Software is subject to restricted rights as follows. If the Software is acquired under the terms of a GSA contract: use, reproduction or disclosure is subject to the restrictions set forth in the applicable ADP Schedule contract. If the Software is acquired under the terms of a DoD or civilian agency contract, use, duplication or disclosure by the Government is subject to the restrictions of this Agreement in accordance with 48 C.F.R. 12.212 of the Federal Acquisition Regulations and its successors and 49 C.F.R. 227.7202-1 of the DoD FAR Supplement and its successors.

12. General. You acknowledge that you have read this Agreement, understand it, and that by using the Software you agree to be bound by its terms and conditions. You further agree that it is the complete and exclusive statement of the agreement between Microsemi and you, and supersedes any proposal or prior agreement, oral or written, and any other communication between Microsemi and you relating to the subject matter of this Agreement. No additional or any different terms will be enforceable against Microsemi unless Microsemi gives its express consent, including an express waiver of the terms of this Agreement, in writing signed by an officer of Microsemi. You assume full responsibility for the use of the Software and agree to use the Software legally and responsibly. This Agreement shall be governed by California law, except as to copyright matters, which are covered by Federal law. This Agreement is deemed entered into at Sunnyvale, California by both parties. Should any provision of this Agreement be declared unenforceable in any jurisdiction, then such provision shall be deemed severable from this
Agreement and shall not affect the remainder hereof. All rights in the Software not specifically granted in this Agreement are reserved by Microsemi.

Should you have any questions concerning this license, contact:

Microsemi Corporation
Legal Department
One Enterprise
Aliso Viejo, CA 92656
(949) 380-6100
# Contents

## 1 About this Guide

1.1 What You Need to Know Before You Begin...1
1.2 Terminology Used in this Guide...2
1.3 How to Find More Information...2

## 2 Introduction to maxView Storage Manager

2.1 Getting Started...4
2.2 About maxView Storage Manager...4
   2.2.1 About maxView Storage Manager Redfish Server...4
   2.2.2 About the maxView Storage Manager Web Server...4
2.3 System Requirements...5
2.4 Browser Support...5
2.5 Typical Storage Space Configurations...6
   2.5.1 A Simple Storage Space...6
   2.5.2 An Advanced Storage Space...6
   2.5.3 Continuing to Grow Your Storage Space...7

## 3 Installing maxView Storage Manager

3.1 Before You Begin the Installation...9
   3.1.1 Gather Installation Information...9
   3.1.2 Download the Installation Package...9
3.2 Installing on Windows...11
3.3 Installing on Red Hat, Citrix XenServer, CentOS, or SuSE Linux...12
3.4 Installing on Debian or Ubuntu Linux...12
3.5 Installing on VMware...13
3.6 Running maxView Storage Manager from a Bootable USB Image...14
3.7 Uninstalling maxView Storage Manager...15
   3.7.1 Uninstalling from Windows...15
   3.7.2 Uninstalling from Red Hat, Citrix XenServer, CentOS, or SuSE Linux...15
   3.7.3 Uninstalling from Ubuntu Linux...15
   3.7.4 Uninstalling from VMware...15

## 4 Exploring maxView Storage Manager

4.1 Starting maxView Storage Manager and Logging In...16
4.2 Working in maxView Storage Manager...16
4.3 Overview of the Main Window...17
   4.3.1 The Enterprise View...18
   4.3.2 The Ribbon...21
   4.3.3 The Storage Dashboard...21
4.4 Checking System Status from the Main Window...22
4.5 Revealing More Device Information...23
4.6 Getting Help...24
4.7 Logging Out of maxView Storage Manager...25

## 5 Building Your Storage Space

5.1 Overview...26
5.2 Choosing a Management System...26
   5.2.1 ‘Local’ or ‘Remote’...26
   5.2.2 Logging in on the Local System...27
5.3 Logging into Remote Systems from the Local System...28
Contents

5.4 Creating Arrays and Logical Drives

5.4.1 Creating a Logical Drive on a New Array

5.4.2 Creating a Logical Drive on an Existing Array

5.4.3 Partitioning and Formatting Your Logical Drives

5.4.4 Creating Logical Drives on Other Systems in Your Storage Space

5.4.5 Controller Support for 4K Drives

6 Protecting Your Data

6.1 Dedicated Spare or Auto-Replace Spare?

6.2 Hot Spare Limitations

6.3 Assigning a Dedicated Hot Spare

6.4 Assigning an Auto-Replace Hot Spare

6.5 Removing a Hot Spare

6.6 Setting the Spare Activation Mode

6.7 Controller Sanitize Lock Freeze/Anti-Freeze

6.7.1 Sanitize Lock Property in Controller Node Properties Tab

6.7.2 Physical Device Sanitize Lock Freeze/Anti-Freeze

6.7.3 Secure Erase Pattern

7 Modifying Your Storage Space

7.1 Understanding Arrays and Logical Drives

7.2 Creating and Modifying Logical Drives

7.2.1 Including Different-sized Disk Drives in a Logical Drive

7.3 Enabling Background Consistency Check

7.4 Optimizing Logical Drive Performance

7.4.1 Enabling Cache Optimizations

7.4.2 Enabling SSD I/O Bypass

7.5 Moving a Logical Drive

7.6 Moving an Array

7.7 Modifying an Array

7.8 Working with Mirrored Arrays

7.8.1 Creating a Split Mirror Backup

7.8.2 Re-mirroring, Rolling Back, or Reactivating a Split Mirror Backup

7.9 Changing the RAID Level of a Logical Drive

7.10 Increasing the Capacity of a Logical Drive

7.11 Changing the Logical Drive Rebuild Priority

7.12 Renaming a Logical Drive

7.13 Deleting an Array or Logical Drive

7.14 Maintaining an Energy-Efficient Storage Space

8 Working with maxCache Devices

8.1 maxCache Limitations

8.2 Creating a maxCache Device

8.3 Changing the Write Cache Mode

8.4 Deleting the maxCache Device

8.5 Analyzing maxCache Performance

9 Working with maxCrypto Devices

9.1 maxCrypto Initial Setup

9.1.1 Managing maxCrypto Accounts

9.1.2 Logging In and Logging Out

9.1.3 Checking maxCrypto Status

9.2 Modifying the maxCrypto Configuration

9.3 Creating an Encrypted Logical Drive

9.4 Converting Plaintext Data to Encrypted Data

9.5 Re-Keying a Logical Drive
Contents

10 Maintaining Physical Devices ..............................................................................................................91
  10.1 Viewing Device Properties ..................................................................................................................91
  10.2 Locating Drives in Your Storage Space ...............................................................................................91
    10.2.1 Locating Disk Drives ....................................................................................................................92
    10.2.2 Locating Physical Disks in an Array or Logical Drive ......................................................................93
    10.2.3 Locating SSDs in the maxCache Device ..........................................................................................93
  10.3 Working with Physical Device Error Counters .....................................................................................94
    10.3.1 Viewing Physical Device Error Counters ......................................................................................95
    10.3.2 Clearing Error Counters from a Physical Device ...........................................................................96
    10.3.3 Clearing Error Counters from a Controller ....................................................................................97
  10.4 Working with Failed or Failing Disk Drives .........................................................................................97
    10.4.1 Replacing Disk Drives in a Logical Drive .......................................................................................97
    10.4.2 Setting a Disk Drive to ‘Failed’ ......................................................................................................98
  10.5 Erasing a Disk Drive ................................................................................................................................98
    10.5.1 Restricted/Unrestricted Secure Erase ............................................................................................99
  10.6 Initializing and Uninitializing Disk Drives ............................................................................................99
    10.6.1 Uninitializing a Disk Drive ..............................................................................................................99
    10.6.2 Initializing/Uninitializing all Drives on a Controller .......................................................................100
  10.7 Setting the Physical Drive Boot Priority ..............................................................................................101
  10.8 Working with Controllers ....................................................................................................................102
    10.8.1 Rescanning a Controller ...............................................................................................................102
    10.8.2 Optimizing Controller Performance ...............................................................................................103
    10.8.3 Changing the Connector Operating Mode .......................................................................................104
  10.9 Updating Controller, Enclosure, and Disk Drive Firmware ...................................................................105
    10.9.1 Before You Begin ...........................................................................................................................105
    10.9.2 Updating the Controller Firmware ................................................................................................105
    10.9.3 Updating the Disk Drive Firmware ................................................................................................109
    10.9.4 Updating the Enclosure Firmware ................................................................................................110

11 Monitoring Status and Activity ............................................................................................................112
  11.1 Monitoring Options .............................................................................................................................112
  11.2 Checking Status from the Main Window ..............................................................................................112
    11.2.1 Viewing Activity Status in the Event Log .......................................................................................113
    11.2.2 Viewing Task Status in the Task Log ..............................................................................................115
    11.2.3 Viewing Component Status in the Storage Dashboard .................................................................115
    11.2.4 Viewing Storage Space Usage in Chart View ...............................................................................118
  11.3 Notifying Users by Email About Status and Activity .............................................................................119
    11.3.1 Setting Up Email Notifications ...................................................................................................119
    11.3.2 Sending a Test Message .................................................................................................................122
    11.3.3 Modifying or Removing an Email Recipient ................................................................................123
    11.3.4 Modifying Email Server Settings ..................................................................................................124
    11.3.5 Disabling Email Notifications ......................................................................................................124
  11.4 Monitoring Advanced Statistics about Activity in Your Storage Space .............................................124
    11.4.1 Setting up Statistics Logging .........................................................................................................125
    11.4.2 Viewing Advanced Statistics .......................................................................................................126
    11.4.3 Resetting the Statistics Counters ..................................................................................................128
  11.5 Changing an Operating System’s Event Log Setting ..........................................................................128

12 Managing Your Storage Space ............................................................................................................130
  12.1 Deploying Servers ..............................................................................................................................130
    12.1.1 Creating a Server Template File ...................................................................................................130
    12.1.2 Duplicating the Server Template ................................................................................................131
12.2 Managing Remote Systems

12.2.1 Adding Remote Systems with the Wizard

12.2.2 Manually Adding a Remote System

12.2.3 Removing a Remote System

12.2.4 Changing the Auto-Discovery Settings

12.2.5 Importing and Exporting Remote Systems

12.3 Clearing the Controller Configuration

12.4 Changing the Web Server Port

12.5 Granting Standard Users Admin Privilege

13 Solving Problems

13.1 General Troubleshooting Tips

13.2 Identifying a Failed or Failing Component

13.3 Recovering from a Disk Drive Failure

13.3.1 Failed Disk Drive Protected by a Hot Spare

13.3.2 Failed Disk Drive Not Protected by a Hot Spare

13.3.3 Failure in Multiple Logical Drives Simultaneously

13.3.4 Disk Drive Failure in a RAID 0 Logical Drive

13.3.5 Forcing a Logical Drive with Multiple Drive Failures Back Online

13.3.6 Healing an Array

13.4 Rebuilding Logical Drives

13.5 Creating a Support Archive File

Appendix A Silent Installation on Windows and Linux

A.1 Completing a Silent Installation

A.1.1 Windows Silent Installation

A.1.2 Linux Silent Installation

A.2 Example Command Line Installations

Appendix B Configuring SNMP Notifications on Windows and Linux

B.1 Setting Up SNMP Notifications on Windows

B.2 Setting Up SNMP Notifications on Linux

Appendix C Using the maxView Plugin for VMware vSphere Web Client

C.1 Installing the maxView Plugin for vSphere Web Client

C.2 Starting the maxView Plugin for vSphere Web Client

C.3 Monitoring maxView Resources in vSphere Web Client

Appendix D Using maxView Storage Manager with HBAs and Non-RAID Mode Controllers

Appendix E Selecting the Best RAID Level

E.1 Comparing RAID Levels

E.2 Non-redundant Logical Drives (RAID 0)

E.3 RAID 1 Logical Drives

E.4 RAID 1 (ADM) Logical Drives

E.5 RAID 10 Logical Drives

E.6 RAID 10 (ADM) Logical Drives

E.7 RAID 5 Logical Drives

E.8 RAID 50 Logical Drive

E.9 RAID 6 Logical Drives

E.10 RAID 60 Logical Drives

Appendix F Icons At-a-Glance

Appendix G Advanced Statistics Descriptions

Appendix H Smart Controller Device Status
1 About this Guide

maxView Storage Manager™ is a browser-based software application that helps you build a storage space using Microsemi Smart Storage Controllers, disk drives, and enclosures, and then manage your stored data, whether you have a single controller installed in a server or multiple controllers, servers, and enclosures. This guide describes how to install and use maxView Storage Manager to build and manage direct attached storage; that is, storage where the controller and disk drives reside inside, or are directly attached to, the computer accessing them, similar to the basic configurations shown in the figures below.

**Note:** This guide focuses on using maxView Storage Manager with Microsemi Smart Storage Controllers (SmartRAID/SmartHBA/SmartIOC/SmartROC). For information about using maxView Storage Manager with Microsemi Adaptec Series 8 (legacy) RAID controllers, see *How to Find More Information* on page 2.
1.1 What You Need to Know Before You Begin

This guide is written for data storage and IT professionals who want to create a storage space for their online data. You should be familiar with computer hardware, operating system administration, and Redundant Array of Independent Disks (RAID) technology.

If you are using maxView Storage Manager as part of a complex storage system, with multiple servers, enclosures and Microsemi Smart Storage Controllers, you should be familiar with network administration, have knowledge of Local Area Networks (knowledge of storage area networks (SANs) is not required), and be familiar with the input/output (I/O) technology of the storage devices on your network, such as Serial ATA (SATA) or Serial Attached SCSI (SAS).

1.2 Terminology Used in this Guide

Because this guide provides information that can be used to manage multiple Smart Storage Controllers in a variety of configurations, the generic term “storage space” is used to refer to the controller(s), disk drives, and systems being managed with maxView Storage Manager.

For efficiency, the term “component” or “components” is used when referring generically to the physical and virtual parts of your storage space, such as systems, disk drives, controllers, and logical drives.

Many of the terms and concepts referred to in this guide are known to computer users by multiple names. In this guide, this terminology is used:

- Controller (also known as adapter, board, or I/O card)
- Disk drive (also known as hard disk, hard drive, or hard disk drive)
- Solid State Drive (also known as SSD or non-rotating storage media)
- Logical drive (also known as a logical device)
- Array (also known as a storage pool or container)
- System (also known as a server, workstation, or computer)
- Enclosure (also known as a storage enclosure or disk drive enclosure)

1.3 How to Find More Information

You can find more information about your Microsemi Smart Storage Controller, management software, and utilities by referring to these documents, available for download at start.microsemi.com and the Microsemi customer portal at www.pmcs.com/myPMC:

- **SmartIOC 2100/SmartROC 3100 Installation and User’s Guide, SmartIOC 2000 Installation and User’s Guide**—Describes how to install drivers and configure the SmartIOC/SmartROC controller for initial use
- **SmartIOC 2100/SmartROC 3100 Software/Firmware Release Notes, SmartIOC 2000 Software/Firmware Release Notes**—Provides driver, firmware, and release package information, and known issues.
- **README: maxView Storage Manager & ARCCONF Command Line Utility**—Provides product information, installation notes, and known issues for maxView Storage Manager and ARCCONF command line utility.
For information about using maxView Storage Manager with Microsemi Adaptec Series 8 (legacy) RAID controllers, see the *maxView Storage Manager User’s Guide for Microsemi ARC Controllers* (CDP-00285-06-A).
2 Introduction to maxView Storage Manager

This section introduces the maxView Storage Manager software, explains the concept of a “storage space,” and provides a checklist of getting-started tasks.

2.1 Getting Started

The first part of this guide provides the information you need to install, start, and begin to use maxView Storage Manager. Follow these general steps:

Step 1: Familiarize yourself with the software components of maxView Storage Manager, review the system requirements, and study the configuration examples that illustrate how to build and grow your storage space (described in the remainder of this chapter).

Step 2: Install maxView Storage Manager on every system that will be part of your storage space (see installing maxView Storage Manager on page 9).

Step 2: Install maxView Storage Manager on every system that will be part of your storage space (see the maxView Storage Manager User's Guide, on the installation DVD).

Step 3: Start maxView Storage Manager and explore its graphical user interface (see Exploring maxView Storage Manager on page 16).

Step 4: Build your storage space (see Building Your Storage Spacebuilding storage space on page 26).

2.2 About maxView Storage Manager

maxView Storage Manager is a browser-based software application that helps you build a storage space for your data, using RAID controllers, disk drives, Solid State Drives (SSDs), and enclosures.

With maxView Storage Manager, you can group disk drives into arrays and logical drives and build in redundancy to protect your data and improve system performance. You can also use maxView Storage Manager to monitor and maintain all the controllers, enclosures, and disk drives in your storage space from a single location.

The maxView Storage Manager GUI, or graphical user interface, runs on most contemporary Web browsers (for a list of supported browsers, see Browser Support on page 5). A software stack comprising a Web server, and Redfish server allows maxView Storage Manager to communicate with the controller(s) in your storage space and coordinate activity in your system.

A flexible installation model allows you to install all software components on a single machine, or distribute components on different machines across your network, with the maxView Storage Manager GUI and Web server on one machine, and the and Redfish server on others.

2.2.1 About maxView Storage Manager Redfish Server

The maxView Storage Manager Redfish Server is an instance of Nodejs. On Windows and Linux systems, the Redfish Server manages the hardware, which monitors the controllers in your system and provide notifications to the maxView Storage Manager. The maxView Storage Manager Redfish Server is installed automatically with the maxView Storage Manager.

2.2.2 About the maxView Storage Manager Web Server

The maxView Storage Manager Web Server is an instance of the open-source Apache Tomcat servlet container. It runs the maxView Storage Manager Web application, and serves static and dynamic content to the maxView Storage Manager GUI. The maxView Web Server is installed automatically with the maxView Storage Manager GUI.
2.3 System Requirements

To install maxView Storage Manager, each system in your storage space must meet these requirements:

- A PC-compatible computer with an Intel Pentium processor, or equivalent
- At least 4 GB of RAM
- 350 MB of free disk drive space
- One of these operating systems:
  - Red Hat® Enterprise Linux
  - SuSE Linux Enterprise Server
  - Ubuntu Linux
  - CentOS
  - Hypervisors:
    - VMware vSphere, VMware ESXi
    - Citrix XenServer
    - Microsoft Hyper-V

See the maxView Storage Manager and ARCCONF Command Line Utility Readme for a complete list of supported operating system versions.

Note: maxView Storage Manager can also be used before an operating system is installed. See Running maxView Storage Manager from a Bootable USB Image on page 14 for more information.

2.4 Browser Support

To run the maxView Storage Manager GUI, each system in your storage space must be running one of these Web browsers:

- Microsoft® Edge browser for Windows 10
- Google® Chrome™ 32 or newer
- Mozilla Firefox® 31 or newer

Note:

From this release onwards maxView does not support the use of Internet Explorer (IE) browser.
2.5 Typical Storage Space Configurations

The following examples show typical storage spaces that you can build with maxView Storage Manager. You can grow your storage space as your requirements change by adding more systems, controllers, disk drives, and enclosures, and by adding redundant logical drives for protection against data loss.

2.5.1 A Simple Storage Space

This example shows a simple storage space that might be appropriate for a small business. This storage space includes one RAID controller and three disk drives installed in a server. For data protection, the disk drives have been used to build a RAID 5 logical drive.

![Diagram of a simple storage space with a RAID 5 logical drive]

2.5.2 An Advanced Storage Space

This example shows how you can grow your storage space as the requirements of your application change. On the first server, segments from each disk drive have been used to build two RAID 5 logical drives. A second server connected to two 12-disk enclosures has been added. The additional storage space has been used to create two RAID 50 logical drives. The Administrator of this storage space can create and modify logical drives and monitor both controllers, disk drives, and enclosures from a single system running the maxView Storage Manager GUI.
2.5.3 Continuing to Grow Your Storage Space

For more advanced applications, such as high-volume transaction processing in a "cloud" or data center environment, maxView Storage Manager helps you grow your storage space to include multiple controllers, storage enclosures, and disk drives in multiple locations.
In this example, multiple systems, servers, disk drives, and enclosures have been added to the storage space. The Administrator can create and modify logical drives and monitor all the controllers, enclosures, and disk drives in the storage space from any system running the maxView Storage Manager GUI.
3 Installing maxView Storage Manager

This section describes how to install and uninstall maxView Storage Manager on the supported operating systems. It also describes how to run maxView Storage Manager from a bootable USB image, before the application is installed on an operating system.

**Note:** To perform a silent installation without messages or user interaction, follow the instructions in *Silent Installation on Windows and Linux* on page 149.

**Note:** VMware users can install the maxView plugin for vSphere Web Client for Windows and monitor storage resources without using the maxView Storage Manager GUI. For more information, see *Using the maxView Plugin for VMware vSphere Web Client* on page 154.

3.1 Before You Begin the Installation

Complete the following steps before you begin the installation.

3.1.1 Gather Installation Information

Prepare the following information:

- Redfish Server port number. The default port is recommended (8081). If the default port is not available, another port number will be automatically assigned. For more information on the Redfish Server, see *About maxView Storage Manager Redfish Server* maxView Storage Manager Redfish ServerRedfish introduction on page 4.

- maxView Web Server port number. The default port is recommended (8443). If the default port is not available, another port number will be automatically assigned. For more information on the Web Server, see *About the maxView Storage Manager Web Server* on page 4.

  **Note:** You can install maxView Storage Manager over an existing installation if it is no more than two versions older than the current release. Otherwise, you must remove the old version first, before beginning a new installation. See *Uninstalling maxView Storage Manager* on page 15 for details.

3.1.1.1 Check Network Configuration

Check your network configuration to ensure that it meets the prerequisites for a standard (non-Standalone Mode) installation:

- Ensure that the system is configured with an IP address.
- Ensure that the OS hostname is per standard.
- Ensure that the hostname-to-IP address mapping is updated in DNS. At minimum, ensure that the hostname-to-IP mapping is entered in the `/etc/hosts` file.

3.1.2 Download the Installation Package

Complete these steps to download the installation package for your operating system(s):

1. Open a browser window, then type `start.microsemi.com` in the address bar.
2. Select your controller family and controller model.
3. Select *Storage Manager Downloads*, then select the appropriate installer package from the list; for instance, maxView Storage Manager for Windows x64 or maxView Storage Manager for Linux.
4. Click Download Now and accept the license agreement.
5. When the download completes, extract the package contents to a temporary location on your machine.

   **Note:** See the *Release Notes* for a complete list of installer packages for the supported operating systems.
3.2 Installing on Windows

This section describes how to install maxView Storage Manager on Windows systems.

**Note:** You need administrator privileges to install maxView Storage Manager. For details on verifying privileges, refer to your operating system documentation.

1. Open Windows Explorer or My Computer, then change to the directory where the Windows installer package is located (see *Download the Installation Package* on page 9 for details).

2. Double-click the setup program for your operating system version:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 64-bit</td>
<td>setup_asm_x64.exe</td>
</tr>
</tbody>
</table>

   The Installation wizard opens.

3. Click Next to begin the installation.

4. Select *I accept the terms in the license agreement* option, then click Next.

5. Accept or modify the default server ports in the maxView Storage Manager Configuration screen:
   a. Web Server Port: 8443 (default)
   b. Redfish Server Port: 8081 (default)

6. To disable remote system management from the GUI, click the **Standalone Mode** check box.

   **Note:** In Standalone mode, maxView Storage Manager displays the system name as "localhost" and events as "127.0.0.1/localhost".

7. Click Next, then click OK to verify the Web Server port and the Redfish Server port numbers. The Direct Attached Storage Setup screen appears on the Installation wizard.

8. Ensure that **GUI and/or Redfish Server** is selected. Optionally, select **CLI Tools**. Click Next.
9. Click **Install** to begin the installation.

10. Repeat these steps to install maxView Storage Manager on every Windows system that will be part of your storage space.

When the installation is complete you receive a confirmation message and the maxView Storage Manager icon is placed on your desktop.

### 3.3 Installing on Red Hat, Citrix XenServer, CentOS, or SuSE Linux

This section describes how to install maxView Storage Manager on systems running Red Hat Linux, CentOS, XenServer, or SuSE Linux. For a list of supported Linux operating systems, see *System Requirements* maxView Storage Manager system requirements operating systems on page 5.

1. Open a shell window, then change to the directory where the Linux installer package is located (see *Download the Installation Package* on page 9 for details).

2. Run the `.bin` file for your operating system version (x.xx-xxxx=version-build number):

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux 64-bit</td>
<td>./StorMan-X.XX-XXXXX.x86_64.bin</td>
</tr>
</tbody>
</table>

3. When prompted for configuration details, enter the following:

   **Standalone Mode:** [default: No]

   **Note:** Standalone Mode *disables* remote system management from the GUI. maxView Storage Manager displays the system name as "localhost", and events as "127.0.0.1/localhost".

4. Repeat these steps to install maxView Storage Manager on every Linux system that will be part of your storage space.

   When the installation completes a confirmation message is displayed and the maxView Storage Manager icon is placed on your desktop.

### 3.4 Installing on Debian or Ubuntu Linux

This section describes how to install maxView Storage Manager on systems running Debian or Ubuntu Linux.

1. Open a shell window, then change to the directory where the Linux installer package is located (see *Download the Installation Package* on page 9 for details).
2. Install the .deb package for your operating system version (x.xx-xxxx=version-build number).

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux 64-bit</td>
<td><code>dpkg -i StorMan-X.XX-XXXXX_amd64.deb</code></td>
</tr>
</tbody>
</table>

3. When prompted for configuration details, enter the following:

   Standalone Mode: [default: No]

   **Note:** Standalone Mode disables remote system management from the GUI. maxView Storage Manager displays the system name as "localhost", and events as "127.0.0.1/localhost".

4. Repeat these steps to install maxView Storage Manager on every Debian and Ubuntu Linux system that will be part of your storage space.

5. Before upgrading/re-installing maxView Storage Manager on an existing Ubuntu/Debian installation, enable the upgrade switch before installing the maxView .deb package:

   ```bash
   export maxView_Upgrade=true
   dpkg -i StorMan-*.deb
   ```

   When the installation is complete you receive a confirmation message and the maxView Storage Manager icon is placed on your desktop.

### 3.5 Installing on VMware

Use the following procedure to install the .vib files for a VMware ESXi system. Perform the installation from a remote system running a Telnet/SSH client. Use a terminal emulator to access the ESXi server remotely.

1. Copy the following files from the installer download location to the /tmp directory on your local ESXi server (see Download the Installation Package on page 9 for details):

   - `vmware-esx-provider-arcconf.vib`
   - `vmware-esx-provider-arc-cim-provider.vib`

   The arcconf.vib is for command line communication.
   The arc-cim-provider.vib is for remote management communication.

2. Check for existing installation of arcconf.

   ```bash
   esxcli software vib list | grep arcconf
   ```

3. Remove the existing arcconf package.

   ```bash
   esxcli software vib remove -n arcconf
   ```

   When the package is removed, you receive the message "Reboot Required: false."

4. Check for an existing installation of arc-cim-provider.

   ```bash
   esxcli software vib list | grep arc-cim-provider
   ```

5. Remove the existing arc-cim-provider package.

   ```bash
   esxcli software vib remove -n arc-cim-provider
   ```

   When the package is removed, you receive the message "Reboot Required: true."

6. Set the installation acceptance level to either PartnerSupported or CommunitySupported:

   ```bash
   esxcli software acceptance set --level=PartnerSupported
   ```

7. Install the arcconf package.

   ```bash
   esxcli software vib install -v /tmp/vmware-esx-provider-arcconf.vib
   ```

   When the package is installed, you receive the message "Reboot Required: false."

8. Install the arc-cim-provider package.

   ```bash
   esxcli software vib install -v /tmp/vmware-esx-provider-arc-cim-provider.vib
   ```

   When the package is installed, you receive the message "Reboot Required: true."

9. Reboot the system.
10. Continue with *Managing Remote Systems* on page 133 to add a remote system.

### 3.6 Running maxView Storage Manager from a Bootable USB Image

Running maxView Storage Manager from a *bootable USB image* allows you to configure your controller before you install the operating system. The procedure consists of three basic steps:

1. Download the bootable USB image from the Microsemi web site

2. Create a "live" image on a USB flash drive
   
   **Note:** We recommend using Rufus bootable USB create ([http://rufus.akeo.ie/](http://rufus.akeo.ie/)).

3. Boot from the USB flash drive, login to maxView Storage Manager and configure your controller

The bootable USB image is not a substitute for running maxView Storage Manager as an installed application. Many of the features and functions described in this guide are not available when you run maxView Storage Manager from a bootable USB image. Use the bootable USB image only to configure your controller before you install an operating system.

**Note:** Before you begin, ensure that your system is set up to boot from a USB drive. Check the system BIOS to see if the USB drive is included in the boot sequence. (For more information, see your system's documentation.) You will need a USB drive with at least 2 GB of storage to complete this task. To run the bootable USB image, the target machine must have at least 4 GB of memory.

To run maxView Storage Manager from a bootable USB image:

1. Download the bootable USB image:
   
   a. Open a browser window, then type `start.microsemi.com` in the address bar.
   
   b. Select your controller family and controller model.
   
   c. Select *Storage Manager Downloads*.
   
   d. Download the bootable USB image (zip file archive).
   
   e. Extract the contents of the bootable image archive file to a temporary location. The archive contains one file: the maxView Storage Manager bootable iso image.

2. Create a "live" image on the USB drive:
   
   a..Run the USB Creator utility setup program at [http://rufus.akeo.ie/](http://rufus.akeo.ie/).
   
   b. Start USB Creator from the Windows All Programs menu.
   
   c. In the Use Existing Live CD field, click Browse, then locate and select the maxView Storage Manager bootable ISO image.
   
   d. In the Target Device field, select the USB flash drive (e:\, for instance).
   
   e. Click Create Live USB.

3. Insert the USB drive on the machine you want to configure.

   The Boot menu opens in a shell window.

4. Select Launch maxView from the menu.

   After a minute or so, the maxView Storage Manager login screen opens in a browser window.

   **Note:** If you prefer to configure the controller from the command line, select Launch arcconf from the Boot menu, then enter root, with no password, for the login credentials.

5. Enter root/root for the login credentials.

6. Continue with *Creating Arrays and Logical Drives*. 

---

Microsemi Smart Storage Controllers User Guide Revision 10

14
3.7 Uninstalling maxView Storage Manager

To uninstall maxView Storage Manager, follow the instructions for your operating system.

3.7.1 Uninstalling from Windows

To uninstall maxView Storage Manager from a Windows system, use the Add or Remove Programs tool in the Control Panel. All maxView Storage Manager components are uninstalled.

When the uninstall process is complete, you receive a confirmation message and the maxView icon is removed from your desktop.

3.7.2 Uninstalling from Red Hat, Citrix XenServer, CentOS, or SuSE Linux

This section describes how to uninstall maxView Storage Manager from systems running Red Hat, XenServer, CentOS, SuSE Linux.

1. Type the command `rpm -e StorMan`

When the uninstall process is complete, you receive a confirmation message and the maxView icon is removed from your desktop.

3.7.3 Uninstalling from Ubuntu Linux

This section describes how to uninstall maxView Storage Manager from systems running Ubuntu Linux.

1. Type the command `dpkg -r StorMan`

2. Type the command to uninstall maxView after the upgrade `export maxView_Ugrade=false dpkg -r storman`

When the uninstall process is complete, you receive a confirmation message and the maxView icon is removed from your desktop.

3.7.4 Uninstalling from VMware

Use the following procedure to remove maxView Storage Manager from a VMware ESXi 5.5 or 6.0 system.

1. Log in with the user name: root

2. List the installed packages:
   ```
   esxcli software vib list | grep arcconf
   esxcli software vib list | grep arc-cim-provider
   ```

3. Remove the arcconf package:
   ```
   esxcli software vib remove -n arcconf
   ```

4. Remove the arc-cim-provider package:
   ```
   esxcli software vib remove -n arc-cim-provider
   ```

5. Reboot the system.

To verify that maxView Storage Manager is uninstalled, repeat Step 2. If no results are shown, the software was uninstalled successfully.
4 Exploring maxView Storage Manager

This section familiarizes you with the main features of the maxView Storage Manager graphical user interface. It describes how to start and log into maxView Storage Manager. It also explains how to get help and log out of maxView Storage Manager when you are finished working with the application.

4.1 Starting maxView Storage Manager and Logging In

The procedure for starting and logging in to maxView Storage Manager is the same for all operating systems with a graphical desktop. You can login as the Administrator, with full management-level access to your storage space, or as a Standard user, with restricted access to your storage space (see Working in maxView Storage Manager on page 16 for more information about access permissions).

1. On the desktop, double-click the maxView Storage Manager desktop icon.

   The login window opens in the default browser.

2. For full management-level access to your storage space, enter the Administrator account username and password for your operating system. For Standard-level access to your storage space, enter your regular network login credentials. Then click Login.

   The maxView Storage Manager main window opens.

   ![Login Window](image)

   **Note:** If you do not have an icon for maxView Storage Manager on your desktop, open a browser window, then type this URL in the address bar and press Return: [https://127.0.0.1:8443/maxview/manager/login.xhtml](https://127.0.0.1:8443/maxview/manager/login.xhtml).

4.2 Working in maxView Storage Manager

You can perform most tasks in maxView Storage Manager by:

- Selecting storage components in the Enterprise View (controllers, hard drives, logical drives, and so on)
- Clicking icons on the ribbon, at the top of the maxView Storage Manager main window
- Working with information in the Storage Dashboard and Chart View
- Checking status in the Event Log and Task Log

If you are logged in as the Administrator, you have full access to manage and modify the components of your storage space, using all of the features of maxView Storage Manager. If you are logged in as a Standard user, you have restricted “view-only” access to your storage space, with limited ability to perform non-destructive operations, as described in the table below.

   **Note:** maxView Storage Manager allows you to give Standard users Administrator privileges. For details, see Granting Standard Users Admin Privilege on page 142.
### 4.3 Overview of the Main Window

The main window of maxView Storage Manager has three main panels—left, right, and bottom—plus the ribbon, at the top of the window.

The left panel always shows the Enterprise View. The bottom panel shows the Event Log and Task Log. The right panel shows the Storage Dashboard and Chart View. Different information appears in the right panel depending on which component is selected in the Enterprise View.

In example below, a controller is selected in the Enterprise View, and the right panel displays the Storage Dashboard for the controller, with a chart view of its storage space.
You can resize the panels and scroll horizontally or vertically as needed, to view more or less information.

4.3.1 The Enterprise View

The Enterprise View is an expandable “tree” that shows the physical and logical components of your storage space. The Enterprise View lists the local system (the system you're working on) and any remote systems that you have logged in to from the local system. (See 'Local' or 'Remote'? on page 26 for more information.) It also lists the maxCache Devices in your system.

Note: maxCache is not supported on all Microsemi Adaptec Smart Storage Controllers. See the Readme for more information. For more information about maxCache, see Working with maxCache Devices on page 73.
Expand a system in the Enterprise View to see its controllers, arrays, logical drives ("devices"), physical drives, enclosures, and maxCache Devices.

In the figure below, a controller is expanded in the Enterprise View, revealing the physical and logical devices associated with that controller.
By selecting a controller in the Enterprise View...

...the disk drives or enclosures and disk drives connected to it and the arrays and logical drives created with those disk drives appear in the Physical and Logical Devices trees.

You can perform most tasks in maxView Storage Manager by selecting a component in the Enterprise View, such as a controller or disk drive, then using the related commands on the ribbon, as described in the section below.

4.3.1.1 What do the Enterprise View Icons Mean?

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Icon]</td>
<td>System with controller and directly attached disk drives or enclosures</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Controller</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Enclosure</td>
</tr>
<tr>
<td>Icon</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>Logical drive (encrypted)²</td>
<td></td>
</tr>
<tr>
<td>maxCache Device (healthy)²</td>
<td></td>
</tr>
<tr>
<td>Array (healthy)</td>
<td></td>
</tr>
<tr>
<td>Hard disk drive</td>
<td></td>
</tr>
<tr>
<td>Solid State Drive (SSD)</td>
<td></td>
</tr>
<tr>
<td>SMR (Shingled Magnetic Recording)³ drive</td>
<td></td>
</tr>
<tr>
<td>Connector or other physical device</td>
<td></td>
</tr>
</tbody>
</table>

### 4.3.2 The Ribbon

Most tasks in maxView Storage Manager are available from the ribbon, at the top of the main window. The ribbon replaces toolbars and menus in maxView Storage Manager to help you quickly find the commands you need to complete a task.

The ribbon is organized into groups of related tasks for Systems, Controllers, Arrays, Logical Devices, Physical Devices, and maxCache Devices. The Home group (on the left) provides commands for working with remote systems (see [Managing Remote Systems](#) on page 133). Active options on the ribbon vary, depending on which type of component is selected in the Enterprise View.

For instance, if you select a controller in the Enterprise View, these options are activated:

- Create Logical Drive in the Logical Device group
- Spare Management in the Physical Device group
- Create maxCache Device in maxCache group (if the controller supports maxCache)
- All options in the Controller group

If you select an array in the Enterprise View, options in the Array group are highlighted; selecting a disk drive highlights options in the Physical Device group; and so on.

For a description of the icons on the ribbon, see [Icons At-a-Glance](#) on page 174.

### 4.3.3 The Storage Dashboard

When you select a component in the Enterprise View, maxView Storage Manager displays detailed information about that component on the Storage Dashboard. Occupying the largest portion of the main

---

¹ A lock in the Enterprise View means that the device is encrypted. For more information, see [Working with maxCrypto Devices](#) on page 77.

² A green check mark in the Enterprise View means that the device is healthy with no problems or issues. For more information, see [Identifying a Failed or Failing Component](#) on page 143.

³ Not supported on all controllers. See the Readme for more information.
window in maxView Storage Manager, the Storage Dashboard provides status information, physical and logical device properties, resources, usage statistics, and reliability indicators for hard drives and SSDs. It also provides a chart view of free and used space in your system.

For more information about the types of information provided on the Storage Dashboard for each component in your storage space, see Viewing Component Information and Status in the Storage Dashboard; also see Revealing More Device Information.

### 4.4 Checking System Status from the Main Window

maxView Storage Manager includes an Event Log and Task Log for at-a-glance status and activity information for all managed systems. The Event Log provides status information and messages about activity (or events) occurring in your storage space. The Task Log provides information about current or recurring processes in your storage space, such as rebuilding a logical device. Single-click any event or task to see more information in an easier-to-read format. For more information about the Event Log and Task Log, see Viewing Activity Status in the Event Log on page 113 and Working with Tasks.
Warning- and Error-level icons appear next to components in the Enterprise View affected by a failure or error, creating a trail, or rapid fault isolation, that helps you identify the source of a problem when it occurs. See Identifying a Failed or Failing Component on page 143 for more information.

If your storage space includes a drive enclosure with a temperature sensor, temperature, fan, and power module status is displayed on the Storage Dashboard (see Monitoring Enclosure Statusenclosures monitoringenclosures temperature statusenclosures fan statustemperature statusenclosures power status on page 117).

For more information about checking status from the main window, see Monitoring Status and Activitymonitoringstatus monitoringactivity on storage space monitoringevents monitoring.

### 4.5 Revealing More Device Information

You can reveal more information about disk drive, array, and logical drive usage in your storage space (including maxCache Devices) with the Resources view on the Storage Dashboard.

To reveal disk drive usage by logical drive (and vice-versa), select a controller in the Enterprise View, then open the Resources tab on the Storage Dashboard. As shown in the figures below, you can click a logical
drive to see its member disk drives and spares; similarly, you can click a physical disk to see which array (if any) it belongs to. In the following figure the disk in Slot 5 belongs to Array A.

**Note:** Click the Arrow icons, on the right side of the Resources table, to jump to that resource in the Enterprise View tree.

---

**4.6 Getting Help**

maxView Storage Manager provides online help that includes conceptual information and descriptions of on-screen items and dialog boxes, in addition to step-by-step instructions for completing tasks.

To open the online help, click the **Help** button at the upper-right corner of the main window.

For help with a dialog box or wizard, click the question-mark icon, in the lower corner of the dialog box, for help with that specific procedure.
For help with individual options in the Set Properties dialog box (for controllers, logical drives, and physical drives), or specific information fields on the Storage Dashboard, mouse over any field or option name for a brief description of that option.

4.7 Logging Out of maxView Storage Manager

To log out of maxView Storage Manager:

1. In the Enterprise View, click on the local system.
2. Click the Logout button at the upper-right corner of the main window:

You are logged out of maxView Storage Manager and the main window is closed.
5 Building Your Storage Space

Follow the instructions in this section to choose a management system, log in to each system in your storage space, and create arrays and logical drives.

Note: Before beginning the tasks in this chapter, ensure that maxView Storage Manager is installed on every system that will be part of your storage space.

5.1 Overview

To build your storage space, complete these steps:

1. Choose at least one management system (see Choosing a Management System).
2. Start and log in to maxView Storage Manager on the management system (see Starting maxView Storage Manager and Logging In logging in on page 16).
3. Log in to all other systems from the management system (see Logging into Remote Systems from the Local System on page 28).
4. Create arrays and logical drives for all systems in your storage space (see Creating Arrays and Logical Drives).

As your storage requirements change, you can add systems, controllers, and disk drives, then modify the arrays and logical drives in your storage space by following the instructions in Modifying Your Storage Space on page 54.

5.2 Choosing a Management System

You must designate at least one system as a management system, a system from which you will manage the storage on all systems in your storage space.

The management system can be any system on your network that has a video monitor and can run the maxView Storage Manager GUI and Web server.

5.2.1 ‘Local’ or ‘Remote’?

Whenever you’re working in maxView Storage Manager, the system that you’re working on is the local system. All other systems in your storage space are remote systems. ‘Local’ and ‘remote’ are relative terms, as shown in the following figure—when you are working on system A (local system), system B is a remote system; when you are working on system B (local system), system A is a remote system.

For the purposes of this guide, the ‘local system’ is the management system.
5.2.2 Logging in on the Local System

To log in on the local system, see *Starting maxView Storage Manager and Logging In logging in* on page 16.
5.3 Logging into Remote Systems from the Local System

Once maxView Storage Manager is running on all systems in your storage space, you can log into the remote systems from the local system.

Once you have logged in to a remote system, it automatically appears in the Enterprise View each time you start maxView Storage Manager on the local system. You can work with a remote system’s controllers, disk drives, and logical drives as if they were part of your local system.

To log in to a remote system:

1. On the ribbon, in the Home group, click Add System.

The Add System window opens, showing a list of "discovered" systems; that is, systems on your network that are running the Redfish.

   Note:
   
   The list of discovered systems appear only when Auto Discovery option is enabled in maxView. For more details on how to change the auto-discovery settings, see Changing the Auto-Discovery Settings on page 135.

2. Select the systems you want to add to the Enterprise View, then enter the systems’ login credentials (username/password) in the space provided. The Single Sign-On option gets enabled if more than one system is selected. Also, ensure that the selected systems should have same login credentials.

   Note: You can add a system manually if you don’t see the system in the list. For more information, see Manually Adding a Remote System on page 136.
3. Click **Add**.

maxView Storage Manager connects to the remote system(s) and adds them to the list of managed systems in the Enterprise View.

For more information about working with remote systems, see *Managing Remote Systems*.

### 5.4 Creating Arrays and Logical Drives

maxView Storage Manager provides a wizard to help you create, or configure, the arrays and logical drives in your storage space. You can choose from two configuration methods:

- Create logical drive on new array—Helps you set the RAID level for the logical drive, group disk drives and SSDs, determine logical drive size and other advanced settings.
  
  For instructions, see *Creating a Logical Drive on a New Array*.

- Create logical drive on existing array—Helps you select an array on which to create the logical drive, set the RAID level, group disk drives and SSDs, determine logical drive size and configure advanced settings.
  
  For instructions, see *Creating a Logical Drive on an Existing Array*.

If maxCrypto is enabled, you can create encrypted or plaintext volumes. (For more information, see *Working with maxCrypto Devices* on page 77.)

**Note:**

1. Mixing SAS and SATA drives within the same logical drive is not supported. The wizard does not allow you to select a combination of SAS and SATA drive types.

2. maxView Storage Manager supports SMR HA⁴ and SMR DM drives for all RAID levels. However, mixing SMR and PMR⁵ drives within the same logical drive is not supported. maxView Storage Manager displays a warning message if you try to create a logical drive using a combination of SMR and PMR device types.

### 5.4.1 Creating a Logical Drive on a New Array

Before you can create a logical drive, you must create an array. Use the On New Array configuration method to step through the process of creating a logical drive on a new array, setting the RAID level, and configuring other settings.

To create a logical drive on an existing array, see *Creating a Logical Drive on an Existing Array*.

By default, maxView Storage Manager uses all available disk space to maximize the capacity of a new logical drive.

To create a logical drive on a new array:

1. In the Enterprise View, select a system, then select a controller on that system.

2. On the ribbon, in the Logical Device group, click **Create Logical Device**.

---


⁵ PMR: Perpendicular Magnetic Recording; standard HDD recording technology.
3. When the wizard opens, select **On New Array**, then click **Next**.

![Image of Create Logical Device window](image1.png)

4. Select a RAID level for the logical drive, then click **Next**.

![Image of Create Logical Device window](image2.png)

**Note:** Not all RAID levels are supported by all controllers. (See the Release Notes for more information.) See **Selecting the Best RAID Level** for more information about RAID levels.

5. Select the disk drives you want to include in the logical drive, then click **Next**. Be sure the drive type is the same for all drives (SAS or SATA, not mixed), and that you select the right number of drives for the RAID level you selected.
6. *(Optional)* In the RAID Attributes panel, customize the logical drive settings.

You can:

- Enter a name for the logical drive. Names can include any combination of letters, numbers, and spaces.
- Set the size and unit of measure for the logical drive. (By default, a new logical drive uses all available disk space.)
- Change the stripe size—the amount of data, in bytes, written per disk in the logical drive. (The default stripe size usually provides the best performance.)
- Enable or disable controller caching.
- Set the initialization method to Default or Build. The initialization method determines how the logical drive is prepared for reading and writing, and how long initialization will take:
  - **Default**—Initializes parity blocks in the background while the logical drive is available for access by the operating system. A lower RAID level results in faster parity initialization.
Build—Overwrites both the data and parity blocks in the foreground. The logical drive remains invisible and unavailable to the operating system until the parity initialization process completes. All parity groups are initialized in parallel, but initialization is faster for single parity groups (RAID 5). RAID level does not affect performance during Build initialization.

Note: Not all initialization methods are available for all RAID levels.

- Create an encrypted or plaintext logical drive (for more information, see Working with maxCrypto Devices on page 77)

7. Click Next, then review the array and logical drive settings.

   This example shows a RAID 5 logical drive ready to be created on Array A.

8. Click Finish.

   maxView Storage Manager builds the array and logical drive. Use the Event Log and Task Log to track build progress.

9. If you have other disk drives or available disk space and want to create additional arrays on the controller, repeat Steps [2] - [8].


11. Partition and format your logical drives. See Partitioning and Formatting Your Logical Drives on page 35.

5.4.2 Creating a Logical Drive on an Existing Array

After you create an array, you can continue to build your storage space by creating more logical drives on that array. Use the On Existing Array configuration method to step through the process of creating a logical drive on an existing array, setting the RAID level, and configuring other settings.

To create a logical drive on a new array, see Creating a Logical Drive on a New Array.

By default, maxView Storage Manager uses all available disk space to maximize the capacity of a new logical drive.

Note:

You can also add/create Logical drives by selecting the existing array from the Enterprise view.
To create a logical drive on an existing array:

1. In the Enterprise View, select a system, then select a controller on that system.
2. On the ribbon, in the Logical Device group, click **Create Logical Device**.

3. When the wizard opens, select **On Existing Array**, then click **Next**.

4. Select the array on which to create the logical drive, then click **Next**.
5. Select a RAID level for the logical drive, then click Next.

![RAID Level Selection](image)

**Note:** Not all RAID levels are supported by all controllers. (See the Release Notes for more information.) See [Selecting the Best RAID Level](#) for more information about RAID levels.

6. *(Optional)* In the RAID Attributes panel, customize the logical drive settings.

![RAID Attributes Panel](image)

You can:
- Enter a name for the logical drive. Names can include any combination of letters, numbers, and spaces.
- Set the size and unit of measure for the logical drive. (By default, a new logical drive uses all available disk space.)
- Change the stripe size—the amount of data, in bytes, written per disk in the logical drive. (The default stripe size usually provides the best performance.)
• Enable or disable controller caching.

• Set the initialization method to Default or Build. The initialization method determines how the logical drive is prepared for reading and writing, and how long initialization will take:
  ◦ **Default**—Initializes parity blocks in the background while the logical drive is available for access by the operating system. A lower RAID level results in faster parity initialization.
  ◦ **Build**—Overwrites both the data and parity blocks in the foreground. The logical drive remains invisible and unavailable to the operating system until the parity initialization process completes. All parity groups are initialized in parallel, but initialization is faster for single parity groups (RAID 5). RAID level does not affect performance during Build initialization.

  **Note:** Not all initialization methods are available for all RAID levels.

• Create an encrypted or plaintext logical drive (for more information, see *Working with maxCrypto Devices* on page 77)

7. Click **Next**, then review the array and logical drive settings.

   This example shows a RAID 5 logical drive ready to be created on Array A.

![Logical Drive Creation](image)

8. Click **Finish**.

   maxView Storage Manager builds the logical drive on the array. Use the Event Log and Task Log to track build progress.

9. If you have other disk drives or available disk space and want to create more logical drives on an existing array, repeat Steps [2]-[8].

10. Repeat Steps [1]-[9] for each controller in your storage space.

11. Partition and format your logical drives. See *Partitioning and Formatting Your Logical Drives* on page 35.

### 5.4.3 Partitioning and Formatting Your Logical Drives

The logical drives you create appear as physical disk drives on your operating system. You must partition and format these logical drives before you can use them to store data.

**Note:** Logical drives that have not been partitioned and formatted cannot be used to store data.
Refer to your operating system documentation for more information.

5.4.4 Creating Logical Drives on Other Systems in Your Storage Space

If you installed maxView Storage Manager and Smart Storage controllers on more than one system, continue building your storage space as follows:

- From each individual system, log in to maxView Storage Manager and repeat the steps to create logical drives on new or existing arrays, or
- From your local system (the system you’re working on), log in to all other systems in your storage space as remote systems (see Logging into Remote Systems from the Local System), then repeat the steps to create logical drives on new or existing arrays, or
- From your local system, create a server template file and deploy the configuration to the remote systems in your storage space (see Deploying Servers Server Template File).

5.4.5 Controller Support for 4K Drives

This section describes how to use the maxView GUI with 4K drives to create and modify logical drives and spares.

5.4.5.1 Creating a Logical Drive

You can create a logical device using 4K drives. 512-byte drives cannot be mixed with 4K drives. This can be done by selecting the Device Type as HDD SATA 4K or HDD SAS 4K. This will ensure that only HDD SATA 4K or HDD SAS 4K devices are displayed.

5.4.5.2 Moving a Logical Drive

A 4K SAS or 4K SATA logical device can be moved to another array of 4K SAS or 4K SATA drives, but cannot be moved to an array with 512-byte drives.
• Moving to a new array: all SATA and SAS 4K drives that are available to move to a new array are listed.

• Moving to an existing array: if the logical device has already been created in a different array using 4K drives, then the user can move a logical device to the existing array of the same block size SAS/SATA 4K drives. Only arrays created using 4K drives will be listed (512-byte arrays will not be listed).
5.4.5.3 Modifying a Logical Drive

Arrays created using 4K drives can be modified.

- Moving drive(s): you can move a drive from one array to another array that uses the same interface type. For example, if an array is created using 4K SATA drives, then you can move a drive(s) from that array to a separate array that also uses 4K SATA drives.
• Changing drive types: you can change the drive interface type from SAS to SATA or from SATA to SAS. For example, if an array is created using 4K SAS drives, you can change the drive type to 4K SATA drives only.

5.4.5.4 Assigning Spares at the Array Level

Spares for 4K logical drives can be assigned at the array level.
1. Dedicated Hot Spare: If the array/logical device is created using 4K SATA drives, then only the 4K SATA devices can be assigned as spares.

2. Auto Replace Hot Spare: The process is the same as the Dedicated Hot Spare.

**5.4.5.5 Assigning Spares at the Physical Device Level**

Spare for 4K logical drives can be assigned at the physical device level.
• If array/logical device is created with 4K SAS drives, then only logical devices that were created with 4K SAS drives are listed.

Note:
- maxCache cannot be created using 4K SATA drives.
- 512-byte maxCache cannot be assigned to 4K logical devices.
- Drive interface types and drive block sizes cannot be mixed.

For example, SATA drives and SAS drives of the same block size cannot be mixed; 512-byte drives and 4K drives of the same interface type cannot be mixed.
6 Protecting Your Data

In addition to standard RAID (RAID 0, RAID 1, RAID 5, RAID 10), controllers provide additional methods of protecting your data, including dedicated and auto-replace hot spare drives.

A hot spare is a disk drive or SSD (Solid State Drive) that automatically replaces any failed drive in a logical drive, and can subsequently be used to rebuild that logical drive. (For more information, see Recovering from a Disk Drive Failure on page 144.)

6.1 Dedicated Spare or Auto-Replace Spare?

A dedicated hot spare is assigned to one or more arrays. It will protect any redundant logical drive on those arrays.

After using a dedicated hot spare to rebuild a failed logical drive, data is moved back to its original location, using a process called copyback, once the controller detects that the failed drive has been replaced. Once the data is copied back, the hot spare becomes available again. You must create an array before you can assign a dedicated hot spare to protect it. To assign a dedicated hot spare, see Assigning a Dedicated Hot Spare on page 43.

An auto-replace hot spare is assigned to a specific array. It will protect any redundant logical drive on that array. After using an auto-replace spare to rebuild a failed logical drive, it becomes a permanent part of the array. You must create an array before you can assign an auto-replace hot spare to protect it. To assign an auto-replace hot spare, see Assigning an Auto-Replace Hot Spare on page 44.

6.2 Hot Spare Limitations

- Hot spares protect redundant logical drives only. To protect non-redundant logical drives, set the spare activation mode of the controller to predictive activation.
- You cannot create a hot spare from a disk drive that is already part of an array.
- You should select a disk drive that is at least as big as the smallest disk drive in the array that it might replace.
- You must designate a SAS hot spare drive for an array comprised of SAS disk drives, and a SATA hot spare drive for an array comprised of SATA disk drives.
- You can designate a SMR HA or SMR DM drive for all hot spare types. A SMR drive cannot protect a PMR drive, or vice-versa.

---

7 PMR: Perpendicular Magnetic Recording; standard HDD recording technology.
6.3 Assigning a Dedicated Hot Spare

A dedicated hot spare is assigned to one or more arrays. It will protect any redundant logical drive on those arrays.

**Note:** You must create the array before you can assign a dedicated hot spare to protect it.

To assign a dedicated spare:

1. In the Enterprise View, select a controller, an array on that controller, or a Ready physical drive.
2. On the ribbon, in the Physical Device group, click **Spare Management**.

The Spare Management wizard opens.

3. Select the **Dedicated** spare type, then click **Next**.

4. If you selected a physical drive in the Enterprise view, select the arrays you want to protect with a dedicated spare, then click **Next**.
5. If you selected an array in the Enterprise view, select the physical drive(s) you want to dedicate as hot spares, then click Next. (See **Hot Spare Limitations** on page 42 for help selecting drives.)

6. Review the summary of dedicated spares and protected arrays, then click Finish.

### 6.4 Assigning an Auto-Replace Hot Spare

An auto-replace hot spare is assigned to a specific array. After using an auto-replace spare to rebuild a failed logical drive, it becomes a permanent part of the array.

To assign an auto-replace hot spare to an array:

1. In the Enterprise View, select an array on that controller.
Note: The auto-replace option is not available, if you select an array with a non-redundant logical device when the controller’s "spare activation mode" is set to "failure activation". However, when you select a physical device itself, the option is available only if one or more auto-replace spares already exist. Otherwise, you can just assign Dedicated spares in the wizard.

2. On the ribbon, in the Physical Device group, click **Spare Management**.

   ![Spare Management](image)

   The Spare Management wizard opens.

3. Select the **Auto-Replace** spare type, then click **Next**.

   ![Spare Management Wizard](image)

4. If you selected a controller in the Enterprise view, select the array you want to protect with an auto-replace spare, then click **Next**.
5. Select the physical drive(s) you want to assign as auto-replace hot spares, then click **Next**. (See [Hot Spare Limitations](#) on page 42 for help selecting drives.)

6. Review the summary of auto-replace spares and protected arrays, then click **Finish**.

### 6.5 Removing a Hot Spare

You can remove a dedicated or auto-replace hot spare from an array. Removing the last hot spare from an array returns the drive to the **Ready** state.

You may want to remove a hot spare to:

- Make disk drive space available for another array or logical drive.
- Convert an auto-replace hot spare into a dedicated hot spare.
- Remove the 'hot spare' designation from a drive that you no longer want to use as a spare.

To remove a hot spare:

1. In the Enterprise View, select an array or an existing hot spare drive.
2. On the ribbon, in the Physical Device group, click **Spare Management**.

   ![Spare Management wizard](image)

   A wizard used to create, modify and delete hotspares (Global/Dedicated (spooled)).

   The Spare Management wizard opens.

3. Select **Un-Assing**, then click **Next**. (Un-Assign is preselected for an existing hot spare.)

4. If you selected a hot spare in the Enterprise view, select the array(s) from which to remove the spare, then click **Next**.
5. If you selected an array in the Enterprise view, select the hot spare(s) to remove from the array, then click **Next**.

6. Review the summary of affected hot spares and arrays, then click **Finish**. If the spare protects only one array, it is deleted and the drive becomes available for other uses in your storage space. If the spare protects more than one array, it is removed from the selected array(s) but continues to protect the other arrays to which it is assigned.

### 6.6 Setting the Spare Activation Mode

The spare activation mode determines when a hot spare is used to rebuild a failed logical drive. You can choose to activate a spare when:

- A data drive fails; this is the default mode.
- A data drive reports a predictive failure (SMART) status.

In normal operations, the firmware starts rebuilding a failed logical drive with a spare only when a data drive fails. With the predictive failure activation mode, rebuilding can begin before the drive fails, reducing the likelihood of data loss.
The spare activation mode applies to all arrays on a controller.

To set the spare activation mode:

1. In the Enterprise View, select a controller.
2. On the ribbon, in the Controller group, click **Set Properties**.

   ![Set Properties](image)

   The Set Properties window opens.

3. Click the **Data Protection** tab.
4. From the Spare Activation Mode drop-down list, select **Failure** (default) or **Predictive**, then click **OK**.

![Set Properties](image)

### 6.7 Controller Sanitize Lock Freeze/Anti-Freeze

The Sanitize Lock Freeze/Anti-Freeze feature provides the controller level of sanitize lock, which helps prevent accidental erasing of user data on the disk after initiating a sanitize command. To accomplish this, you have the option of applying a controller-wide Sanitize Lock Freeze/Anti-Freeze policy. The freeze and anti-freeze commands will be used to block and unblock the sanitize commands that would erase user data on the disk.

The sanitize lock feature has three options:

- **Freeze**: prevents the user from performing any sanitize erase operation.
- **Anti-Freeze**: locks the freeze command, enabling the user to perform any sanitize erase operation.
- **None**: enables the user to perform any sanitize erase operation

This is applicable only to SATA drives which support Sanitize Erase, Freeze, and Anti-Freeze.

To set the Sanitize Lock:
1. In the Enterprise View, select a controller.
2. On the ribbon, in the Controller group, click **Set Properties**.

The Set Properties window opens.

3. Click the **Data Protection** tab.
4. From the Sanitize Lock drop-down list, select one of the three following options: **None** (default), **Freeze**, or **Anti-Freeze**.

   **Note:**
   
   If the Sanitize Lock is set to any value other than **None**, the following warning message will be displayed in the menu header:
   
   Changing the Sanitize Lock will require a reboot to apply the new state to the controller, and require all physical devices to be power cycled or hot-plugged for the lock state to be applied to the physical devices.

5. Click **OK**.

**6.7.1 Sanitize Lock Property in Controller Node Properties Tab**

The properties of the Sanitize Lock feature are displayed in the controller node properties tab as shown in the following screen capture.
The Sanitize Lock property will display the current setting in which the controller is operating. When the Sanitize Lock property is changed in the Set Properties dialog, the pending Sanitize Lock property will show the changed value. When the machine is rebooted, the pending Sanitize Lock value will be "Not Applicable", and the Sanitize Lock value will be set to the previous pending Sanitize Lock value.

6.7.2 Physical Device Sanitize Lock Freeze/Anti-Freeze

This feature is supported only on SATA drives that are connected to the controller. If the drive supports the Sanitize Lock Freeze feature, it may or may not support the Sanitize Lock Anti-freeze. Based on the support bit on the drive, the Sanitize Lock policy can be set from the controller and it will be applied on the drives that support Sanitize Freeze/Anti-Freeze.

The Sanitize Lock property is dependent upon the following conditions:

- If the drive does not support Sanitize Erase, the Sanitize Lock property is not displayed.
- If the drive supports Sanitize Erase but does not support Freeze/Anti-Freeze, then the Sanitize Lock property will be listed as "Not Applicable".
- If the controller Sanitize Lock is in the Freeze state, then no Sanitize Erase can be performed.
- If the controller Sanitize Lock is in the Anti-Freeze or None state, then all Sanitize Erase commands can be performed.

Once the controller Sanitize Lock is in the freeze state, then no Sanitize Erase operations will listed during the secure erase operation.
6.7.3 Secure Erase Pattern

If the drive or controller Sanitize Lock is in the freeze state, then all the Sanitize Erase patterns will not be listed when you click on the Secure Erase ribbon icon in the physical device ribbon group.

Only three secure erases can be performed.

If the drive and controller Sanitize Lock is in Anti-Freeze or None states, then the Sanitize Erase pattern will be listed.
**Note:** When you perform the Sanitize Erase operation, it sets the controller Sanitize Lock to freeze, and reboots the system, the drive will remember the percentage completion for the Sanitize Secure Erase after the reboot. The freeze state will be applied only after the Sanitize Erase is completed and the sanitize erase operation cannot be stopped.
7 Modifying Your Storage Space

This section provides additional scenarios for creating and modifying arrays and logical drives. It explains how to check your logical drives for bad or inconsistent data; optimize controller and logical drive performance; move arrays and logical drives; and perform advanced operations, such as creating a split mirror backup array.

7.1 Understanding Arrays and Logical Drives

A logical drive is a group of physical disk drives that appears to your operating system as a single drive that can be used to store data.

The group of physical drives containing the logical drive is called a drive array, or just array. An array can contain several logical drives, each of a different size.

You can include the same disk drive in two different logical drives by using just a portion of the space on the disk drive in each, as shown in the following figure.
Disk drive space that has been assigned to a logical drive is called a segment. A segment can include all or just a portion of a disk drive’s space. A disk drive with one segment is part of one logical drive, a disk drive with two segments is part of two logical drives, and so on. When a logical drive is deleted, the segments that comprised it revert to available space (or free segments).

A logical drive can include redundancy, depending on its RAID level. (See Selecting the Best RAID Level for more information.)

You can also protect your logical drives by assigning one or more hot spares to them. (See Protecting Your Data on page 42 for more information.)

7.2 Creating and Modifying Logical Drives

For basic instructions for creating logical drives, see Building Your Storage Space on page 26.

This section describes additional scenarios for creating logical drives:

- To create a logical drive from different-sized disk drives, see Including Different-sized Disk Drives in a Logical Drive on page 55.
- To create a logical drive using available segments of disk drives, see Creating a Logical Drive Using Available Segments.

7.2.1 Including Different-sized Disk Drives in a Logical Drive

You can combine disk drives of different sizes in the same logical drive. If the logical drive includes redundancy, however, the size of each segment can be no larger than the size of the smallest disk drive. (See Selecting the Best RAID Level for more information about redundancy.)

**Note:** You cannot combine SAS and SATA disk drives and also different block size like 512 bytes or 4K within the same array or logical drive.

To create a logical drive with disk drives of different sizes, follow the instructions in Creating a Logical Drive on a New Array. When the wizard displays the RAID Members panel, select different size drives, as shown in the figure below, then complete the wizard.
When the logical drive is created, check its resources on the Storage Dashboard: it should appear similar to the next figure, where a RAID 5 logical drive includes two disk drives of one size and one of another.

RAID5 with different size disks. No segment is larger than smallest disk drive (931.5 GB, in this example).
7.3 Enabling Background Consistency Check

When background consistency check is enabled, maxView Storage Manager continually and automatically checks your logical drives for bad or inconsistent data, and then fixes any problems. Enabling consistency check ensures that you can recover data if a logical drive fails. The scanning process checks physical drives in fault-tolerant logical drives for bad sectors. It also verifies the consistency of parity data, if applicable. The available modes are High, Disable, Idle. If you select the Idle mode, you must also specify a delay value and parallel scan count.

To enable or disable background consistency check:

1. In the Enterprise View, select a controller.
2. On the ribbon, in the Controller group, click Set Properties.

The Set Properties window opens.

3. Click the Data Protection tab.
4. In Consistency Check Mode drop-down list, select High, Disabled, or Idle.

5. If you selected the Idle mode, enter the consistency check delay (in seconds) and parallel consistency check count:
   - **Consistency Check Delay**—Amount of time the controller must be inactive before the consistency check is started. Enter a value from 0-30. A value of 0 disables the scan.
   - **Parallel Consistency Check Count**—Number of logical drives on which the controller will perform the consistency check in parallel.

6. Click **OK**.

### 7.4 Optimizing Logical Drive Performance

This section describes how to enable controller cache optimizations and SSD I/O bypass acceleration to improve I/O throughput on the logical drives in your storage space. You can apply cache optimizations independently on a per controller or per logical drive basis. You can apply I/O bypass acceleration on arrays comprised of SSDs only.

#### 7.4.1 Enabling Cache Optimizations

Use this option to enable the following cache optimizations on the controllers in your storage space. You can apply cache optimizations independently on a per controller or per logical drive basis.

**Note:** You cannot use controller caching and maxCache caching concurrently. Controller caching is available only if maxCache is not enabled on the controller. For more information about maxCache, see *Working with maxCache Devices* on page 73.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cache Ratio</td>
<td>Sets the global Read:Write cache ratio.</td>
</tr>
<tr>
<td>Write Cache Bypass Threshold</td>
<td>Sets the write cache block size threshold, above which data is written directly to the drive.</td>
</tr>
<tr>
<td>No Battery Write Cache</td>
<td>Enables write caching on controllers without a backup module.</td>
</tr>
<tr>
<td>Wait for Cache Room</td>
<td>Waits for cache space (if none is available) before completing the request.</td>
</tr>
</tbody>
</table>
To enable cache optimizations on a controller:
1. In the Enterprise View, select a controller.
2. On the ribbon, in the Controller group, click **Set Properties**.

When the Set Properties window opens, click the **Cache** tab.
3. Adjust cache settings, as needed.

4. Click **OK**.

### 7.4.1.1 Enabling Cache Optimization for a Logical Drive

You can enable/disable cache optimization for each logical drive in your storage space:

1. In the Enterprise View, select a controller, then select a logical drive.
2. On the ribbon, in the Logical Device group, click **Set Properties**.
3. In the Write-Cache Mode drop down-list, select **Disabled (Write-Through)** or **Enabled (Write-Back)**.
4. Click **OK**.
7.4.2 Enabling SSD I/O Bypass

Use this option to enable I/O Bypass acceleration for logical drives comprised of SSDs only. This option enables I/O requests to bypass the controller firmware and access SSDs directly. This process accelerates reads for all RAID levels and writes for RAID 0.

To enable I/O Bypass acceleration:

1. In the Enterprise View, select a controller, then select an array on the controller.
2. On the ribbon, in the Array group, click Set Properties.

The Set Properties window opens; the General tab is selected, by default.

3. From the SSD I/O Bypass drop-down, select Enabled or Disabled.

4. Click OK.

7.5 Moving a Logical Drive

maxView Storage Manager allows you to move a single logical drive from one array to another array. You can choose the following destinations:

- Move Logical Drive To a New Array
- Move Logical Drive To an Existing Array

If you move the logical drive to a new array, the array is created automatically. If you move the logical drive to an existing array, it must have sufficient space and member disk drives to store the logical drive data and accommodate the RAID level; for example, three drives, minimum, for a RAID 5.
Note: Moving a logical drive can be a time-consuming process. All data in the logical drive is moved onto the new or existing array, and the controller continues to service I/O requests to other logical drives.

To move a logical drive:

1. In the Enterprise View, select a logical drive.
2. On the ribbon, in the Logical Device group, click **Move Logical Device**.

3. When the wizard opens, select **To New Array** or **To Existing Array**, then click **Next**.

4. If you are moving the logical drive to a new array, select the physical drives for the array. Be sure the drive type is the same for all drives (SAS or SATA, not mixed).
Note: The drives must have sufficient capacity to store the logical drive data.

5. If you are moving the logical drive to an existing array, expand the Arrays and Logical Devices list, then select the destination array.

6. Click Next, review the summary information, then click Finish. maxView Storage Manager moves the logical drive onto the new or existing array. If you moved the last logical drive on an array, maxView Storage Manager deletes the array and removes it from the Enterprise View.

7.6 Moving an Array

You can move an array by replacing its physical drives with drives of the same type or different type. For example, you can replace SAS drives in the array with other SAS drives, or replace SAS drives with SATA drives. You cannot combine drive types in the same array, however. If you choose to replace SAS drives
with SATA drives, for example, all drives in the array must be replaced with SATA drives. The replacement drives must be in the Ready state; that is, not part of any array or assigned as a spare.

Moving an array automatically removes any previously assigned spare drives. Replaced drives in the array are freed and become Ready drives that can be used in other arrays, logical drives, or as spares.

**Note:** Moving an array can be a time-consuming process. All data in each logical drive is copied to the replacement drives, and the controller continues to service I/O requests to other logical drives.

To move an array:

1. In the Enterprise View, select an array.
2. On the ribbon, in the Array group, click **Modify Array**.

3. When the wizard opens, select an action, then click **Next**:
   - Select **Move Drives** to replace array drives with drives of the same type.
   - Select **Change Drive Type** to replace array drives with drives of a different type.

4. Select one or more drives. For Move Drives, the wizard displays only physical devices of the same type. For Change Drive Type, the wizard displays only physical devices of a different type. The RAID level determines the number of drives you need to select.
Note: The drives must have sufficient capacity to hold all of the logical drives in the source array.

5. Click Next, review the summary information, then click Finish.

7.7 Modifying an Array

maxView Storage Manager allows you to perform different actions to reconfigure an array. You can choose the following destinations:

- Add Drives To an Array
- Move Drives To an Array

If you add the logical drives, you are expanding the array by adding the data drives. If you move the logical drive to an existing array, you need to replace the array drives with the drives of the same type.

Note: Moving a logical drive can be a time-consuming process. All data in the logical drive is moved onto the new or existing array, and the controller continues to service I/O requests to other logical drives.

To add or remove drives in an array:

1. In the Enterprise View, select an array.
2. On the ribbon, in the Array group, click Modify Array.
3. When the wizard opens, select Add Drive(s) or Move Drive(s), then click Next.
4. If you are adding the new drives to an array, select the physical drives for the array. Be sure the drive type is the same for all drives (SAS or SATA, not mixed).

Note: The drives must have sufficient capacity to store the logical drive data.

5. Click Next, review the summary information, then click Finish. maxView Storage Manager moves the logical drive onto the new or existing array. If you moved the last logical drive on an array, maxView Storage Manager deletes the array and removes it from the Enterprise View.

7.8 Working with Mirrored Arrays

maxView Storage Manager allows you to split a mirrored array and then recombine it. This process entails splitting a RAID 1, RAID 1(ADM), RAID 10, or RAID 10(ADM) array into two identical new arrays consisting of RAID 0 logical drives. Arrays with other RAID configurations cannot be split.
7.8.1 Creating a Split Mirror Backup

Use this option to split a mirrored array, consisting of one or more RAID 1, RAID 1(ADM), RAID 10, or RAID 10(ADM) logical drives, into two arrays: a primary array and a backup array, with these characteristics:

- The primary array and backup array will contain identical RAID 0 logical drives.
- The primary array continues to be fully accessible to the operating system.
- The backup array is hidden from the operating system and data on the drive is frozen.

**Note:** You can use the backup array to restore the primary array with its original contents. See Re-mirroring, Rolling Back, or Reactivating a Split Mirror Backup on page 66.

- The primary array includes the designation "Split Mirror Set Primary" as the device type.
- The backup array includes the designation "Split Mirror Set Backup" as the device type.

If the array is protected by a spare drive, the drive is unassigned after the split.

To create a split mirror backup:

1. In the Enterprise View, select a mirrored array.
2. On the ribbon, in the Array group, click **Split Mirror Backup**.
3. When prompted to create the backup array, click **OK**.

7.8.2 Re-mirroring, Rolling Back, or Reactivating a Split Mirror Backup

When you re-mirror a split mirrored array, you recombine the primary array and backup array into a single array. You can:

- Re-mirror the array and preserve the existing data; the backup array is discarded. This option re-creates the original mirrored array with the current contents of the primary array.
- Re-mirror the array and roll back to the contents of the backup array; existing data is discarded. This option re-creates the mirrored array but restores its original contents from the backup array.

You can also reactivate the split mirror backup. This option makes the backup array fully accessible to the operating system. maxView Storage Manager removes the "Split Mirror Set Backup" designation and re-designates it as a Data Array.
To re-mirror, roll back, or reactivate a split mirror backup:

1. In the Enterprise View, select the Split Mirror Set Primary array; that is, an array with an existing split mirror backup.
   
   **Note:** Use the Summary tab on the Storage Dashboard to verify the array type.

2. On the ribbon, in the Array group, click Remirror/Activate Backup.

   ![Remirror/Activate Backup button](image)

3. When prompted to select a re-mirroring task, choose: Re-mirror array, Re-mirror with roll-back, or Activate Backup.
   
   **Note:** Microsemi recommends that you do not perform a re-mirror with roll back if the logical drive to be rolled back is mounted or in use by the operating system.

4. Click OK.

### 7.9 Changing the RAID Level of a Logical Drive

If your storage needs or application requirements change, you can change, or migrate, the RAID level of your logical drives to another, more suitable, RAID level. You might want to change the RAID level to add redundancy, further protect your data, or to improve data availability for speedier access. See Selecting the Best RAID Level for more information.

The following RAID level migrations are supported:

- RAID 0 to RAID 5
- RAID 0 to RAID 10
- RAID 5 to RAID 6
- RAID 6 to RAID 5
- RAID 10 to RAID 5
- RAID 5 to RAID 10
- RAID 1 to RAID 5

To change the RAID level of a logical drive:

1. In the Enterprise View, select a controller, then select the logical drive that you want to migrate.

2. On the ribbon, in the Logical Device group, click Expand/Migrate.
The Expand/Migrate Logical Device wizard opens.

3. Click **Migrate**, then click **Next**.

4. Select a new RAID level, then click **Next**. Only valid RAID level options are offered.

5. Select the sub array count for RAID 50 and RAID 60.

6. Select the logical drive stripe size from the drop-down list.
Note: The default stripe size usually provides the best performance.

7. Click Next.
8. Review the summary of logical drive settings. To make changes, click Back.
9. Click Finish.
   The logical drive is reconfigured and migrates to the new RAID level.

7.10 Increasing the Capacity of a Logical Drive

You can add more disk drive space, or expand, a logical drive, to increase its capacity.

The expanded logical drive must have a capacity that is greater than or equal to the original logical drive.

Note: You can expand a logical drive only into the free space of the host array. To add physical drives in an array, see Modifying an Array on page 64.

To increase the capacity of a logical drive:
1. In the Enterprise View, select a controller, then select the logical drive you want to expand.
2. On the ribbon, in the Logical Device group, click Expand/Migrate.

The Expand/Migrate Logical Device wizard opens.

3. Click Expand, then click Next.

4. Enter the new logical drive size in the space provided. It must be greater than or equal to the current size.
5. Click **Next**.

6. Review the summary of logical drive settings. To make changes, click **Back**.

7. Click **Finish**.
   
The logical drive is expanded and its capacity is increased to the new size.

### 7.11 Changing the Logical Drive Rebuild Priority

The Rebuild Priority setting determines the urgency with which the controller treats an internal command to rebuild a failed logical drive:

- At the low setting, normal system operations take priority over a rebuild.
- At the medium setting, normal system operations and rebuilds get equal priority.
- At the medium high setting, rebuilds get higher priority than normal system operations.
- At the high setting, rebuilds take precedence over all other system operations.

If the logical drive is part of an array with an online spare, rebuilding begins automatically when drive failure occurs. If the array does not have an online spare, rebuilding begins when the failed physical drive is replaced. For more information, see *Rebuilding Logical Drives* on page 147.

To change the rebuild priority:

1. In the Enterprise View, select a controller.

2. On the ribbon, in the Controller group, click **Set Properties**.

   ![Set Properties Window](image)

   The Set Properties window opens.

3. In Rebuild Priority Mode drop-down list, select **Low**, **Medium**, **Medium High**, or **High**. The Rebuild Priority field is circled in the next figure.
4. Click OK.

### 7.12 Renaming a Logical Drive

To change the name of a logical drive:

1. In the Enterprise View, select a controller, then select the logical drive you want to rename.
2. On the ribbon, in the Logical Device group, click Set Properties.

The Set Properties window opens.

3. In the Logical Device Name field, type the new name, then click OK. Names can include any combination of letters, numbers, and spaces.

   maxView Storage Manager updates the logical drive name and displays the new name in the Enterprise View.

### 7.13 Deleting an Array or Logical Drive

When you delete an array or logical drive, it is removed from the Enterprise View and the disk drives or segments in the logical drive(s) become available to use in a new array or logical drive (see Creating a Logical Drive Using Available Segments).

**Caution:** When you delete an array you lose all data on the logical drive(s) within the array, in addition to the array itself. When you delete a logical drive, you lose all data stored on that logical drive. Be sure you no longer need the data on the array or logical drive before you delete it.

To delete an array or logical drive:

1. In the Enterprise View, select the array or logical drive you want to delete.
2. On the ribbon, in the Array group or Logical Device group (shown below), click Delete.

3. When prompted to continue, click Delete to delete the array or logical drive.

   **Note:** If a deleted logical drive is the only logical in the array, the array itself is also deleted.

### 7.14 Maintaining an Energy-Efficient Storage Space

The power management options in maxView Storage Manager control the power profile of the physical drives on a controller. They offer a balance between maximum performance and minimum power usage. To ensure continued operations when temperature thresholds are exceeded, you can enable Survival mode to throttle dynamic power settings to their minimum values.
To set the power management options for a controller:

1. In the Enterprise View, select a controller.

2. On the ribbon, in the Controller group, click **Set Properties**.

The Set Properties window opens.

3. Click the **Power Management** tab.

4. In the Power Mode drop-down list, select:
   - Minimum Power—Set power settings to lowest possible values and reduce power dynamically, based on workload.
   - Maximum Performance—Set power settings to highest possible values and do not reduce power dynamically.

5. In the Survival Mode drop-down list, select:
   - Enabled—Allows the controller to throttle back dynamic power settings to their minimum values when temperatures exceed the warning threshold.
     
     **Note:** Enabling Survival mode allows the server to continue running in more situations, but may affect performance.
   - Disabled—Disables Survival mode.

6. Click **OK**.
8 Working with maxCache Devices

Microsemi Adaptec Smart Storage Controllers support an advanced SSD caching technology called maxCache™. maxCache uses a reserved logical drive, called the maxCache Device, to support read and redundant write caching for storage connected directly to your controller. The maxCache Device is comprised of SSDs only.

With maxCache read caching enabled, the system copies frequently read "hot" data to the maxCache Device for faster retrieval. With maxCache write caching enabled, the maxCache Device is populated with certain "hot" blocks from the logical drives on the controller. All writes to these hot blocks go directly to the maxCache Device. The data remain on the maxCache Device until it is full or some other "hotter" data replaces it.

8.1 maxCache Limitations

- maxCache is not supported on all Microsemi Adaptec Smart Storage Controllers. For more information, see PMC-2153191 maxView Storage Manager and ARCCONF Command Line Utility Readme.
- If the maxCache controller has a green backup module, the super capacitor must be fully charged.
- Following are the limitations on maxCache device:
  - It must be created with SSDs
  - It must have logical block size of 512 bytes
  - Minimum maxCache device capacity is 16 GB
  - Maximum aggregate maxCache device sizes can be ~1.7TB for 64KB cache line size, ~6.8TB for 256KB cache line size.
- Following are the limitations on the data logical device for which the maxCache device to be assigned:
  - It must have the capacity at least as large as the maxCache device
  - It must have logical block size of 512 bytes
  - Maximum data logical device size can be 256TB for the maxCache created with 64KB cache line size, 1024TB for the maxCache created with 256KB cache line size
- The following operations are not available when maxCache is enabled:
  - Expand Array/Logical Device
  - Move Logical Device
  - Replace Array Drives
  - Split Mirror
  - Heal Array
  - Migrate Array

8.2 Creating a maxCache Device

To create a maxCache Device:

1. In the Enterprise View, select a system, then select a controller on that system. You can also create a maxCache device by selecting a logical device node.

2. On the ribbon, in the maxCache group, click Create maxCache.
3. When the wizard opens, select a RAID level for the maxCache Device, then click **Next**.

   See *Selecting the Best RAID Level* for more information about RAID levels.

4. Select the SSDs that you want to include in the maxCache Device, then click **Next**. Be sure to select the right number of SSDs for the RAID level you selected.

5. Select the data logical drive (16 GB minimum), then click **Next**.

6. *(Optional)* In the Cache Attributes panel, customize the maxCache Device settings. You can:
   
   - Set a smaller logical drive size. (By default, the maxCache Device uses up to the maxSize of the data logical drive.)
   - Set the write cache mode to Write-Back (default) or Write-Through.
• Select the Cache Line Size. The Cache Line Size impacts the cache performance and the maximum size selected. To create a large size maxCache you need to select the larger cache line size supported by that controller.

7. Click **Next**, then review the logical drive settings.

8. Click **Finish**, then click **OK**.

   maxView Storage Manager updates the configuration, then adds an array and logical device to the maxCache Device tree in the Enterprise View.

### 8.3 Changing the Write Cache Mode

The write cache mode determines when data is stored on the maxCache Device and when the controller communicates with the operating system. You can set the Write Cache mode to:

- **Write-Through**—The controller sends (or writes) the data to the maxCache Device, then sends confirmation to the operating system that the data was received. Use this setting when performance is less important than data protection.
- **Write-Back**—The controller sends confirmation to the operating system that the data was received, then writes the data to the maxCache Device. Use this setting when performance is more important than data protection.

To change the maxCache write cache mode:

1. In the Enterprise View, select a controller, then select a maxCache Device on that controller.

2. On the ribbon, in the maxCache group, click **Set Properties**.

   The Set Properties window opens.

3. In the Write Cache drop-down list, select **Write-Back** or **Write-Through**.

4. Click **OK**.

### 8.4 Deleting the maxCache Device

When you delete the maxCache Device, the component SSDs become available and can be used to create a new logical drive, hot spare, or new maxCache Device.

**Caution:** Be sure that the maxCache controller is quiescent before deleting the maxCache Device; otherwise you may lose data.

**Note:**

Also, the delete maxCache option is available only when the write-cache policy is set to "write-through" and is the last maxCache logical device in the maxCache array.

To delete the maxCache Device:

1. In the Enterprise View, select a controller, then select the maxCache Device.

2. On the ribbon, in the maxCache group, click **Delete**.
3. When prompted, click **Delete**, then click **OK**. Click **Cancel** to cancel the action.

**8.5 Analyzing maxCache Performance**

maxView Storage Manager provides advanced usage statistics about the maxCache Devices on your Microsemi Smart Storage controllers. You can use these statistics to gain a better understanding of how maxCache is performing in your storage space. Use the Statistics Viewer to view the maxCache statistics; see **Viewing Advanced Statistics** on page 126 for more information.
9 Working with maxCrypto Devices

Microsemi Smart Storage Controllers support an advanced controller-based encryption (CBE) technology called maxCrypto™. It provides an enterprise-class encryption solution that protects sensitive data on storage connected directly to your controller.

maxCrypto supports two roles for managing encryption services:

- A Crypto Officer (Admin) role that can perform all encryption operations
- A User role with reduced privileges

maxCrypto allows you to selectively encrypt arrays and logical drives, regardless of RAID level; create storage spaces with mixed encrypted and plaintext volumes; and convert plaintext volumes to encrypted volumes.

**Note:** Encryption of non-RAID volumes (such as physical, raw, or pass-through devices) is not supported. Consequently, HBAs and controllers operating in HBA Mode do not support maxCrypto.

9.1 maxCrypto Initial Setup

Before you can begin using maxCrypto in your storage space, you must complete the initial setup task to create the Crypto Officer account and configure the initial maxCrypto settings, including the Crypto Officer login credentials, maxCrypto master encryption key, and other basic information. You must also accept the maxCrypto Certificate of Use.

To setup maxCrypto:

1. In the Enterprise View, select a system, then select a controller on that system.
2. On the ribbon, in the Controller group, click **maxCrypto Settings**.

![maxCrypto Settings](Image)

The Set maxCrypto Configuration window opens; the Initial Setup tab is selected, by default.
3. In the maxCrypto Mode drop-down, select **Enabled** to activate maxCrypto. Select **Disabled** to deactivate maxCrypto.

4. In the Allow New Plaintext Logical Device(s) drop-down, select **Enabled** to allow plaintext logical devices to be created, in addition to encrypted logical devices. Select **Disabled** to allow only encrypted logical devices to be created.

   **Note:** To create plaintext logical devices, both maxCrypto Mode and Allow New Plaintext Logical Device(s) must be enabled.

5. In the Master Key field, enter the maxCrypto master encryption key. The Master Key is a 10-32 character string, comprising all printable ASCII characters.

   **Caution:** Be sure to record the master key and store in a safe place. Once set, the Master Key cannot be displayed or recovered, only reset. Failure to provide the Master Key may result in encrypted data being irretrievable.

6. In the Enter Crypto Password field, enter the Crypto Officer password. The password is a 8-16 character string, comprising all printable ASCII characters. It must include at least one uppercase character, one lowercase character, one numeric, and one special character (#,!,@,...).

7. In the Re-Enter Crypto Password field, re-enter the Crypto Officer password.

8. Click **OK**.

9. When the maxCrypto Certificate of Use window opens, click **Agree** to complete the maxCrypto activation.
9.1.1 Managing maxCrypto Accounts

After initial setup is complete, the Crypto Officer account is logged in, by default. As the Crypto Officer, you can perform all account management operations, including configuring the standard User account, changing passwords, and enabling password recovery options. If you are logged into the standard User account, you have the ability to perform a limited number of maxCrypto operations, as described in the table below.

<table>
<thead>
<tr>
<th>Standard users can:</th>
<th>Standard users can’t:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log into maxCrypto</td>
<td>Perform initial setup</td>
</tr>
<tr>
<td>Lock/Unlock firmware update</td>
<td>Recover password</td>
</tr>
<tr>
<td>Enter/Re-Enter new password</td>
<td>Allow new plaintext logical device(s)</td>
</tr>
<tr>
<td>Create encrypted and plaintext logical drives</td>
<td>Set/Change master key</td>
</tr>
<tr>
<td>Convert plaintext array/logical drive to encrypted data</td>
<td>Import master key</td>
</tr>
<tr>
<td>Crypto erase array/logical drive</td>
<td>Set/Change password recovery question</td>
</tr>
<tr>
<td>Clear maxCrypto configuration</td>
<td></td>
</tr>
</tbody>
</table>

To manage maxCrypto accounts:

1. In the Enterprise View, select a system, then select a controller on that system.
2. On the ribbon, in the Controller group, click maxCrypto Settings.

When the Set maxCrypto Configuration window opens, click the Account tab.
3. In the User Role drop-down, select the Crypto Officer or User account.

4. In the Enter New Password field, enter the password for the account.

   The password is a 8-16 character string, comprising all printable ASCII characters. It must include at least one uppercase character, one lowercase character, one numeric, and one special character (#,!,@,...).

   **Note:** The first time you enable the User account, this entry defines the initial login credentials for the account. For an existing account, this entry changes the login credentials.

5. In the Re-Enter New Password field, re-enter the password for the user account.

6. For the Crypto Officer account, set/change the password recovery question and answer:
   a. In the Set/Change Password Recovery Question field, enter a recovery question for a forgotten password.
   b. In the Set/Change Password Recovery Answer field, enter the answer to the recovery question.

   **Note:** Password recovery is available only for the Crypto Officer. The recovery question/answer fields are deactivated for the User account.

7. Click OK.

**9.1.2 Logging In and Logging Out**

You must be logged into maxCrypto to use the encryption features in maxView Storage Manager, from encrypting a logical drive, to enabling plaintext volumes, to simply changing a maxCrypto password.

After initial setup is complete, the Crypto Officer account is logged in, by default.

To logout of the account (ending the maxCrypto session), simply click the **Logout** button on the Account tab or General tab in the Set maxCrypto Configuration window.
To login back in, or to login to a different account:

1. In the Enterprise View, select a system, then select a controller on that system.
2. On the ribbon, in the Controller group, click **maxCrypto Settings**.

When the Set maxCrypto Configuration window opens, click the **Login tab**.

3. In the User Role drop-down, select the **Crypto Officer** or **User account**.
4. In the Password field, enter the password for the user role.
   
   **Note:** If you’re logging in as the Crypto Officer and forgot the password, you can reset
the password by following the steps below.

5. Click OK.

To reset the Crypto Officer password:

1. In the Login tab, select the **Crypto Officer** user role, as described above.
2. Click **Forgot Password**.
3. In the Recovery Answer field, enter the answer to the recovery question.
4. Enter a new password for the Crypto Officer account.
   
   The password is a 8-16 character string, comprising all printable ASCII characters. It must include at
least one uppercase character, one lowercase character, one numeric, and one special character
(#,!,@,...).
5. Re-enter the new Crypto Officer password.
6. Click **OK**.

9.1.3 Checking maxCrypto Status

To check the maxCrypto status, select a controller in the Enterprise view, then click the **maxCrypto tab** on
the storage dashboard. Before completing the initial setup steps, most maxCrypto properties will be listed
as "Not Configured". After completing the initial setup steps, the main maxCrypto properties will be
Configured, as described in the table below.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>maxCrypto Status</td>
<td>When Enabled, both Encrypted and Plaintext logical devices can be created, based on the Allow New Plaintext Volumes property. When Disabled, only Plaintext logical devices can be created.</td>
</tr>
<tr>
<td>Allow New Plaintext Volumes</td>
<td>When Enabled, both Plaintext and Encrypted logical devices can be created. When Disabled, only Encrypted logical devices can be created, when maxCrypto Status is Enabled.</td>
</tr>
</tbody>
</table>
### 9.2 Modifying the maxCrypto Configuration

To modify the maxCrypto configuration, use the General tab on the Set maxCrypto Configuration window.

If you are logged in as the Crypto Officer, you can:
- Enable/Disable maxCrypto
- Enable/Disable new plaintext volumes
- Lock/Unlock firmware upgrade
- Change the maxCrypto master encryption key

If you are logged in as the maxCrypto User, you can only Lock/Unlock firmware upgrade.

To modify the maxCrypto configuration:
1. In the Enterprise View, select a system, then select a controller on that system.
2. On the ribbon, in the Controller group, click **maxCrypto Settings**.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master Key</td>
<td>After Initial setup, Master Key value is displayed as Configured.</td>
</tr>
<tr>
<td>Firmware Locked for Update</td>
<td>If Unlocked, firmware upgrade is enabled. If Locked, firmware upgrade is disabled.</td>
</tr>
<tr>
<td>Number of maxCrypto Logical Devices</td>
<td>Total count of the encrypted logical devices.</td>
</tr>
<tr>
<td>Number of maxCrypto Physical Devices</td>
<td>Total count of encrypted physical devices.</td>
</tr>
<tr>
<td>Crypto Officer Password</td>
<td>After Initial setup, Crypto Officer Password will be displayed as Configured.</td>
</tr>
<tr>
<td>Login Status</td>
<td>If logged-in as the Crypto Officer (Admin), displays &quot;Logged-in as Crypto&quot;. If logged in as User, displays &quot;Logged-in as User&quot;. If maxCrypto session timed out, displays &quot;Timeout&quot;. If maxCrypto is logged-out, displays as &quot;Not Logged In&quot;.</td>
</tr>
<tr>
<td>User Password</td>
<td>If the User account is configured, displays as &quot;Configured&quot;; otherwise, displays as &quot;Not Configured&quot;.</td>
</tr>
<tr>
<td>Crypto Password Unlock Attempts Remaining</td>
<td>Countdown of Crypto Officer attempts remaining after a failed login. Note: After 10 failed login attempts, the Crypto Officer account is locked for 15 minutes.</td>
</tr>
<tr>
<td>User Password Unlock Attempts Remaining</td>
<td>Countdown of User role attempts remaining after a failed login. Note: After 10 failed login attempts, the User account is locked for 15 minutes.</td>
</tr>
<tr>
<td>Crypto Officer Password Recovery Parameters</td>
<td>Displays as &quot;Configured&quot; when Crypto Officer sets the password recovery question and answer. Displays as &quot;Not Configured&quot; when Crypto Officer has not set the password recovery question and answer.</td>
</tr>
</tbody>
</table>
When the Set maxCrypto Configuration window opens, click the **General tab**.

3. Adjust the maxCrypto settings, as needed:
   - In the **maxCrypto** field, select **Enabled** or **Disabled** to enable/disable the maxCrypto system.
   - In the **Allow New Plaintext Volumes** field, select **Enabled** to allow plaintext volumes and encrypted volumes in your storage space. Select **Disabled** to allow encrypted volumes only in your storage space.
   - In the **Firmware Locked for Update** field, select **Unlocked** to allow firmware upgrades. Select **Locked** to block firmware upgrades.
   - To change the master encryption key, click **Change Master Key**, then enter the new key in the **Set/Change Master Key** field.

   **Caution:** Be sure to record the master key and store in a safe place. Once set, the Master Key cannot be displayed or recovered, only reset. Failure to provide the Master Key may result in encrypted data being irretrievable.

4. Click **OK**.

### 9.3 Creating an Encrypted Logical Drive

Use the Create Logical Device wizard to create encrypted and plaintext logical drives on an existing array or a new array. See **Creating Arrays and Logical Drives** on page 29.

When the wizard reaches the RAID Attributes panel, click **Create Encrypted Logical(s)** to encrypt the logical device. Un-check the check box to create a plaintext logical device.
Working with maxCrypto Devices

Note:
1. If maxCrypto status is Disabled, only plaintext logical drives can be created.

2. If maxCrypto status is Enabled and Allow New Plaintext Volumes property is Enabled, both encrypted and plaintext logical drives can be created; the default is encrypted.
   
   Note: You must be logged in to maxCrypto to create plaintext volumes, even if maxCrypto status and Allow New Plaintext Volumes are both Enabled; see Logging In and Logging Out on page 80.

3. If maxCrypto status is Enabled and Allow New Plaintext Volumes property is Disabled, only encrypted logical drives can be created.

9.4 Converting Plaintext Data to Encrypted Data

Use this operation to convert plaintext data to encrypted data. You can convert an unencrypted logical drive or all unencrypted logical drives on an array. Additionally, you can choose to preserve or discard the existing data during conversion.

To convert plaintext data:

1. In the Enterprise View, select a controller, then select a plaintext (unencrypted) logical drive or an array.

2. On the ribbon, in the Logical Device group or Array group, click Set Properties.

When Set Properties window opens, click the maxCrypto tab.
3. Click the Convert Plaintext Data to Encrypted Data check box.
4. To preserve the data during conversion, click the Preserve Existing Data check box. Leave it un-checked to discard the data.
   Note: When you convert a plaintext volume to an encrypted volume without preserving existing data, the old plaintext data remains on disk and is still available if the logical device is deleted.
5. Click OK.

9.5 Re-Keying a Logical Drive

maxCrypto allows you to re-key a logical drive for added security. The logical drive key is used with the master key to encrypt the device.

Optionally, you can re-key an array to generate a new key for all encrypted logical drives on the array.

To re-key a logical drive:
1. In the Enterprise View, select a controller, then select an encrypted logical drive or array.
2. On the ribbon, in the Logical Device group or Array group, click Set Properties.

When Set Properties window opens, click the maxCrypto tab.
3. Click the **Logical Device(s) Key ReKey** check box.

4. Click **OK**.

### 9.6 Clearing the maxCrypto Configuration

You can clear the maxCrypto configuration to restore the default maxCrypto settings. Clearing the maxCrypto configuration resets all keys, passwords, and users, including the maxCrypto Officer account and User account.

**Note:** To clear the maxCrypto configuration, ensure that there is no encrypted logical drive available in your storage space.

To clear the maxCrypto configuration:

1. In the Enterprise View, select a system, then select a controller on that system.
2. On the ribbon, in the Controller group, click **Manage Configuration**.

The Manage Configuration wizard opens.
3. Select **Clear maxCrypto**, then click **Next**.
4. Review the Summary information, then click **Finish**.

## 9.7 Erasing an Encrypted Logical Drive

You can cryptographically erase the data on any encrypted logical drive in the Optimal state. Crypto erase performs an instant/quick erase. The logical drive remains in the Enterprise View and ready to store new data.

Optionally, you can cryptographically erase an array, to erase the data on all encrypted logical drives on the array.

**Caution:** When you cryptographically erase a logical drive, you lose all data on that drive.

To cryptographically erase a logical drive:

1. In the Enterprise View, select a controller, then select an encrypted logical drive or array.
2. On the ribbon, in the Logical Device group or Array group, click **Crypto Erase**.

The Crypto Erase Logical Device window opens.
3. Click **Erase**.

### 9.8 Importing a Foreign Master Key

When an encrypted logical drive is moved from another controller, the master key used to encrypt the logical drive is needed to decrypt it. Use the Import Foreign Master Key option to import the master key so that the logical drive data can be accessed and managed on the new controller.

To import a foreign master key:

1. In the Enterprise View, select a system, then select a controller on that system.
2. On the ribbon, in the Controller group, click **maxCrypto Settings**.

   ![maxCrypto Settings](image)

When the Set maxCrypto Configuration window opens, click the **General tab**.

3. In the Import Foreign Local Master Key field, enter the master key originally used to encrypt the logical drive.
   The Master Key is a 10-32 character string, comprising all printable ASCII characters.
4. Click OK.
10 Maintaining Physical Devices

This section describes how to manage the controllers, disk drives, solid state drives, and enclosures in your storage space.

10.1 Viewing Device Properties

Click on any physical device in the Enterprise View then, on the Storage Dashboard, click the **Properties** tab to view version numbers, status, model numbers, features, and other information about the device. The properties listed vary, depending on which type of device you select. The figure below shows the properties for a controller. For more information about using the Storage Dashboard to monitor the components in your storage space, see [Viewing Component Status in the Storage Dashboard](#).

10.2 Locating Drives in Your Storage Space

You can blink the LEDs on disk drives and SSDs to identify where they are physically located in your storage space. This table describes how to locate specific devices.

**Note:**

Once any of the device is located, the timeout value will be overwritten with the latest timeout value for all the located devices.

<table>
<thead>
<tr>
<th>To Locate...</th>
<th>Select...</th>
</tr>
</thead>
<tbody>
<tr>
<td>A disk drive</td>
<td>Disk Drive icon:</td>
</tr>
<tr>
<td>All disk drives on a controller</td>
<td>Controller icon:</td>
</tr>
</tbody>
</table>
### 10.2.1 Locating Disk Drives

To locate an individual disk drive or all physical drives on the controller:

1. In the Enterprise View, select a controller or an individual drive on the controller.
2. On the ribbon, in the Physical Device group, click **Locate**.

The Locate Physical Device window opens.

3. From the drop-down list, select the timeout period (1 hour, 4 hours, 24 hours).
4. Click the **Locate** button.
   - The LED on the disk drive(s) begin to blink.
5. To stop blinking the drive(s) immediately, click **Stop**.
6. Click **Cancel** to close the Locate Physical Device window.
   - The LED(s) continue to blink for the duration of the timeout period.

<table>
<thead>
<tr>
<th>To Locate...</th>
<th>Select...</th>
</tr>
</thead>
<tbody>
<tr>
<td>All disk drives included in an array</td>
<td>Array icon:</td>
</tr>
<tr>
<td>All disk drives included in a logical drive</td>
<td>Logical Drive icon:</td>
</tr>
<tr>
<td>All SSDs in the maxCache Device</td>
<td>maxCache Device icon:</td>
</tr>
</tbody>
</table>
10.2.2 Locating Physical Disks in an Array or Logical Drive

To locate all physical disks in an array or logical drive:

1. In the Enterprise View, open the Arrays and Logical Devices tree for a controller, then select an array or logical drive.

2. On the ribbon, in the Array group or Logical Device group (shown below), click Locate.

   ![Locate Logical Device](image)

The Locate Logical Device window opens and displays a list of the physical disks associated with the array or logical drive.

3. Select the timeout period (1 hour, 4 hours, 24 hours), then click Locate.

   ![Locate Logical Device](image)

The LEDs on the disk drives begin to blink.

4. Click Cancel to close the Locate window.
   The LEDs continue to blink for the duration of the timeout period.

5. Click Stop to stop blinking the drives immediately.

10.2.3 Locating SSDs in the maxCache Device

To locate the Solid State Drives (SSDs) in the maxCache Device:

1. In the Enterprise View, select a controller; then select the maxCache Device on that controller. You can select the maxCache array or logical device.

2. On the ribbon, in the maxCache group, click Locate.
3. Select the time-out period from the drop-down list: 1 hour, 4 hours, 24 hours.

4. Click the Locate button.

The LEDs on the SSDs begin to flash.

5. Click Stop to stop blinking the SSDs.

6. Click Cancel to close the Locate maxCache window.

10.3 Working with Physical Device Error Counters

This section explains how to view the physical device error counters and how to clear the error counters from a physical device and a controller.

The clear device error counters feature provides an option to clear the device error counters on the physical devices. This option is available at the controller level to clear the device error counters on all the physical devices connected to it and at the physical device level to clear the error counters on the specific device.
### Viewing Physical Device Error Counters

To view the physical device error counters for a hard drive or SSD, select the drive in the Enterprise View then, on the Storage Dashboard, click the **Error Counters** tab. The table below describes the error counters.

<table>
<thead>
<tr>
<th>Error Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aborted Command</td>
<td>Number of times a drive was failed due to aborted commands that could not be retried successfully.</td>
</tr>
<tr>
<td>Bad Target Error</td>
<td>Number of times that this drive did something that did not conform to the SCSI Bus Protocol. It will cause a reset of the SCSI bus that this drive is attached to.</td>
</tr>
<tr>
<td>ECC Recovered Read Errors</td>
<td>Number of ECC-corrected read errors.</td>
</tr>
<tr>
<td>Failed Read Recover</td>
<td>Number of times a recover of another physical drive in the logical volume failed due to a hard read error from this drive.</td>
</tr>
<tr>
<td>Failed Write Recover</td>
<td>Number of times a recover of this physical drive failed due to an error occurring on this drive during a write operation.</td>
</tr>
<tr>
<td>Format Error</td>
<td>Number of times a Format command (used when remapping defects) failed. A failed remap operation may cause the controller to fail a drive.</td>
</tr>
<tr>
<td>Hardware Error</td>
<td>Number of times a drive returned a bad hardware status. The drive may be failed if retries do not work.</td>
</tr>
<tr>
<td>Hard Read Error</td>
<td>Number of unrecoverable read errors.</td>
</tr>
<tr>
<td>Hard Write Error</td>
<td>Number of unrecoverable write errors.</td>
</tr>
<tr>
<td>Hot-Plug Count</td>
<td>Number of times this drive was hot-plugged (removed) from a box.</td>
</tr>
<tr>
<td>Media Failure</td>
<td>Number of times a drive was failed due to unrecoverable media errors.</td>
</tr>
<tr>
<td>Not Ready Error</td>
<td>Number of times the drive was failed because it never became ready after the “spin up” command was issued. If retries or drive spin-ups fail, the drive will be failed.</td>
</tr>
<tr>
<td>Other Timeouts</td>
<td>Timeouts other than Data ReQuest Timeouts (DRQ).</td>
</tr>
<tr>
<td>Predictive Failure</td>
<td>Number of times that the drive returned a predictive failure error.</td>
</tr>
</tbody>
</table>
### Error Counter Description

<table>
<thead>
<tr>
<th>Error Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retry Recovered Read Error</td>
<td>Number of retry-recovered read errors.</td>
</tr>
<tr>
<td>Retry Recovered Write Error</td>
<td>Number of retry-recovered write errors.</td>
</tr>
<tr>
<td>SCSI Bus Fault</td>
<td>Number of “bus faults”, which we define as SCSI bus parity errors, overrun/underrun conditions, etc.</td>
</tr>
<tr>
<td>Service Hours</td>
<td>Number of service hours since the last power cycle.</td>
</tr>
<tr>
<td>Sectors Written</td>
<td>Number of sectors written to media.</td>
</tr>
<tr>
<td>Sectors Read</td>
<td>Number of sectors read from the media. This value will include sectors read into the on-drive cache buffer only if the drive keeps track of this value. Otherwise, only sectors requested through the drive interface are counted.</td>
</tr>
</tbody>
</table>

### 10.3.2 Clearing Error Counters from a Physical Device

Use this option to clear the device error counters of a specific physical device.

To clear the error counters from a physical device:

1. In the Enterprise View, select a physical drive node.
2. On the ribbon, in the Physical Device group, click **Set Properties**.

   ![Set Properties](image.png)

   The Set Properties window opens.

   ![Set Properties Window](image2.png)

3. To clear the device errors, select the Clear Device Error Counter(s) check box.
4. Click OK.

10.3.3 Clearing Error Counters from a Controller
Use this option to clear the device error counters of all the physical devices from controller.

To clear the device errors from a controller:
1. In the Enterprise View, select a controller, then select a physical drive on the controller.
2. On the ribbon, in the Physical Device group, click Set Properties.

The Set Properties window opens.

3. To clear the device errors, select the Clear Device Error Counter(s) check box.
4. Click OK.

10.4 Working with Failed or Failing Disk Drives
This section describes how to use maxView Storage Manager to manage failed or failing disk drives in your storage space.

10.4.1 Replacing Disk Drives in a Logical Drive
You can replace one or more disk drives in a logical drive. You may want to replace a drive to upgrade to larger disk drives, or to make disk drive size uniform across the logical drive.

Caution: If another disk drive in the logical drive fails during rebuild (see Rebuilding Logical Drives on page 147), you
may lose data. For help solving disk drive problems, see Recovering from a Disk Drive Failure.

To replace a disk drive in a logical drive:

1. In the Physical Devices tree in the Enterprise View, find the disk drive you want to replace; note its size and location (for instance Slot 1 in Enclosure 0).
2. Set the drive state to failed. (See Setting a Disk Drive to ‘Failed’ on page 98.)
3. Remove and replace the disk drive with one of equal or greater size.
4. Wait for the logical drive to rebuild. (See Rebuilding Logical Drives on page 147.)
5. Repeat these steps for each disk drive you want to replace.

10.4.2 Setting a Disk Drive to ‘Failed’

Before you can remove a disk drive, you should set it to the Failed state to protect your data. To fail a disk drive (or SSD), use the Force Offline option for physical devices.

You can set a disk drive to the Failed state if:

- The disk drive is not part of a logical drive,
- The disk drive is part of a redundant, healthy logical drive

Once you force a drive offline, it can be brought online again only after power-cycling the controller. 

Caution: You may lose data or damage your disk drive if you remove a disk drive without first setting it to a failed state.

To set a disk drive to Failed:

1. In the Enterprise View, select a controller then, in the Physical Devices tree, select the drive you want to set to Failed.
2. On the ribbon, in the Physical Devices group, click **Force Offline**.

The Force Offline window opens.

3. Click **Force**.

The drive is taken offline and set to the Failed state.

**Note:** If the drive is part of a healthy logical drive, the drive is degraded and a warning message is displayed in the Event Log.

10.5 Erasing a Disk Drive

You can use maxView Storage Manager to securely erase existing data on any disk drive or SSD in the Ready state. Secure erase completely destroys the data on the drive; the data is completely and irretrievably eradicated.

Optionally, you can choose the erase pattern.

To securely erase a disk drive or SSD:
1. In the Enterprise View, select a controller then, in the Physical Devices tree, select the drive you want to erase.

2. On the ribbon, in the Physical Device group, click Secure Erase.

The Secure Erase Physical Device window opens.

3. From the drop-down list, select the erase pattern:
   - **Zero** (default)—Initializes all blocks to zero.
   - **Random Zero**—Initializes block to random value then zero.
   - **Random Random Zero**—Initializes block to random value, next block to random value, then zero.
   - **Sanitize Overwrite**—(HDD only) Fills every physical sector of the drive with a pattern.
   - **Sanitize Block Erase**—(SSD only) Sets the blocks on the drive to a vendor-specific value, removing all user data. It provides a very fast, complete, and robust erasure of the solid state device.
   - **Sanitize Crypto Scramble**—(Self-Encrypting Drives (SED) only) Changes the internal encryption keys that are used for user data, making the data irretrievable. This option is implemented for both HDD and SSD SED devices.

4. Click Erase to erase the drive.

**10.5.1 Restricted/Unrestricted Secure Erase**

For the Sanitize erase patterns (Overwrite, Block Erase, Crypto Scramble), the following erase methods are applicable if your drive supports the method:

- **Restricted**: the drive will be unusable until the sanitize operation is completed successfully. If a restricted sanitize operation fails, you are only allowed to start another sanitize operation.
- **Unrestricted**: the drive will be recoverable in the case that the sanitize erase operation fails. User data may still be present on the drive. Not all drives support this sanitize method.

For more information about Sanitize erase patterns, see *Erasing a Disk Drive* on page 98.

**10.6 Initializing and Uninitializing Disk Drives**

This section describes how to initialize or erase data and meta-data (including logical drive and partition information) from the disk drives (and SSDs) in your storage space. You can initialize or uninitialize individual disks, or use the wizard to initialize/uninitialize all disks on a controller.

**10.6.1 Uninitializing a Disk Drive**

You can uninitialize any disk drive (or SSD) containing Smart Controller configuration metadata. Uninitializing a disk drive clears the meta-data and reserved space from the drive and removes any OS partitions; existing data on the drive is destroyed.

**Note:** Uninitialized drives change from their current state to the Raw state. Raw drives are compatible with any Host Bus Adapter (HBA), including RAID controllers operating in HBA mode, and can be exchanged with drives on the motherboard's SATA interface.

To uninitialize a disk drive:
1. In the Enterprise View, select a controller; then, in Physical Devices tree, select the disk drive you want to uninitialize.

2. On the ribbon, in the Physical Device group, click **Initialize**.

The Initialize/Uninitialize Physical Device window opens.

3. Click the **Uninitialize** button, then click **OK**.

4. When prompted, click **OK** to close the Initialize/Uninitialize Device window.

### 10.6.2 Initializing/Uninitializing all Drives on a Controller

To initialize or uninitialize all disk drives (or SSDs) on a controller, use the Initialize/Uninitialize Physical Devices wizard to clear the meta-data on all drives at once.

To initialize or uninitialize drives with the wizard:

1. In the Enterprise View, select a controller.

2. On the ribbon, in the Physical Device group, click **Initialize**.

The Initialize/Uninitialize Physical Devices wizard opens.

3. Select Initialize or Uninitialize, then click **Next**.
4. Select drives on the controller to initialize or uninitialize, then click Next.
5. Review the Summary, then click Finish.

10.7 Setting the Physical Drive Boot Priority

Use this option to set the boot priority of a physical device to Primary, Secondary, Primary and Secondary, or None (default). A controller can have only one physical (or logical) device as the primary or secondary boot device. When you select a new physical device as the primary/secondary boot drive, the boot priority of the existing primary/secondary boot drive is overwritten and set to None.

To set the boot priority of a physical device:
1. In the Enterprise View, select a controller, then select a physical drive on the controller.
2. On the ribbon, in the Physical Device group, click Set Properties.

The Set Properties window opens.
3. From the Boot Type drop-down list, select Primary, Secondary, Primary and Secondary, or None.
4. Click OK.

10.8 Working with Controllers

This section describes how to use maxView Storage Manager to manage the controllers in your storage space:
- To re-scan a controller, see Rescanning a Controller on page 102.
- To optimize controller performance, see Optimizing Controller Performance on page 103.
- To change the operating mode of connectors on the controller, see Changing the Connector Operating Mode on page 104.

10.8.1 Rescanning a Controller

After you connect a disk drive or remove a Ready (non-failed) disk drive from a controller, maxView Storage Manager may not recognize the change until it rescans the controller.

To rescan a controller:
1. In the Enterprise View, select the controller.
2. On the ribbon, in the Controller group, click Rescan.

The Rescan window opens.
3. Click the Rescan button (on the Rescan window).
   maxView Storage Manager scans all the channels or ports on the controller you selected.
4. When the rescan is finished, click Cancel to close the Rescan window.
10.8.2 Optimizing Controller Performance

You can enable the following performance optimizations on a controller to improve I/O throughput and ensure optimal performance of the arrays and logical drives in your storage space.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queue Depth</td>
<td>Sets the max drive request queue depth for the controller. Valid values are Automatic, 2, 4, 8, 16, and 32.</td>
</tr>
<tr>
<td>Monitor and Performance Delay</td>
<td>Sets the MNP Analysis delay for the controller, in seconds. Set the value to zero to disable Monitor and Performance Analysis. Default is 60 minutes (3600 seconds).</td>
</tr>
<tr>
<td>Elevator Sort</td>
<td>Sets the behavior of the drive’s write Elevator sort algorithm, a scheduling optimization that prioritizes I/O requests such that disk arm and head motion continues in the same direction. Enabling the elevator sort improves seek times and disabling the elevator sort improves throughput.</td>
</tr>
<tr>
<td>Degraded Performance Optimiza-</td>
<td>For degraded RAID 5 logical drives, enabling this setting directs the controller to attempt to improve performance of large read requests by buffering physical drive requests. Disabling this setting forces the controller to read from the same drives multiple times.</td>
</tr>
<tr>
<td>tion</td>
<td>Latency</td>
</tr>
<tr>
<td></td>
<td>Enables Flexible Latency Optimization for HDDs. When latency optimization is enabled, the controller detects high-latency I/O requests and applies a cutoff, or threshold, value, after which it suspends elevator sorting and services the request right away. You can set the latency optimization to low, medium, high, aggressive level 1, or aggressive level 2.</td>
</tr>
</tbody>
</table>

To enable/disable performance optimizations on a controller:

1. In the Enterprise View, select a controller.
2. On the ribbon, in the Controller group, click Set Properties.

When the Set Properties window opens, click the Performance tab.
3. Enable/disable performance optimizations, as needed.
4. Click OK.

10.8.3 Changing the Connector Operating Mode

Use this option to change the behavior of the connectors on your Microsemi Adaptec Smart Storage Controller. The connectors on the controller can operate in three modes:

- HBA Mode: exposes physical drives to the operating system
- RAID Mode: exposes only RAID volumes to the operating system
- Mixed Mode: exposes RAID volumes and physical drives to the operating system

By default, products with RAID support are configured to operate in Mixed Mode. Mode options vary, depending on the configuration of logical and physical devices on the connector. For example, you cannot switch the connector to HBA mode if the connector is already configured with a RAID volume.

A reboot is required for connector mode changes to take effect.

**Note:** Changing from Mixed Mode or HBA Mode to RAID Mode removes access to the physical drives from the operating system.

To change the connector mode on a controller:

1. In the Enterprise View, select a controller.
2. On the ribbon, in the Controller group, click **Set Properties**.

When the Set Properties window opens, click the **Connector** tab.

3. From the drop-down list, change the connector mode for each port to RAID, HBA, or Mixed.
4. Click OK.
5. Reboot the server.

10.9 Updating Controller, Enclosure, and Disk Drive Firmware

**Note:** This task is recommended for advanced users only.

maxView Storage Manager includes a wizard to help you update the firmware on the controllers, enclosures, and disk drives in your storage space. The wizard updates the firmware for devices of the same type on the local or a remote system.

For example, if your storage space includes disk drives from two different manufacturers, you must update the firmware for each manufacturer's drives separately, by running the wizard twice. Additionally, if you have more than one system in your storage space, you must run the wizard for each system separately.

To update the firmware on the controllers, enclosures, or disk drives in your storage space, review the prerequisites in **Before You Begin** on page 105, then follow one of these sets of instructions:

- **Updating the Controller Firmware** on page 105
- **Updating the Disk Drive Firmware** on page 109
- **Updating the Enclosure Firmware** on page 110

10.9.1 Before You Begin

Before you begin, download the latest firmware images from [www.adaptec.com](http://www.adaptec.com), or from your vendor's support site on the World Wide Web. Controller images come in sets of one or more files and have a .bin file extension. Disk drive and enclosure image file names vary by manufacturer.

10.9.2 Updating the Controller Firmware

Use the Firmware Update wizard to update the firmware for one or more controllers of the same type on the local or a remote system.

To update the controller firmware:
1. In the Enterprise View, select a system.
2. On the ribbon, in the System group, click **Firmware Update**.

![Firmware Update](image1.png)

3. When the wizard opens, select Controller, then click **Next**.

![Select Device Type](image2.png)

4. Select the controllers you want to update, then click **Next**.

![Select Device](image3.png)
5. Select flash options for the update, then click **Next**. Choose Toggle Image to replace the active image with the backup image.

   **Note:** If you choose Toggle Image, Step [6], Select Files, is skipped.

6. Click **Choose**, browse the file system for the firmware update file (typically, a `.bin` file), click **Open** to select the file (the button label may be different on your browser).

7. When the file name appears in the Uploaded Firmware File(s) list, click **Next**.

8. Review the update summary, then click **Finish**.
Caution: Do *not* power down the controller(s) while the update is in progress!

9. When the update is complete, click **OK**. Restart the server to activate the new firmware image.
### 10.9.3 Updating the Disk Drive Firmware

Use the Firmware Update wizard to update the firmware for one or more disk drives of the same type on the local or a remote system. The procedure is similar to updating the controller firmware (see Updating the Controller Firmware on page 105).

To update the disk drive firmware:

1. In the Enterprise View, select a system.
2. On the ribbon, in the System group, click **Firmware Update**.
3. When the wizard opens, select **Disk Drive**, then click **Next**.
4. In the Select Files panel, click **Choose**, browse the file system for the firmware update file, click **Open** to select the file (the button label may be different on your browser).
5. When the file name appears in the Uploaded Firmware File(s) list, click **Next**.
6. In the Attributes panel, select the Chunk Size, from 1-n, in kilobytes (KB), then click **Next**.
7. In the Select Devices panel, select the disk drives you want to update, then click **Next**.
8. Review the update summary, then click **Finish**.
   
   **Caution**: Do not power down the controller(s) while the update is in progress!
9. When the update is complete, click **OK**. Restart the server to activate the new firmware image.
10.9.4 Updating the Enclosure Firmware

Use the Firmware Update wizard to update the firmware for one or more enclosures or expanders of the same type on the local or a remote system.

To update the enclosure/expander firmware:

1. In the Enterprise View, select a system.
2. On the ribbon, in the System group, click Firmware Update.
3. When the wizard opens, select Enclosure/Expander, then click Next.
4. In the Select Files panel, click Choose, browse the file system for the firmware update file, click Open to select the file (the button label may be different on your browser).
   Note: If the upgrade requires multiple firmware update files, update one file at a time or use a combined firmware image to complete the upgrade.
5. When the file name appears in the Uploaded Firmware File(s) list, click Next.
6. Select the Chunk Size, from 1-n, in kilobytes (KB).
7. Select the firmware Upgrade Type:
   - Firmware—update the firmware image on the expander or enclosure
   - Manufacturer—update the manufacturing image (BOOT SEEPROM) on the expander or enclosure
   - CPLD—update the CPLD image on the expander or enclosure
8. Select the firmware upgrade Mode:
   - Download Microcode Data Only—transfer microcode to the device using one or more write buffer commands; requires system reset or power cycle to activate.
• **Download Microcode with Offsets and Activate**—transfer microcode to the device using one or more write buffer commands and activate immediately.

• **Download Microcode with Offsets, Save and Activate**—transfer microcode to the device using one or more write buffer commands, save to non-volatile storage, then activate.

  **Note:** In this release, maxView Storage Manager supports option 3 only for expander firmware upgrade: Download Microcode with Offsets, Save and Activate.

9. When you are ready to continue, click **Next**.

10. In the Select Devices panel, select the enclosure(s) you want to update, then click **Next**.

11. Review the summary information, then click **Finish**.

  **Caution:** Do not power down the controller or enclosure(s) while the update is in progress!

12. When the update is complete, click **OK**. Restart the server to activate the new firmware image, as needed.
11 Monitoring Status and Activity

This section describes how maxView Storage Manager helps you monitor status and activity in your storage space.

11.1 Monitoring Options

maxView Storage Manager provides many ways to monitor the status of your storage space:

- **Event Log**—The main window of maxView Storage Manager features an event log that provides at-a-glance status information about activity (or events) occurring in your storage space. All Warning- and Error-level events are also recorded in your operating system’s event log.

  See [Viewing Activity Status in the Event Log](#) on page 113 and [Changing an Operating System’s Event Log Setting](#) on page 128.

- **Task Log**—The main window also features a task log that provides status information about the progress of tasks in your storage space, such as the creation of a logical drive.

  See [Viewing Task Status in the Task Log](#) on page 115.

- **Storage Dashboard**—Occupying the largest portion of the main window in maxView Storage Manager, the Storage Dashboard provides complete, at-a-glance, information about the components of your storage space, including status information, physical and logical device properties, resources, and reliability indicators for hard drives and SSDs.

  See [Viewing Component Status in the Storage Dashboard](#).

- **Chart View**—Provides a visual representation of free and used space for a system, controller, or your entire storage space.

  See [Viewing Storage Space Usage in Chart View](#) on page 118.

- **Notifications**—You can set maxView Storage Manager to email status notifications in your choice of format to help you monitor activities in your storage space, such as:
  - Changes in the status of physical devices, such as disk drive failures.
  - Changes on local or remote systems, such as the creation of a hot spare.
  - Changes in temperature in storage enclosures, or that fans or power supplies within an enclosure have failed.

  See [Notifying Users by Email About Status and Activity](#) on page 119.

- **Advanced Statistics**—You can set maxView Storage Manager to log advanced I/O and usage statistics for the RAID controllers in your system.

  See [Monitoring Advanced Statistics about Activity in Your Storage Space](#) on page 124.

- **Audible Alarm**—A series of beeps sounds whenever a serious event occurs on your storage space.

  See [Working with System Alarms](#).

11.2 Checking Status from the Main Window

You can view status information and messages about the activity occurring in your storage space by looking at the event log, status icons, and task log in the main window of maxView Storage Manager. (You can also view all events for a system in its operating system event log; see [Changing an Operating System’s Event Log Setting](#) on page 128.) Using the Storage Dashboard and Chart View, you can also monitor the physical
and logical components of your storage space from the main window, including summary information and status, physical and logical device properties and resources, and usage and I/O statistics.

### 11.2.1 Viewing Activity Status in the Event Log

The Event Log lists activity occurring in your storage space, with the most recent event listed at the top. Status is indicated by icons (see *What Do the Event Status Icons Mean?* on page 114) in the left-hand column, as shown in the figure below.

You can view events as they occur in the bottom panel of the maxView Storage Manager main window. The main window displays the last 100 events in your storage space. To view more events, filtered by device (a controller, for example), open the **Event tab** on the Storage Dashboard (see *Viewing Component Status in the Storage Dashboard*).

Single-click any event to open the Event Log Detail window to see more information in an easier-to-read format. Use the up and down arrows to view previous or following events.
To make it easier to find a specific event, click on the column heads to sort the events. For example, sorting the events by Severity can help you find specific Error- or Warning-level events quickly.

### 11.2.1 What Do the Event Status Icons Mean?

maxView Storage Manager indicates event status with icons. This table lists the three categories, or types, of events based on severity.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Status</th>
<th>Examples</th>
</tr>
</thead>
</table>
| ![Information](icon) | Information | The local system successfully connected to a remote system.  
A logical drive was created.  
A hot spare was deleted. |
| ![Warning](icon) | Warning | A logical drive is in a degraded state.  
A disk drive is being rebuilt.  
A controller is not responding to an enclosure. |
| ![Error](icon) | Error | A controller has failed.  
A logical drive has failed.  
A disk drive or hot spare has failed.  
An enclosure is overheating.  
Multiple fans or power supplies within an enclosure have failed.  
An enclosure is not responding. |

**Note:** All Warning- and Error-level events also cause the audible alarm to sound. See *Working with Controllers* on page 102 for more information.
11.2.2 Viewing Task Status in the Task Log

The Task Log shows the status and progress of tasks in your storage space, with the most recent task listed at the top.

Single-click any task to open the Task Log Detail window to see more information in an easier-to-read format.

11.2.3 Viewing Component Status in the Storage Dashboard

The Storage Dashboard provides detailed information about the components of your storage space, including local and remote systems, controllers, arrays, logical drives, enclosures, disk drives and SSDs, and maxCache Devices. Occupying the largest portion of the main window in maxView Storage Manager, the Storage Dashboard organizes component information by category, with a tabs providing one-click access to summary information and status, properties, resources, and usage statistics.

The information on the Storage Dashboard varies, depending on which component is selected in the Enterprise View. The figure below shows the Storage Dashboard for a controller. Tabs provide access to summary information, controller properties, and resources. The Events tab shows filtered events for the selected device (see Viewing Activity Status in the Event Log on page 113).

Note: For information about Chart View, on the right side of the Storage Dashboard, see Viewing Storage Space Usage in Chart View on page 118.
The following table lists the categories and types of information provided on the Storage Dashboard for each component in your storage space. All top-level nodes in the Enterprise View (System, Controller, Arrays, Logical Drives, Physical Devices, and so on) include a Summary tab and Events tab.

<table>
<thead>
<tr>
<th>Component</th>
<th>Categories/Tabs</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>Summary, Properties</td>
<td>System name and IP address</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Operating system</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Number and type of controllers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Alarm status (see <a href="#">Working with System Alarms</a>)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Web Server settings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SMTP settings</td>
</tr>
<tr>
<td>Controller</td>
<td>Summary, Properties</td>
<td>Model, key features, manufacturing data, driver and firmware version</td>
</tr>
<tr>
<td></td>
<td></td>
<td>controller mode, and status</td>
</tr>
<tr>
<td></td>
<td>Resources</td>
<td>Number of physical drives, arrays, logical drives, and status</td>
</tr>
<tr>
<td></td>
<td>Connectors</td>
<td>Power management features</td>
</tr>
<tr>
<td></td>
<td>maxCrypto</td>
<td>I2C address for PBSI interface (hex), I2C clock speed and clock</td>
</tr>
<tr>
<td></td>
<td></td>
<td>stretching status</td>
</tr>
<tr>
<td></td>
<td></td>
<td>maxCache status (see <a href="#">Checking maxCrypto Status</a> on page 82)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Health and activity of flash backup module, if present (&quot;Green backup&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>status)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Connector functional mode</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Performance optimizations and other settings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Physical drive assignments by logical device (see <a href="#">Revealing More Device Information</a> on page 23)</td>
</tr>
<tr>
<td>Arrays</td>
<td>Summary, Resources</td>
<td>Total size and unused size</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Spare rebuild mode</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Logical drive RAID level, size, status</td>
</tr>
<tr>
<td>Logical drives and</td>
<td>Summary, Resources</td>
<td>Raid level, segment and group (RAID 10 only), size, mount point, status</td>
</tr>
<tr>
<td>maxCache Device</td>
<td></td>
<td>Member drives and sizes</td>
</tr>
<tr>
<td>Enclosure</td>
<td>Summary, Resources, Slots</td>
<td>Enclosure type, vendor, model and status</td>
</tr>
</tbody>
</table>

Microsemi Smart Storage Controllers User Guide Revision 10

116
11.2.3.1 Monitoring Enclosure Status

If your storage space includes an enclosure with an enclosure management device, such as a SCSI Accessed Fault-Tolerant Enclosure (SAF-TE) processor, maxView Storage Manager displays temperature, fan, and power module status on the Storage Dashboard, as shown in the figure below.

<table>
<thead>
<tr>
<th>Resources</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fan(s)</td>
<td>6</td>
</tr>
<tr>
<td>Optimal</td>
<td>6</td>
</tr>
<tr>
<td>Malfunctioning</td>
<td>0</td>
</tr>
<tr>
<td>Not Installed</td>
<td>0</td>
</tr>
<tr>
<td>Power Supplies</td>
<td>2</td>
</tr>
<tr>
<td>Optimal</td>
<td>2</td>
</tr>
<tr>
<td>Malfunctioning</td>
<td>0</td>
</tr>
<tr>
<td>Not Installed</td>
<td>0</td>
</tr>
<tr>
<td>Temperature Sensor(s)</td>
<td>2</td>
</tr>
<tr>
<td>Normal</td>
<td>2</td>
</tr>
<tr>
<td>Abnormal</td>
<td>0</td>
</tr>
<tr>
<td>Not Installed</td>
<td>0</td>
</tr>
<tr>
<td>Speaker(s)</td>
<td>1</td>
</tr>
<tr>
<td>On</td>
<td>1</td>
</tr>
<tr>
<td>Off</td>
<td>0</td>
</tr>
<tr>
<td>Not Installed</td>
<td>0</td>
</tr>
</tbody>
</table>

11.2.3.2 Viewing SMART Statistics

You can use the Storage Dashboard to view various indicators of reliability for the SATA hard drives and SSDs in your storage space. maxView Storage Manager displays SMART statistics for the drives using Self-Monitoring, Analysis and Reporting Technology available on most contemporary hard drives and SSDs.
Monitoring Status and Activity

non-spinning storage devices. You can use this information to verify the health of your hard drives and SSDs and to predict drive failures.

To view the SMART statistics for a hard drive or SSD, select the drive in the Enterprise View, then click the SMART tab on the Storage Dashboard. For SSDs, the statistics include wear-level and longevity indicators, as shown in next figure. Refer to your drive vendor’s data sheet for a description of individual report items.

### 11.2.4 Viewing Storage Space Usage in Chart View

Chart View provides a visual representation of the free and used space for a system, controller, array, or your entire storage space (all systems and controllers). Located on the right side of the Storage Dashboard in the maxView main window, Chart View displays a pie chart of storage space usage.

To view storage space usage in Chart View, simply select a component in the Enterprise View (a system, for instance); the chart view is updated immediately.
11.3 Notifying Users by Email About Status and Activity

You can set up maxView Storage Manager to send email messages (or notifications) to one or more email addresses when an event occurs on a system, such as the creation of a logical drive or the failure of a disk drive. Email notifications can help you monitor activity on your entire storage space from any location, and are especially useful in storage spaces that include multiple systems running the maxView Storage Manager only.

Only the users you specify receive email notifications. You can specify which types of events generate email messages (Error, Informational, Warning). You can also specify if you want to be notified instantly when an event occurs to ensure that urgent issues receive immediate attention from the right people. Alternatively, you can specify that you want events “coalesced” and receive only one email message for each event type.

Follow the instructions in this section to:
- Set up email notifications (see Setting Up Email Notificationsemail notifications setupEmail Notifications Manager openingmonitoring email notificationssetupemail notifications recipient addressesmonitoring email notificationsrecipient addresses on page 119).
- Send a test email (see Sending a Test MessageEmail Notifications Manager test eemailsemail notifications test emailsmonitoring email notifications test emails on page 122).
- Modify or remove an email recipient (see Modifying or Removing an Email Recipient email notifications modifying recipient informationemail notifications removing recipientsmonitoring email notificationsremoving recipientsmonitoring email notificationsmodifying recipient information on page 123).
- Modify email server settings (see Modifying Email Server Settingsemail notifications changing "from" adresseemail notifications changing SMTP servermonitoring email notificationschanging "from" addressmonitoring email notificationschanging SMTP serverSMTP server on page 124).
- Disable email notifications (see Disabling Email Notificationsemail notifications disabling on page 124)

11.3.1 Setting Up Email Notifications

This section describes how to set up email notifications for one system. If you want to monitor multiple systems by email, you must complete the tasks in this section for each one separately.

Before you begin, note this information:
- The address of your Simple Mail Transfer Protocol (SMTP) server (host name and domain, or TCP/IP address)
- The email address of each person who will receive email notifications
To set up email notifications:

1. Select the Enterprise View node.
2. On the ribbon, in the System group, click **System Settings**.

![System Settings](image)

3. When the System settings window opens, click the **SMTP** tab.
4. Select **Enable Email Notifications**.
5. Enter the IP address of your SMTP server and the server’s port number (or use the default port).

![System Settings](image)

6. If authentication is enabled on your SMTP server (that is, the server requires authentication details before it will send messages to users), select **Use Secure Mail Server**, then enter the SMTP server’s login credentials (username/password) in the space provided.

7. On the System settings window, click the **Email** tab. The Email Notifications Manager opens.
8. Click Add Email. When the Add Email window opens, enter the recipient’s email address, select the level of events that will trigger an email notification for that recipient (Error, Error/Warning, Error/Warning/Informational), then select the notification type—Instant or Coalesced. To include a support archive file with the email, click Attach Support.zip, then click OK. (For more information about event levels, see What Do the Event Status Icons Mean? on page 114; for more information about the support archive file, see Creating a Support Archive File on page 148.)

Repeat this step to add more email recipients.

Each recipient appears in the Email Notifications Manager, as shown below:
9. When you’re done adding email recipients, click **OK**. The email recipients and your SMTP server settings are saved.

10. Repeat the steps in this section for each system you want to monitor with email notifications, then continue by sending test messages to all recipients (see Sending a Test MessageEmail Notifications Manager test emailsemail notifications test emailsmonitoring email notificationstest emails on page 122).

### 11.3.2 Sending a Test Message

To ensure that an email recipient is receiving event notifications, you can send them a test message.

To send a test message:

1. Select the Enterprise View node.

2. On the ribbon, in the System group, click **System Settings**.

3. When the System settings window opens, click the **Email** tab. The Email Notifications Manager opens.

4. Select one or more email addresses to send a test message to. To select all addresses, click the check box at the top of the list, as shown in the figure below.
5. Click **Send Test Email**.

   If the test is successful, the email recipient(s) receive the test message. If the test fails:
   - Ensure that the recipient's email address is correct. (See *Modifying or Removing an Email Recipient*
     email notifications modifying recipient informationemail notifications removing recipientsmonitoring
e-mail notificationsremoving recipientsmonitoring email notificationsmodifying recipient information
     on page 123.)
   - Ensure that your SMTP server address is correct. (See *Modifying Email Server Settingsemail
     notifications changing "from" addressemail notifications changing SMTP servermonitoring email
     notificationschanging "from" addressmonitoring email notificationschanging SMTP serverSMTP
     server* on page 124.)
   - Try sending the test message again.

### 11.3.3 Modifying or Removing an Email Recipient

This section describes how to modify a recipient's email address, change the types of event notifications
the recipient receives, or stop sending email notifications to a recipient from a selected system.

To modify recipient information or to stop sending email notifications to a recipient:

1. Select the Enterprise View node.
2. On the ribbon, in the System group, click **System Settings**.

![System Settings](image)

3. When the System settings window opens, click the **Email** tab.
   
The Email Notifications Manager opens.

4. Select the email recipient you want to modify or remove, then:
   - Click **Modify Email**, change the recipient information, as needed, then click **Modify** to save your
     changes.
Or,

- Click **Delete Email** to remove the recipient from the notification list.

The changes become effective immediately.

5. Click **OK** to close the Email Notifications Manager.

### 11.3.4 Modifying Email Server Settings

You can modify these email server settings, if required:

- Address and port of your SMTP server
- ‘From’ address that will appear in email notifications
- Secure server login credentials

To modify email server settings:

1. Select the Enterprise View node.
2. On the ribbon, in the System group, click **System Settings**.

3. When the System settings window opens, click the **SMTP** tab.
4. Edit the SMTP server settings as required, then click **OK** to save your changes.

### 11.3.5 Disabling Email Notifications

This section describes how to disable email notifications on a selected system.

**Note:** If you disable email notifications, events continue to be generated but email messages won’t be sent.

To disable email notifications:

1. Select the Enterprise View node.
2. On the ribbon, in the System group, click **System Settings**.

3. When the System settings window opens, click the **SMTP** tab.
4. Clear the **Enable Email Notifications** check box.
5. Click **OK** to save your changes.

### 11.4 Monitoring Advanced Statistics about Activity in Your Storage Space

You can set maxView Storage Manager to log advanced I/O and usage statistics about the RAID controllers, hard drives, SSDs, and logical drives in your storage space, including maxCache caching statistics.
Follow the instructions in this section to:

- Enable statistics logging on a controller (see Setting up Statistics Logging on page 125).
- View the advanced statistics for a controller, hard drive, SSD, logical drive, or maxCache Device (see Viewing Advanced Statistics on page 126).
- Reset the statistics counters (see Resetting the Statistics Counters on page 128).

### 11.4.1 Setting up Statistics Logging

To set up statistics logging for the controllers in your storage space:

1. In the Enterprise View, select a system, then select a controller.
2. On the ribbon, in the Controller group, click Set Properties.

The Set Properties window opens.

3. In the Advanced Statistics drop-down list, select Enabled.

4. Click OK.
11.4.2 **Viewing Advanced Statistics**

Use the Statistics Viewer to view the advanced statistics for the controllers, hard drives, SSDs, logical drives, and maxCache Devices in your storage space. To view the statistics for a component, select it in the Enterprise View then, on the Storage Dashboard, click the Advanced Statistics tab. See Advanced Statistics Descriptions on page 180 for a complete list of Advanced Statistics descriptions.

The statistics listed vary, depending on which type of component you select. The following example shows the advanced statistics for a controller (on the left) and the maxCache statistics for a logical drive, including cache hits and misses and a histogram of cache hit distribution.
Monitoring Status and Activity

Controller Statistics

## Memory Statistics

### for a Logical Drive

### maxCache Statistics

### Controller Statistics

### maxCache Statistics

---

Microsemi Smart Storage Controllers User Guide Revision 10

127
11.4.3 **Resetting the Statistics Counters**

In maxView Storage Manager, advanced statistics are cumulative. That is, the statistics continue to accumulate until you reset the counters for a controller to zero.

To reset the statistics counters for a controller:

1. In the Enterprise View, select a system, then select the controller you want to reset.
2. On the ribbon, in the Controller group, click **Set Properties**.

![Set Properties window](image)

The Set Properties window opens.

3. Click the **Reset Now** button, then click **Apply**.

![Reset Now button](image)

The statistics counters are reset.

11.5 **Changing an Operating System's Event Log Setting**

In addition to the maxView Storage Manager event log, all Warning- and Error-level events on a system are recorded in its operating system event log. You can select the type of events that are recorded, or you can disable operating system event logging.

To change or disable operating system event logging on a system:

1. Select the Enterprise View node.
2. On the ribbon, in the System group, click **System Settings**.

![System Settings window](image)

The System Settings window opens.

3. In the Save Events to OS Log drop-down list, select the type of events that you want to log, then click **OK**.
4. Restart maxView Storage Manager to apply the new setting.
Managing Your Storage Space

This section describes the advanced features in maxView Storage Manager that help you manage your storage space. You can:

- Deploy servers with a **server template file**
- Manage remote systems and auto-discovery tasks with the Remote System wizard
- Clear a controller configuration
- Change the Web Server port
- Grant Standard users Admin Privilege

12.1 Deploying Servers

maxView Storage Manager helps you deploy servers in your storage space without configuring each server manually. You can select an optimally configured server in your storage space, save its configuration to a server template file, then duplicate the configuration on servers throughout your network.

The basic procedure works like this:

1. Choose the system you want to use as the model for other servers in your storage space.
2. Save the configuration to a server template file.
3. Log in to each remote system in your storage space and restore the configuration from the server template file.

The following sections provide details on each of these steps.

12.1.1 Creating a Server Template File

This procedure saves the configuration of a system that you want to use as a model for other servers in your storage space. It creates a server template file in XML format, which defines the controller type(s), operational settings, physical drive size, logical drive size, RAID level, and more. The default name of the server template file is `ControllerConf.xml`.

To create a server template file:

1. In the Enterprise View, select a system.
2. On the ribbon, in the System group, click **Manage Configuration**.

   ![Manage Configuration](image)

   The Manage Configuration wizard opens.

3. Select **Save Configuration**, then click **Next**.
4. Review the Summary information, then click Finish.

5. When the File Download window opens, click Save File, then click OK.
   
   **Note:** The procedure for downloading and saving the template file may vary, depending on the Web browser.

6. Continue with Duplicating the Server Template to deploy the same configuration on multiple systems in your storage space.

### 12.1.2 Duplicating the Server Template

When you are ready to duplicate the server template on other systems in your storage space, you can restore the configuration from the server template file.

Keep in mind that:

- The server template file (default, ControllerConf.xml) is editable. For example, you may need to change the disk drive capacity or logical drive size to accommodate the differences on each machine.
- Drives from the same vendor with slightly different capacities (147 GB vs. 150 GB, for instance) are considered interchangeable. If the logical drive capacity changes as a result of the size difference, it is scaled accordingly. For example, if the new drives have 4% more capacity due to vendor or model changes, then all logical drives are increased in size by 4%.

To duplicate the server template on another system:

1. In the Enterprise View, select a system.

2. On the ribbon, in the System group, click Manage Configuration.

   The Manage Configuration wizard opens.

3. Select Restore Configuration, then click Next.
4. In the Configuration File panel, click **Choose**, navigate the file system to your server template file, then click **Open**. When the file name appears in the “selected file” area (circled in blue in figure below), click **Upload**, wait for the upload to complete, then click **Next**.

5. In the Restore Options panel, choose a Force option if a controller does not support all of the features of the template controller, or if the drive capacity on the new system does not match the configuration in the server template file. The default is Force None. You can choose to:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Force All</td>
<td>To force deployment of all features</td>
</tr>
<tr>
<td>Force Size</td>
<td>To force deployment of just the logical drives</td>
</tr>
</tbody>
</table>
6. To apply the configuration based on SlotID rather than DeviceID, click the Slot ID check box.

7. Click Next, review the summary information, then click Finish.

maxView Storage Manager duplicates the system configuration on the new controller.

12.2 Managing Remote Systems

maxView Storage Manager has a wizard to help you manage the remote systems in your storage space. The wizard simplifies the process of connecting to remote systems from the local system and adding them to the Enterprise View.

When you start maxView Storage Manager, an “auto-discovery” task runs in the background, continuously searching your network for systems running the maxView Redfish server. The wizard presents a list of discovered systems (see figure below). You can select systems to add to the Enterprise View when you start maxView Storage Manager; add systems manually if they are not discovered automatically; and remove systems that you no longer want to manage.
12.2.1 Adding Remote Systems with the Wizard

For basic instructions for adding remote systems with the wizard, see Logging into Remote Systems from the Local System. Once you add a system in the wizard, it automatically appears in the Enterprise View each time you start maxView Storage Manager. You can work with a remote system's controllers, disk drives, and logical drives as if they were part of your local system.

**Note:** The wizard adds all selected systems to the Enterprise view even if login fails on some systems. For those systems, try running the wizard again with different login credentials.

12.2.2 Manually Adding a Remote System

You can add a remote system manually if auto-discovery fails to find the system on your network.

To manually add a remote system:

1. On the ribbon, in the Home group, click Add System.

2. When the Add System window opens, click System Not Present.
   The Add System Manually window opens.

3. Enter the system name and login credentials in the space provided. Select the Management Protocol from the drop-down list and specify the Port number, then click Add.

   ![Add System Manually Window](image)

   The window closes and the system appears in the discovered systems list in the Add System window.

4. Select the system, then click Add.
   maxView Storage Manager connects to the remote system and adds it to the Enterprise View.

12.2.3 Removing a Remote System

If you no longer want to manage a remote system, you can remove it from the Enterprise View.

**Note:** Removing a remote system from the Enterprise View does not take it off-line.
To remove a remote system:

1. On the ribbon, in the Home group, click **Delete System**.

![Delete System window](image)

The Delete System window opens.

2. Select the system(s) you want to remove. To select all systems in the list, click the checkbox at the top of the window.

![Delete Systems window](image)

3. Click **Delete**.

maxView Storage Manager removes the remote system(s) from the Enterprise View.

### 12.2.4 Changing the Auto-Discovery Settings

Auto-discovery, in maxView Storage Manager, is disabled by default. If enabled, the auto-discovery task runs in the background each time maxView Storage Manager is started. You can enable the auto-discovery if desired, and configure the auto-discovery settings described below.

To change the auto-discovery settings on a system:

1. Select the Enterprise View node.

2. On the ribbon, in the System group, click **System Settings**.
The System Settings window opens for that system. The auto-discovery settings appear at the bottom.

3. To enable/disable auto-discovery, select **Enable Auto Discovery**. (This option toggles between enabled and disabled.)

4. Update the auto-discovery settings. In the Auto Discovery Interval field, enter the number of seconds between each auto-discovery check. This number determines how often maxView Storage Manager checks for changes in remote system resources.

5. Click **OK** to save the changes.

### 12.2.5 Importing and Exporting Remote Systems

maxView provides the ‘Import and Export systems’ feature to add multiple systems and export the added systems in “SystemConf.json” file, which can be used later to import the added systems in maxView running on another system.

The Import and Export feature gets enabled at the “Enterprise View” level in the Manage Configuration ribbon icon.

**Note:**

Export feature is applicable only when maxView GUI manages at least one remote system.

To export a system:

1. Select the Enterprise View node.

2. On the ribbon, in the System group, click **Manage Configuration**.
The Manage Configuration wizard opens for that system.

3. Select **Export System(s)** option, then click **Next**.

4. Select the systems that need to be exported. Click **Next**.
Note:

To get the details of the respective systems, hover the cursor on the system name. It shows details like system name, IP address, operating system, and communication protocol.

The Manage Configuration Summary page appears.

5. Click Finish.

The exported systems are downloaded in a “SystemConf.json” file.

To import a system:

1. Select the Enterprise View node.

2. On the ribbon, in the System group, click Manage Configuration.

The Manage Configuration wizard opens for that system.

3. Select Import System(s) option, then click Next.

4. Click Choose to specify the path of the “SystemConf.json” file.
5. Click Next.

The Select Systems screen appears.

6. Select the system name(s) and specify the login credentials. Select Single Sign-On option to specify the User Name and Password for all the selected systems that have same credentials. Otherwise, specify each system's credentials manually.

    **Note:**

    Single sign-on option is enabled only when more than one system is selected for import.

Hover the cursor on the system name to get the details of the respective systems. It shows details like system name, IP address, operating system, and communication protocol.
7. Click **Next**.

The **Manage Configuration Summary** page appears that shows the list of imported systems.

8. Click **Finish**.

The imported systems will appear in the Enterprise View.

**12.3 Clearing the Controller Configuration**

You can clear the configuration of a controller to accommodate changes in your storage space. For example, you may want to clear a controller if you upgraded your hardware or if you plan to move the controller to another machine. Clearing the configuration destroys the controller meta-data, including array and logical device information, partition information, maxCache information, and so on. Once you clear the controller configuration, your online data is no longer accessible.

**Caution:** When you clear a controller configuration, you lose all data stored on that controller. Be sure you no longer need the data on the controller before proceeding.

To clear the controller configuration:

1. In the Enterprise View, select a system, then select a controller on that system.
2. On the ribbon, in the Controller group, click **Manage Configuration**.

The Manage Configuration wizard opens.

3. Select **Clear Configuration**, then click **Next**.
4. Review the Summary information, then click Finish.

12.4 Changing the Web Server Port

You can change the port used by the maxView Storage Manager Web Server, if needed, to accommodate changes in your network or IT requirements. The Web Server can use any open port for communication. The default port is 8443. If you change the port, you must restart maxView Storage Manager for the change to take effect.

To change the Web Server port:

1. Select the Enterprise View node.
2. On the ribbon, in the System group, click System Settings.

When the System Settings window opens, click the Web Server tab.
3. Enter the new Web Server port. Optionally, click Secured Protocol to enable/disable secure communication over https.

4. Click Apply.

5. Restart maxView Storage Manager.

12.5 Granting Standard Users Admin Privilege

Normally, Standard users have restricted access to your storage space, with limited ability to perform non-destructive operations in maxView Storage Manager (see Working in maxView Storage Manager on page 16). You can grant Standard users Admin Privilege to accommodate changes in your system policies or IT requirements.

To grant Admin privilege to Standard users:

1. Select the Enterprise View node.

2. On the ribbon, in the System group, click System Settings.

The System Settings window opens.

3. Click the Allow Standard User as Admin check box, then click Apply.

4. Restart the webserver.
13 Solving Problems

This section describes how to troubleshoot the components in your storage space.

13.1 General Troubleshooting Tips

If you experience problems installing or using maxView Storage Manager, try these troubleshooting tips first:

- Ensure that all managed systems are powered on and that you are logged in to any remote systems that you want to manage. (See *Logging into Remote Systems from the Local System* on page 28 for more information.)
- Check all cable connections.
- Try uninstalling and reinstalling maxView Storage Manager.
- Check the Release Notes for compatibility issues and known problems.

13.2 Identifying a Failed or Failing Component

When you receive notice of a Warning- or Error-level event, use maxView Storage Manager’s *rapid fault isolation* feature to quickly identify the source of the problem.

For instance, in this example, a disk drive has failed. To find the failed disk drive, expand the tree in the Enterprise View, look for the orange and red warning and error icons, then continue tracing the problem to its source.
13.3 Recovering from a Disk Drive Failure

This section describes how to recover when a disk drive or SSD fails:

- If the logical drive is protected by a hot spare, see Failed Disk Drive Protected by a Hot Sparedisk drives failure recoverywith hot spare on page 144.
- If the logical drive is not protected by a hot spare, see Failed Disk Drive Not Protected by a Hot Sparedisk drives failure recoverywithout hot sparefailed disk drives without hot spare.
- If there is a disk drive failure in more than one logical drive simultaneously, see Failure in Multiple Logical Drives Simultaneouslydisk drives failure recoverymultiple logical drivesfailed disk drives multiple logical drives on page 145.
- If it is a RAID 0 logical drive, see Disk Drive Failure in a RAID 0 Logical Drivedisk drives failure recoveryRAID 0 logical drivesfailed disk drives RAID 0 logical drives on page 145.
- If multiple disk drives fail within the same logical drive, see Forcing a Logical Drive with Multiple Drive Failures Back Onlinedisk drives failure recoverymultiple disk drivesfailed logical driveforce online on page 145.

13.3.1 Failed Disk Drive Protected by a Hot Spare

If a disk drive in a logical drive fails and that logical drive is protected by a hot spare, the hot spare is automatically incorporated into the logical drive and takes over for the failed drive.
For example, if a disk drive fails in a RAID 5 logical drive, the logical drive is automatically rebuilt, with its data reconstructed using the hot spare in place of the failed drive. You can access the logical drive while it’s rebuilding.

To recover from the failure:

1. Remove and replace the failed disk drive, following the manufacturer’s instructions.
2. If the logical drive is protected with a dedicated hot spare, data is moved back to its original location once the controller detects that the failed drive has been replaced. Once the data is copied back, the hot spare becomes a permanent part of the array on failure of array. No further action is necessary. If the logical drive is protected with an auto-replace hot spare, the spare becomes a permanent part of the array. You must designate a new hot spare to protect the logical drive(s) on that array.

See Protecting Your Data on page 42 for more information about managing spares.

13.3.2 Failed Disk Drive Not Protected by a Hot Spare

If a disk drive in a logical drive fails when the logical drive is not protected by a hot spare, remove and replace the failed disk drive. The controller detects the new disk drive and begins to rebuild it. You can access the logical drive while it’s rebuilding.

For example, when one of the disk drives fails in a RAID 1 logical drive, the logical drive is not automatically rebuilt. The failed disk drive must be removed and replaced before the logical drive can be rebuilt.

If the controller fails to rebuild the logical drive, check that the cables, disk drives, and controllers are properly installed and connected. Then, if necessary, follow the instructions in Rebuilding Logical Drivesrebuilding logical driveslogical drives hot-swap rebuilding.

13.3.3 Failure in Multiple Logical Drives Simultaneously

If a disk drive fails in more than one logical drive at the same time (one failure per logical drive), and the logical drives have hot spares protecting them, the controller rebuilds the logical drives with these limitations:

- A hot spare must be at least as big as the smallest disk drive in the array that it might replace.
- Failed disk drives are replaced with hot spares in the order in which they failed. (The logical drive that includes the disk drive that failed first is rebuilt first, assuming an appropriate hot spare is available—see the previous bullet.)

Note: If the number of disk drive failures exceeds the number of hot spares, see Failed Disk Drive Not Protected by a Hot Sparedisk drives failure recoverywithout hot sparefailed disk drives without hot spare.

13.3.4 Disk Drive Failure in a RAID 0 Logical Drive

Because RAID 0 volumes do not include redundancy, if a disk drive fails in a RAID 0 logical drive, the data cannot be recovered.

Correct the cause of the failure or replace the failed disk drives. Then, restore your data from backup, if available. To protect the RAID 0 logical drive, set the spare activation mode to “predictive”.

13.3.5 Forcing a Logical Drive with Multiple Drive Failures Back Online

If multiple disk drives fail in the same logical drive, you may be able to recover the data by forcing the logical drive back online. For instance, if two drives fail in a RAID 5, forcing it online may allow you to access the data, depending on which disk drives failed.

Caution: This procedure is not guaranteed to successfully recover your logical drive. The surest way to recover your data is to restore the failed logical drive from backup.

To force a logical drive online:
1. In the Enterprise view, select the failed logical drive (see Identifying a Failed or Failing Component on page 143).
2. On the ribbon, in the Logical Device group, click Force Online.

3. Click Force, then click OK.

13.3.6 Healing an Array

You can use the Heal Array operation to replace failed physical drives in the array with healthy physical drives. After replacement, the original array and logical drive numbering is unaffected.

The Heal Array operation is part of the Modify Array wizard (see Moving an Array on page 62). It is available in the wizard only if:

- The array has at least one failed drive.
- The array is not rebuilding to a spare.
- A sufficient number of Ready physical drives of the same type and correct size are available to replace each failed physical drive in the array.

Note: The correct size is defined as a drive as large as the smallest drive on the array, but no larger than the smallest spare.

For a RAID 0 volume, the heal operation recreates the volume. For other RAID volume types, the heal operation rebuilds the volume.

To heal an array:

1. In the Enterprise View, select an array.
2. On the ribbon, in the Array group, click Modify Array.

3. When the wizard opens, select Heal Array, then click Next.
4. Select one or more drives to replace the failed drives in the array.

   ![Modify Array window](image)

   **Note:** The drives must have sufficient capacity to hold all of the logical drives in the array.

5. Click **Next**, review the summary information, then click **Finish**.

### 13.4 Rebuilding Logical Drives

A *hot-swap rebuild* occurs when a controller detects that a failed disk drive in a logical drive has been removed and then reinserted.

**Note:** You can use the Heal Array operation as an alternative to a hot-swap rebuild if you have a sufficient number of Ready physical drives of the same type in your storage space. See *Healing an Array* on page 146.

To start a hot-swap rebuild:
1. Following manufacturer’s instructions, gently pull the failed disk drive from the server without fully removing it, then wait for it to spin down fully before continuing.

2. If there is nothing wrong with the disk drive, reinstall it, following manufacturer’s instructions.
   If necessary, replace the failed disk drive with a new disk drive of equal or larger size.

3. The controller detects the reinserted (or new) disk drive and begins to rebuild the logical drive.

13.5 Creating a Support Archive File

Your support representative might ask you to create a support archive file to help diagnose a problem with your system. Saved information includes device logs, drive logs, event logs, error logs, controller logs, history logs, and SMART statistics.

To create the support archive file:

1. In the Enterprise View, select the system on which the problem is occurring. (Look for the orange or red error icons in the Enterprise View.)

2. On the ribbon, in the System group, click **Archive Management**.

The Archive Management window opens.

3. Select the logs you want to save.

4. Click **Save**.

5. When the File Download window opens, click **OK**.

6. In the Archive Management window, click **Clear All Logs** to clear, or **Cancel** to exit.
A Silent Installation on Windows and Linux

This appendix describes how to complete a silent installation of maxView Storage Manager on Windows and Linux systems. A silent installation uses command line parameters to complete an installation without messages or user interaction.

Note: Silent installation on Linux is supported on Red Hat, CentOS, and SLES only.

A.1 Completing a Silent Installation

This section describes the silent installation process for Windows and Linux.

A.1.1 Windows Silent Installation

To complete a silent installation on Windows:

1. Open a command prompt window, then change to the directory where you downloaded the Windows setup program (see Downloading the Installer Package for details).

2. Run the silent installation from the command line:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 64-bit</td>
<td>setup_asm_x64.exe /s /v&quot;/qn &lt;properties&gt;&quot;</td>
</tr>
</tbody>
</table>

where <properties> is one or more of the options listed in Switches, Properties, and Values silent installation switches, properties, and values on page 150.

Separate properties with spaces and enclose all properties after /v in quotes, with NO leading space. Separate feature names for the ADDLOCAL property with commas.
A.1.1 Switches, Properties, and Values

This section describes the command line options for Windows silent installation. These options are not supported on Linux.

<table>
<thead>
<tr>
<th>Switch or Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/s (required)</td>
<td>Suppress dialog boxes.</td>
</tr>
<tr>
<td>/v (required)</td>
<td>Pass command line parameters to the setup program.</td>
</tr>
<tr>
<td>/qn</td>
<td>Suppress progress bar during installation.</td>
</tr>
<tr>
<td>/qb</td>
<td>Show progress bar during installation.</td>
</tr>
<tr>
<td>/lv* &lt;path&gt; (optional)</td>
<td>Generate verbose installation log at &lt;path&gt;. Example: /lv* c:\pmc.log</td>
</tr>
<tr>
<td>INSTALLDIR (optional)</td>
<td>Specifies the installation path. If specified, the installation path must be enclosed in escaped quotation marks. Example: INSTALLDIR=&quot;C:\Program Files\Adaptec\maxView Storage Manager&quot; Note: The default installation path is &quot;C:\Program Files\Adaptec\maxView Storage Manager&quot;.</td>
</tr>
<tr>
<td>ADDLOCAL (optional)</td>
<td>• ALL (default)—Installs the maxView Storage Manager Console (GUI and Redfish server), and ARCCONFIG (CLI). If you specify ALL, do not specify any of the following values. • ARCCONFIG—Installs the Command Line Interface tool (ARCCONF) • RestfulServer—Installs the maxView Storage Manager Redfish Server • Console—Installs the maxView Storage Manager GUI Note: Use commas to separate multiple values.</td>
</tr>
</tbody>
</table>

A.1.2 Linux Silent Installation

To complete a silent installation on Red Hat Linux, CentOS, or SLES:

1. Open a shell window, then change to the directory where you downloaded the Linux installer package (see Downloading the Installer Package Download the Installation Package for details).

2. Run the silent installation from the command line using one of these commands (x.xx-xxxxxxx=version-build number):

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux 64-bit</td>
<td>.\StorMan-X.XX-XXXXX.x86_64.bin --silent</td>
</tr>
</tbody>
</table>

**Note:** Linux systems also support silent upgrade and silent removal. See Example Command Line Installations on page 151.
A.2 Example Command Line Installations

This section shows typical command line installations for Windows and Linux. In the Linux examples, `<x.xx>-<xxxxx>=version-build number.`

- Normal Windows Installation:

```
setup_asm_x64.exe /s /v"/qb /lv* c:\pmc.log"
```

- Install to Specific Location on Windows:

```
setup_asm_x64.exe /s /v"/qb INSTALLDIR="C:\Program Files\Adaptec\maxView Storage Manager\"
```

- Install Specific Feature on Windows:

```
setup_asm_x64.exe /s /v"/qb ADDLOCAL=ARCCONF /lv* c:\pmc.log"
```

- Normal Linux Installation:

```
./StorMan-<x.xx>-<xxxxx>.x86_64.bin --silent
```

- Linux Software Upgrade:

```
./StorMan-<x.xx>-<xxxxx>.x86_64.bin --upgrade
```

- Linux uninstallation (removal):

```
./StorMan-<x.xx>-<xxxxx>.x86_64.bin --remove
```

**Alternative:** `rpm -e StorMan`
B Configuring SNMP Notifications on Windows and Linux

This appendix describes how to enable SNMP trap notifications on Windows and Linux. After installing and configuring the SNMP service, you can monitor activity in your storage space with the maxView Storage Manager GUI or any OS monitoring tool, such as a Mib Browser.

B.1 Setting Up SNMP Notifications on Windows

1. Install and enable the SNMP service on your Windows system. Define the SNMP community to which to send trap messages ("public", for instance). Then designate that name as an Accepted Community in the SNMP Service Properties.

For details on installing and configuring SNMP on Windows, refer to your operating system documentation.

2. On Windows Server 2012 and Windows 8.x systems, the SNMP sub-agent does not have permission to open a socket over TCP/IP or UDP, preventing it from communicating with the maxView Storage Manager.

   Use the following PowerShell scripts to allow the SNMP sub-agent to communicate with the maxView Storage Manager and send trap notifications:

   a. Outbound Rule for Port 34572:

   ```powershell
   $OutBound = @{
   DisplayName = "Maxview Outbound Rule on TCP port 34572 for SNMP Service"
   Direction = "Outbound"
   InterfaceType = "Any"
   Action = "Allow"
   Protocol = "TCP"
   Service = "snmp"
   Program = "$(env:systemdrive)\WINDOWS\system32\snmp.exe"
   Enabled = "TRUE"
   RemotePort = "34572"
   PolicyStore = "ConfigurableServiceStore"
   }
   New-NetFirewallRule @OutBound
   ```

   b. Inbound Rule for Port 34572:

   ```powershell
   $InBound = @{
   DisplayName = "Maxview Inbound Rule on TCP port 34572 for SNMP Service"
   Direction = "Inbound"
   InterfaceType = "Any"
   Action = "Allow"
   Protocol = "TCP"
   Service = "snmp"
   Program = "$(env:systemdrive)\WINDOWS\system32\snmp.exe"
   Enabled = "TRUE"
   RemotePort = "34572"
   PolicyStore = "ConfigurableServiceStore"
   }
   New-NetFirewallRule @InBound
   ```

3. To remove the NetFirewall rules (as needed):

   a. Outbound Rule for Port 34572:

   ```powershell
   Remove-NetFirewallRule -DisplayName "Maxview Outbound Rule on TCP port 34572 for SNMP Service" -PolicyStore "ConfigurableServiceStore"
   ```
b. Inbound Rule for Port 34572:

Remove-NetFirewallRule -DisplayName "Maxview Inbound Rule on TCP port 34572 for SNMP Service" -PolicyStore "ConfigurableServiceStore"

B.2 Setting Up SNMP Notifications on Linux

1. Install the Net-SNMP RPM packages:
   - net-snmp
   - libsnmp15
   - snmp-mibs

2. In `/etc/snmp/snmpd.conf` configuration file:
   - Comment out the com2sec entry:
     ```
     # com2sec notConfigUser  default       public
     ```
   - Add the following lines at the end of the file:
     ```
     rocommunity public
     trapsink localhost
     master agentx
     ```
   - (SLES 10 only) Register the agentx socket:
     ```
     agentxsocket /var/agentx/master
     ```

3. Copy `aus.mib` from `/usr/StorMan` to `/usr/share/snmp/mibs`:

   ```
   #cp /usr/StorMan/aus.mib /usr/share/snmp/mibs
   ```

4. Restart the SNMP agent:

   ```
   #service snmpd restart
   ```

5. Start `aus-snmpd` from `/usr/StorMan`:

   ```
   #./aus-snmpd
   ```
C Using the maxView Plugin for VMware vSphere Web Client

The maxView plugin for VMware vSphere Web Client is a monitoring tool that lets you explore your storage resources directly from the vSphere Web client, without using maxView Storage Manager as a separate Web GUI. It replicates most of the information on the maxView Storage Manager Dashboard (see The Storage Dashboard) for the controllers, logical devices, physical devices, enclosures, and systems (hosts) in your storage space. It offers a vSphere "look and feel" and native navigation.

Note: The maxView plugin is a monitoring tool only. To modify your storage space, such as creating or deleting a logical drive or designating a hot spare, you must use the maxView Storage Manager GUI or CLI (ARCCONF).

C.1 Installing the maxView Plugin for vSphere Web Client

Follow the instructions in this section to install the maxView plugin for vSphere Web Client on a Windows x64 system.

Note: Before you begin, ensure that VMware vSphere Web Client is already installed on the Windows host. You need administrator privileges to install the maxView plugin.

1. Download the setup program for the maxView vSphere plugin from the Web site (see Download the Installation Package).

2. Double-click the setup program:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware ESXi 6.0 client</td>
<td>setup_maxView_VWC6_Plugin_x64.exe</td>
</tr>
<tr>
<td>VMware ESXi 6.5 client</td>
<td>setup_maxView_VWC65_Plugin_x64.exe</td>
</tr>
</tbody>
</table>

The Installation wizard opens.

3. Click Next to begin the installation, accept the terms in the license agreement, then click Next.

4. Enter the following configuration settings for your VMware ESXi server, then click Next:

   a. Hypervisor IP address
   b. Hypervisor user name
   c. Hypervisor password
5. In the Features screen, ensure that maxView VWC Plugin is selected. Optionally, select CLI Tools. Then click Next.

6. Click Install to begin the installation.

When the installation is complete, you receive a confirmation message that the plugin is installed.

C.2 Starting the maxView Plugin for vSphere Web Client

1. Launch the VMware vSphere Web Client: double-click the vSphere desktop icon, then enter your login credentials.

2. In the Monitoring section on the vSphere Home screen (on the right), click the maxView icon; the Controller information screen opens.

3. Alternatively, in the Navigation pane (on the left), click vCenter, scroll down to the maxView tree, then select a resource category, such as Controller, Logical Device, Physical Device, or Enclosure, to open the information screen for that item.
C.3 Monitoring maxView Resources in vSphere Web Client

For each maxView resource in your storage space—controller, logical device, physical device, and so on—you can view summary information about the resource (or "object") and view its related resources, such as the physical devices in a logical drive, the logical drives on a controller, or the controllers on a host.

For example, the figure below shows the summary information screen for a logical drive, with expandable information fields containing general information about the logical drive, its settings, and resources. (Each expandable field has an arrow next to it.)
Click on the **Related Objects tab** (next to the Summary tab) to show the physical devices comprising the logical drive, the logical drive's controller, or a filtered list of events for that logical drive.

To drill down further, click on any item in the related objects table, below the button bar. For example, click on a physical device in the table shown below to view summary information for that device, its related objects, and so on.

When you're ready to monitor a different resource, click the resource category in the Navigation pane (on the left). Or click on the History window one or more times (in the upper-left corner of the vSphere client) to return to the vCenter top-level screen; then select a resource in the maxView tree.
Once you return to the top-level screen or choose a resource in the Navigation pane, the procedure for viewing the resource summary and drilling down for more detail is identical for all maxView resources in your storage space.

For more information about the types of information provided on the summary screen and related objects screens for each maxView resource, see Viewing Component Status in the Storage Dashboard.
Using maxView Storage Manager with HBAs and Non-RAID Mode Controllers

maxView Storage Manager allows you to manage storage resources on Microsemi Adaptec Host Bus Adapters (HBAs) and RAID controllers operating in HBA mode (see Changing the Connector Operating Mode on page 104). In the Enterprise View, maxView Storage Manager displays HBAs and non-RAID mode controllers in the controller list. Drives on the HBA are surfaced to the OS as Raw devices; that is, storage devices without Microsemi Adaptec RAID meta-data.

Note: maxView Storage Manager identifies the drive as a Raw device even if it has an OS partition.

With HBAs and non-RAID mode controllers, maxView Storage Manager limits access to features that are not used to configure and maintain RAID volumes (see table below). For example, on the Ribbon, you can use the options in the Controller group to manage your controller, but not options in the Array group or Logical Device group (because HBAs don't support logical volumes); similarly, you can use options in the System group to upgrade the controller firmware, but not the Spare Management option in the Physical Devices group (because HBAs don't support spares); and so on.

<table>
<thead>
<tr>
<th>Ribbon</th>
<th>Options for HBAs / Non-RAID Mode Controllers</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Group</td>
<td>Firmware Update</td>
</tr>
<tr>
<td>Controller Group</td>
<td>Rescan, Properties (non-RAID mode controllers only)</td>
</tr>
<tr>
<td>Array Group</td>
<td>None</td>
</tr>
<tr>
<td>Logical Device Group</td>
<td>None</td>
</tr>
<tr>
<td>Physical Devices Group</td>
<td>Force Offline, Uninitialize, Locate</td>
</tr>
<tr>
<td>maxCache Group</td>
<td>None</td>
</tr>
</tbody>
</table>

The Storage Dashboard provides detailed information about the HBAs and non-RAID mode controllers in your storage space (similar to its function for RAID controllers), including the enclosures, disk drives, and SSDs connected to them (for more information about the dashboard, see Viewing Component Status in the Storage Dashboard).
Tabs on the dashboard provide quick access to summary information, controller properties, resources, and the connector configuration. The Events tab shows filtered events for the device (see Viewing Activity Status in the Event Log on page 113).

The following table lists the categories and types of information provided on the Storage Dashboard for HBAs and connected devices.

<table>
<thead>
<tr>
<th>Component</th>
<th>Categories</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controller</td>
<td>Summary Properties</td>
<td>Model, WWN, key features, firmware version, controller mode, status, number and type of physical devices.</td>
</tr>
<tr>
<td></td>
<td>Resources Connectors</td>
<td>Slot, driver version, bus type and speed, number of ports, settings (mostly disabled) Physical drive assignments by connector, including protocol, state, free and used space Connector name, number of devices, functional mode</td>
</tr>
<tr>
<td>Physical Devices</td>
<td>Summary</td>
<td>Physical drive assignments by connector, including protocol, state, free and used space</td>
</tr>
<tr>
<td>(node)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connector</td>
<td>Summary</td>
<td>Functional mode, number of devices</td>
</tr>
<tr>
<td>Enclosure</td>
<td>Summary</td>
<td>Enclosure type, vendor, model, ID, channel, firmware version, status Fan, power supply, and temperature status (see Monitoring Enclosure Status enclosures monitoring enclosures temperature status enclosures fan status temperature status enclosures power status on page 117) Slot allocation and usage</td>
</tr>
<tr>
<td>Hard drives and SSDs</td>
<td>Summary Resources</td>
<td>Drive type (hard drive, SSD), vendor, interface (SAS/SATA), and model Block size, total size, rotational speed Boot type Firmware version, WWN, transfer speed Free space, used space, reserved space SMART statistics (see Viewing SMART Statistics on page 117)</td>
</tr>
<tr>
<td></td>
<td>SMART</td>
<td></td>
</tr>
</tbody>
</table>
E  Selecting the Best RAID Level

When you create logical drives in maxView Storage Manager, you can assign a RAID level to protect your data.

Each RAID level offers a unique combination of performance and redundancy. RAID levels also vary by the number of disk drives they support.

This section provides a comparison of all the RAID levels supported by maxView Storage Manager, and provides a basic overview of each to help you select the best level of protection for your storage system.

Note: Not all RAID levels are supported by all controllers. See the Release Notes for supported RAID levels on specific controller models.

E.1  Comparing RAID Levels

Use this table to select the RAID levels that are most appropriate for the logical drives on your storage space, based on the number of available disk drives and your requirements for performance and reliability.

<table>
<thead>
<tr>
<th>RAID Level</th>
<th>Redundancy</th>
<th>Disk Drive Usage</th>
<th>Read Performance</th>
<th>Write Performance</th>
<th>Built-in Hot Spare</th>
<th>Minimum Disk Drives</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAID 0</td>
<td>No</td>
<td>100%</td>
<td>***</td>
<td>***</td>
<td>No</td>
<td>2</td>
</tr>
<tr>
<td>RAID 1</td>
<td>Yes</td>
<td>50%</td>
<td>**</td>
<td>**</td>
<td>No</td>
<td>2</td>
</tr>
<tr>
<td>RAID 1(ADM)</td>
<td>Yes</td>
<td>33%</td>
<td>**</td>
<td>**</td>
<td>No</td>
<td>3</td>
</tr>
<tr>
<td>RAID 1E</td>
<td>Yes</td>
<td>50%</td>
<td>**</td>
<td>**</td>
<td>No</td>
<td>3</td>
</tr>
<tr>
<td>RAID 10</td>
<td>Yes</td>
<td>50%</td>
<td>**</td>
<td>**</td>
<td>No</td>
<td>4</td>
</tr>
<tr>
<td>RAID 10(ADM)</td>
<td>Yes</td>
<td>33%</td>
<td>**</td>
<td>**</td>
<td>No</td>
<td>6</td>
</tr>
<tr>
<td>RAID 5</td>
<td>Yes</td>
<td>67 – 94%</td>
<td>***</td>
<td>*</td>
<td>No</td>
<td>3</td>
</tr>
<tr>
<td>RAID 50</td>
<td>Yes</td>
<td>67 – 94%</td>
<td>***</td>
<td>*</td>
<td>No</td>
<td>6</td>
</tr>
<tr>
<td>RAID 6</td>
<td>Yes</td>
<td>50 – 88%</td>
<td>**</td>
<td>*</td>
<td>No</td>
<td>4</td>
</tr>
<tr>
<td>RAID 60</td>
<td>Yes</td>
<td>50 – 88%</td>
<td>**</td>
<td>*</td>
<td>No</td>
<td>8</td>
</tr>
</tbody>
</table>

Disk drive usage, read performance, and write performance depend on the number of drives in the logical drive. In general, the more drives, the better the performance.
E.2 Non-redundant Logical Drives (RAID 0)

A logical drive with RAID 0 includes one or more disk drives and provides data *striping*, where data is distributed evenly across the disk drives in equal-sized sections. However, RAID 0 logical drives do not maintain redundant data, so they offer *no data protection*.

Compared to an equal-sized group of independent disks, a RAID 0 logical drives provides improved I/O performance.

Drive segment size is limited to the size of the smallest disk drive in the logical drive. For instance, an array with two 250 GB disk drives and two 400 GB disk drives can create a RAID 0 drive segment of 250 GB, for a total of 1000 GB for the volume, as shown in this figure.
E.3 RAID 1 Logical Drives

A RAID 1 logical drive is built from two disk drives, where one disk drive is a mirror of the other (the same data is stored on each disk drive). Compared to independent disk drives, RAID 1 logical drives provide improved performance, with up to twice the read rate and an equal write rate of single disks. However, capacity is only 50 percent of independent disk drives.

If the RAID 1 logical drive is built from different-sized disk drives, the free space, drive segment size is the size of the smaller disk drive, as shown in this figure.
E.4 RAID 1 (ADM) Logical Drives

RAID 1 Advanced Data Mirroring, or ADM, is similar to RAID 1, but creates fault tolerance by maintaining redundant copies of data using three disk drives, rather than two. All three drives contain mirrored duplicated user data.

If a drive fails, the remaining drives provide backup copies of the files and normal system operations are not interrupted.
### E.5 RAID 10 Logical Drives

A RAID 10 logical drive is built from two or more equal-sized RAID 1 logical drives. Data in a RAID 10 logical drive is both striped and mirrored. Mirroring provides data protection, and striping improves performance.

Drive segment size is limited to the size of the smallest disk drive in the logical drive. For instance, an array with two 250 GB disk drives and two 400 GB disk drives can create two mirrored drive segments of 250 GB, for a total of 500 GB for the logical drive, as shown in this figure.
E.6 RAID 10 (ADM) Logical Drives

RAID 10 Advanced Data Mirroring, or ADM, is similar to RAID 10, but creates fault tolerance by maintaining redundant copies of data using at least six disk drives. Data is striped across two or more sets of RAID 1 (ADM) drives for rapid access.

If a drive fails, the remaining drives provide backup copies of the files and normal system operations are not interrupted.
Selecting the Best RAID Level

Disk Drives in Logical Drive

Drive Segment Size (Smallest Disk Drive)

Disk Drive 1
250 GB

Disk Drive 2
250 GB

Disk Drive 3
250 GB

Disk Drive 4
250 GB

Disk Drive 5
400 GB

Disk Drive 6
400 GB

Disk Drive 1
1 3 ... 499

Disk Drive 2
2 4 ... 500

Disk Drive 3
1 3 ... 499

Disk Drive 4
2 4 ... 500

Disk Drive 5
1 3 ... 499

Disk Drive 6
2 4 ... 500

Unused Space = 150 GB

Unused Space = 150 GB

RAID 10(ADM) Logical Drive = 500 GB
A RAID 5 logical drive is built from a minimum of three disk drives, and uses data striping and *parity* data to provide redundancy. Parity data provides data protection, and striping improves performance.

Parity data is an error-correcting redundancy that's used to re-create data if a disk drive fails. In RAID 5 logical drives, parity data (represented by Ps in the next figure) is striped evenly across the disk drives with the stored data.

Drive segment size is limited to the size of the smallest disk drive in the logical drive. For instance, an array with two 250 GB disk drives and two 400 GB disk drives can contain 750 GB of stored data and 250 GB of parity data, as shown in this figure.
Selecting the Best RAID Level

Disk Drive 1  250 GB
Disk Drive 2  250 GB
Disk Drive 3  400 GB
Disk Drive 4  400 GB

Disk Drives in Logical Drive

Drive Segment Size (Smallest Disk Drive)

Disk Drive 1  1 4 \ldots P
Disk Drive 2  2 5 \ldots 748
Disk Drive 3  3 P \ldots 749
Disk Drive 4  P 6 \ldots 750

Unused Space = 150 GB
Unused Space = 150 GB

Disk Drive 1
Disk Drive 2
Disk Drive 3
Disk Drive 4

RAID 5 Logical Drive = 750 GB plus Parity
E.8 **RAID 50 Logical Drive**

A RAID 50 logical drive is built from six to forty-eight disk drives configured as two or more RAID 5 arrays, and stripes stored data and parity data across all disk drives in both RAID 5 logical drives. (For more information, see *RAID 5 Logical Drives*.)

The parity data provides data protection, and striping improves performance. RAID 50 logical drives also provide high data transfer speeds.

Drive segment size is limited to the size of the smallest disk drive in the logical drive. For example, three 250 GB disk drives and three 400 GB disk drives comprise two equal-sized RAID 5 logical drives with 500 GB of stored data and 250 GB of parity data. The RAID 50 logical drive can therefore contain 1000 GB (2 x 500 GB) of stored data and 500 GB of parity data.

In this figure, P represents the distributed parity data.
Selecting the Best RAID Level

RAID 50
Logical Drive =
1000 GB
plus Parity

Each RAID 5 Logical Drive has
500 GB Data Storage
250 GB Parity Data

RAID 5
A

1, 5, P
Drive 1
250 GB

3, P, 9
Drive 2
250 GB

P, 7, 11
Drive 3
250 GB

RAID 5
B

2, 8, P
Drive 4
400 GB

4, P, 10
Drive 5
400 GB

P, 8, 12
Drive 6
400 GB

Total Unused
Space = 150 GB
E.9 **RAID 6 Logical Drives**

A RAID 6 logical drive—also known as dual drive failure protection—is similar to a RAID 5 logical drive because it uses data striping and parity data to provide redundancy. However, RAID 6 logical drives include two independent sets of parity data instead of one. Both sets of parity data are striped separately across all disk drives in the logical drive.

RAID 6 logical drives provide extra protection for your data because they can recover from two simultaneous disk drive failures. However, the extra parity calculation slows performance (compared to RAID 5 logical drives).

RAID 6 logical drives must be built from at least four disk drives. Maximum stripe size depends on the number of disk drives in the logical drive.

Based on the drive segment sizes used: RAID 6 Logical Drive = 500 GB plus parity (P1 & P2)
E.10 RAID 60 Logical Drives

Similar to a RAID 50 logical drive (see RAID 50 Logical Drive), a RAID 60 logical drive—also known as dual drive failure protection—is built from eight disk drives configured as two or more RAID 6 logical drives, and stripes stored data and two sets of parity data across all disk drives in both RAID 6 logical drives.

Two sets of parity data provide enhanced data protection, and striping improves performance. RAID 60 logical drives also provide high data transfer speeds.
Icons At-a-Glance

The following is a complete list of icons used in maxView Storage Manager. It contains the icons on the ribbon, in the Enterprise View, and on tabs and dialog boxes.

See *Overview of the Main Window* for more information.

### Ribbon Home Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Remote system add icon]</td>
<td>Remote system add</td>
</tr>
<tr>
<td>![Remote system delete icon]</td>
<td>Remote system delete</td>
</tr>
</tbody>
</table>

### Ribbon System Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![System settings icon]</td>
<td>System settings</td>
</tr>
<tr>
<td>![Manage configuration icon]</td>
<td>Manage configuration (save/restore)</td>
</tr>
<tr>
<td>![Firmware update icon]</td>
<td>Firmware update</td>
</tr>
<tr>
<td>![Save archive file icon]</td>
<td>Save archive file</td>
</tr>
</tbody>
</table>

### Ribbon Controller Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Controller settings icon]</td>
<td>Controller settings</td>
</tr>
<tr>
<td>![Manage configuration icon]</td>
<td>Manage configuration (clear)</td>
</tr>
<tr>
<td>![Controller rescan icon]</td>
<td>Controller rescan</td>
</tr>
<tr>
<td>![maxCrypto settings icon]</td>
<td>maxCrypto settings</td>
</tr>
</tbody>
</table>

### Ribbon Array Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Array settings icon]</td>
<td>Array settings</td>
</tr>
<tr>
<td>![Array modify icon]</td>
<td>Array modify</td>
</tr>
<tr>
<td>Icon</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Array split/mirror</td>
<td></td>
</tr>
<tr>
<td>Array locate</td>
<td></td>
</tr>
<tr>
<td>Array delete</td>
<td></td>
</tr>
</tbody>
</table>

### Ribbon Logical Device Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical drive settings</td>
<td></td>
</tr>
<tr>
<td>Logical drive create</td>
<td></td>
</tr>
<tr>
<td>Logical drive expand/migrate</td>
<td></td>
</tr>
<tr>
<td>Logical drive locate</td>
<td></td>
</tr>
<tr>
<td>Logical drive delete</td>
<td></td>
</tr>
<tr>
<td>Logical drive force online</td>
<td></td>
</tr>
</tbody>
</table>

### Ribbon Physical Device Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical disk properties</td>
<td></td>
</tr>
<tr>
<td>Assign/unassign physical disk as spare</td>
<td></td>
</tr>
<tr>
<td>Force physical disk offline</td>
<td></td>
</tr>
<tr>
<td>Physical disk secure erase</td>
<td></td>
</tr>
<tr>
<td>Physical disk locate</td>
<td></td>
</tr>
</tbody>
</table>

### Ribbon maxCache Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>maxCache Device create</td>
<td></td>
</tr>
<tr>
<td>maxCache Device set properties</td>
<td></td>
</tr>
<tr>
<td>maxCache Device locate</td>
<td></td>
</tr>
</tbody>
</table>
### Icons At-a-Glance

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="maxCache Device delete" /></td>
<td>maxCache Device delete</td>
</tr>
<tr>
<td><img src="image2" alt="maxCache Device disable" /></td>
<td>maxCache Device disable</td>
</tr>
</tbody>
</table>

### Enterprise View Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image3" alt="Enterprise View" /></td>
<td>Enterprise View</td>
</tr>
<tr>
<td><img src="image4" alt="Local or remote system" /></td>
<td>Local or remote system</td>
</tr>
<tr>
<td><img src="image5" alt="Controller" /></td>
<td>Controller</td>
</tr>
<tr>
<td><img src="image6" alt="Enclosure" /></td>
<td>Enclosure</td>
</tr>
<tr>
<td><img src="image7" alt="Logical disk" /></td>
<td>Logical disk</td>
</tr>
<tr>
<td><img src="image8" alt="Logical disks" /></td>
<td>Logical disks</td>
</tr>
<tr>
<td><img src="image9" alt="Physical disk" /></td>
<td>Physical disk</td>
</tr>
<tr>
<td><img src="image10" alt="Hard disk drive" /></td>
<td>Hard disk drive</td>
</tr>
<tr>
<td><img src="image11" alt="Solid State drive" /></td>
<td>Solid State drive</td>
</tr>
<tr>
<td><img src="image12" alt="SMR drive" /></td>
<td>SMR drive</td>
</tr>
<tr>
<td><img src="image13" alt="Physical disks" /></td>
<td>Physical disks</td>
</tr>
<tr>
<td><img src="image14" alt="Enclosure" /></td>
<td>Enclosure</td>
</tr>
<tr>
<td><img src="image15" alt="Connector or other physical device" /></td>
<td>Connector or other physical device</td>
</tr>
</tbody>
</table>

### Enterprise View Status Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image16" alt="Enterprise OK" /></td>
<td>Enterprise OK</td>
</tr>
<tr>
<td><img src="image17" alt="Enterprise error" /></td>
<td>Enterprise error</td>
</tr>
<tr>
<td><img src="image18" alt="Enterprise no access" /></td>
<td>Enterprise no access</td>
</tr>
<tr>
<td>Icon</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
<tr>
<td>![Enterprise warning icon]</td>
<td>Enterprise warning</td>
</tr>
</tbody>
</table>

### Enterprise View System Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![System OK icon]</td>
<td>System OK</td>
</tr>
<tr>
<td>![System error icon]</td>
<td>System error</td>
</tr>
<tr>
<td>![System missing icon]</td>
<td>System missing</td>
</tr>
<tr>
<td>![System no access icon]</td>
<td>System no access</td>
</tr>
<tr>
<td>![System warning icon]</td>
<td>System warning</td>
</tr>
</tbody>
</table>

### Enterprise View Connector Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Connector OK icon]</td>
<td>Connector OK</td>
</tr>
<tr>
<td>![Connector failed icon]</td>
<td>Connector failed</td>
</tr>
<tr>
<td>![Connector missing icon]</td>
<td>Connector missing</td>
</tr>
<tr>
<td>![Connector warning icon]</td>
<td>Connector warning</td>
</tr>
</tbody>
</table>

### Enterprise View Controller Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Controller OK icon]</td>
<td>Controller OK</td>
</tr>
<tr>
<td>![Controller failed icon]</td>
<td>Controller failed</td>
</tr>
<tr>
<td>![Controller missing icon]</td>
<td>Controller missing</td>
</tr>
<tr>
<td>![Controller warning icon]</td>
<td>Controller warning</td>
</tr>
<tr>
<td>![Controller encrypted icon]</td>
<td>Controller encrypted</td>
</tr>
</tbody>
</table>
### Enterprise View Enclosure Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Enclosure Management OK" /></td>
<td>Enclosure Management OK</td>
</tr>
<tr>
<td><img src="image2" alt="Enclosure Management failed" /></td>
<td>Enclosure Management failed</td>
</tr>
<tr>
<td><img src="image3" alt="Enclosure missing" /></td>
<td>Enclosure missing</td>
</tr>
<tr>
<td><img src="image4" alt="Enclosure Management warning" /></td>
<td>Enclosure Management warning</td>
</tr>
</tbody>
</table>

### Enterprise View Physical Disk Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image5" alt="Physical disk OK" /></td>
<td>Physical disk OK</td>
</tr>
<tr>
<td><img src="image6" alt="Physical disks OK" /></td>
<td>Physical disks OK</td>
</tr>
<tr>
<td><img src="image7" alt="Physical disks failure" /></td>
<td>Physical disks failure</td>
</tr>
<tr>
<td><img src="image8" alt="Physical disks missing" /></td>
<td>Physical disks missing</td>
</tr>
<tr>
<td><img src="image9" alt="Physical disks warning" /></td>
<td>Physical disks warning</td>
</tr>
<tr>
<td><img src="image10" alt="Physical disk encrypted" /></td>
<td>Physical disk encrypted</td>
</tr>
</tbody>
</table>

### Enterprise View MaxCache Device Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image11" alt="maxCache Device error" /></td>
<td>maxCache Device error</td>
</tr>
<tr>
<td><img src="image12" alt="maxCache Device missing" /></td>
<td>maxCache Device missing</td>
</tr>
<tr>
<td><img src="image13" alt="maxCache Device OK" /></td>
<td>maxCache Device OK</td>
</tr>
<tr>
<td><img src="image14" alt="maxCache Device warning" /></td>
<td>maxCache Device warning</td>
</tr>
</tbody>
</table>

### Tab Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image15" alt="Summary" /></td>
<td>Summary</td>
</tr>
</tbody>
</table>
## Icons At-a-Glance

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>📄</td>
<td>Properties</td>
</tr>
<tr>
<td>🔍</td>
<td>Resources</td>
</tr>
<tr>
<td>🗓️</td>
<td>Events</td>
</tr>
<tr>
<td>📄</td>
<td>Task</td>
</tr>
<tr>
<td>🛠️</td>
<td>maxCrypto</td>
</tr>
</tbody>
</table>

### Dialog Box Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>📧</td>
<td>E-mail notification</td>
</tr>
<tr>
<td>📈</td>
<td>Chart</td>
</tr>
</tbody>
</table>
The following table describes the advanced statistics properties by device type.

See Viewing Advanced Statistics on page 126 for more information.

<table>
<thead>
<tr>
<th>Type</th>
<th>Property</th>
<th>Description</th>
<th>Units</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controller</td>
<td>Average Dirty Cache Lines</td>
<td>The average number of dirty cache lines that are waiting to be flushed. Dirty cache lines that are in the process of being flushed are not included in this count. Note that lines in the read-ahead cache may also be &quot;dirty,&quot; so the number of dirty cache lines may exceed the number of write cache lines.</td>
<td></td>
</tr>
<tr>
<td>Controller</td>
<td>Free Largest Transfer Buffer Sectors</td>
<td>The average number of consecutive transfer buffer sectors available in the controller's internal pool.</td>
<td></td>
</tr>
<tr>
<td>Controller</td>
<td>Average Free Total Transfer Buffer Sectors</td>
<td>The average number of transfer buffer sectors available in the controller's internal pool.</td>
<td></td>
</tr>
<tr>
<td>Controller</td>
<td>Average Free Logical Requests</td>
<td>The average number of logical request structures available in the controller's internal pool.</td>
<td></td>
</tr>
<tr>
<td>Controller</td>
<td>Average Free Processor RAM in kB</td>
<td>The average amount of available processor RAM in kB available in the controller's internal pool.</td>
<td></td>
</tr>
<tr>
<td>Controller</td>
<td>Average Locked Stripes</td>
<td>The average number of stripes that are locked. In this context, a stripe is a group of physical sectors across a RAID group that is busy performing a write operation (other operations to the same sectors are locked out during this process).</td>
<td></td>
</tr>
<tr>
<td>Controller</td>
<td>Average Locked Stripes Waiting</td>
<td>The average number of requests that are stalled waiting to access stripes that are locked. A large value indicates random writes over a small area of a RAID 5 array.</td>
<td></td>
</tr>
<tr>
<td>Controller</td>
<td>Average Write Cache Sectors</td>
<td>The average number of 512-byte blocks that there is room for in the write cache. Controller cache is currently organized in 16 kB “lines,” so divide this value by 32 to determine the number of available write cache lines.</td>
<td></td>
</tr>
<tr>
<td>Controller</td>
<td>Command List Count</td>
<td>Number of command lists submitted by the host.</td>
<td></td>
</tr>
<tr>
<td>Controller</td>
<td>Command List Latency</td>
<td>Average command latency in hundredths of milliseconds.</td>
<td>Hundredths of milliseconds</td>
</tr>
<tr>
<td>Controller</td>
<td>Logical Request Count</td>
<td>Number of logical requests submitted by the host.</td>
<td></td>
</tr>
<tr>
<td>Controller</td>
<td>Maximum DMA Transfer Queue Depth</td>
<td>The maximum number of DMA transfer (WCXC bus master) requests that have been queued up at any time since performance monitoring was started.</td>
<td></td>
</tr>
<tr>
<td>Controller</td>
<td>Maximum Outstanding Command List</td>
<td>Maximum number of outstanding command lists.</td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>Property</td>
<td>Description</td>
<td>Units</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Controller</td>
<td>Percent Active</td>
<td>Percentage of time (in tenths of a percent) that at least one logical request is outstanding, including event-notification commands.</td>
<td>Tenths of a percent</td>
</tr>
<tr>
<td>Controller</td>
<td>Percent Busy</td>
<td>Percentage of time (in percent) that the controller’s CPU is not just sitting in the &quot;idle&quot; task. Note that background activity such as surface analysis is not considered &quot;idle&quot; time.</td>
<td>Percent</td>
</tr>
<tr>
<td>Controller</td>
<td>Percent Time Waiting For DMA</td>
<td>The percentage of time (in tenths of a percent) that the local CPU has been stalled waiting for DMA (WCXC bus master) transfers.</td>
<td>Tenths of a percent</td>
</tr>
<tr>
<td>Controller</td>
<td>Sample Interval</td>
<td>Time since performance monitoring was last cleared, in tenths of seconds.</td>
<td>Tenths of seconds</td>
</tr>
<tr>
<td>Logical D-</td>
<td>Average Queue Depth</td>
<td>Average number of logical read and write requests queued.</td>
<td></td>
</tr>
<tr>
<td>rive</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logical D-</td>
<td>Average Read Latency</td>
<td>Average latency for logical read requests in hundredths of milliseconds.</td>
<td>Hundredths of milli-seconds</td>
</tr>
<tr>
<td>rive</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logical D-</td>
<td>Average Write Latency</td>
<td>Average latency for logical write requests in hundredths of milliseconds.</td>
<td>Hundredths of milli-seconds</td>
</tr>
<tr>
<td>rive</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logical D-</td>
<td>Cache Hits</td>
<td>Number of cache hits (host-generated logical read requests which could be serviced entirely by the cache without any disk access).</td>
<td></td>
</tr>
<tr>
<td>rive</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logical D-</td>
<td>Cache Misses</td>
<td>Number of cache misses.</td>
<td></td>
</tr>
<tr>
<td>rive</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logical D-</td>
<td>Coalesced Requests</td>
<td>Number of host requests to this volume that were coalesced by firmware.</td>
<td></td>
</tr>
<tr>
<td>rive</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logical D-</td>
<td>Flush Read Requests</td>
<td>Number of read-fill requests issued by the cache flush task. The flush task generates read requests to make a dirty cache line completely valid so that it can be flushed in a single write request.</td>
<td></td>
</tr>
<tr>
<td>rive</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logical D-</td>
<td>Flush Write Requests</td>
<td>Number of flush requests issued by the cache flush task.</td>
<td></td>
</tr>
<tr>
<td>rive</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logical D-</td>
<td>Logical Reads</td>
<td>Number of logical read requests submitted by the host, excluding requests coalesced by firmware.</td>
<td></td>
</tr>
<tr>
<td>rive</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logical D-</td>
<td>Logical Writes</td>
<td>Number of logical write requests submitted by the host, excluding requests coalesced by firmware.</td>
<td></td>
</tr>
<tr>
<td>rive</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logical D-</td>
<td>Maximum Read Request Latency</td>
<td>Maximum latency for logical read requests to this volume in hundredths of milliseconds.</td>
<td>Hundredths of milliseconds</td>
</tr>
<tr>
<td>rive</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logical D-</td>
<td>Maximum Write Request Latency</td>
<td>Maximum latency for logical write requests to this volume in hundredths of milliseconds.</td>
<td>Hundredths of milliseconds</td>
</tr>
<tr>
<td>rive</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logical D-</td>
<td>Non-Sequential Reads</td>
<td>Number of non-consecutive or non-sequential read requests from the host. A non-sequential request is defined as a logical request with a starting logical block that is not equal to 1 plus the ending logical block of the previously received logical request.</td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>Property</td>
<td>Description</td>
<td>Units</td>
</tr>
<tr>
<td>--------------------</td>
<td>------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>Logical Drive</td>
<td>Non-Sequential Writes</td>
<td>Number of non-consecutive or non-sequential write requests from the host. A non-sequential request is defined as a logical request with a starting logical block that is not equal to 1 plus the ending logical block of the previously received logical request.</td>
<td></td>
</tr>
<tr>
<td>Logical Drive</td>
<td>Posted Writes</td>
<td>Number of host write operations that were absorbed by the posted write cache.</td>
<td></td>
</tr>
<tr>
<td>Logical Drive</td>
<td>Read Ahead Sector Count</td>
<td>Number of sectors pre-fetched.</td>
<td></td>
</tr>
<tr>
<td>Logical Drive</td>
<td>SectorsFlushed</td>
<td>Total number of sectors in all flush requests issued by the cache flush task.</td>
<td></td>
</tr>
<tr>
<td>Logical Drive</td>
<td>Sectors Read</td>
<td>Number of logical blocks read from this volume by the host. Does not include any internally generated read requests (such as read-ahead, capacity expansion, etc.).</td>
<td></td>
</tr>
<tr>
<td>Logical Drive</td>
<td>Sectors Written</td>
<td>Number of logical blocks written to this volume by the host. Does not include any internally generated write requests (such as read-ahead, capacity expansion, etc.).</td>
<td></td>
</tr>
<tr>
<td>Logical Drive</td>
<td>Unaligned Reads</td>
<td>Number of unaligned read requests from the host. An unaligned logical request is defined as one that spans multiple physical drives but has a block count smaller than or equal to the distribution factor.</td>
<td></td>
</tr>
<tr>
<td>Logical Drive</td>
<td>Unaligned Writes</td>
<td>Number of unaligned write requests from the host. An unaligned logical request is defined as one that spans multiple physical drives but has a block count smaller than or equal to the distribution factor.</td>
<td></td>
</tr>
<tr>
<td>Physical Drive</td>
<td>Average Request Latency</td>
<td>Average latency for physical read/write requests in hundredths of milliseconds.</td>
<td>Hundredths of milliseconds</td>
</tr>
<tr>
<td>Physical Drive</td>
<td>Maximum Queue Depth</td>
<td>Maximum number of physical (SCSI) requests in the queue for this drive, including both those queued up on the drive and those on the array controller’s elevator queue.</td>
<td></td>
</tr>
<tr>
<td>Physical Drive</td>
<td>Maximum Request Latency</td>
<td>Maximum latency for physical read/write requests in hundredths of milliseconds.</td>
<td>Hundredths of milliseconds</td>
</tr>
<tr>
<td>Physical Drive</td>
<td>Maximum Wait Time Between Completions</td>
<td>Maximum amount of time between completion of outstanding requests (when multiple requests are outstanding), in hundredths of milliseconds. A high value may indicate that the drive is experiencing errors.</td>
<td>Hundredths of milliseconds</td>
</tr>
<tr>
<td>Physical Drive</td>
<td>Read Requests</td>
<td>Number of physical (SCSI) read requests generated from host and cache read-ahead logical requests (not counting internal requests such as surface analysis, rebuild, expand, snapshot, M&amp;P, etc.).</td>
<td></td>
</tr>
<tr>
<td>Physical Drive</td>
<td>Write Requests</td>
<td>Number of physical (SCSI) write requests generated from host and cache-flush logical requests (not counting internal requests such as surface analysis, rebuild, expand, snapshot, M&amp;P, RIS saves, etc.).</td>
<td></td>
</tr>
<tr>
<td>Physical Drive</td>
<td>Aborted Commands</td>
<td>The number of times a drive was failed due to aborted commands that could not be retried successfully.</td>
<td></td>
</tr>
</tbody>
</table>
### Advanced Statistics Descriptions

<table>
<thead>
<tr>
<th>Type</th>
<th>Property</th>
<th>Description</th>
<th>Units</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Drive</td>
<td>Medium Errors</td>
<td>The number of times a drive was failed due to unrecoverable media errors.</td>
<td></td>
</tr>
<tr>
<td>Physical Drive</td>
<td>Parity Errors</td>
<td>The total number of times that write memory errors were detected on transfers to/from cache memory from other components. This includes parity errors, ECC corrected errors, and ECC un-corrected errors, depending upon the controller.</td>
<td></td>
</tr>
<tr>
<td>Physical Drive</td>
<td>Hardware Errors</td>
<td>The number of times a drive returned a bad hardware status.</td>
<td></td>
</tr>
</tbody>
</table>
# Smart Controller Device Status

The following is a complete list of the Smart Controller devices, their status, and their descriptions used in maxView Storage Manager.

## Status Details of an Array

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ok</td>
<td>The array has all the logical device(s) in optimal state</td>
</tr>
<tr>
<td>Has Initializing Logical Device</td>
<td>One or more member logical device(s) has RPI in progress</td>
</tr>
<tr>
<td>Logical Devices Not Contiguous</td>
<td>The logical devices in this array are not in contiguous order. Perform consolidate space operation to consolidate all the free space to the end of the array.</td>
</tr>
<tr>
<td>Has Failed Physical Device</td>
<td>Array has a bad or missing physical device</td>
</tr>
<tr>
<td>Has Failed Logical Device</td>
<td>One or more logical device(s) in the array has failed</td>
</tr>
</tbody>
</table>

## Status Details of a Logical Device

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optimal</td>
<td>The logical device is healthy and is readily accessible by the host</td>
</tr>
<tr>
<td>Queued for Expansion</td>
<td>The logical device is queued for expansion</td>
</tr>
<tr>
<td>Expanding</td>
<td>The logical device is undergoing online capacity expansion</td>
</tr>
<tr>
<td>Ready for Recovery</td>
<td>The logical device is queued to be recovered from a failed physical device</td>
</tr>
<tr>
<td>Recovering</td>
<td>The logical device is rebuilding a physical device from fault tolerant data</td>
</tr>
<tr>
<td>Wrong Drive Replaced</td>
<td>A wrong physical device was replaced</td>
</tr>
<tr>
<td>RPI In Progress</td>
<td>Rapid parity initialization is currently in progress on this logical device</td>
</tr>
<tr>
<td>RPI Queued</td>
<td>Rapid parity initialization is currently queued on this logical device. It will start once other progress tasks are completed.</td>
</tr>
<tr>
<td>Unsupported on The Controller</td>
<td>Logical device is unsupported on this controller. Host access to this volume is denied. Logical device can still be deleted/reconfigured with data loss.</td>
</tr>
<tr>
<td>Encrypted Logical Device Without Key</td>
<td>The encrypted logical device is exported from a foreign controller with different master key. Please import the foreign master key to access the logical device.</td>
</tr>
<tr>
<td>Encryption Migration</td>
<td>The logical device is being migrated between plaintext and ciphertext</td>
</tr>
<tr>
<td>Encrypted Logical Device Rekeying</td>
<td>The logical device is encrypted and all data is being re-keyed using the background 'online capacity expansion' transformation task. The cache memory is being used to keep track of progress.</td>
</tr>
<tr>
<td>Encrypted Logical Device With maxCrypto Off</td>
<td>The logical device is encrypted, exported from a foreign controller and cannot be accessed as the controller does not have encryption enabled/not configured.</td>
</tr>
</tbody>
</table>
### Status

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption Migration Requested</td>
<td>The logical device has received a request to migrate from plaintext to ciphertext. But this process has not yet started. The plaintext volume is currently online.</td>
</tr>
<tr>
<td>Encrypted Logical Device Rekey Requested</td>
<td>The logical device is encrypted and has received a request to re-key all data with a new encryption key</td>
</tr>
<tr>
<td>Unknown</td>
<td>The status of logical device is unknown</td>
</tr>
<tr>
<td>Erase In Progress</td>
<td>The logical device is offline and has erase in progress</td>
</tr>
<tr>
<td>Ejected</td>
<td>The logical device is offline from being ejected. Reinstall the removed physical devices.</td>
</tr>
<tr>
<td>Not Yet Available</td>
<td>An expand, shrink, or move operation on the array is in progress. This logical device will remain in this state until all expand, shrink, or move operations on this array are completed. All I/O requests sent to the logical drive in this state will be rejected.</td>
</tr>
<tr>
<td>Not Configured</td>
<td>The logical device is not yet configured</td>
</tr>
<tr>
<td>Interim Recovery</td>
<td>The logical device has a bad or missing drive. Logical device is operating with reduced performance and a further physical drive failure may result in data loss depending on the fault tolerance. To correct this problem, check the data and power connections to the physical drives or replace the failed drive.</td>
</tr>
<tr>
<td>Failed</td>
<td>The logical device has bad or missing physical device(s).</td>
</tr>
<tr>
<td>Disabled From SCSI ID Conflict</td>
<td>A conflict with an existing SCSI ID exists. Check all SCSI components to make sure they all have a unique SCSI ID.</td>
</tr>
</tbody>
</table>

### Status Details of a Physical Device

<table>
<thead>
<tr>
<th>Status</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ready</td>
<td>The physical device is readily available for RAID configuration</td>
</tr>
<tr>
<td>Optimal</td>
<td>The physical device is part of an array/logical device</td>
</tr>
<tr>
<td>Waiting For Rebuild</td>
<td>The physical device is waiting to be rebuilt</td>
</tr>
<tr>
<td>Rebuilding</td>
<td>The data on the physical device is being rebuilt. The physical device will be accessible. But performance will be less than optimal during the rebuilding process.</td>
</tr>
<tr>
<td>Queued For Erase</td>
<td>The physical device is currently queued for erase and the will not be available for use until the erase operation is completed</td>
</tr>
<tr>
<td>Erase In Progress</td>
<td>The physical device is currently being erased and the will not be available for use until the erase operation is completed</td>
</tr>
<tr>
<td>Erase Completed</td>
<td>Erase process has been completed on the physical device and the physical device is offline. The physical device may now be brought online through the initialize operation.</td>
</tr>
<tr>
<td>Erase Failed</td>
<td>The physical device erase process is failed and the is offline. The physical device may now be brought online through the initialize operation.</td>
</tr>
<tr>
<td>Erase Aborted</td>
<td>The physical device is offline due to a aborted erase process</td>
</tr>
<tr>
<td>Status</td>
<td>Details</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Predictive Failure</td>
<td>This physical device is predicted to fail soon. Backup all the data on the drive and replace the drive.</td>
</tr>
<tr>
<td>Transient Data Drive</td>
<td>The physical device is in transition from being a member of an array to being an unassigned physical device as a result of shrink array/move array operation</td>
</tr>
<tr>
<td>Failed</td>
<td>The physical device is bad or missing</td>
</tr>
<tr>
<td>Failed Due To Predictive Spare Activation</td>
<td>The physical device has been failed by the controller after completing a predictive spare activation</td>
</tr>
<tr>
<td>Unsupported</td>
<td>The physical device is not supported by the controller</td>
</tr>
<tr>
<td>Not Supported</td>
<td>The controller firmware version does not support this physical device. Replace the physical device with the one supported by the controller.</td>
</tr>
</tbody>
</table>
Index

A

activity in storage space 22
event log 22
task log 22
activity on storage space, See monitoring adapters, See controllers
Add System wizard 134
archive file x, 148
arrays viii, 71
deleting viii, 71
auto-discovery 133
auto-replace hot spares 42

B

background consistency check viii, 57
boards, See controllers
bootable USB image vii, 14
build method 32, 35
Build 32, 35
Default 32, 35
building storage space viii, 29, 32, 73
adding maxCache SSD caching viii, 73
on existing array viii, 32
on new array viii, 29

C

cache optimizations 58
cards, See controllers
components ix, 2, 91
defined 2
viewing properties ix, 91
Configuration Event Detail window 113
configuring viii, 29, 32
   See also building storage space
connector modes 104
controller vii, x, 23, 140
clearing configuration x, 140
controller connector modes 104
controller performance optimization 103
controllers viii–ix, 82, 91, 102, 105
maxCrypto properties viii, 82
properties ix, 91
rescanning ix, 102
updating firmware ix, 105

D

dedicated hot spares viii, 42–43, 46
creating viii, 43
removing viii, 46
deleting logical drives viii, 71
direct attached storage 1
defined 1
disk drive ix, 109
updating firmware ix, 109
disk drives viii–x, 30, 54–55, 91, 97–100, 105, 144–145
contextual graphic 54
different sizes in same logical drive viii, 55
failed state ix, 98
   failure recovery x, 144–145
   multiple disk drives x, 145
   multiple logical drives x, 145
   RAID 0 logical drives x, 145
   with hot spare x, 144
   without hot spare x, 145
identifying ix, 91
initializing ix, 91
locating ix, 100
properties ix, 91
replacing in logical drives ix, 97
secure erasing ix, 98
uninitializing ix, 99
updating firmware ix, 105
within logical drives 30
drives ix, 91
identifying ix, 91
locating ix, 91

E

email notifications ix, 119–120, 122–124
changing “from” address ix, 124
cranging SMTP server ix, 124
disabling ix, 124
failed test emails 123
modifying recipient information ix, 123
recipient addresses ix, 119
removing recipients ix, 123
setup ix, 119
SMTP server settings 120
test emails ix, 122
Email Notifications Manager ix, 119, 122
opening ix, 119
test emails ix, 122
enclosure ix, 110
updating firmware ix, 110
enclosures ix, 23, 91, 117
fan status 117
identifying ix, 91
locating ix, 91
monitoring 117
power status 117
status 23
temperature status 117
Enterprise View vii, 18, 20
icons 20
event log ix, 22, 112
event log (operating system) 128
events 22

Microsemi Smart Storage Controllers User Guide Revision 10
187
expander ix, 110
updating firmware ix, 110
expanding logical drives viii, 69

F
failed disk drives x, 145
multiple logical drives x, 145
RAID 0 logical drives x, 145
without hot spare x, 145
failed logical drive x, 145
force online x, 145
firmware ix, 105, 109–110
Firmware Update wizard ix, 105
force online x, 145
formatting logical drives viii, 35

G
Green Backup status 116

H
hard disk 2
hard disk drive 2
hard drive, See disk drive
help vii, 24
hot spare activation viii, 48
hot spares viii, 42–44, 46
auto-replace viii, 44
creating dedicated viii, 43
limitations viii, 42
removing viii, 46

I
icons 20, 114
Enterprise View 20
event status icons 114
identifying components ix, 91
initializing disk drives ix, 100

L
local systems 26
locating drives ix, 91
logging in vii, 16, 27
logging into remote systems 28
logging out vii, 25
build method 32, 35
building on existing array viii, 32
building on new array viii, 29
changing RAID levels viii, 67
defined 54
deleting viii, 71
different-sized disk drives viii, 55
disabling background consistency check viii, 57
logical drives (continued) enabling background consistency check viii, 57
encrypting viii, 84
expanding viii, 69
formatting viii, 35
hot-swap rebuilding x, 147
increasing capacity viii, 69
non-redundant x, 162
options for creating 29
partitioning viii, 35
RAID 1 x, 163
RAID 1 (ADM) x, 164
RAID 10 x, 165
RAID 10 (ADM) x, 166
RAID 5 x, 168
RAID 50 x, 170
RAID 6 x, 172
RAID 60 x, 173
rebuild priority viii, 70
rebuilding 145
renaming viii, 71
replacing disk drives ix, 97
selecting disk drives 30
selecting RAID levels 30, 34
Shingled Magnetic Recording device 29
SMR drive 29
Device Managed (SMR DM) 29
Host Aware (SMR HA) 29
Host Managed (SMR HM) 29
Perpendicular Magnetic Recording device (PMR) 29

M
main window vii, ix, 17, 25, 112–115
event details 113
event log ix, 112
Logout button 25
monitoring activity and status ix, 112
notification types ix, 112, 114
event log ix, 112
event status icons 114
overview vii, 17
status icons 114
Storage Dashboard ix, 115
task details 115
maxCache viii, 73, 75, 126
cache hits and misses 126
limitations viii, 73
write cache setting viii, 75
write caching
maxCache Device viii, 73–75
creating viii, 73
deleting viii, 75
selecting a RAID level 74
selecting SSDs 74
maxCache statistics ix, 126
maxCrypto viii–ix, 77, 79, 82–83, 86–87, 89
accounts viii, 79
checking status viii, 82
configuration viii, 83
importing a master key ix, 89
Index

maxCrypto  (continued)
re-keying a logical drive viii, 86
resetting ix, 87
setup viii, 77
maxView Storage Manager vii, ix, 4–5, 17–18, 20–21, 28, 112
beginning steps 4
Enterprise View vii, 18
event log ix, 112
icons 20
introduction vii, 4
logging into remote systems 28
main window overview vii, 17
maxCache devices vii, 18
Redfish Server vii, 4
ribbon vii, 21
Ribbon vii, 18
system requirements vii, 5
monitoring ix, 22, 91, 112–115, 119–120, 122–124
device properties ix, 91
email notifications ix, 119–120, 122–124
changing "from" address ix, 124
changing SMTP server ix, 124
failed test emails 123
modifying recipient information ix, 123
recipient addresses ix, 119
removing recipients ix, 123
setup ix, 119
SMTP server settings 120
test emails ix, 122
Email Notifications Manager ix, 119
event details 113
event log ix, 22, 112
options ix, 112
status icons 114
Storage Dashboard ix, 115
task details 115
task log 22

N

network requirements 9
non-RAID Mode controllers x, 159–160
non-redundant logical drives x, 162
notification types ix, 119
e-mail notifications ix, 119

O

online help vii, 24
operating system event log 128
operating systems vii, 5

P

partitioning logical drives viii, 35
physical device error counters ix, 95
power management viii, 71
Properties tab ix, 91
pure HBAs x, 159–160

R

RAID x, 162–166, 168, 170, 172–173
non-redundant logical drives x, 162
RAID 0 x, 162
RAID 1 x, 163
RAID 1 (ADM) x, 164
RAID 10 x, 165
RAID 10 (ADM) x, 166
RAID 5 x, 168
RAID 50 x, 170
RAID 6 x, 172
RAID 60 x, 173
RAID levels viii, 30, 34, 67
changing viii, 67
selecting 30, 34
RAW drive ix, 99
RAW state ix, 99
reactivating split mirror backup viii, 66
rebuild priority viii, 70
rebuilding (defined) 145
remirroring split mirror backup viii, 66
remote systems x, 26, 134
adding manually x, 134
removing x, 134
renaming logical drives viii, 71
rescanning controllers ix, 102
Resources View vii, 23
ribbon vii, 21, 28, 67, 69, 71, 102, 148
Add system 28
Change logical device name 71
Expand or change logical device 67, 69
overview vii, 21
Rescan 102
Save support archive 148
Ribbon vii, 18

S

secure erase ix, 98
segments 55
Self-Monitoring Analysis and Reporting Technology (SMART) 118
Server Template File ix, 130
Shingled Magnetic Recording device viii, 42
silent installation 150
switches, properties, and values 150
SMART statistics 118
SMR drive viii, 42
Device Managed (SMR DM) viii, 42
Host Aware (SMR HA) viii, 42
Host Managed (SMR HM) viii, 42
Perpendicular Magnetic Recording device (PMR) viii, 42
SMTP server ix, 124
split mirror backup array viii, 66
SSD IO Bypass viii, 60
statistics counters 128
resetting 128
statistics logging ix, 125–126, 128
counters 128
enabling 125
viewing ix, 126
Statistics Viewer ix, 126
status 22–23
enclosures 23
event log 22
task log 22
See also monitoring
status icons 114
main window 114
Storage Dashboard ix, 91, 115
storage space vii, 2, 6
examples vii, 6
support archive file x, 148
Survival mode viii, 71
system requirements vii, 5
systems ix, 26, 91
local systems 26
systems (continued)
properties ix, 91
remote systems 26
T
task log 22
temperature status 117
terminology vii, 2
U
uninitializing disk drives ix, 99–100
updating firmware ix, 105, 109–110
W
write cache viii, 75
write-back 75
write-through 75
Microsemi makes no warranty, representation, or guarantee regarding the information contained herein or the suitability of its products and services for any particular purpose, nor does Microsemi assume any liability whatsoever arising out of the application or use of any product or circuit. The products sold hereunder and any other products sold by Microsemi have been subject to limited testing and should not be used in conjunction with mission-critical equipment or applications. Any performance specifications are believed to be reliable but are not verified, and Buyer must conduct and complete all performance and other testing of the products, alone and together with, or installed in, any end-products. Buyer shall not rely on any data and performance specifications or parameters provided by Microsemi. It is the Buyer’s responsibility to independently determine suitability of any products and to test and verify the same. The information provided by Microsemi hereunder is provided “as is, where is” and with all faults, and the entire risk associated with such information is entirely with the Buyer. Microsemi does not grant, explicitly or implicitly, to any party any patent rights, licenses, or any other IP rights, whether with regard to such information itself or anything described by such information. Information provided in this document is proprietary to Microsemi, and Microsemi reserves the right to make any changes to the information in this document or to any products and services at any time without notice.