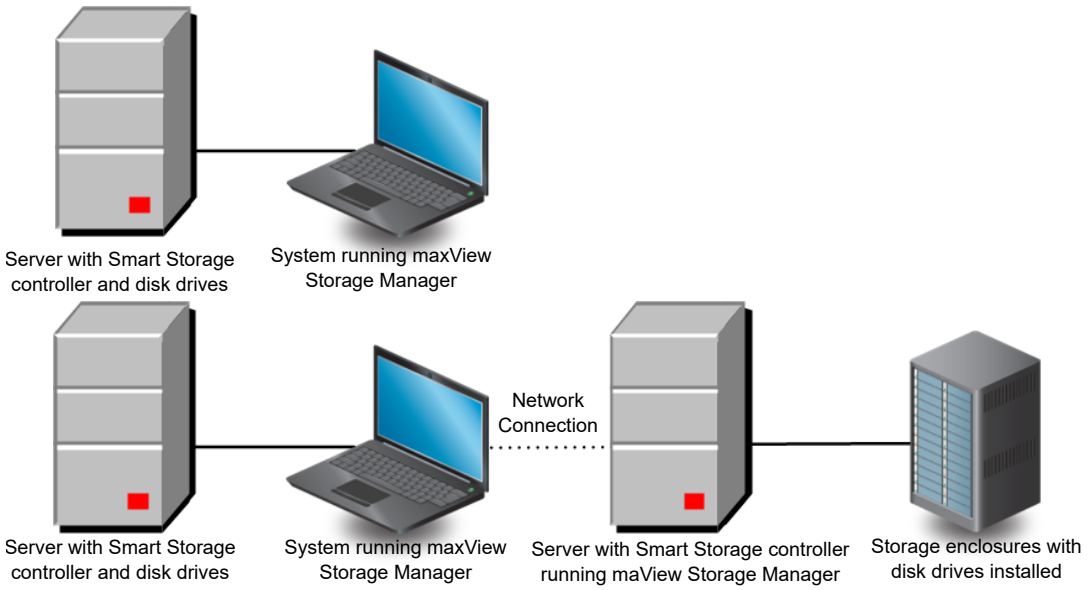
maxView™ Storage Manager User Guide for Adaptec® Smart Storage Controllers

About this Guide

maxView™ Storage Manager™ is a browser-based software application that helps you build a storage space using Microchip 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 Microchip Smart Storage Controllers (SmartRAID/SmartHBA/SmartIOC/SmartROC). For information about using maxView Storage Manager with Adaptec Series 8 (legacy) RAID controllers, see 3 How to Find More Information.



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 Microchip 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).

© 2021 Microchip Technology Inc. and its subsidiaries

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)

How to Find More Information

You can find more information about your Microchip Smart Storage Controller, management software, and utilities by referring to these documents, available for download at start.adaptec.com and the Microchip customer portal at www.microchip.com/wwwregister/default.aspx:

- *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*
- *ARCCONF Command Line Utility User's Guide for Smart Storage Controllers, SmartIOC 2000 Command Line Utility User's Guide*—Describes how to use the ARCCONF utility to perform RAID configuration and storage management tasks from an interactive command line.
- *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.
- *Microchip Adaptec® SmartRAID 3100 Series and SmartHBA 2100 Series Host Bus Adapters Installation and User's Guide*—Describes how to install drivers and configure the SmartRAID 3100 or SmartHBA 2100 Series Host Bus Adapter.
- *HBA 1100 Software/Firmware Release Notes*—Provides driver, firmware, and release package information, and known issues.
- *SmartHBA 2100 and SmartRAID 3100 Software/Firmware Release Notes*—Provides driver, firmware, and release package information, and known issues.

For information about using maxView Storage Manager with Microchip Adaptec Series 8 (legacy) RAID controllers, see the *maxView Storage Manager User's Guide for Adaptec ARC Controllers* (CDP-00285-06-A).

Table of Contents

About this Guide....1

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

1. Introduction to maxView Storage Manager....7
   - 1.1. Getting Started....7
   - 1.2. About maxView Storage Manager....7
   - 1.3. System Requirements....7
   - 1.4. Browser Support....8
   - 1.5. Typical Storage Space Configurations....8

2. Installing maxView Storage Manager....11
   - 2.1. Before You Begin the Installation....11
   - 2.2. Installing on Windows....11
   - 2.3. Installing on Red Hat, Citrix XenServer, CentOS, or SuSE Linux....13
   - 2.4. Installing on Debian or Ubuntu Linux....13
   - 2.5. Installing on VMware 6.x....13
   - 2.6. Installing on VMware 7.x....14
   - 2.7. Running maxView Storage Manager from a Bootable USB Image....15
   - 2.8. Uninstalling maxView Storage Manager....15

3. Exploring maxView Storage Manager....17
   - 3.1. Starting maxView Storage Manager and Logging In....17
   - 3.2. Working in maxView Storage Manager....17
   - 3.3. Overview of the Main Window....18
   - 3.4. Checking System Status from the Main Window....22
   - 3.5. Revealing More Device Information....23
   - 3.6. Getting Help....24
   - 3.7. Logging Out of maxView Storage Manager....25

4. Building Your Storage Space....26
   - 4.1. Overview....26
   - 4.2. Choosing a Management System....26
   - 4.3. Logging into Remote Systems from the Local System....27
   - 4.4. Creating Arrays and Logical Drives....28
   - 4.5. Controller Support for 4K Drives....35
   - 4.6. Controller Support for SED....41

5. Protecting Your Data....44
   - 5.1. Dedicated Spare or Auto-Replace Spare?....44
   - 5.2. Hot Spare Limitations....44
   - 5.3. Assigning a Dedicated Hot Spare....44
   - 5.4. Assigning an Auto-Replace Hot Spare....46
   - 5.5. Removing a Hot Spare....48
   - 5.6. Setting the Spare Activation Mode....50
   - 5.7. Controller Sanitize Lock Freeze/Anti-Freeze....51

© 2021 Microchip Technology Inc. and its subsidiaries

6. Modifying Your Storage Space....55
6.1. Understanding Arrays and Logical Drives....55
6.2. Creating and Modifying Logical Drives....55
6.3. Enabling Background Consistency Check....57
6.4. Optimizing Logical Drive Performance....57
6.5. Moving a Logical Drive....60
6.6. Moving an Array....62
6.7. Modifying an Array....63
6.8. Working with Mirrored Arrays....65
6.9. Changing the RAID Level of a Logical Drive....66
6.10. Increasing the Capacity of a Logical Drive....67
6.11. Changing the Logical Drive Rebuild Priority....68
6.12. Renaming a Logical Drive....69
6.13. Deleting an Array or Logical Drive....70
6.14. Maintaining an Energy-Efficient Storage Space....70

7. Working with maxCache Devices....72
7.1. maxCache Limitations....72
7.2. Creating a maxCache Device....72
7.3. Changing the Write Cache Mode....74
7.4. Deleting the maxCache Device....74
7.5. Analyzing maxCache Performance....74

8. Working with maxCrypto™ Devices....75
8.1. maxCrypto Initial Setup....75
8.2. Modifying the maxCrypto Configuration....80
8.3. Creating an Encrypted Logical Drive....81
8.4. Converting Plaintext Data to Encrypted Data....82
8.5. Re-Keying a Logical Drive....83
8.6. Clearing the maxCrypto Configuration....84
8.7. Erasing an Encrypted Logical Drive....85
8.8. Importing a Foreign Master Key....86

9. Maintaining Physical Devices....87
9.1. Viewing Device Properties....87
9.2. Locating Drives in Your Storage Space....87
9.3. Working with Physical Device Error Counters....90
9.4. Refresh SED Security Status....93
9.5. Working with Failed or Failing Disk Drives....95
9.6. Erasing a Disk Drive....96
9.7. Initializing and Uninitializing Disk Drives....97
9.8. Setting the Physical Drive Boot Priority....98
9.9. Working with Controllers....99
9.10. Updating Controller, Enclosure, and Disk Drive Firmware....103

10. Monitoring Status and Activity....109
10.1. Monitoring Options....109
10.2. Checking Status from the Main Window....109

10.3. Notifying Users by Email About Status and Activity 114
10.4. Monitoring Advanced Statistics about Activity in Your Storage Space..... 119
10.5. Changing an Operating System's Event Log Setting..... 121

11. Managing Your Storage Space..... 123
11.1. Deploying Servers 123
11.2. Managing Remote Systems..... 126
11.3. Clearing the Controller Configuration..... 133
11.4. Changing the Web Server Port..... 133
11.5. Granting Standard Users Admin Privilege..... 134

12. Solving Problems..... 135
12.1. General Troubleshooting Tips..... 135
12.2. Identifying a Failed or Failing Component..... 135
12.3. Recovering from a Disk Drive Failure..... 136
12.4. Rebuilding Logical Drives..... 138
12.5. Creating a Support Archive File..... 139

13. Silent Installation on Windows and Linux..... 140
13.1. Completing a Silent Installation..... 140
13.2. Example Command Line Installations..... 141

14. Configuring SNMP Notifications on Windows and Linux..... 142
14.1. Setting Up SNMP Notifications on Windows..... 142
14.2. Setting Up SNMP Notifications on Linux..... 142

15. Using the maxView Plugin for VMware vSphere Web Client..... 144
15.1. Installing the maxView Plugin for vSphere Web Client..... 144
15.2. Starting the maxView Plugin for vSphere Web Client..... 145
15.3. Monitoring maxView Resources in vSphere Web Client..... 146

16. Using the maxView Plugin for VMware vSphere HTML5..... 149
16.1. Installing the maxView Plugin for vSphere HTML5 Client..... 149
16.2. Starting the maxView Plugin for vSphere HTML Client..... 150
16.3. Monitoring maxView Resources in vSphere HTML Client..... 151
16.4. Import and Export Remote ESXi Systems using maxView Plugin..... 154

17. Using maxView Storage Manager with HBAs and Non-RAID Mode Controllers..... 158

18. Selecting the Best RAID Level..... 160
18.1. Comparing RAID Levels..... 160
18.2. Non-redundant Logical Drives (RAID 0)..... 160
18.3. RAID 1 Logical Drives 161
18.4. RAID 1 Triple Logical Drives..... 161
18.5. RAID 10 Logical Drives..... 162
18.6. RAID 10 Triple Logical Drives..... 163
18.7. RAID 5 Logical Drives..... 163
18.8. RAID 50 Logical Drive..... 164
18.9. RAID 6 Logical Drives..... 165
18.10. RAID 60 Logical Drives..... 166

19. Icons At-a-Glance..... 167
20. Advanced Statistics Descriptions..... 172
21. Smart Controller Device Status..... 176
22. Display Properties of a Controller, Array, Logical Device, and a Physical Device..... 180
23. maxView Video Tutorials..... 190
24. Revision History..... 192
The Microchip Website..... 193
Product Change Notification Service..... 193
Customer Support..... 193
Microchip Devices Code Protection Feature..... 193
Legal Notice..... 193
Trademarks..... 194
Quality Management System..... 195
Worldwide Sales and Service..... 196

1. 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.

1.1 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 2. Installing maxView Storage Manager).

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

Step 4: Build your storage space (see 4. Building Your Storage Space).

1.2 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 1.4 Browser Support). 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.

1.2.1 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.

1.2.2 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.

1.3 System Requirements

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

- PC-compatible computer with Intel Pentium processor, or equivalent
- At least 4 GB of RAM
- 350 MB of free disk drive space

© 2021 Microchip Technology Inc. and its subsidiaries

- One of these operating systems:
  - Microsoft® Windows® Server, Windows SBS, Windows 10, Windows 8.1
  - 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 2.7 Running maxView Storage Manager from a Bootable USB Image for more information.

1.4 Browser Support

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

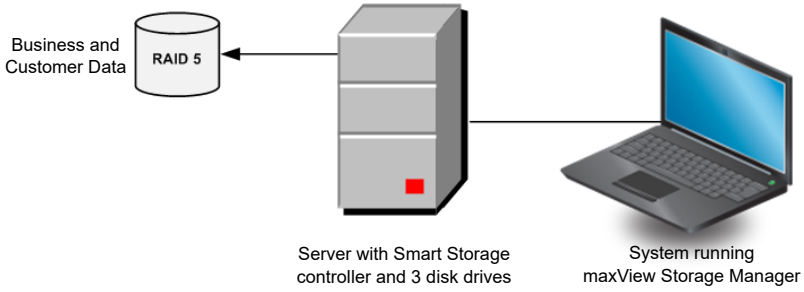
- Microsoft® Edge browser for Windows 10
- Google® Chrome™ 32 or newer
- Mozilla Firefox® 31 or newer

1.5 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.

1.5.1 A Simple Storage Space

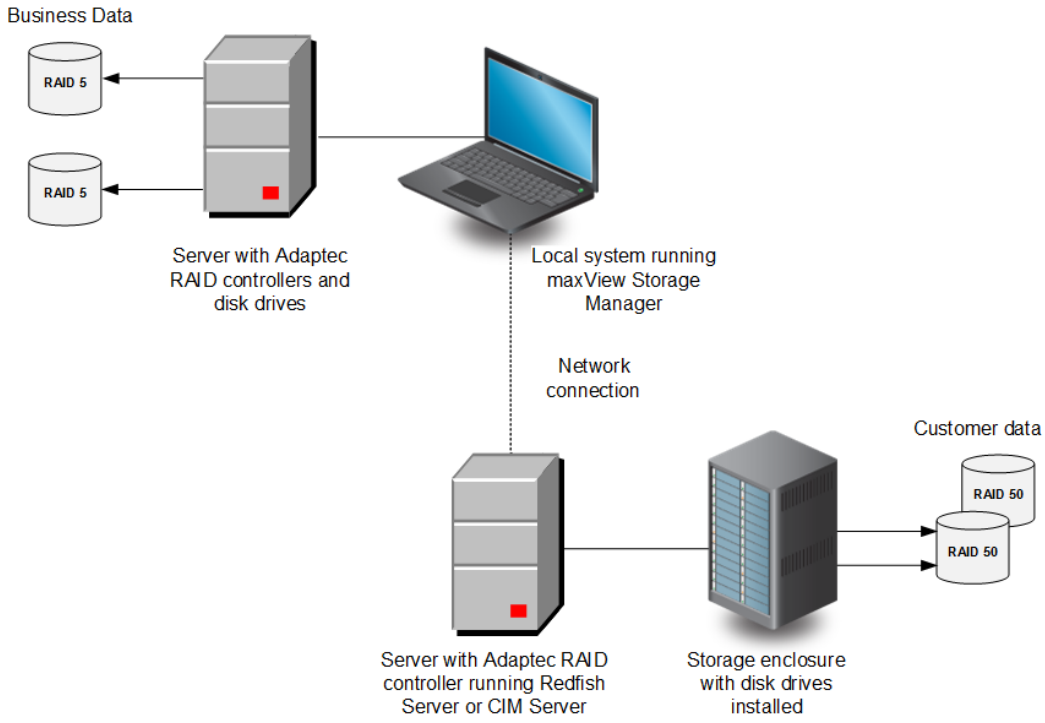
This example shows a simple storage space that might be appropriate for a small business. This storage space includes one RAID controller and three disk drives installed in a server. For data protection, the disk drives have been used to build a RAID 5 logical drive.



1.5.2 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.

© 2021 Microchip Technology Inc.
and its subsidiaries

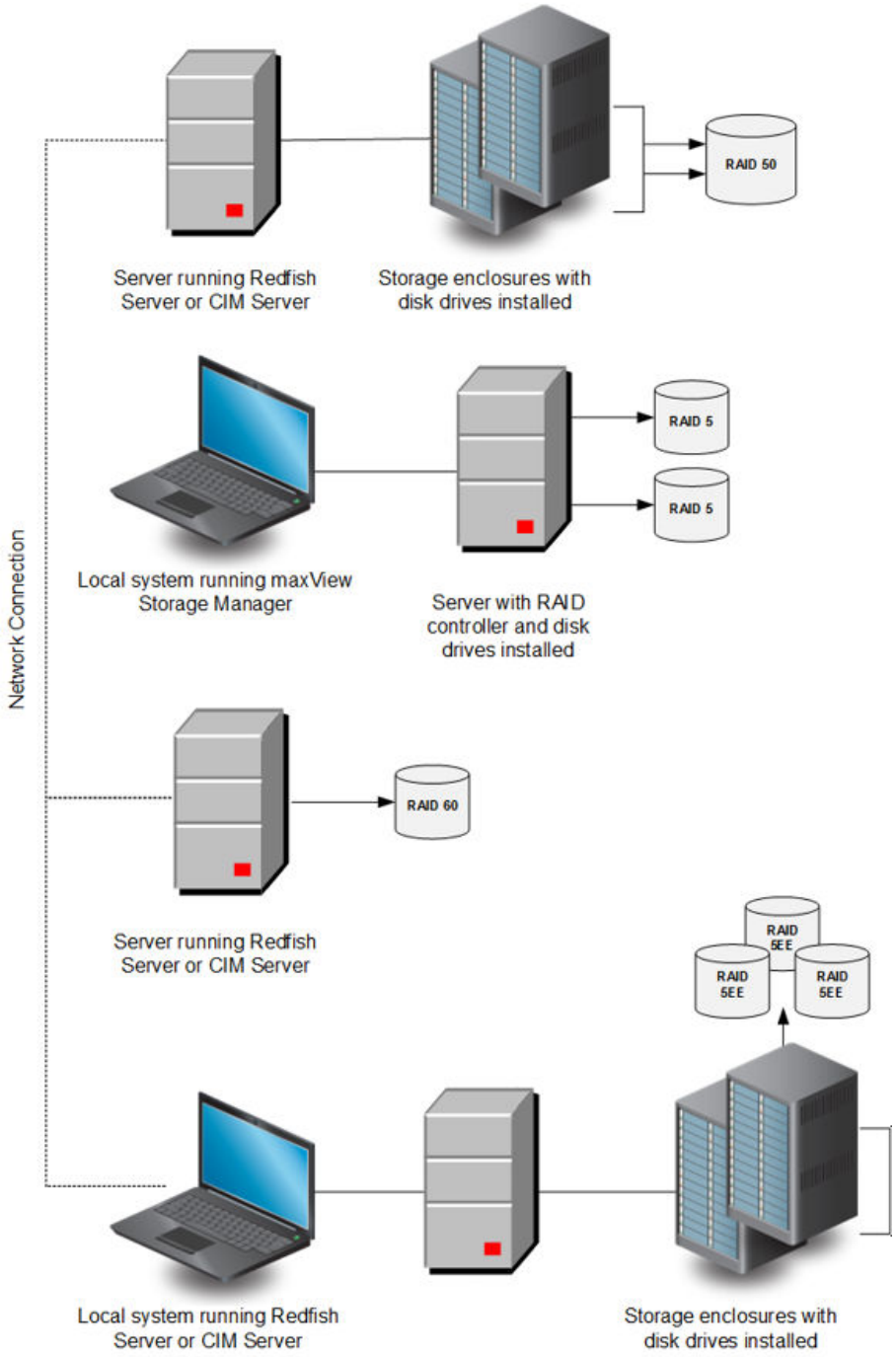


1.5.3 Continuing to Grow Your Storage Space

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.

© 2021 Microchip Technology Inc. and its subsidiaries


RAID 50
Server running Redfish Server or CIM Server
Storage enclosures with disk drives installed
RAID 5
RAID 5
Local system running maxView Storage Manager
Server with RAID controller and disk drives installed
Network Connection
RAID 60
Server running Redfish Server or CIM Server
RAID 5EE
RAID 5EE
RAID 5EE
Local system running Redfish Server or CIM Server
Storage enclosures with disk drives installed

2. 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 13. Silent Installation on Windows and Linux.

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 15. Using the maxView Plugin for VMware vSphere Web Client.

2.1 Before You Begin the Installation

Complete the following steps before you begin the installation.

2.1.1 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 1.2.1 About maxView Storage Manager Redfish Server .
- 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 1.2.2 About the maxView Storage Manager Web Server.

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 2.8 Uninstalling maxView Storage Manager for details.

2.1.1.1 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.
- Ensure that firewall is enabled or network is configured to allow the connection to withstand for five minutes.

2.1.2 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.adaptec.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.

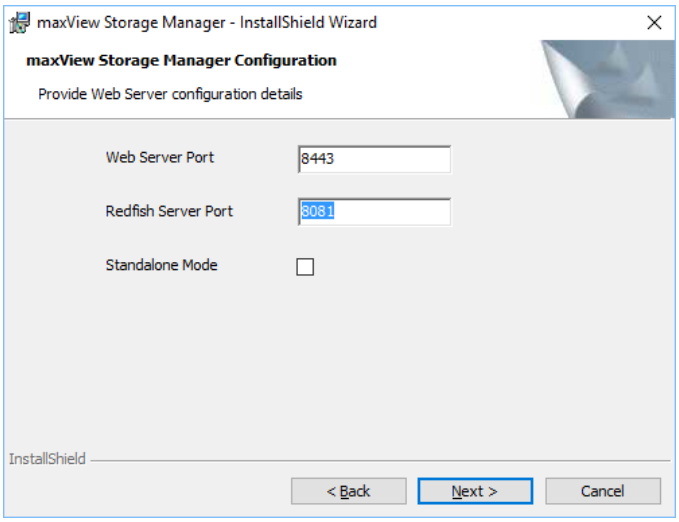
2.2 Installing on Windows

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.

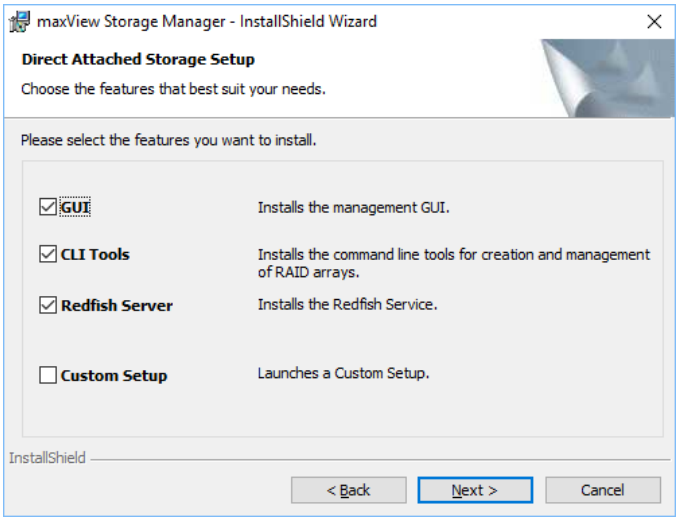
1. Open Windows Explorer or My Computer, then change to the directory where the Windows installer package is located (see 2.1.2 Download the Installation Package for details).
2. Double-click the setup program for your operating system version:

Option	Description
Windows 64-bit	setup_asm_x64.exe

   The Installation wizard opens.
3. Click **Next** to begin the installation.
   The License Agreement screen on the Installation wizard appears.
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.

2.3 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 1.3 System Requirements.

1. Open a shell window, then change to the directory where the Linux installer package is located (see 2.1.2 Download the Installation Package for details).
2. Run the `.bin` file for your operating system version (x.xx-xxxxx=version-build number):

Option	Description
Linux 64-bit	./StorMan-X.XX-XXXXX.x86_64.bin

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.

2.4 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 2.1.2 Download the Installation Package for details).
2. Install the `.deb` package for your operating system version (x.xx-xxxxx=version-build number).

Option	Description
Linux 64-bit	dpkg -i StorMan-X.XX-XXXXX_amd64.deb

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:
   ```
   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.

2.5 Installing on VMware 6.x

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.

© 2021 Microchip Technology Inc. and its subsidiaries

1. Copy the following files from the installer download location to the `/tmp` directory on your local ESXi server (see 2.1.2 Download the Installation Package 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.
   `esxcli software vib list | grep arcconf`
3. Remove the existing arcconf package.
   `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.
   `esxcli software vib list | grep arc-cim-provider`
5. Remove the existing arc-cim-provider package.
   `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:
   `esxcli software acceptance set --level=PartnerSupported`
7. Install the arcconf package.
   `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.
   `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 11.2 Managing Remote Systems to add a remote system.

2.6 Installing on VMware 7.x

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.
   - vmware-esx-arcconf.vib
   - VMW-esx-7.0.1-AdaptecRedfishServer-x.xx.xxxxx-MIS.7.0.1.16850804.vib

   The arcconf.vib is for command line communication. The `VMW-esx-7.0.1-AdaptecRedfishServer-x.xx.xxxxx-MIS.7.0.1.16850804.vib` is for remote management communication.
2. Check for existing installation of ARCCONF.
   `esxcli software vib list | grep arcconf`
3. Remove the existing ARCCONF package.
   `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 adaptecredfishserver.
   `esxcli software vib list | grep adaptecredfishserver`
5. Remove the existing adaptecredfishserver package.
   `esxcli software vib remove -n adaptecredfishserver`

   When the package is removed, you receive the message "Reboot Required: false."
6. Set the installation acceptance level to either PartnerSupported or CommunitySupported:
   `esxcli software acceptance set --level=PartnerSupported`
7. Install the ARCCONF package.
   `esxcli software vib install -v /tmp/vmware-esx-arcconf.vib`

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

© 2021 Microchip Technology Inc. and its subsidiaries

8. Install the adaptecredfishserver package.
   ```
   esxcli software vib install -v /tmp/VMW-esx-7.0.1-AdaptecRedfishServer-
   x.xx.xxxxx-MIS.7.0.1.16850804.vib
   ```
   When the package is installed, you receive the message "Reboot Required: false."
9. To add a remote system, see 11.2 Managing Remote Systems.

Note: arc-cim-provider is not supported for VMware 7.x.

2.7 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 Microchip web site
2. Create a "live" image on a USB flash drive
   Note: We recommend using Rufus bootable USB create (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.adaptec.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/.
   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 4.4 Creating Arrays and Logical Drives.

2.8 Uninstalling maxView Storage Manager

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

© 2021 Microchip Technology Inc. and its subsidiaries

2.8.1 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.

2.8.2 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, or 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.

2.8.3 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_Upgrade=false dpkg -r storman`

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

2.8.4 Uninstalling from VMware 6.x

Use the following procedure to remove maxView Storage Manager from a VMware ESXi 6.x 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.

2.8.5 Uninstalling from VMware 7.x

Use the following procedure to remove maxView Storage Manager from a VMware ESXi 7.x 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 adaptecredfishserver
   ```
3. Remove the arcconf package:
   ```
   esxcli software vib remove -n arcconf
   ```
4. Remove the adaptecredfishserver:
   ```
   esxcli software vib remove -n adaptecredfishserver
   ```
5. Reboot the system.

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

© 2021 Microchip Technology Inc.
and its subsidiaries

3. Exploring maxView Storage Manager

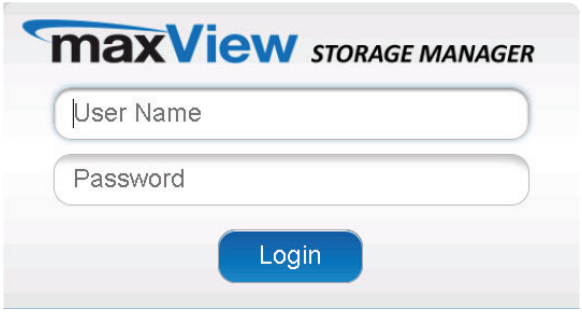
This section familiarizes you with the main features of the maxView Storage Manager graphical user interface. It describes how to start and log into maxView Storage Manager. It also explains how to get help and log out of maxView Storage Manager when you are finished working with the application.

3.1 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 3.2 Working in maxView Storage Manager 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.



   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.

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.

3.2 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 11.5 Granting Standard Users Admin Privilege.

Standard users can:	Standard users can't:
Rescan controllers	Create arrays and logical drives
Save activity logs	Modify arrays and logical drives

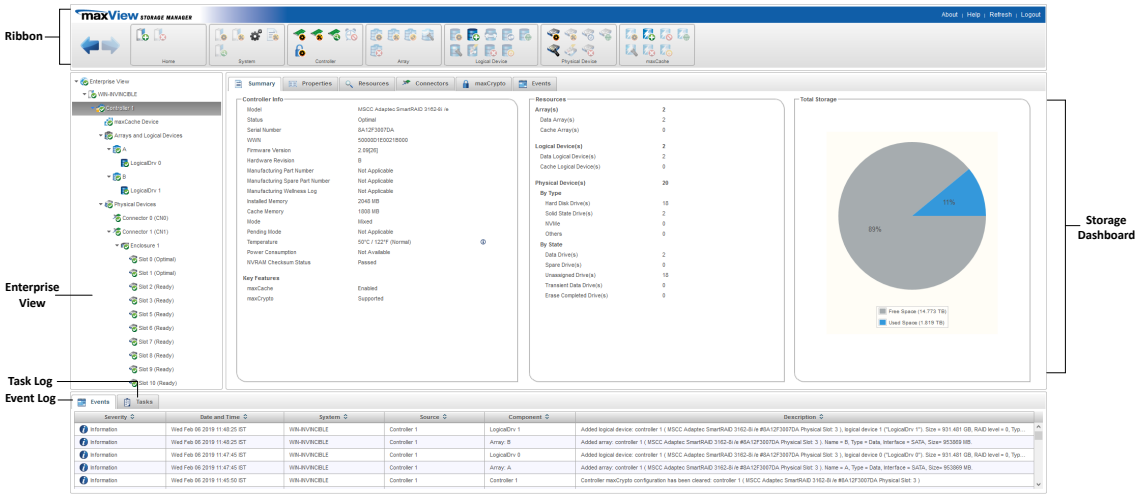
.....continued	
Standard users can:	**Standard users can't:**
Identify physical devices, logical devices, and enclosures	Delete arrays and logical drives
Silence alarms	Perform data migrations
View component properties on the Storage Dashboard	Clear the controller configuration

3.3 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.

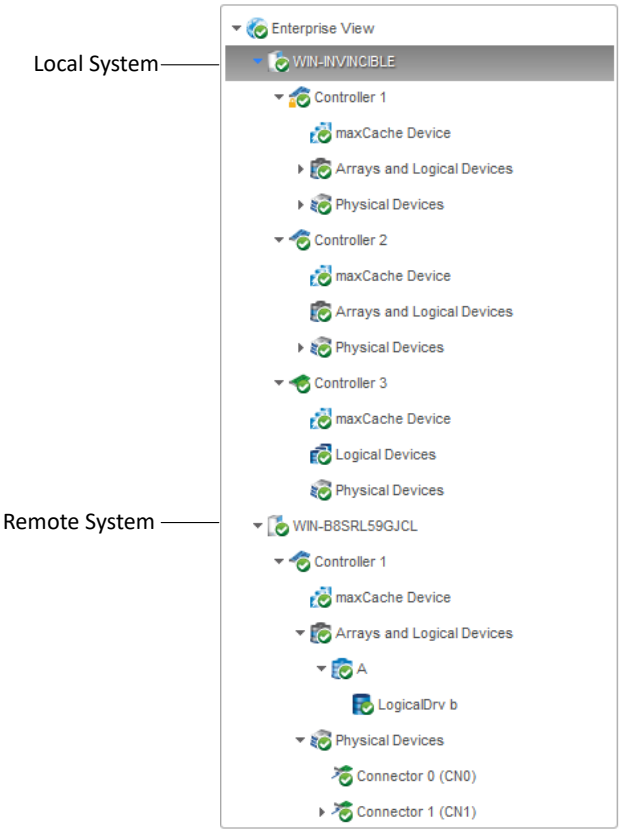


You can resize the panels and scroll horizontally or vertically as needed, to view more or less information.

3.3.1 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 4.2.1 ‘Local’ or ‘Remote’? for more information.) It also lists the *maxCache Devices* in your system.

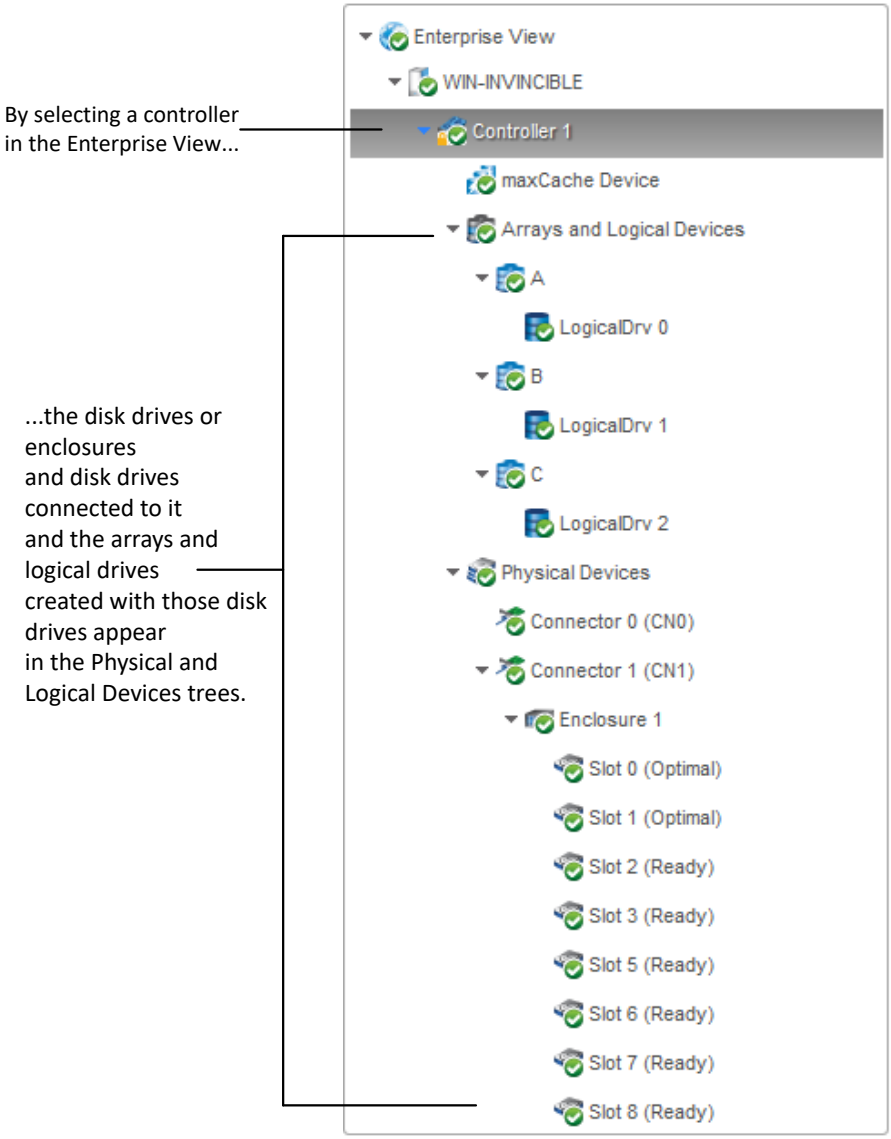
Note: maxCache is not supported on all Adaptec Smart Storage Controllers. See the Readme for more information. For more information about maxCache, see 7. Working with maxCache Devices.



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.

© 2021 Microchip Technology Inc.
and its subsidiaries



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.

3.3.1.1 What do the Enterprise View Icons Mean?

Icon	Description
	System with controller and directly attached disk drives or enclosures
	Controller
	Enclosure
	Logical drive (encrypted)[1]
	maxCache Device (healthy)[2]

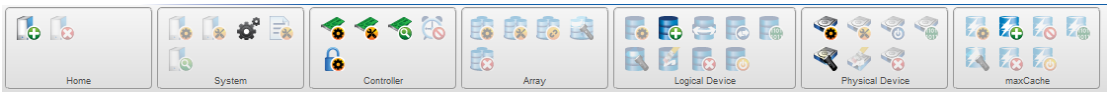
[1] A lock in the Enterprise View means that the device is encrypted. For more information, see 8. Working with maxCrypto™ Devices.

.....continued

Icon	Description
	Array (healthy)
	Hard disk drive
	Solid State Drive (SSD)
	SMR (Shingled Magnetic Recording) drive[3]
	Connector or other physical device

3.3.2 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 11.2 Managing Remote Systems). 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.

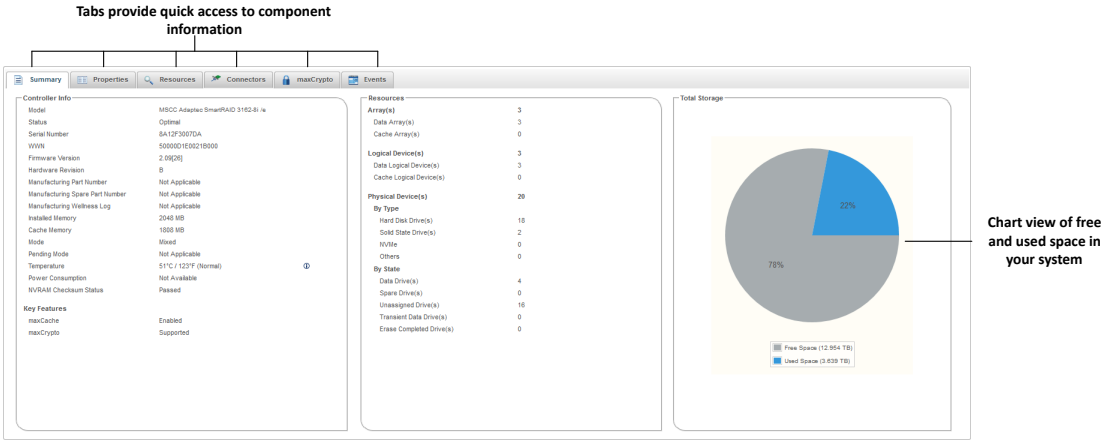
For a description of the icons on the ribbon, see 19. Icons At-a-Glance.

3.3.3 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 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.

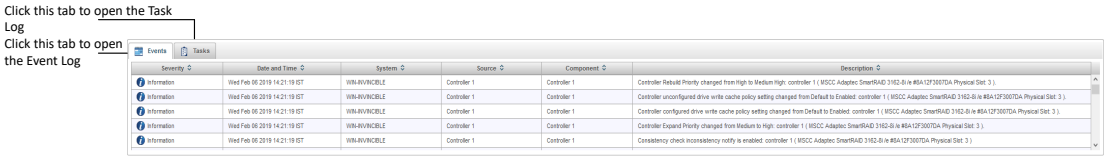
[2] A green check mark in the Enterprise View means that the device is healthy with no problems or issues. For more information, see 12.2 Identifying a Failed or Failing Component.

[3] Not supported on all controllers. See the Readme for more information.

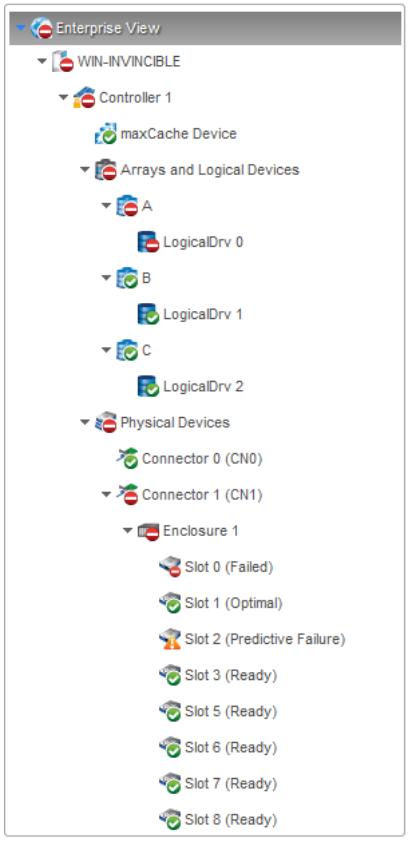


For more information about the types of information provided on the Storage Dashboard for each component in your storage space, see 10.2.3 Viewing Component Status in the Storage Dashboard; also see 3.5 Revealing More Device Information .

3.4 Checking System Status from the Main Window



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 12.2 Identifying a Failed or Failing Component 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 10.2.3.1 Monitoring Enclosure Status).

For more information about checking status from the main window, see Monitoring Status and Activity.

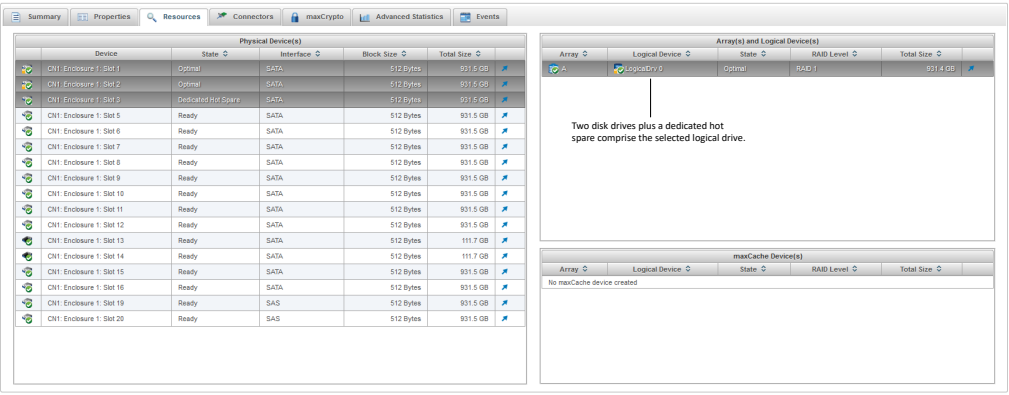
3.5 Revealing More Device Information

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.

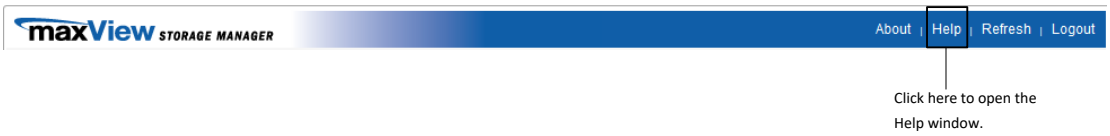
© 2021 Microchip Technology Inc. and its subsidiaries



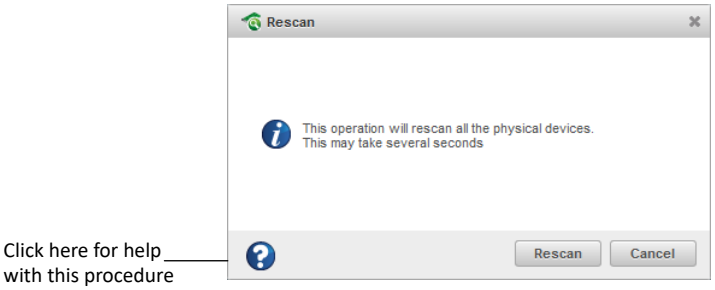
3.6 Getting Help

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.

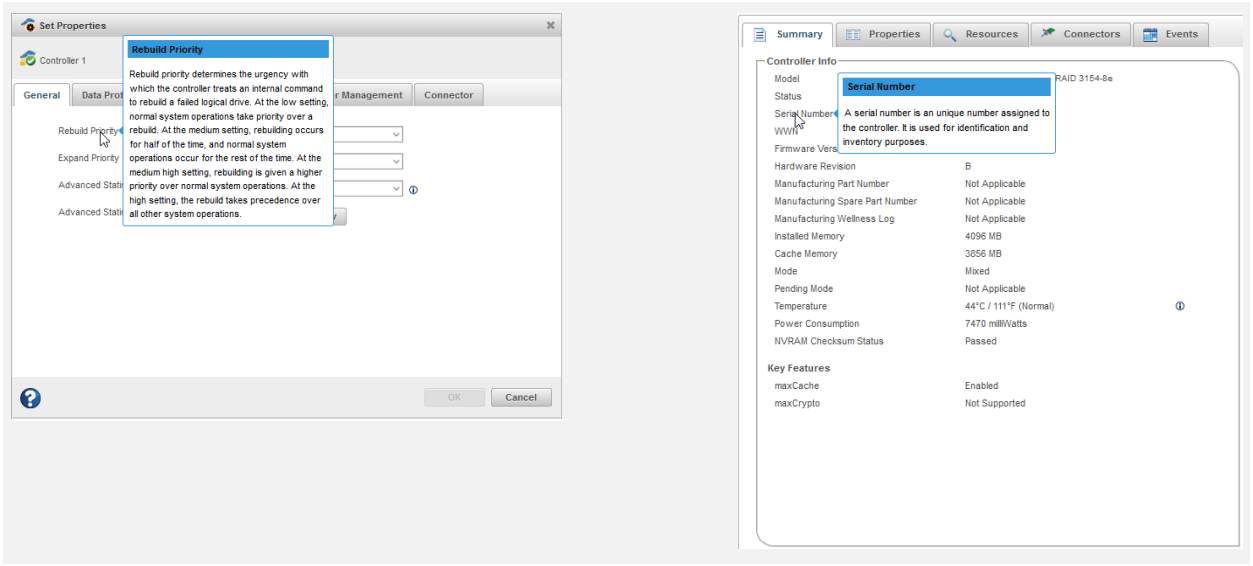
To open the online help, click the **Help** button at the upper-right corner of the main window.



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.



3.7 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.

4. 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.

4.1 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 3.1 Starting maxView Storage Manager and Logging In).
3. Log in to all other systems from the management system (see 4.3 Logging into Remote Systems from the Local System).
4. Create arrays and logical drives for all systems in your storage space (see 4.4 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 6. Modifying Your Storage Space.

4.2 Choosing a Management System

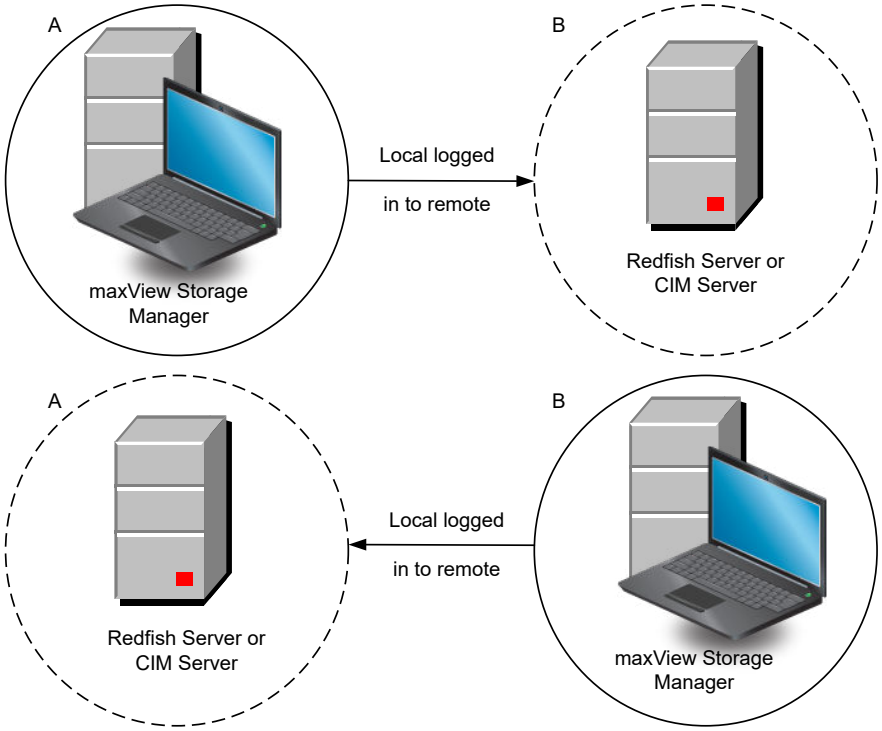
You must designate at least one system as a *management system*, a system from which you will manage the storage on all systems in your storage space.

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.

4.2.1 '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.



4.2.2 Logging in on the Local System

To log in on the local system, see 3.1 Starting maxView Storage Manager and Logging In .

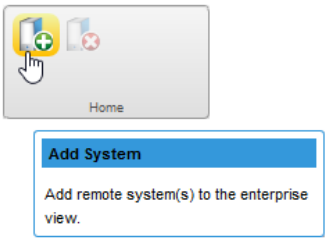
4.3 Logging into Remote Systems from the Local System

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:

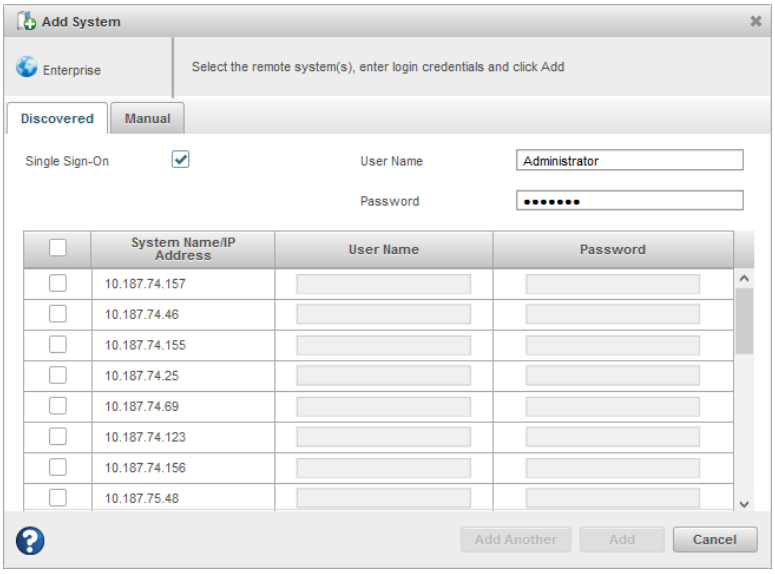
1. On the ribbon, in the Home group, click **Add System**.



   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 11.2.4 Changing the Auto-Discovery Settings.

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 .

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.

4.4 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 4.4.1 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 4.4.2 Creating a Logical Drive on an Existing Array.

If maxCrypto is enabled, you can create encrypted or plaintext volumes. (For more information, see 8. Working with maxCrypto™ Devices.)

Notes:

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 HA[4] and SMR DM drives for all RAID levels. However, mixing SMR and PMR[5] 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.

4.4.1 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 4.4.2 Creating a Logical Drive on an Existing Array.

[4] SMR: Shingled Magnetic Recording. HA: Host Aware (backward compatible with standard HDD). DM: Device Managed (backward compatible with standard HDD).
[5] PMR: Perpendicular Magnetic Recording; standard HDD recording technology.

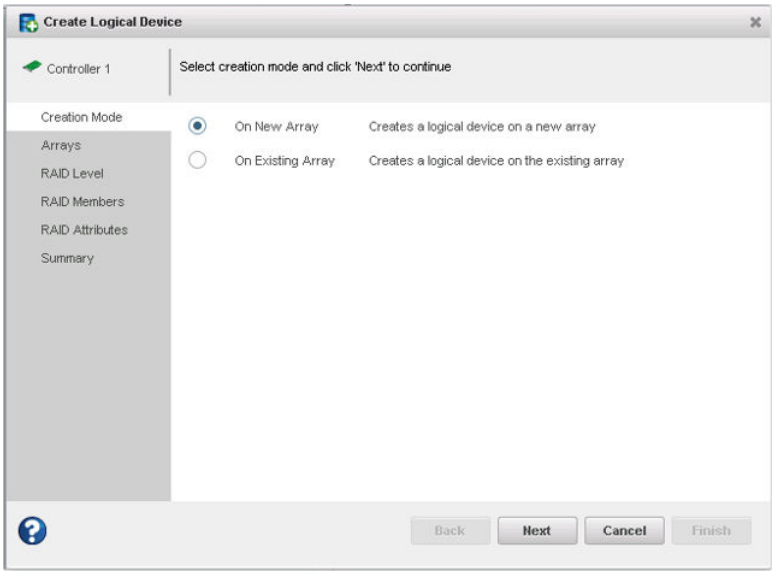
By default, maxView Storage Manager uses all available disk space to maximize the capacity of a new logical drive.

To create a logical drive on a new array:

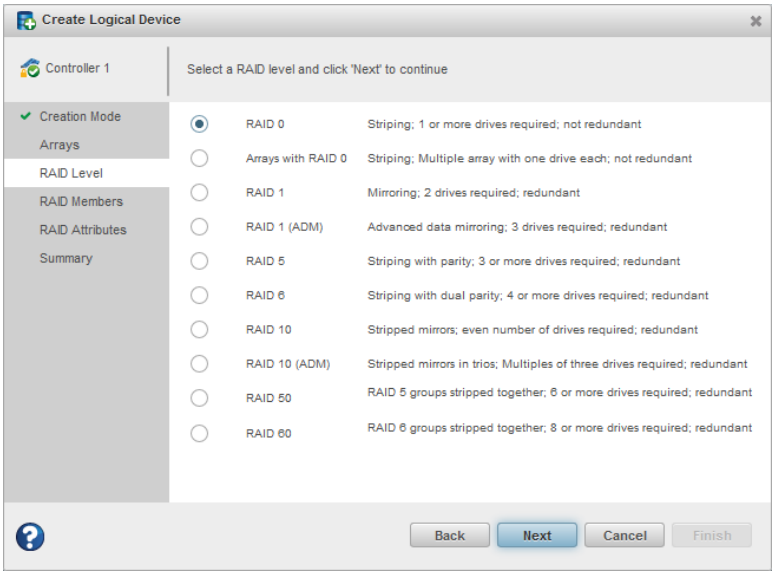
1. In the Enterprise View, select a system, then select a controller on that system.
2. On the ribbon, in the Logical Device group, click **Create Logical Device**.



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

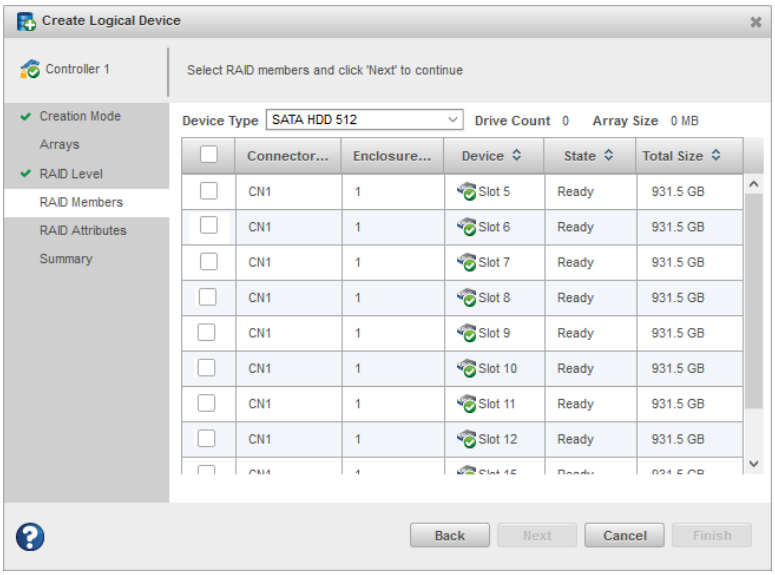


4. Select a RAID level for the logical drive, then click **Next**.



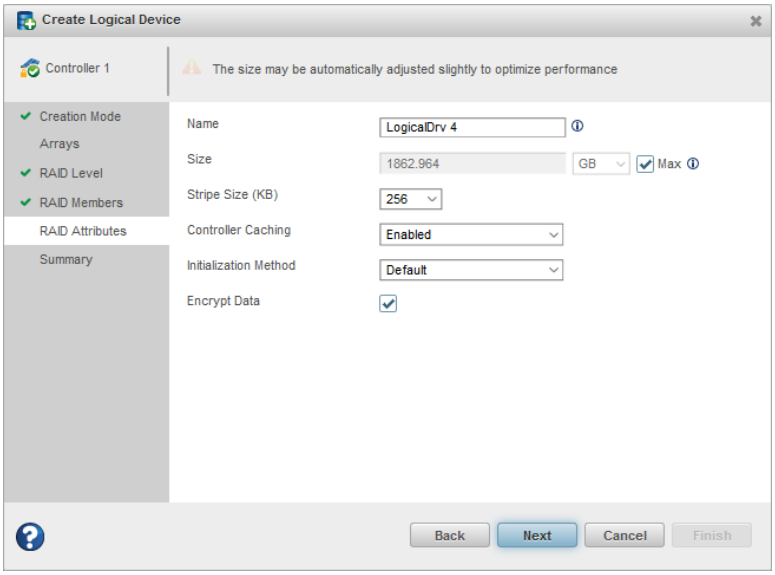
Note: Not all RAID levels are supported by all controllers. (See the Release Notes for more information.) See Selecting the Best RAID Level for more information about RAID levels.

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.



Note:
For details on SED support operations on a new array while creating a logical device, see 4.6.1 Create Logical Device.

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

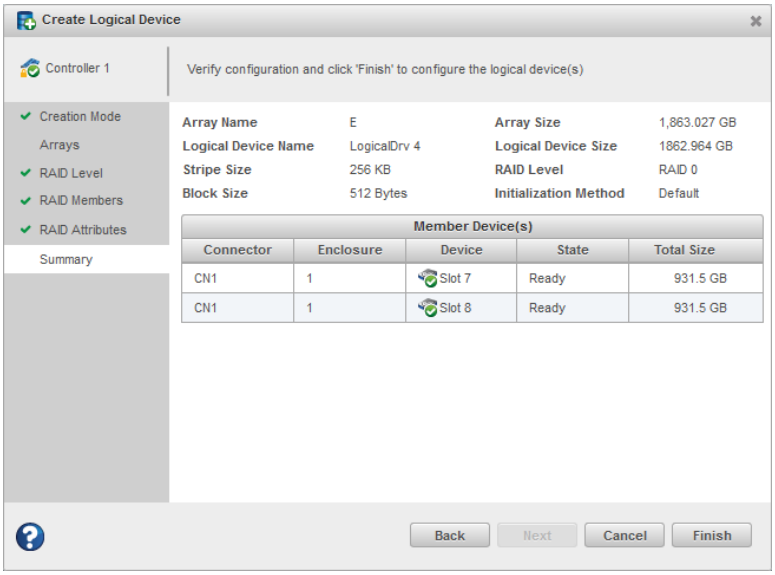
parity groups are initialized in parallel, but initialization is faster for single parity groups (RAID 5). RAID level does not affect performance during Build initialization.

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

- Create an encrypted or plaintext logical drive (for more information, see 8. Working with maxCrypto™ Devices)

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 .
10. Repeat Steps 1–9 for each controller in your storage space.
11. Partition and format your logical drives. See 4.4.3 Partitioning and Formatting Your Logical Drives.

4.4.2 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 4.4.1 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.

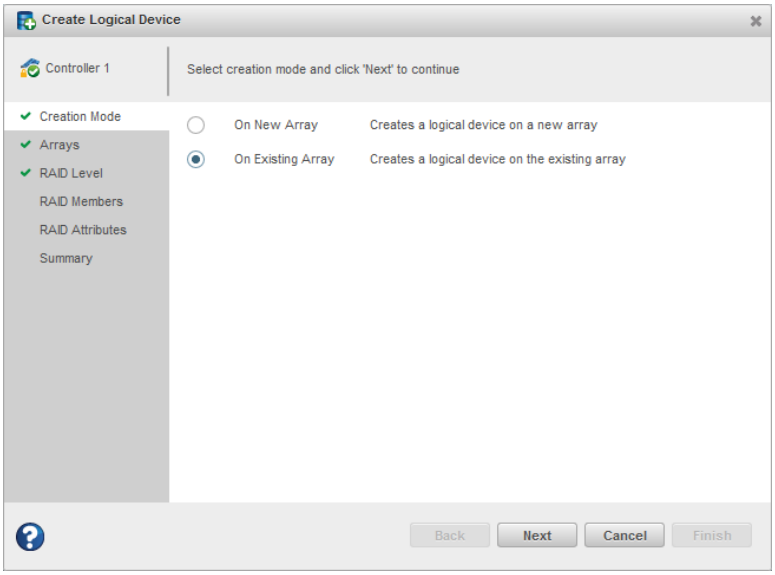
Note:
You can also add/create Logical drives by selecting the existing array from the Enterprise view.

To create a logical drive on an existing array:

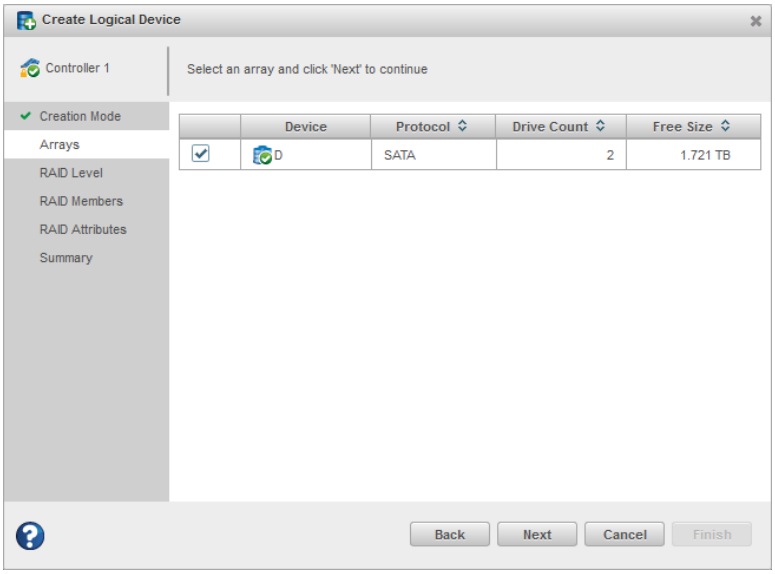
1. In the Enterprise View, select a system, then select a controller on that system.
2. On the ribbon, in the Logical Device group, click **Create Logical Device**.



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

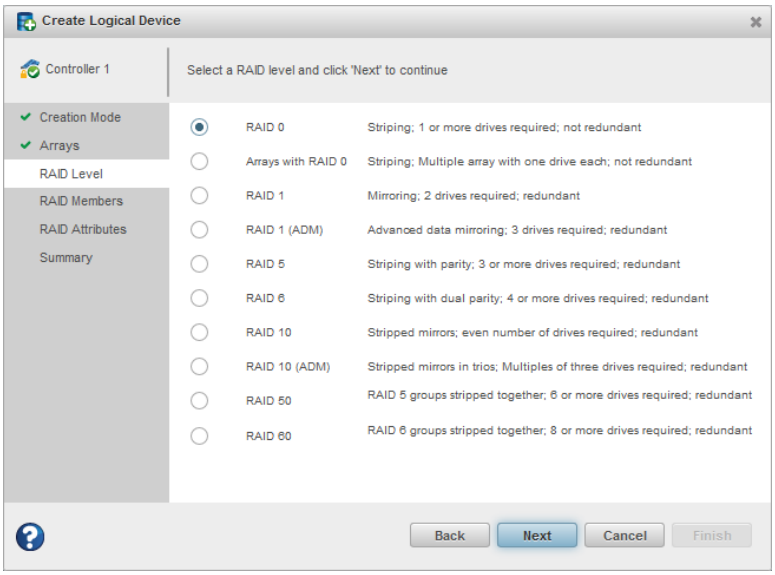


4. Select the array on which to create the logical drive, then click **Next**.



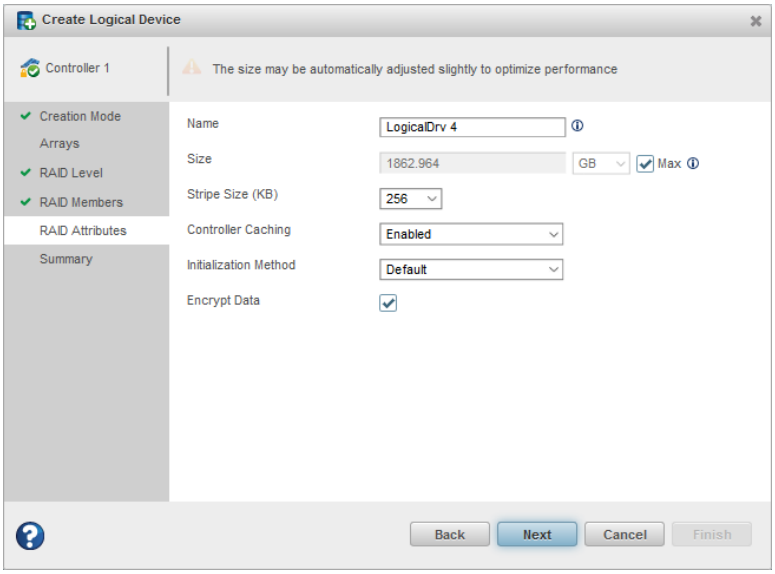
Note:
For details on SED support operations on an existing array while creating a logical device, see 4.6.1 Create Logical Device.

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



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.



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

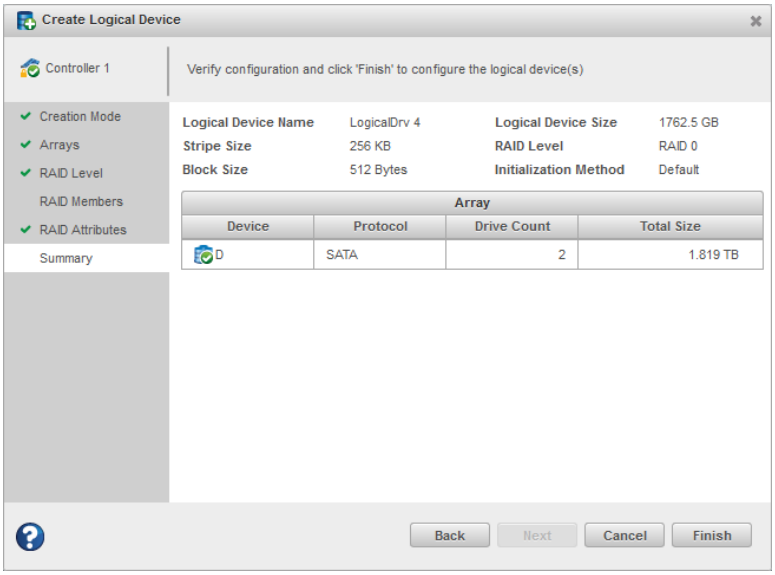
parity groups are initialized in parallel, but initialization is faster for single parity groups (RAID 5). RAID level does not affect performance during Build initialization.

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

- Create an encrypted or plaintext logical drive (for more information, see 8. Working with maxCrypto™ Devices)

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 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 4.4.3 Partitioning and Formatting Your Logical Drives.

4.4.3 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.

4.4.4 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), 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).

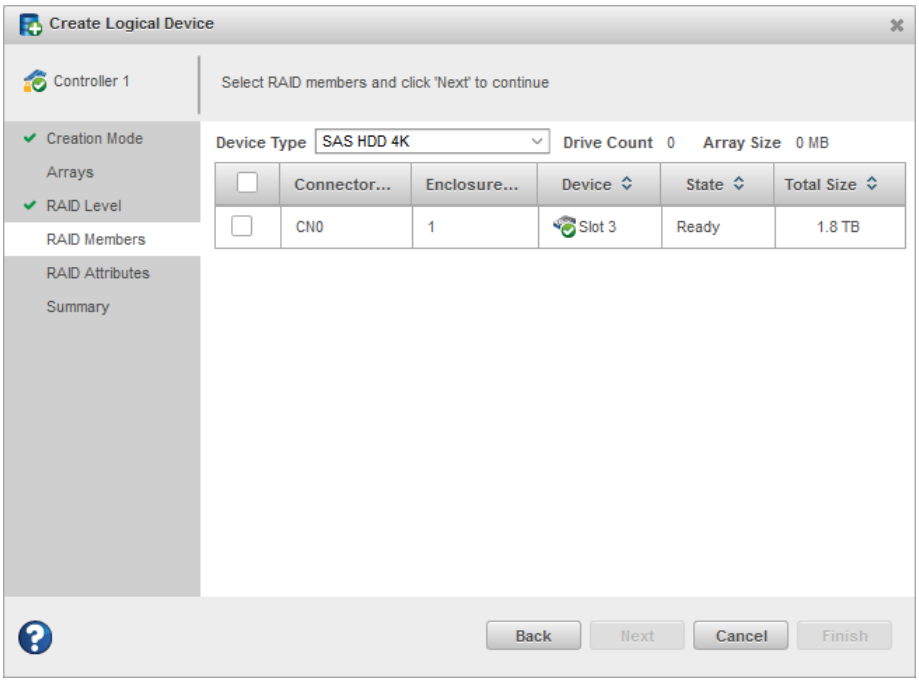
© 2021 Microchip Technology Inc. and its subsidiaries

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.

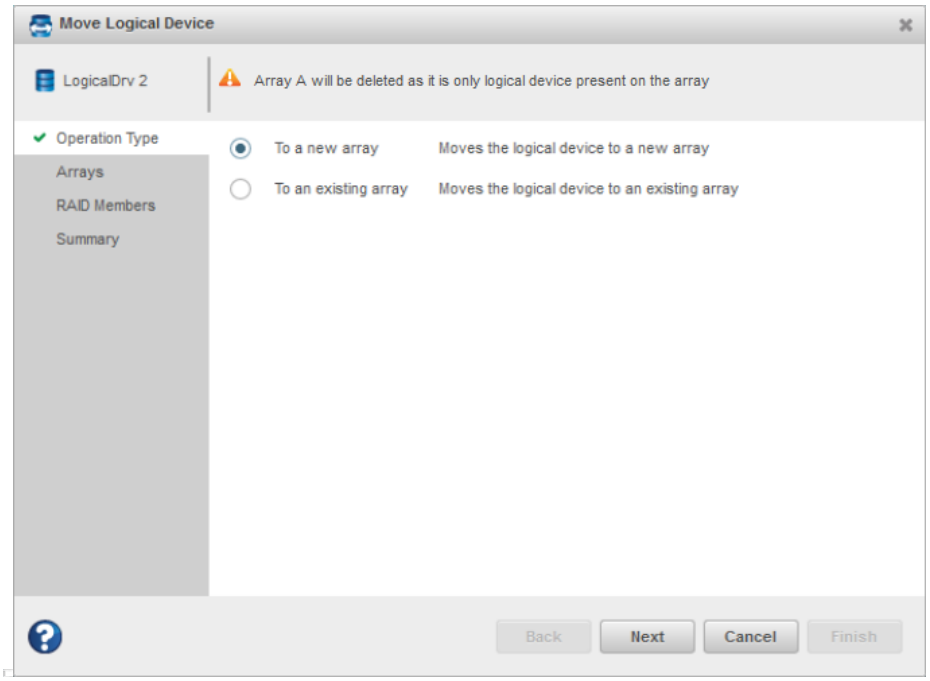
4.5.1 Creating a Logical Drive

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.

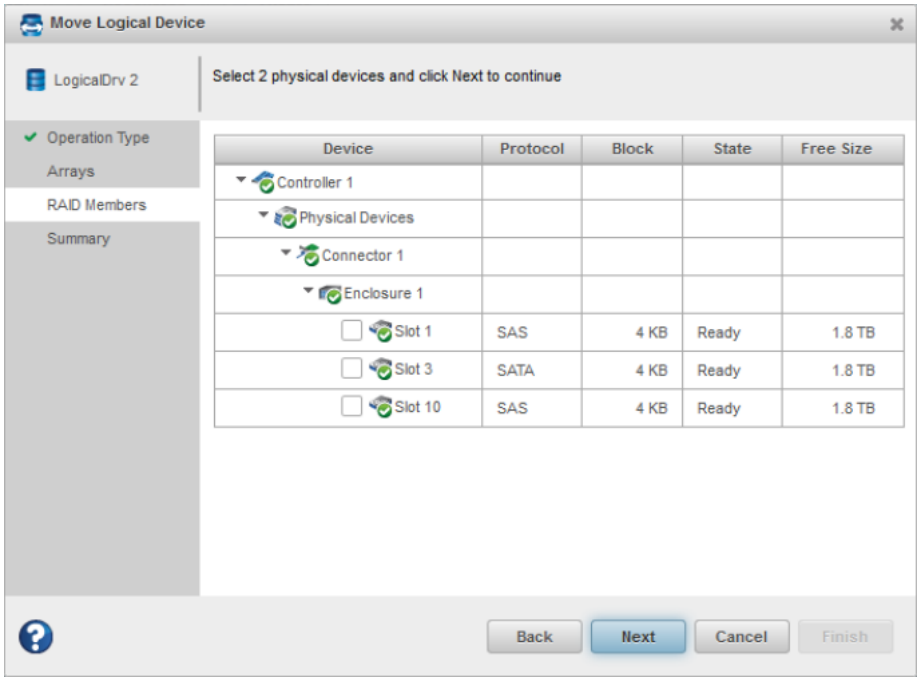


4.5.2 Moving a Logical Drive

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.

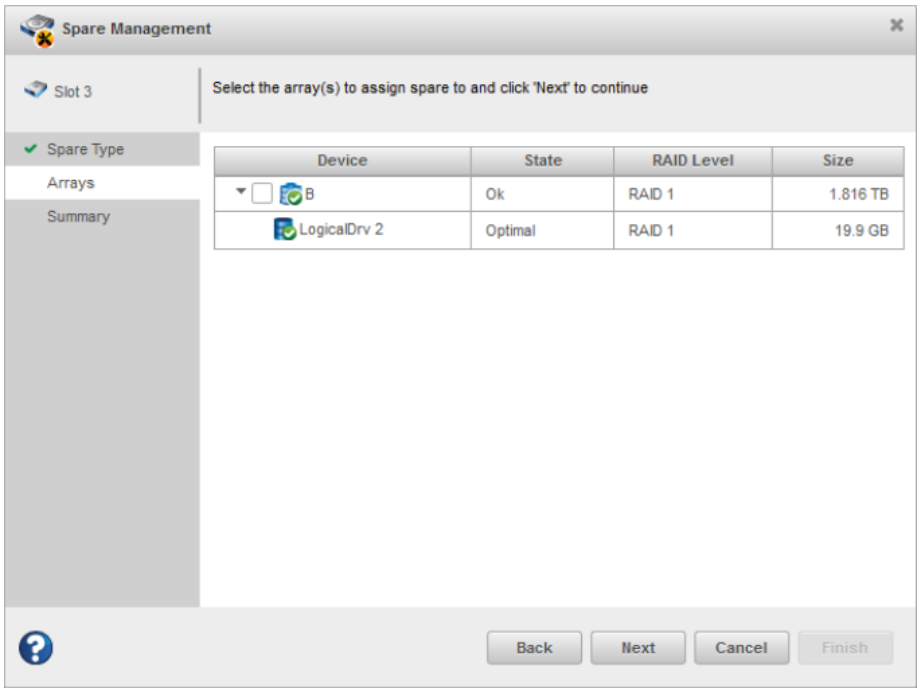


- Moving to a new array: all SATA and SAS 4K drives that are available to move to a new array are listed.



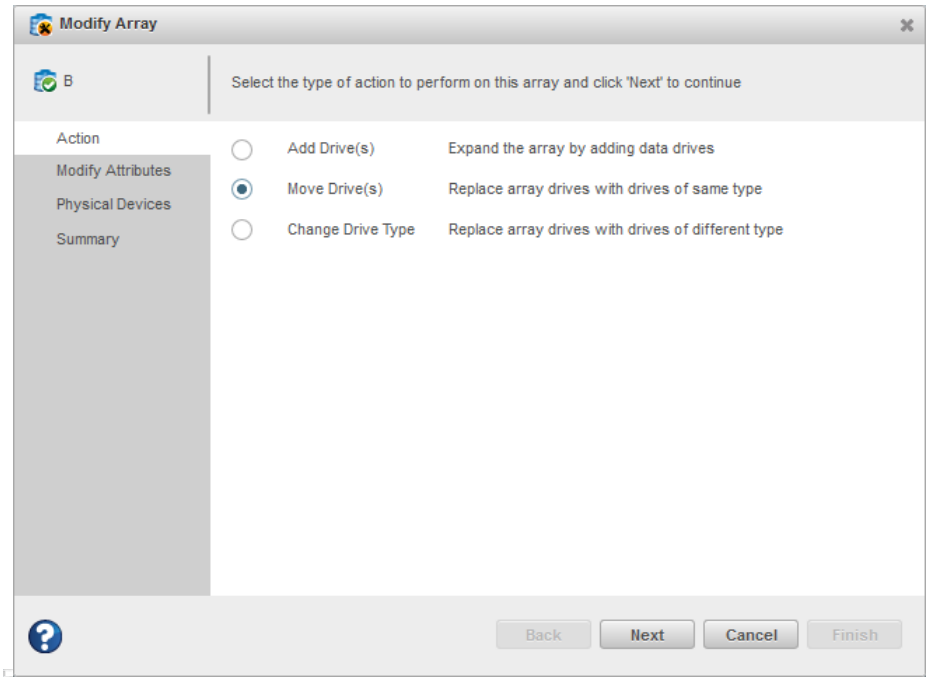
- Moving to an existing array: if the logical device has already been created in a different array using 4K drives, then the user can move a logical device to the existing array of the same block size SAS/SATA 4K drives. Only arrays created using 4K drives will be listed (512-byte arrays will not be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

© 2021 Microchip Technology Inc. and its subsidiaries



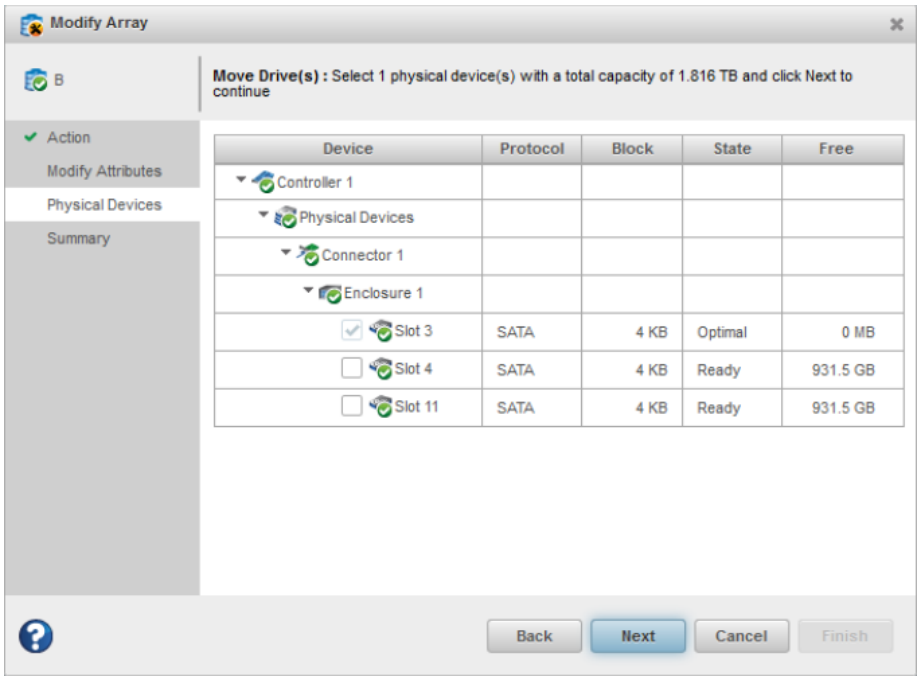
4.5.3 Modifying a Logical Drive

Arrays created using 4K drives can be modified.

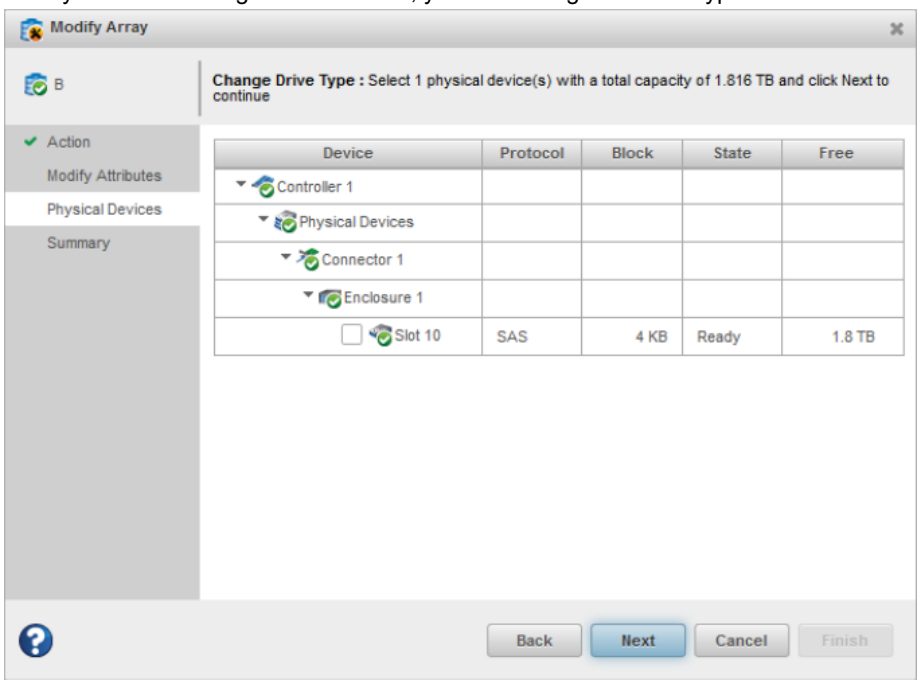


- Moving drive(s): you can move a drive from one array to another array that uses the same interface type. For example, if an array is created using 4K SATA drives, then you can move a drive(s) from that array to a separate array that also uses 4K SATA drives.

© 2021 Microchip Technology Inc. and its subsidiaries

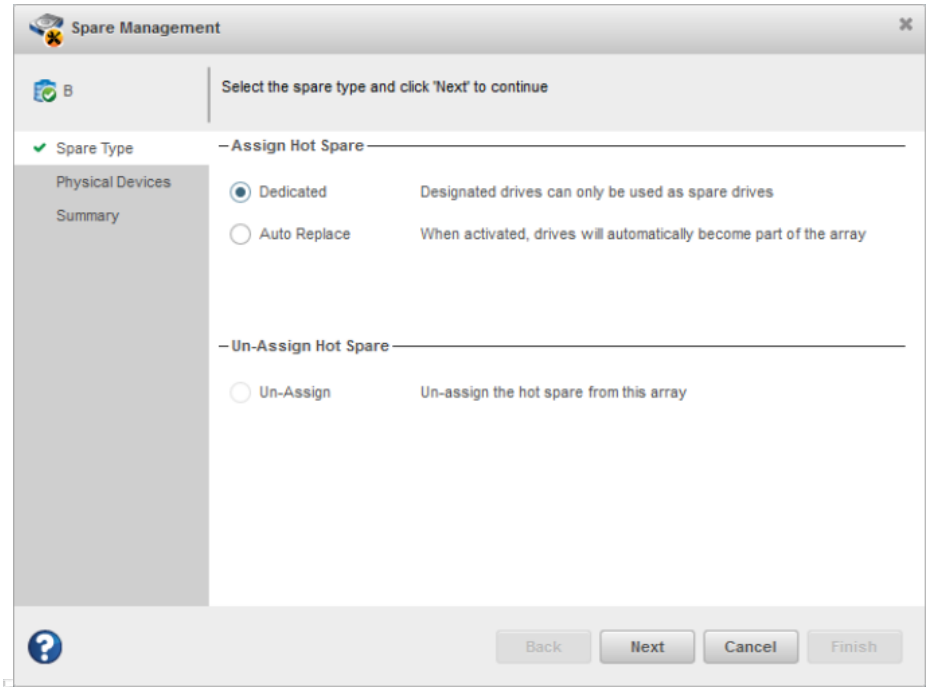


- Changing drive types: you can change the drive interface type from SAS to SATA or from SATA to SAS. For example, if an array is created using 4K SAS drives, you can change the drive type to 4K SATA drives only.

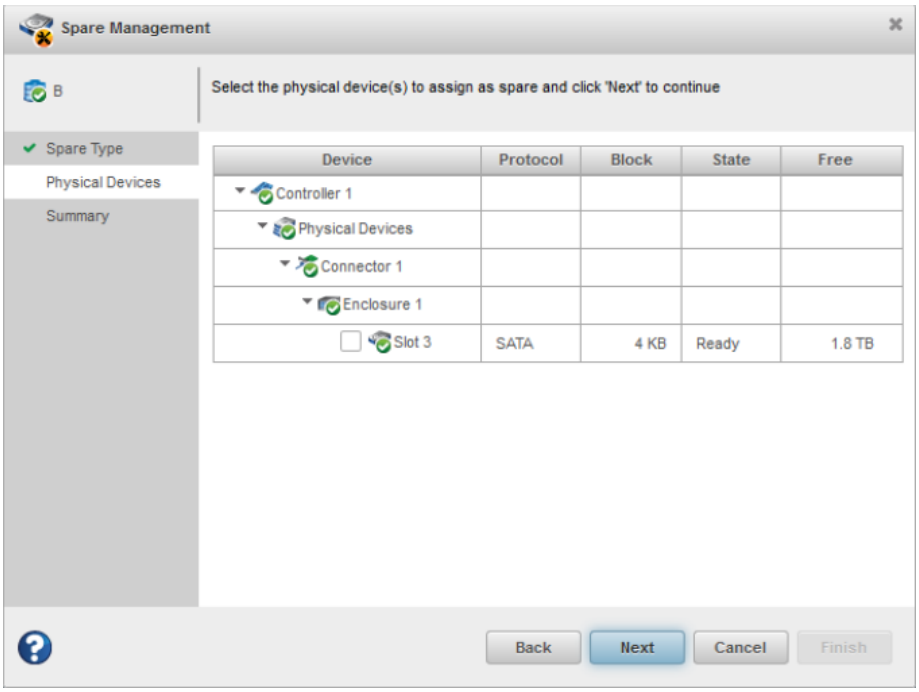


4.5.4 Assigning Spares at the Array Level

Spares for 4K logical drives can be assigned at the array level.

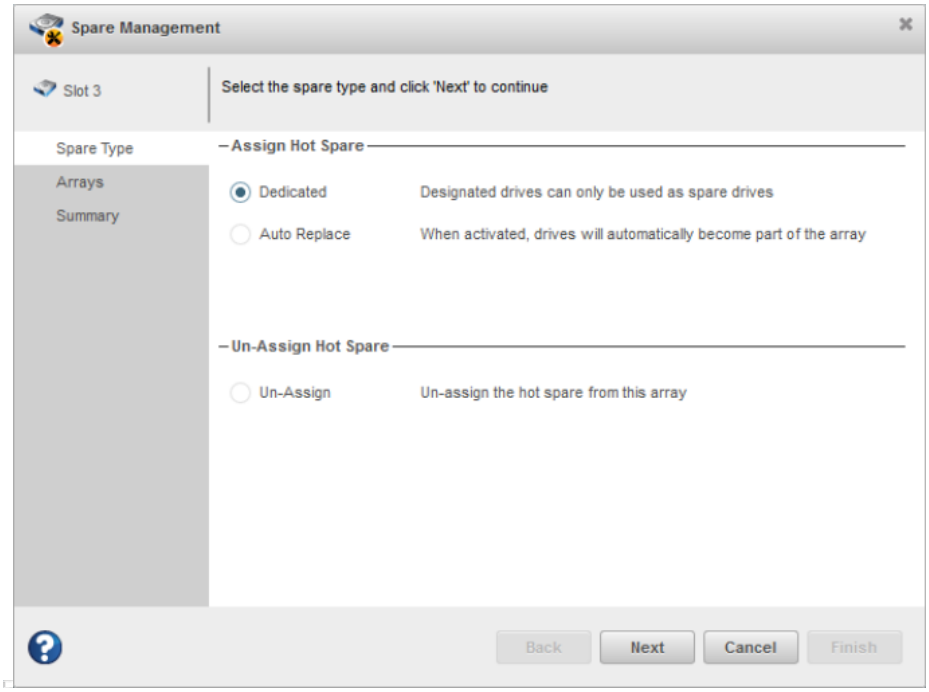


1. Dedicated Hot Spare: If the array/logical device is created using 4K SATA drives, then only the 4K SATA devices can be assigned as spares.
2. Auto Replace Hot Spare: The process is the same as the Dedicated Hot Spare.

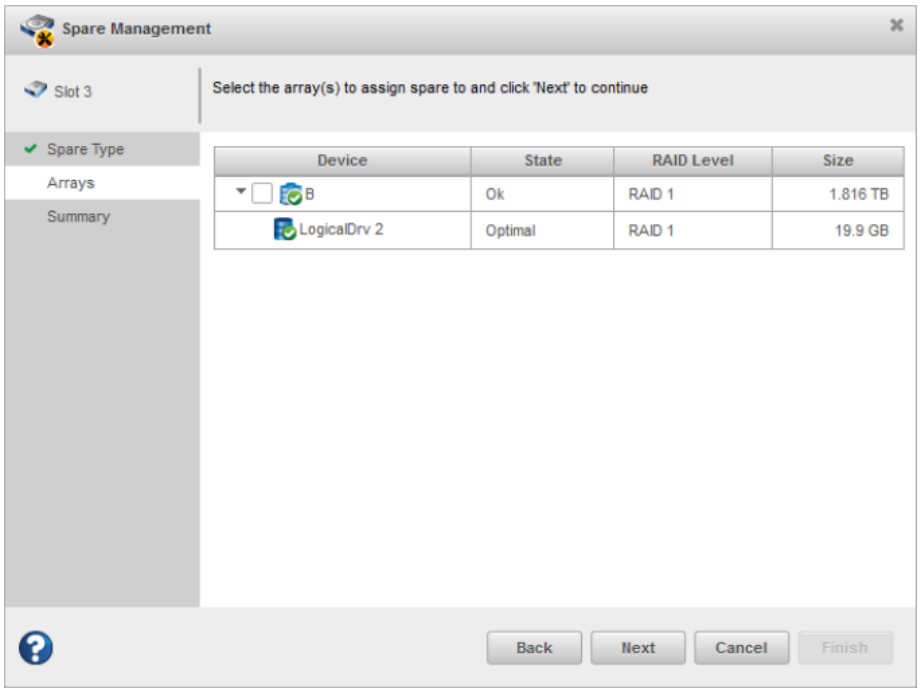


4.5.5 Assigning Spares at the Physical Device Level

Spares 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.



Notes:

- 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.

4.6 Controller Support for SED

An SED (Self Encrypting Drive) is a type of hard drive that automatically and continuously encrypts the data on the drive without any user interaction. If an SED gets locked, the volumes on the array may become degraded or inaccessible. If this occurs, unlock the SED(s) and warm-boot the server.

This section lists the operations that are allowed/not allowed based on the Array, logical device status, physical device's SED security status, and SED qualification status.

4.6.1 Create Logical Device

On Existing Array

Create logical device operation on an existing array will be blocked when the target Array has the following status:

Array Status	Create Array Allowed/Not Allowed
One or more logical drives undergoing or failed SED qualification	Creation not allowed

On New Array

The following table lists the physical device SED security status and SED qualification status, based on which the SED drives can be included in the new Array creation.

SED Security Status	SED Qualification Status	Create Array Allowed/Not Allowed
Locked	Not Applicable	Creation not allowed
Not Applicable	Failed Locking Enabled	Creation allowed
Not Applicable	Failed Range Length Set	Creation allowed

4.6.2 Modify Array

Add Drives

When the Array status is “OK”, adding the SED drives to the array is not allowed based on the following conditions:

SED Security Status	SED Qualification Status	Add Drives Allowed/Not Allowed
Locked	Not Applicable	Add drives not allowed
Not Applicable	Failed Locking Enabled	Add drives not allowed
Not Applicable	Failed Range Length Set	Add drives not allowed

Add drives operation to an existing array will be blocked when the Array has the following status:

Array Status	Create Array Allowed/Not Allowed
One or more logical drives undergoing or failed SED qualification	Add drives not allowed

Move Drives

When the Array status is “OK”, changing an existing drive(s) with SED drives of same type in the array is not allowed based on the following status:

SED Security Status	SED Qualification Status	Move Drives Allowed/Not Allowed
Locked	Not Applicable	Move drives not allowed
Not Applicable	Failed Locking Enabled	Move drives not allowed

© 2021 Microchip Technology Inc. and its subsidiaries

.....continued		
SED Security Status	**SED Qualification Status**	**Move Drives Allowed/Not Allowed**
Not Applicable	Failed Range Length Set	Move drives not allowed

Move drives operation on array will be blocked when the Array has the following status:

Array Status	Move Drives Allowed/Not Allowed
One or more logical drives undergoing or failed SED qualification	Move drives not allowed

Change Drive Type

When the Array status is “OK”, changing existing drives of different type with SED drives of different type in the array is not allowed based on the following physical device SED security status and SED qualification status:

SED Security Status	SED Qualification Status	Change Drive Type Allowed/Not Allowed
Locked	Not Applicable	Move drives not allowed
Not Applicable	Failed Locking Enabled	Move drives not allowed
Not Applicable	Failed Range Length Set	Move drives not allowed

Change drive type operation on array will be blocked when the Array has the following status:

Array Status	Move Drives Allowed/Not Allowed
One or more logical drives undergoing or failed SED qualification	Move drives not allowed

Heal Array

When the Array status is “Has Failed Physical Device”, replacing failed drives with SED drives in the array is not allowed based on the following physical device SED security status and SED qualification status:

SED Security Status	SED Qualification Status	Heal Array Allowed/Not Allowed
Locked	Not Applicable	Heal Array not allowed
Not Applicable	Failed Locking Enabled	Heal Array not allowed
Not Applicable	Failed Range Length Set	Heal Array not allowed

4.6.3 Move Logical Device

To a New Array

When the Array status is “OK”, moving a logical device with new set of SED drives is not allowed based on the following physical device SED security status and SED qualification status:

SED Security Status	SED Qualification Status	Move Logical Device Allowed/Not Allowed
Locked	Not Applicable	Move logical device not allowed
Not Applicable	Failed Locking Enabled	Move logical device not allowed
Not Applicable	Failed Range Length Set	Move logical device not allowed

To an Existing Array

Move logical device to an existing array operation on logical device will be blocked when the Array has the following status:

Array Status	Move Logical Device Allowed/Not Allowed
One or more logical drives undergoing or failed SED qualification	Move logical device not allowed

Move logical device ribbon icon should be disabled on the following logical device status:

Logical Device Status	Move Logical Device Allowed/Not Allowed
SED Qual Failed	Move logical device not allowed
SED Qual In Progress	Move logical device not allowed

4.6.4 Spare Management

When the Array status is “OK”, assigning a spare to an array with SED drives is not allowed based on the following physical device SED security status and SED qualification status:

SED Security Status	SED Qualification Status	Assign Spare Allowed/Not Allowed
Locked	Not Applicable	Assign spare not allowed
Not Applicable	Failed Locking Enabled	Assign spare not allowed
Not Applicable	Failed Range Length Set	Assign spare not allowed

Spare management ribbon icon should be disabled on the array based on the following array status:

Array Status	Assign Spare Allowed/Not Allowed
One or more logical drives undergoing or failed SED qualification	Assign spare not allowed

4.6.5 maxCache

On Existing Array

Create logical device operation on an existing array will be blocked when the target Array has the following status:

Array Status	Create maxCache Allowed/Not Allowed
One or more logical drives undergoing or failed SED qualification	Creation Not allowed

On New Array

The SED drives can be included in the new Array creation based on the following physical device SED security and SED qualification status.

SED Security Status	SED Qualification Status	Create maxCache Allowed/Not Allowed
Locked	Not Applicable	Creation not allowed
Not Applicable	Failed Locking Enabled	Creation not allowed
Not Applicable	Failed Range Length Set	Creation not allowed

© 2021 Microchip Technology Inc. and its subsidiaries

5. 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.

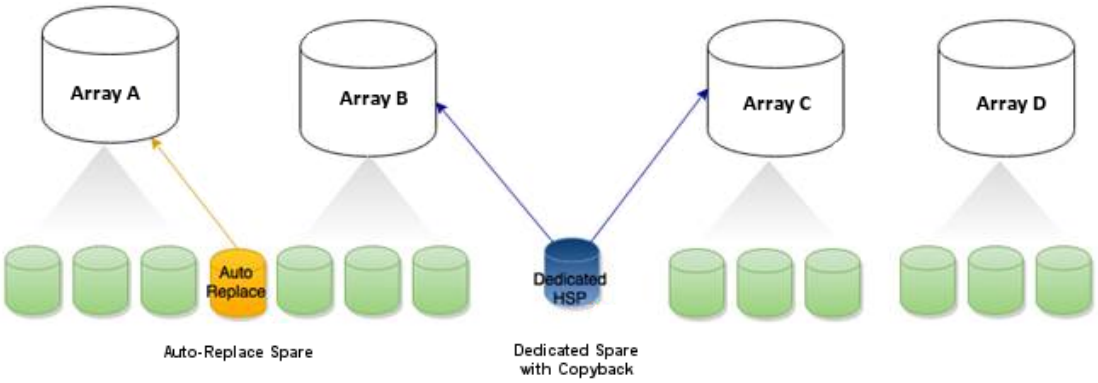
A *hot spare* is a disk drive or SSD (Solid State Drive) that automatically replaces any failed drive in a logical drive, and can subsequently be used to rebuild that logical drive. (For more information, see 12.3 Recovering from a Disk Drive Failure.)

5.1 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 5.3 Assigning a Dedicated Hot Spare.

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 5.4 Assigning an Auto-Replace Hot Spare.



5.2 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[6] or SMR DM drive for all hot spare types. A SMR drive cannot protect a PMR drive, [7] or vice-versa.

5.3 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.

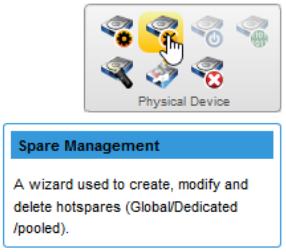
[6] SMR: Shingled Magnetic Recording. HA: Host Aware (backward compatible with standard HDD). DM: Device Managed (backward compatible with standard HDD).

[7] PMR: Perpendicular Magnetic Recording; standard HDD recording technology.

© 2021 Microchip Technology Inc. and its subsidiaries

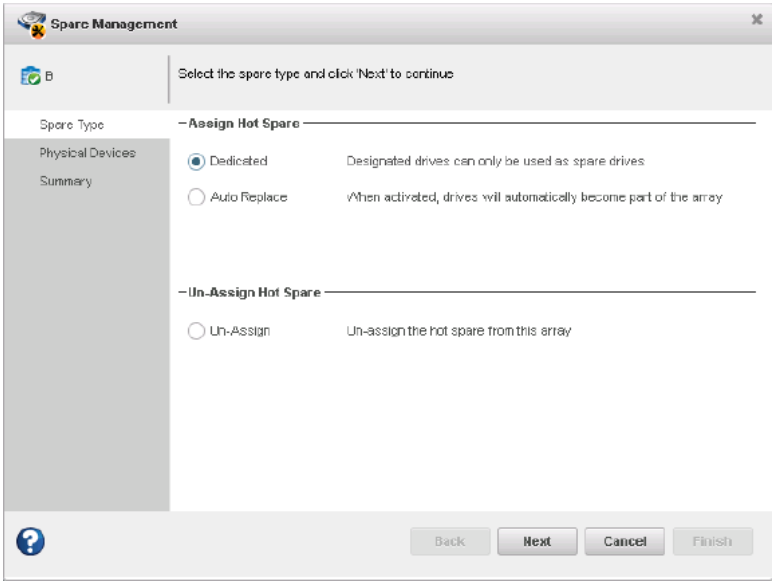
To assign a dedicated spare:

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**.

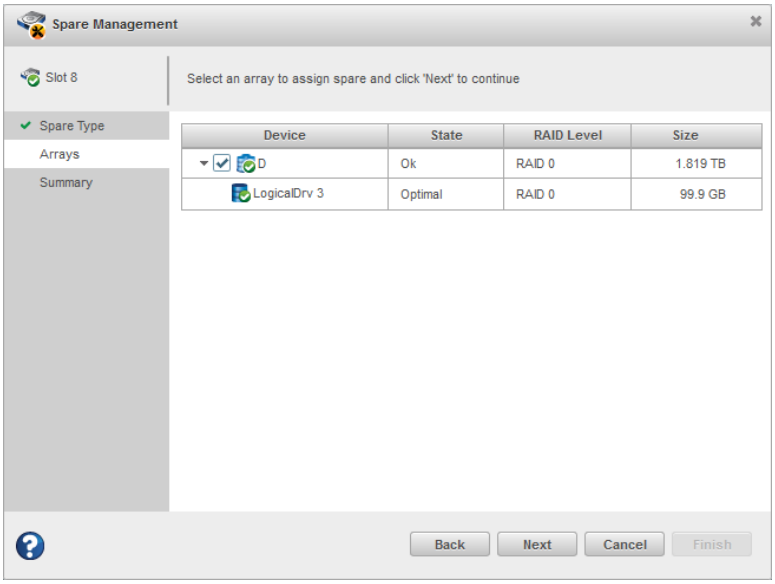


The Spare Management wizard opens.

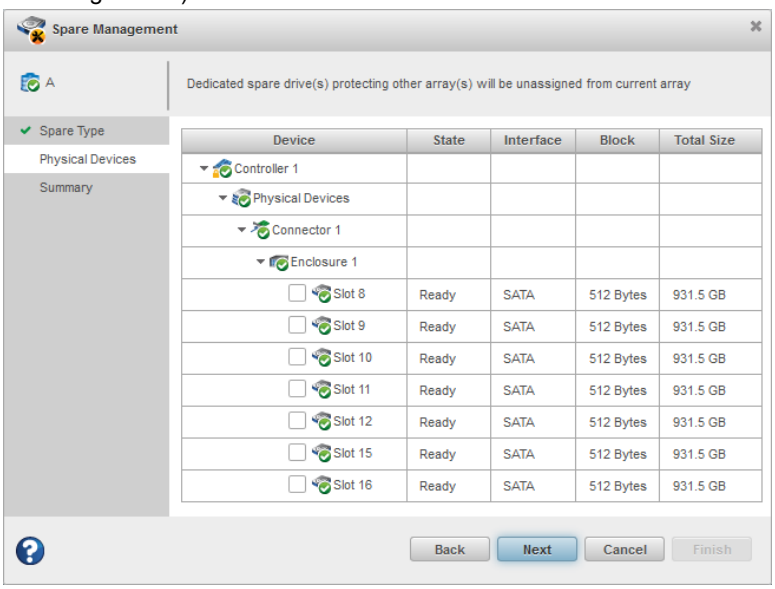
3. Select the **Dedicated** spare type, then click **Next**.



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**. For details on SED support operations, see 4.6.4 Spare Management. (See 5.2 Hot Spare Limitations for help selecting drives.)



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

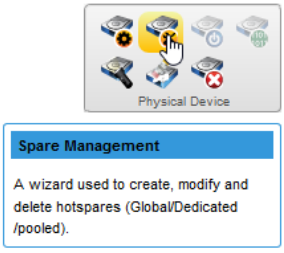
5.4 Assigning an Auto-Replace Hot Spare

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.

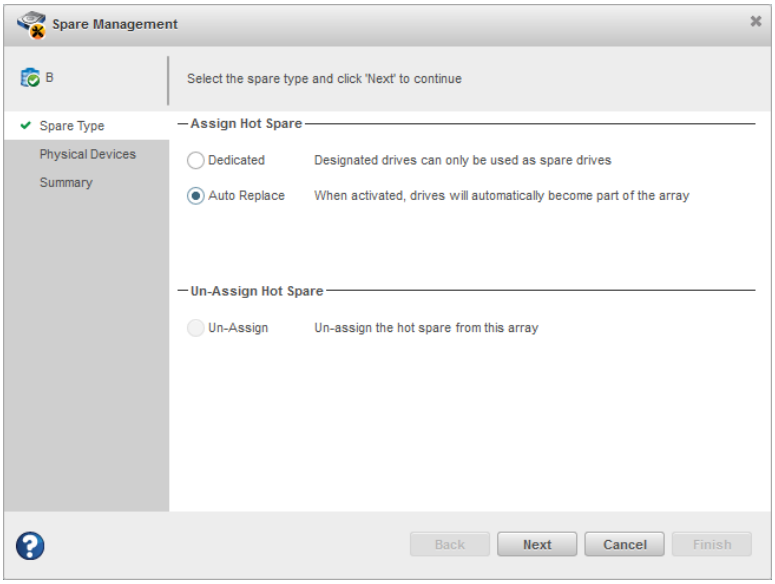
To assign an auto-replace hot spare to an array:

1. In the Enterprise View, select an array on that controller.

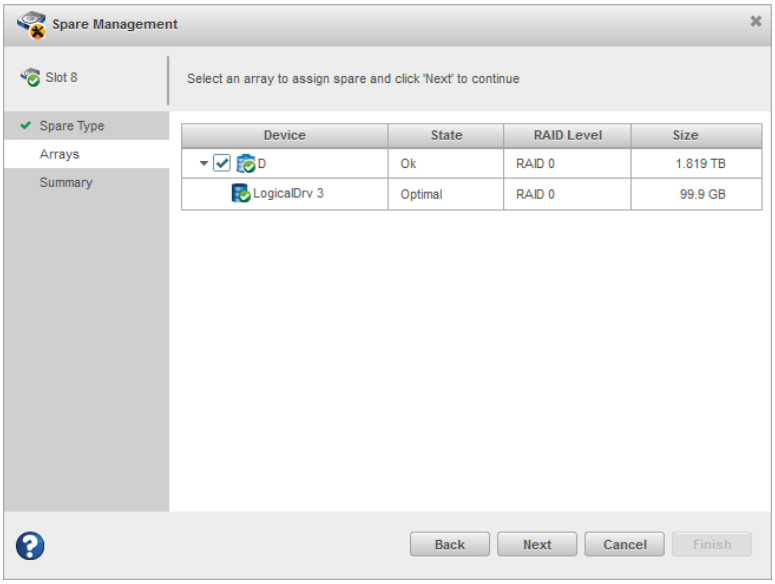
   Note: The auto-replace option is not available, if you select an array with a non-redundant logical device when the controller's "spare activation mode" is set to "failure activation". However, when you select a physical device itself, the option is available only if one or more auto-replace spares already exist. Otherwise, you can just assign Dedicated spares in the wizard.
2. On the ribbon, in the Physical Device group, click **Spare Management**.



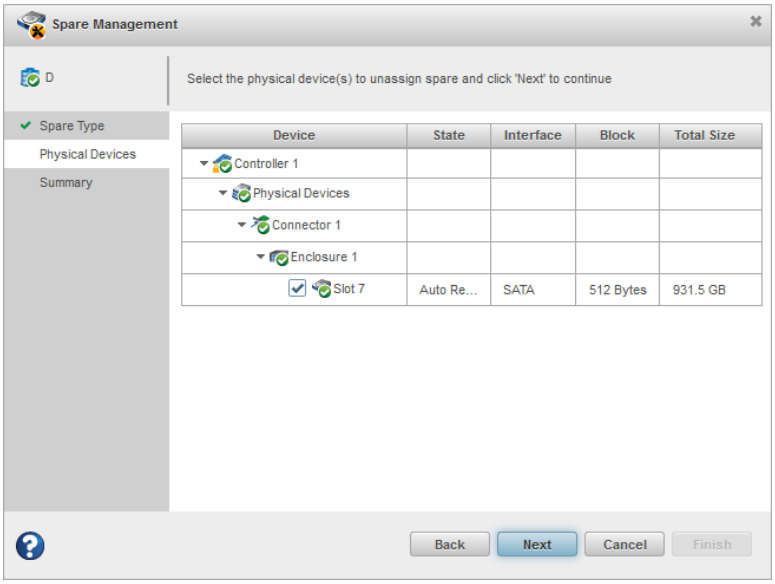
   The Spare Management wizard opens.
3. Select the **Auto-Replace** spare type, then click **Next**.



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**. For details on SED support operations, see 4.6.4 Spare Management. (See 5.2 Hot Spare Limitations for help selecting drives.)



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

5.5 Removing a Hot Spare

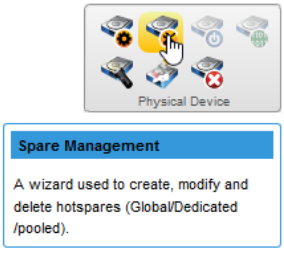
You can remove a dedicated or auto-replace hot spare from an array. Removing the last hot spare from an array returns the drive to the Ready state.

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.

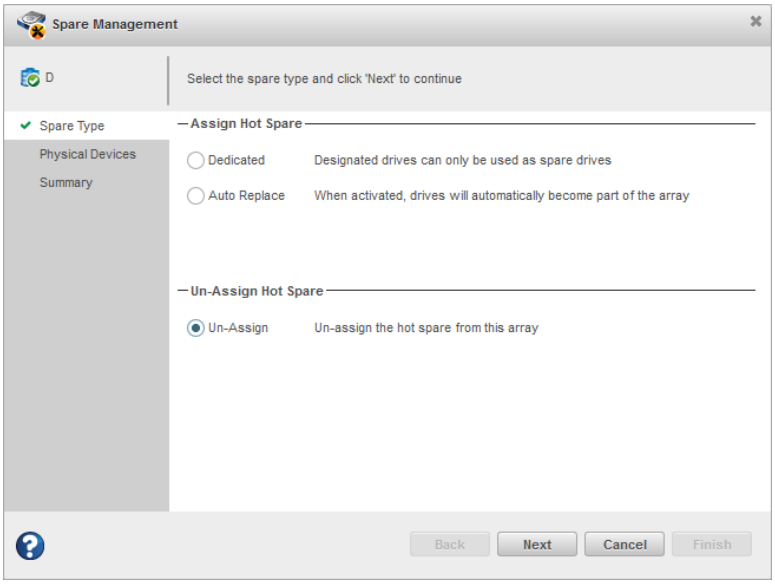
To remove a hot spare:

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**.

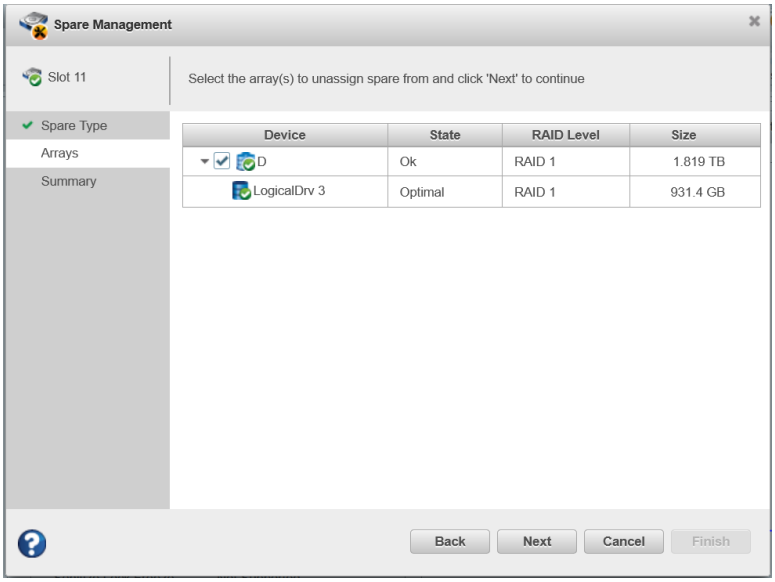


The Spare Management wizard opens.

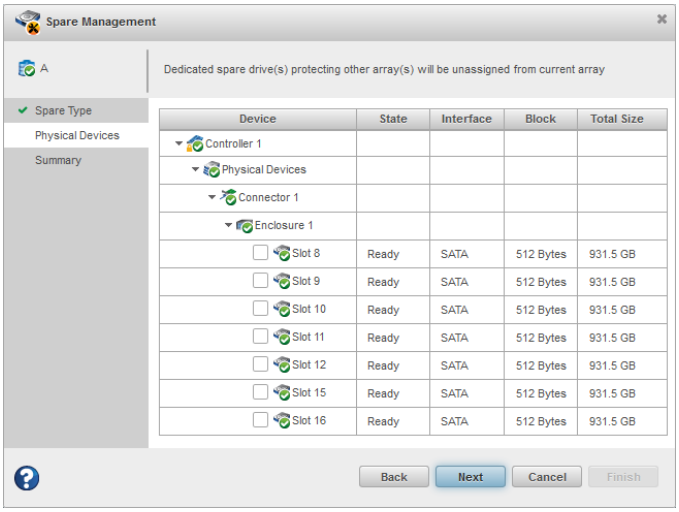
3. Select **Un-Assign**, then click **Next**. (Un-Assign is preselected for an existing hot spare.)



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.

5.6 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:

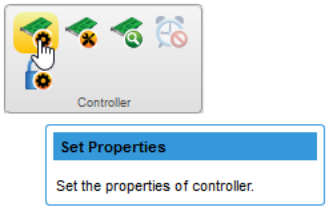
- A data drive fails; this is the default mode.
- A data drive reports a predictive failure (SMART) status.

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.

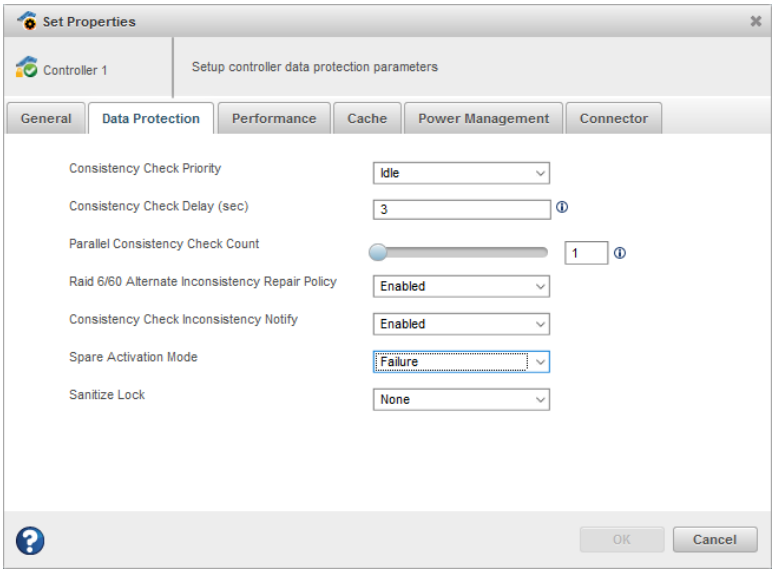
The spare activation mode applies to all arrays on a controller.

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**.



   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**.



5.7 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.

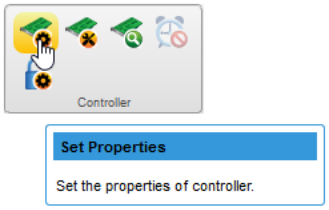
The sanitize lock feature has three options:

- 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

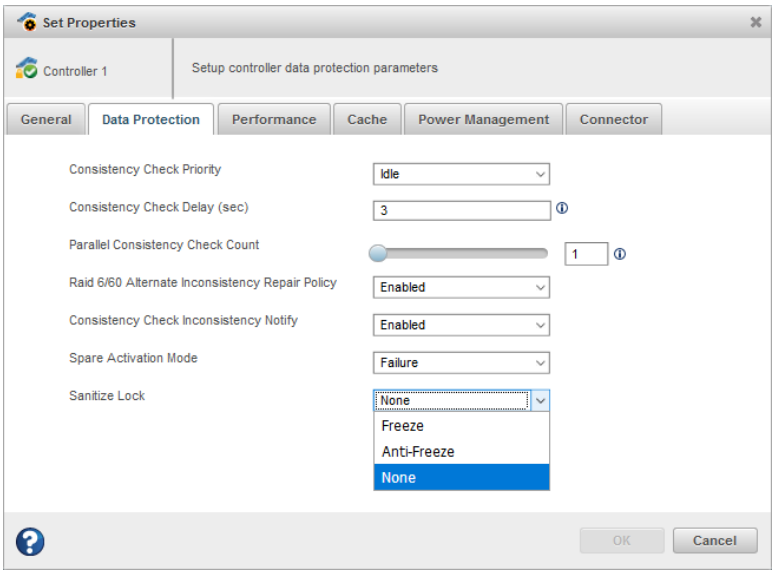
This is applicable only to SATA drives which support Sanitize Erase, Freeze, and Anti-Freeze.

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**.



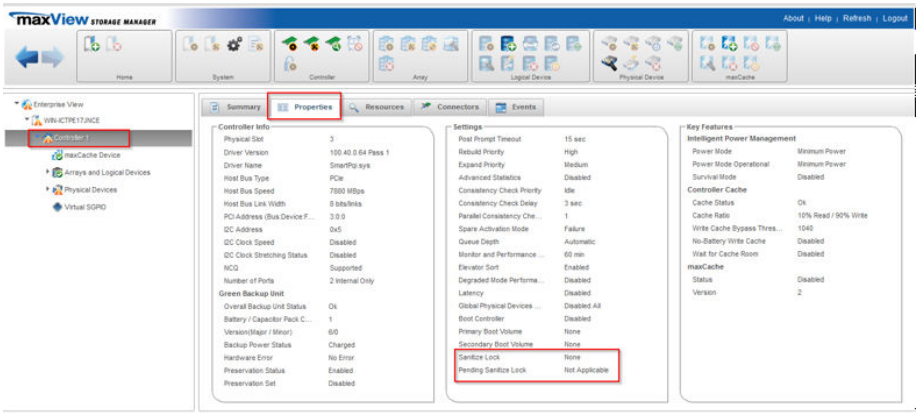
Note:
If the Sanitize Lock is set to any value other than **None**, the following warning message will be displayed in the menu header:

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**.

5.7.1 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.

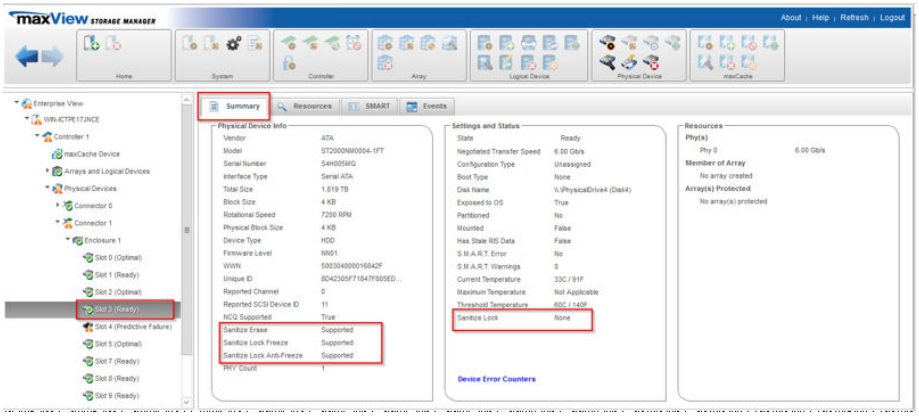
When the Sanitize Lock property is changed in the Set Properties dialog, the pending Sanitize Lock property will show the changed value.

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.

5.7.2 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.

© 2021 Microchip Technology Inc. and its subsidiaries



The Sanitize Lock property is dependent upon the following conditions:

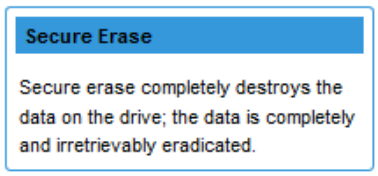
- If the drive does not support Sanitize Erase, the Sanitize Lock property is not displayed.
- If the drive supports Sanitize Erase but does not support Freeze/Anti-Freeze, then the Sanitize Lock property will be listed as "Not Applicable".
- If the controller Sanitize Lock is in the Freeze state, then 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.

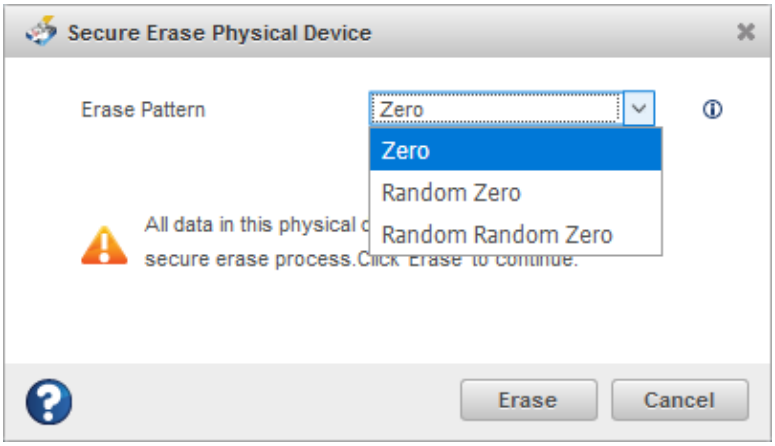
Once the controller Sanitize Lock is in the freeze state, then no Sanitize Erase operations will listed during the secure erase operation.

5.7.3 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.

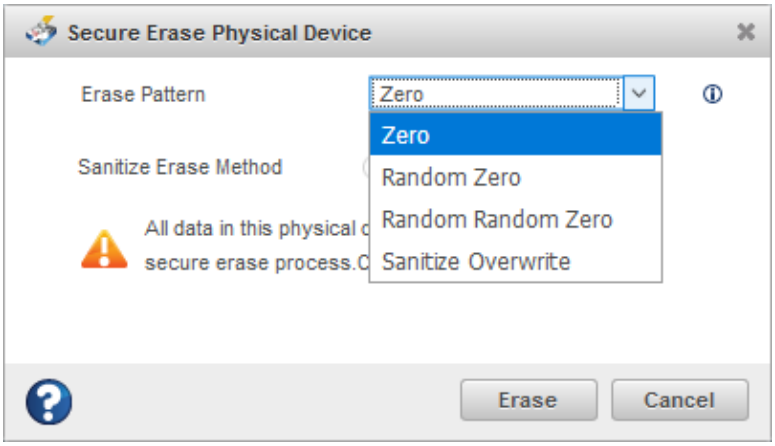






Only three secure erases can be performed.

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.

6. Modifying Your Storage Space

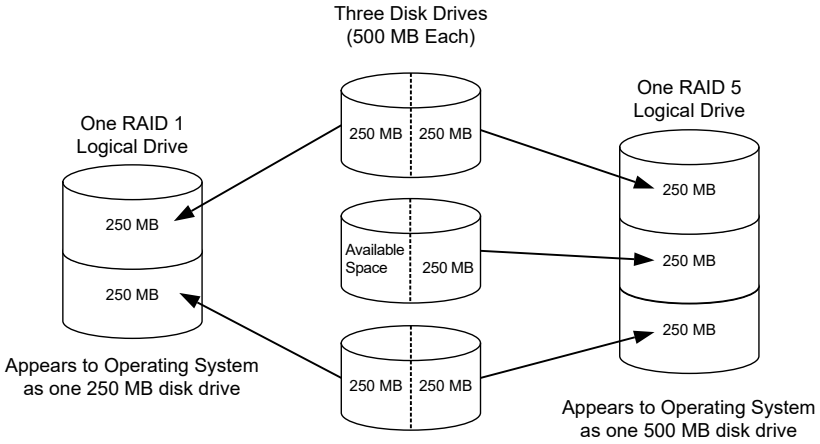
This section provides additional scenarios for creating and modifying arrays and logical drives. It explains how to check your logical drives for bad or inconsistent data; optimize controller and logical drive performance; move arrays and logical drives; and perform advanced operations, such as creating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

6.1 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 5. Protecting Your Data for more information.)

6.2 Creating and Modifying Logical Drives

For basic instructions for creating logical drives, see 4. Building Your Storage Space.

This section describes additional scenarios for creating logical drives:

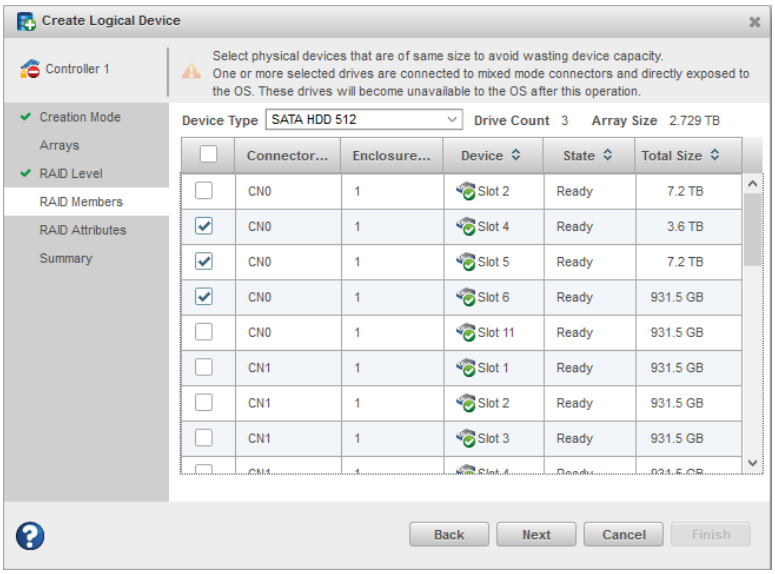
- To create a logical drive from different-sized disk drives, see 6.2.1 Including Different-sized Disk Drives in a Logical Drive.

6.2.1 Including Different-sized Disk Drives in a Logical Drive

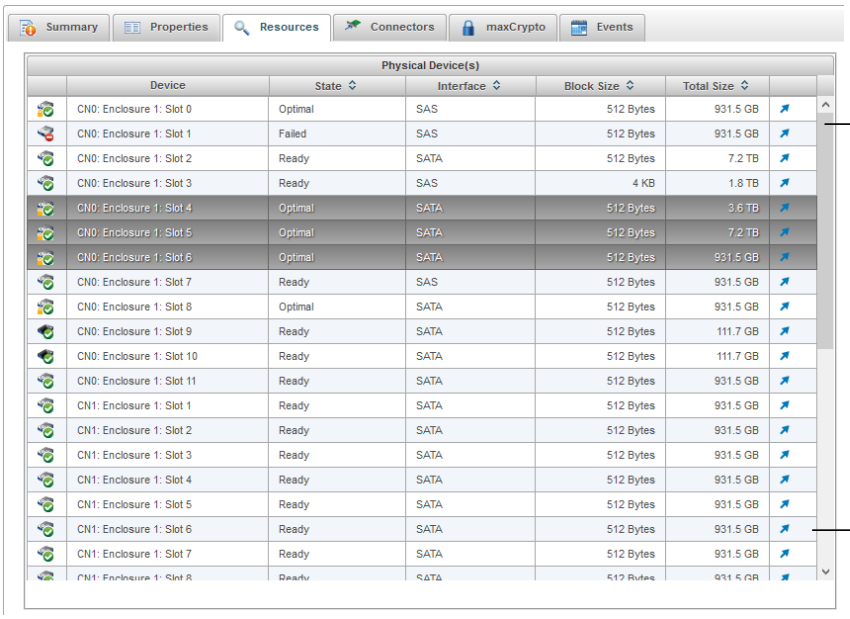
You can combine disk drives of different sizes in the same logical drive. If the logical drive includes redundancy, however, the size of each segment can be no larger than the size of the smallest disk drive. (See Selecting the Best RAID Level for more information about redundancy.)

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 4.4.1 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.

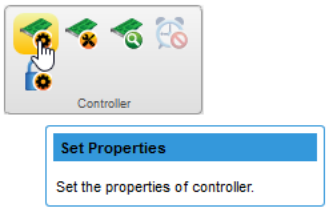


6.3 Enabling Background Consistency Check

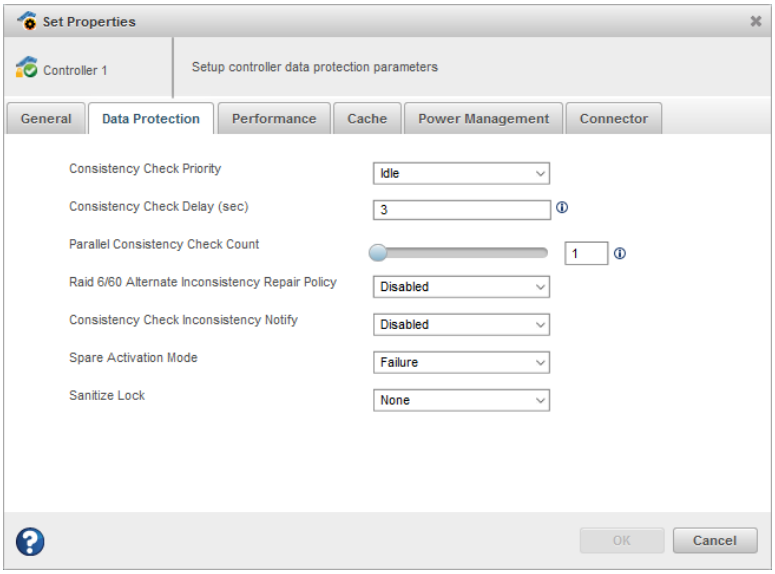
When background consistency check is enabled, maxView Storage Manager continually and automatically checks your logical drives for bad or inconsistent data, and then fixes any problems. Enabling consistency check ensures that you can recover data if a logical drive fails. The scanning process checks 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**.

6.4 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.

© 2021 Microchip Technology Inc. and its subsidiaries

6.4.1 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.

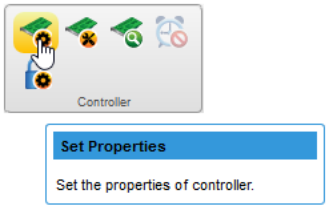
Note: You cannot use controller caching and maxCache caching concurrently. Controller caching is available only if maxCache is not enabled on the controller. For more information about maxCache, see 7. Working with maxCache Devices.

Option	Description
Cache Ratio	Sets the global Read:Write cache ratio.
Write Cache Bypass Threshold	Sets the write cache block size threshold, above which data is written directly to the drive.
No Battery Write Cache	Enables write caching on controllers without a backup module.
Wait for Cache Room	Waits for cache space (if none is available) before completing the request.
Global Physical Devices Write Cache Policy	Sets the write cache policy for the physical drives on the controller. ⚠ CAUTION Enabling drive write caching can improve performance. However, a power, device, system failure, or dirty shut down may result in data loss or file-system corruption.
Drive Write Cache Policy for Configured Drives	Sets the write cache policy for the configured physical devices on the controller • Default: Allows the controller to control the drive write cache policy of all configured physical devices. • Enabled: The drive write cache for the physical device will be enabled by the controller. Setting to enabled can increase write performance but risks losing the data in the cache on sudden power loss to all configured physical devices. • Disabled: The drive write cache for the physical devices will be disabled by the controller. • Unchanged: Sets the physical devices factory default policy for all configured drives.
Drive Write Cache Policy for Unconfigured Drives	Sets the write cache policy for the unconfigured physical devices on the controller • Default: The controller does not modify the drive write cache of the physical devices. • Enabled: The drive write cache for the physical device will be enabled by the controller. Setting to enabled can increase write performance but risks losing the data in the cache on sudden power loss to all unconfigured physical devices. • Disabled: The drive write cache for the physical devices will be disabled by the controller.
Drive Write Cache Policy for HBA Drives	Sets the write cache policy for the HBA physical devices on the controller • Default: The controller does not modify the drive write cache of the physical devices. • Enabled: The drive write cache for the physical drive will be enabled by the controller. Setting to enabled can increase write performance but risks losing the data in the cache on sudden power loss to all physical devices. • Disabled: The drive write cache for the physical devices will be disabled by the controller.

© 2021 Microchip Technology Inc. and its subsidiaries

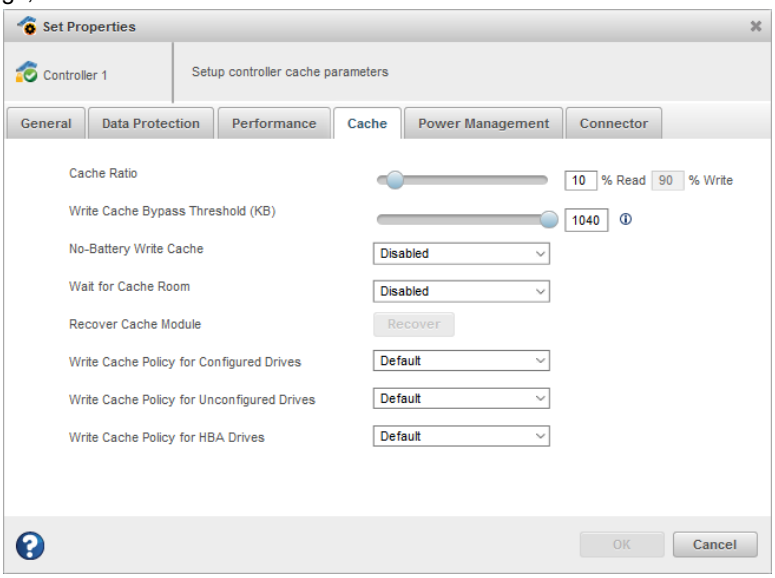
To enable cache optimizations on a controller:

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**.

6.4.1.1 Enabling Cache Optimization for a Logical Drive

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

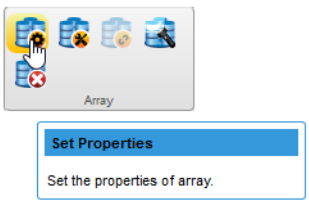
1. In the Enterprise View, select a controller, then select a logical drive.
2. On the ribbon, in the Logical Device group, click **Set Properties**.
3. In the Controller Caching drop down-list, select `Disabled` or `Enabled`.
4. Click **OK**.

6.4.2 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.

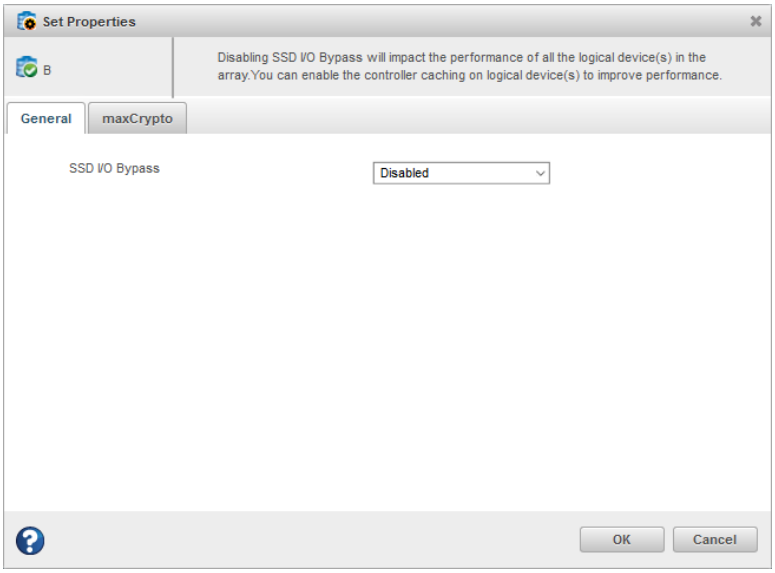
To enable I/O Bypass acceleration:

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**.

6.5 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:

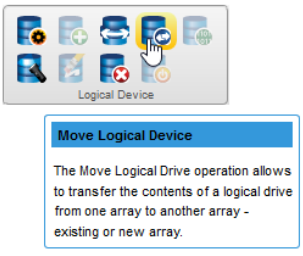
- Move Logical Drive To a New Array
- Move Logical Drive To an Existing Array

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.

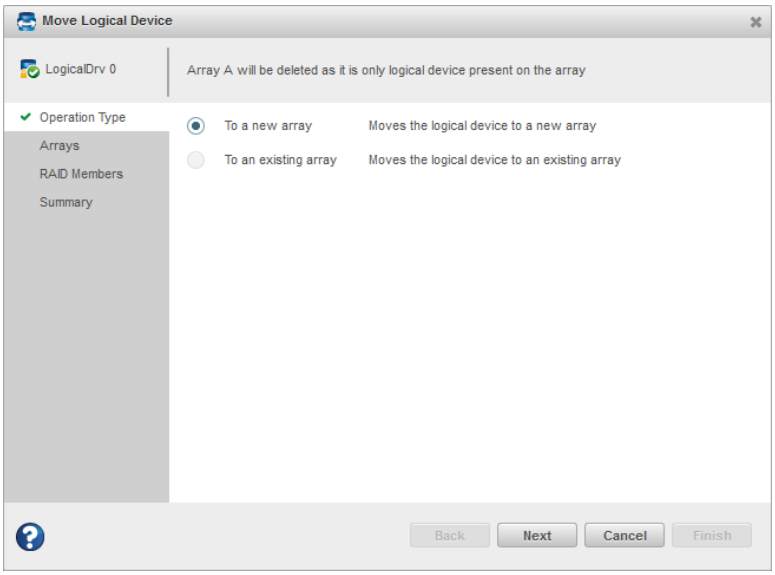
Note: Moving a logical drive can be a time-consuming process. All data in the logical drive is moved onto the new or existing array, and the controller continues to service I/O requests to other logical drives.

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**.

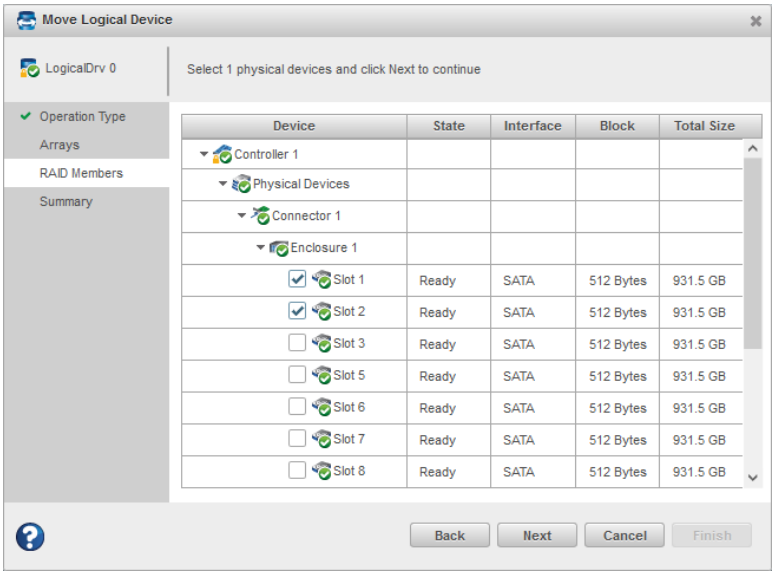


3. When the wizard opens, select **To New Array** or **To Existing Array**, then click **Next**.



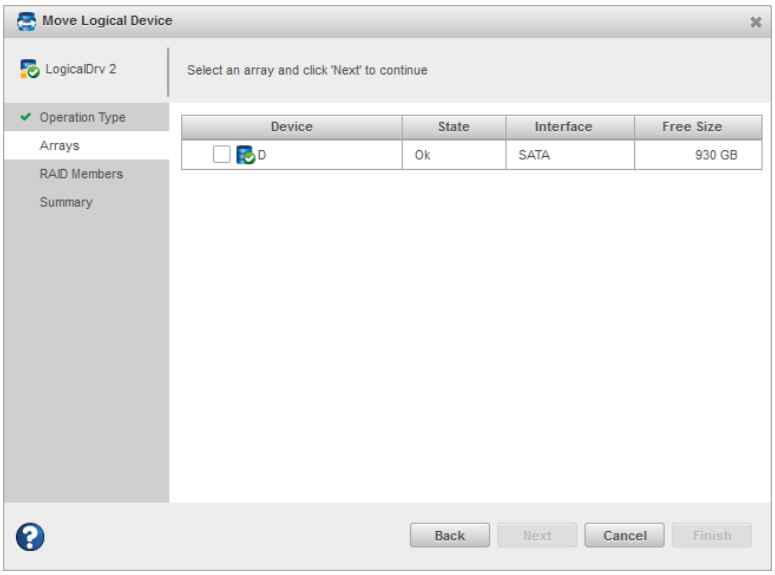
Note:
For details on SED support operations on moving a logical device, see 4.6.3 Move Logical Device.

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.

6.6 Moving an Array

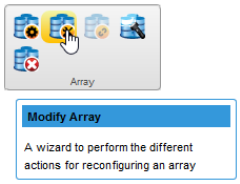
You can move an array by replacing its physical drives with drives of the same type or different type. For example, you can replace SAS drives in the array with other SAS drives, or replace SAS drives with SATA drives. You cannot combine drive types in the same array, however. If you choose to replace 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.

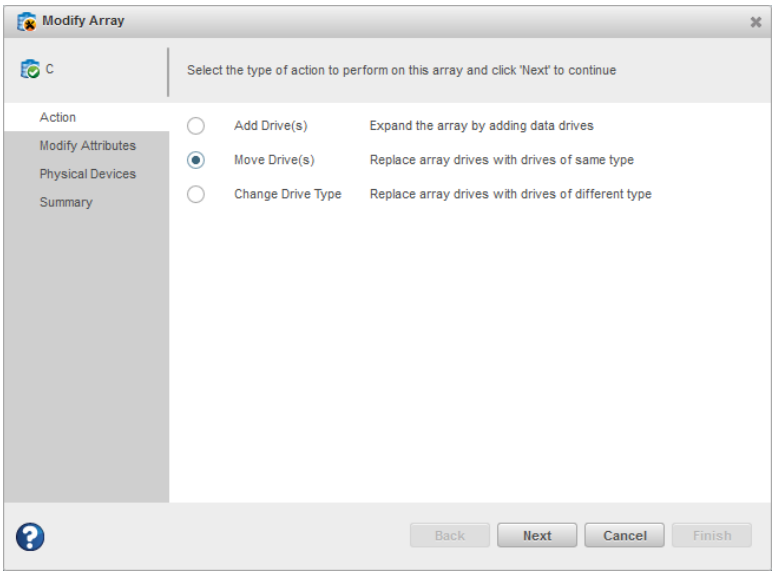
Note: Moving an array can be a time-consuming process. All data in each logical drive is copied to the replacement drives, and the controller continues to service I/O requests to other logical drives.

To move an array:

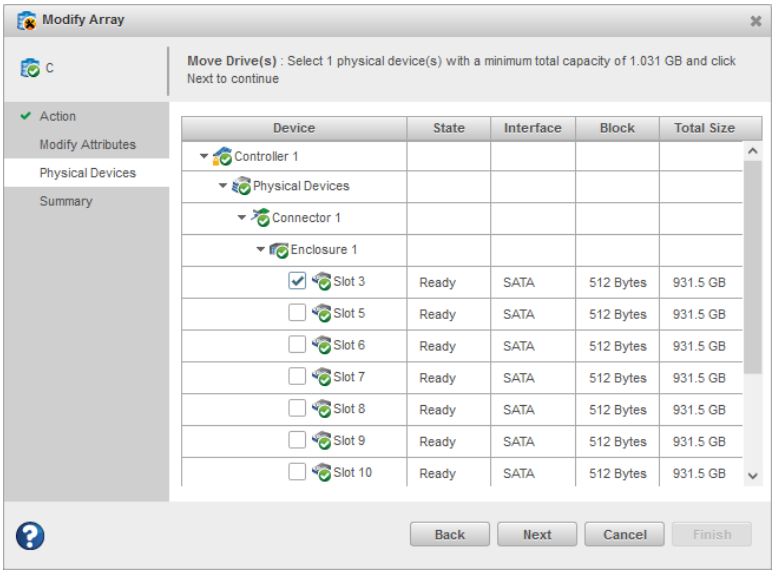
1. In the Enterprise View, select an array.
2. On the ribbon, in the Array group, click **Modify Array**.



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.

Note:
For details on SED support operations while modifying an array, see 4.6.2 Modify Array.

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

6.7 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

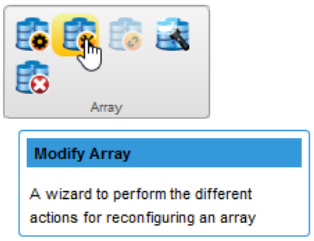
If you add the logical drives, you are expanding the array by adding the data drives. If you move the logical drive to an existing array, you need to replace the array drives with the drives of the same type.

© 2021 Microchip Technology Inc. and its subsidiaries

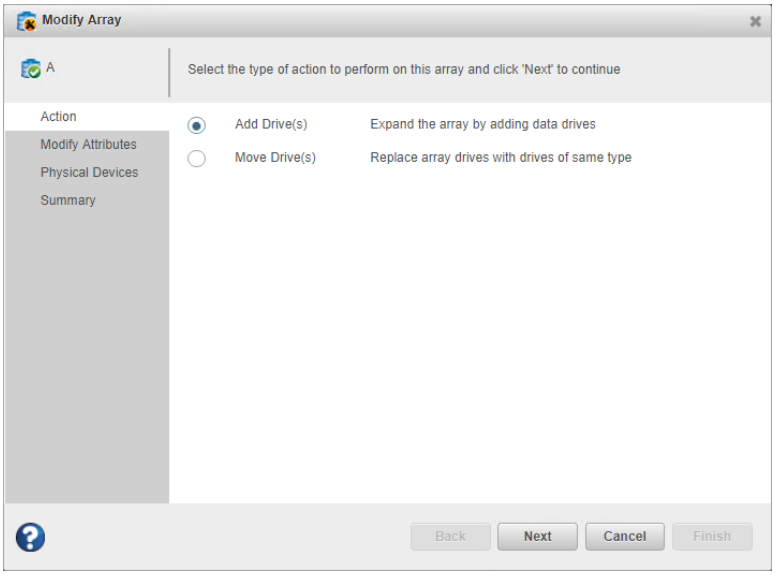
Note: Moving a logical drive can be a time-consuming process. All data in the logical drive is moved onto the new or existing array, and the controller continues to service I/O requests to other logical drives.

To add or remove drives in an array:

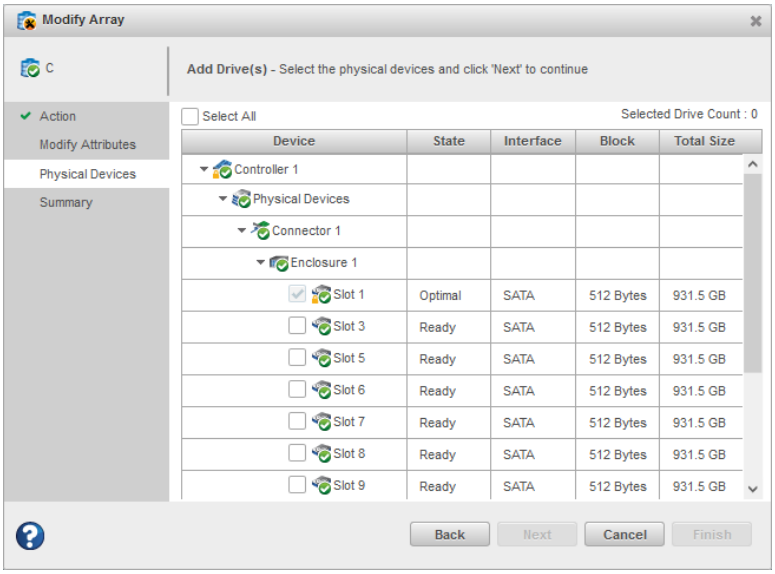
1. In the Enterprise View, select an array.
2. On the ribbon, in the Array group, click **Modify Array**.



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.

Note:
For details on SED support operations to add drives, see 4.6.2 Modify Array.

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.

6.8 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(Triple), RAID 10, or RAID 10(Triple) array into two identical new arrays consisting of RAID 0 logical drives. Arrays with other RAID configurations cannot be split.

6.8.1 Creating a Split Mirror Backup

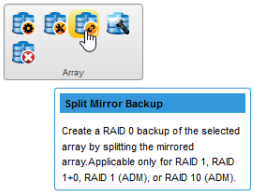
Use this option to split a mirrored array, consisting of one or more RAID 1, RAID 1(Triple), RAID 10, or RAID 10(Triple) logical drives, into two arrays: a primary array and a backup array, with these characteristics:

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

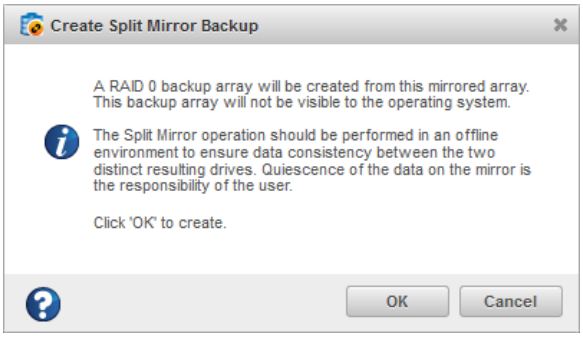
If the array is protected by a spare drive, the drive is unassigned after the split.

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**.



6.8.2 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.

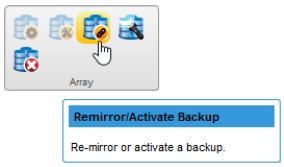
- Re-mirror the array and roll back to the contents of the backup array; existing data is discarded. This option re-creates the mirrored array but restores its original contents from the backup array.

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:

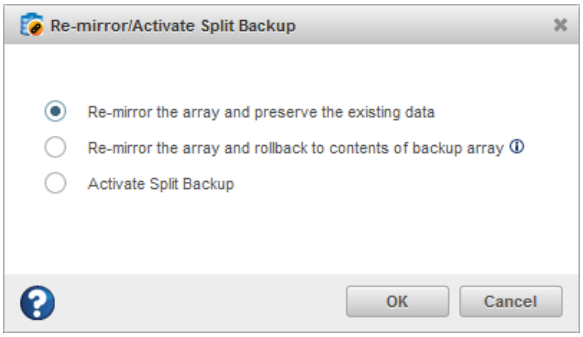
1. In the Enterprise View, select the Split Mirror Set Primary array; that is, an array with an existing split mirror backup.

   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**.



3. When prompted to select a re-mirroring task, choose: `Re-mirror array`, `Re-mirror with roll-back`, or `Activate Backup`.

   Note: Microchip 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.



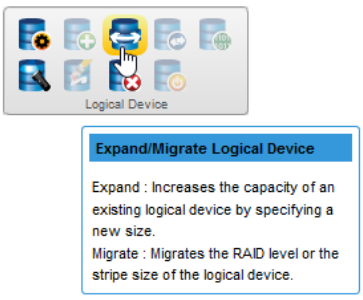
4. Click **OK**.

6.9 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.

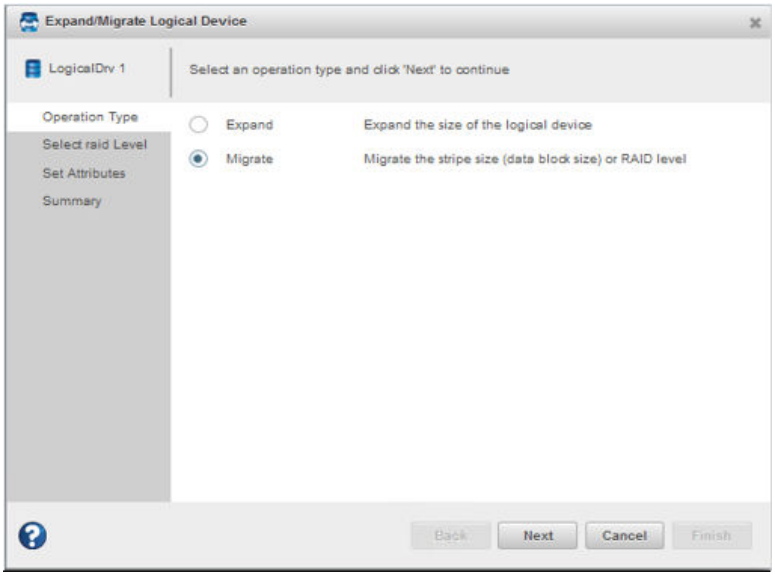
To change the RAID level of a logical drive:

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**.

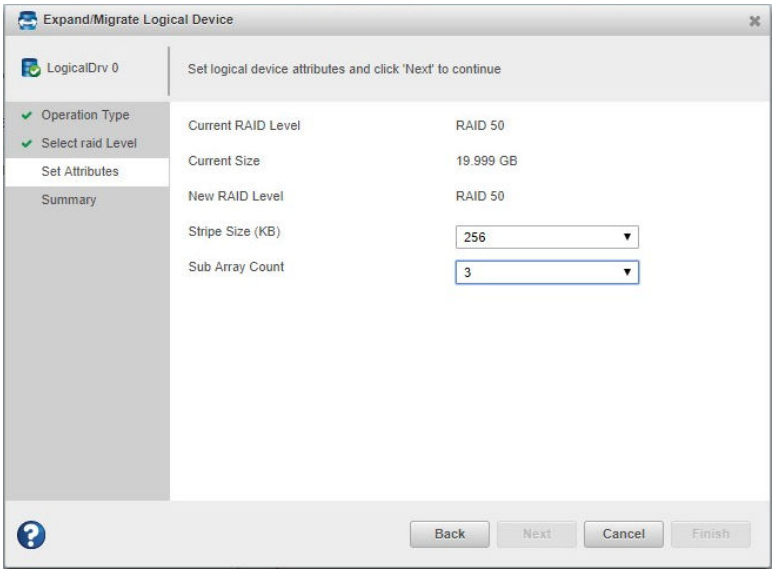


The Expand/Migrate Logical Device wizard opens.

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.

6.10 Increasing the Capacity of a Logical Drive

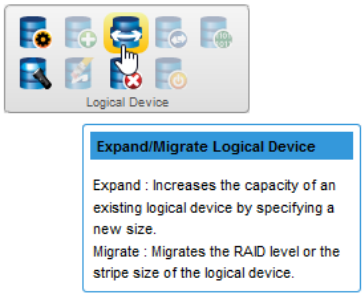
You can add more disk drive space, or *expand*, a logical drive, to increase its capacity.

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 6.7 Modifying an Array

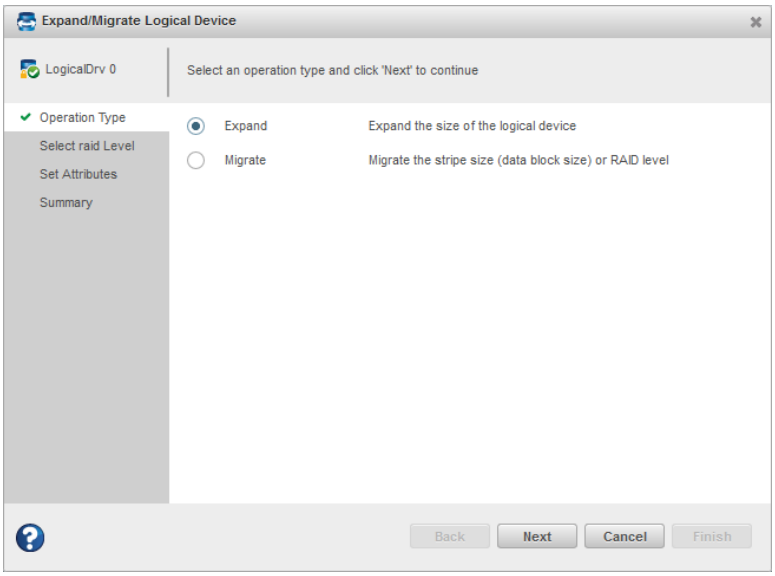
To increase the capacity of a logical drive:

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.

6.11 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 12.4 Rebuilding Logical Drives.

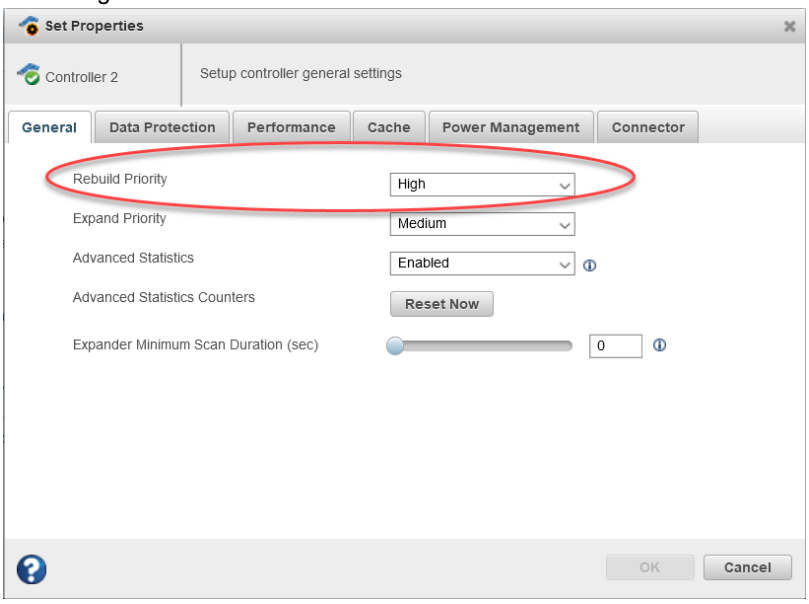
To change the rebuild priority:

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. In Rebuild Priority Mode drop-down list, select `Low`, `Medium`, `Medium High`, or `High`. The Rebuild Priority field is circled in the next figure.

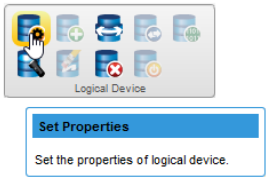


4. Click **OK**.

6.12 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.

© 2021 Microchip Technology Inc. and its subsidiaries

6.13 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.

⚠ 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.

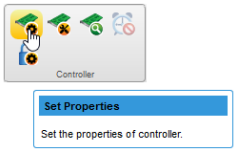
   Note: If a deleted logical drive is the only logical in the array, the array itself is also deleted.

6.14 Maintaining an Energy-Efficient Storage Space

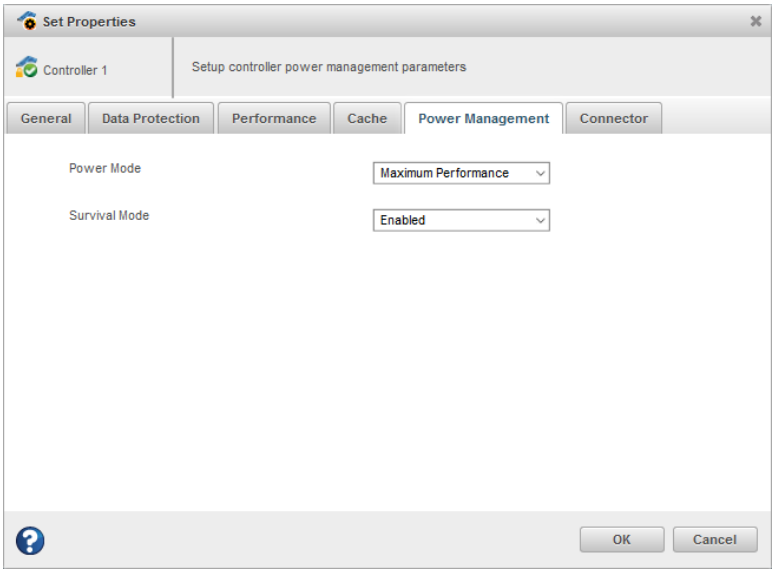
The power management options in maxView Storage Manager control the power profile of the physical drives on a controller. They offer a balance between maximum performance and minimum power usage. To ensure continued operations when temperature thresholds are exceeded, you can enable Survival mode to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

7. Working with maxCache Devices

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.

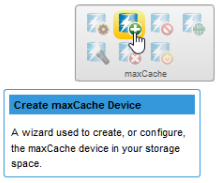
7.1 maxCache Limitations

- maxCache is not supported on all 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
  - For assigning maxCache to a SSD data logical device, SSD I/O bypass property should be disabled on the corresponding SSD data array
- 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

7.2 Creating a maxCache Device

To create a maxCache Device:

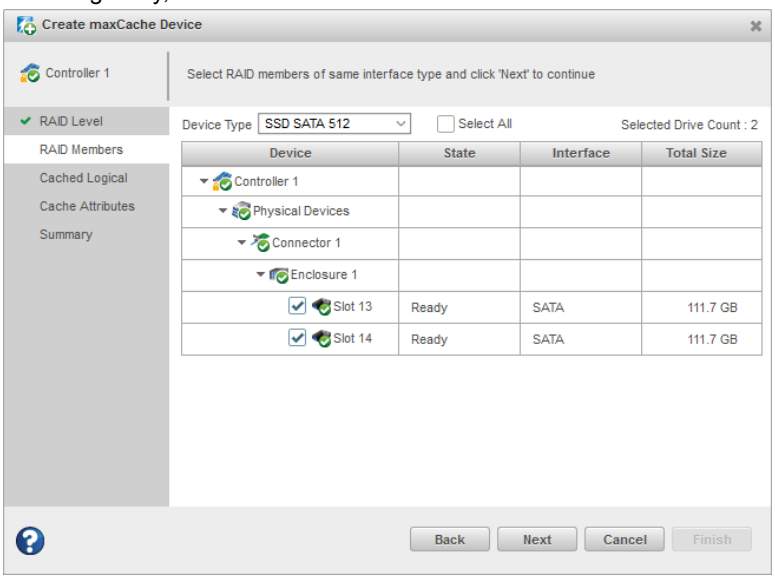
1. In the Enterprise View, select a system, then select a controller on that system. You can also create a maxCache device by selecting a logical device node.
2. On the ribbon, in the maxCache group, click **Create maxCache**.



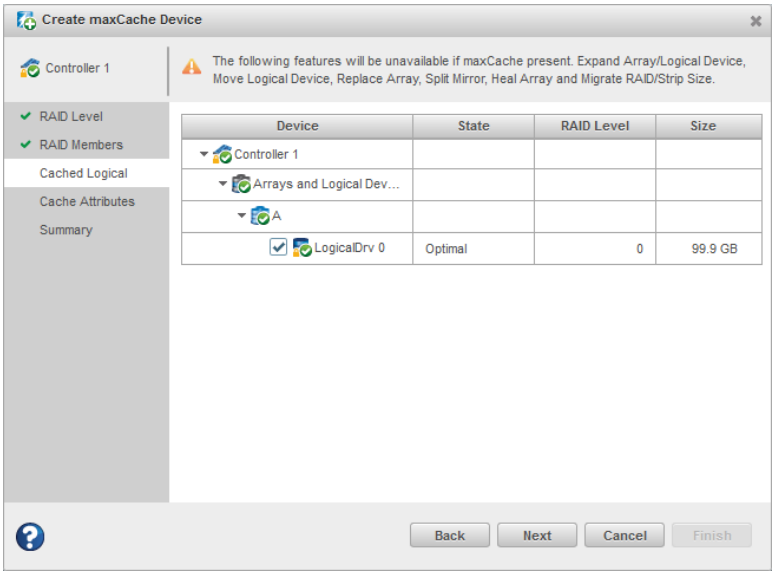
3. When the wizard opens, select a RAID level for the maxCache Device, then click **Next**.

   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. For details on SED support operations on maxCache while working on a new or existing array, see 4.6.5 maxCache.



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.

7.3 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**.

7.4 Deleting the maxCache Device

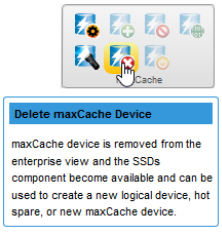
When you delete the maxCache Device, the component SSDs become available and can be used to create a new logical drive, hot spare, or new maxCache Device.

⚠ 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.

7.5 Analyzing maxCache Performance

maxView Storage Manager provides advanced usage statistics about the maxCache Devices on your Microchip 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 10.4.2 Viewing Advanced Statistics for more information.

© 2021 Microchip Technology Inc. and its subsidiaries

8. Working with maxCrypto™ Devices

Microchip 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.

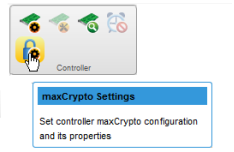
Note: Encryption of non-RAID volumes (such as physical, raw, or pass-through devices) is not supported. Consequently, HBAs and controllers operating in HBA Mode do not support maxCrypto.

8.1 maxCrypto Initial Setup

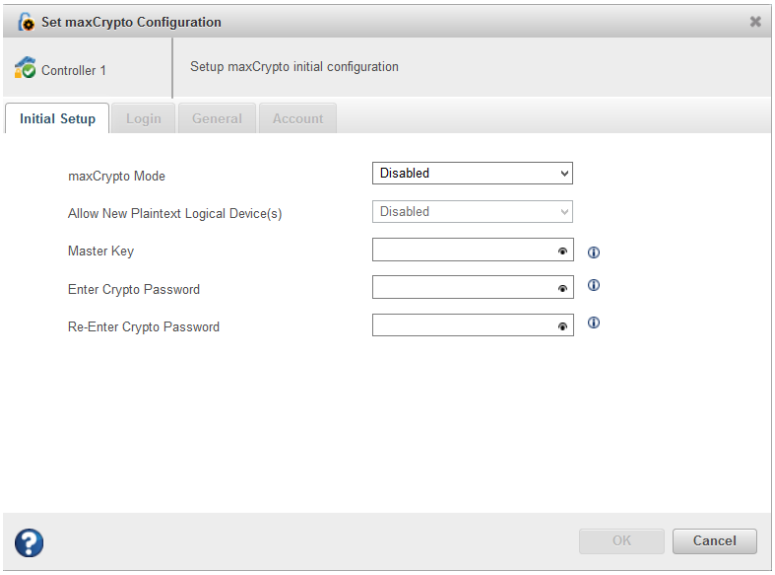
Before you can begin using maxCrypto in your storage space, you must complete the initial setup task to create the Crypto Officer account and configure the initial maxCrypto settings, including the Crypto Officer login credentials, maxCrypto master encryption key, and other basic information. You must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



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.

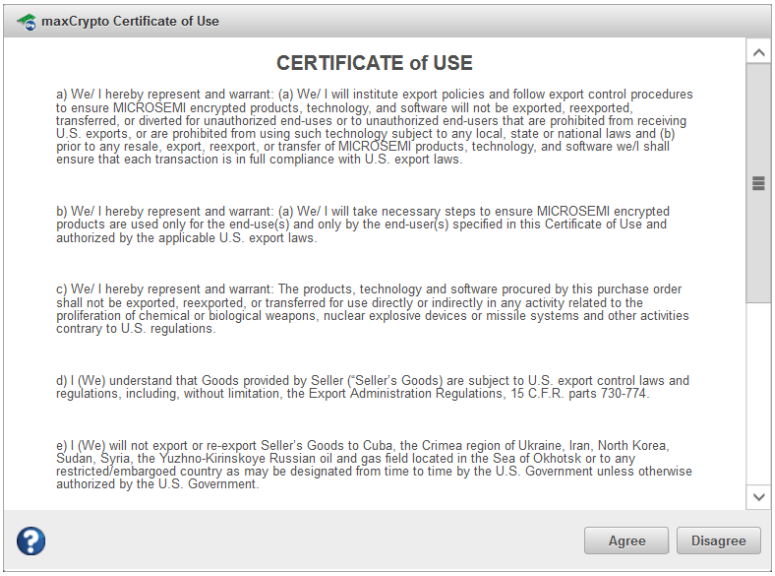
4. In the Allow New Plaintext Logical Device(s) drop-down, select `Enabled` to allow plaintext logical devices to be created, in addition to encrypted logical devices. Select `Disabled` to allow only encrypted logical devices to be created.

   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.



8.1.1 Managing maxCrypto Accounts

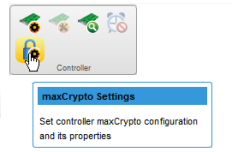
After initial setup is complete, the Crypto Officer account is logged in, by default. As the Crypto Officer, you can perform all account management operations, including configuring the standard User account, changing passwords, and enabling password recovery options. If you are logged into the standard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

Standard users can:	Standard users can't:
Log into maxCrypto	Perform initial setup
Lock/Unlock firmware update	Recover password
Enter/Re-Enter new password	Allow new plaintext logical device(s)
Create encrypted and plaintext logical drives	Set/Change master key
Convert plaintext array/logical drive to encrypted data	Import master key

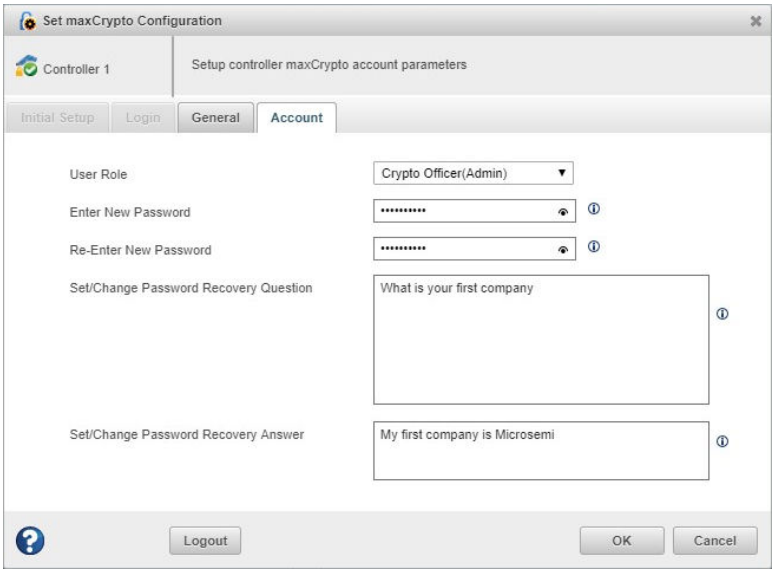
.....continued	
Standard users can:	**Standard users can't:**
Crypto erase array/logical drive	Set/Change password recovery question
Clear maxCrypto configuration	

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 qustion/answer fields are deactivated for the User account.
7. Click **OK**.

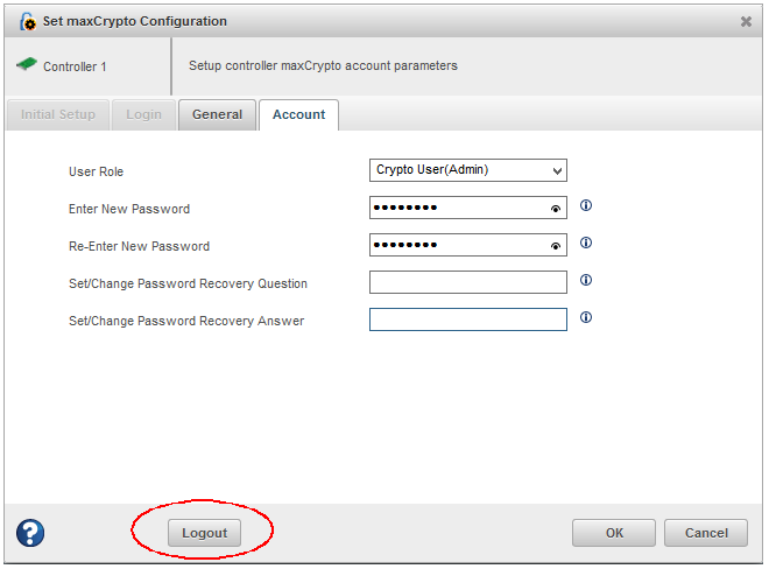
8.1.2 Logging In and Logging Out

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.

© 2021 Microchip Technology Inc. and its subsidiaries

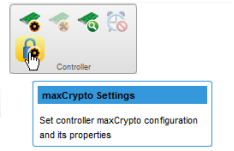
After initial setup is complete, the Crypto Officer account is logged in, by default.

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.

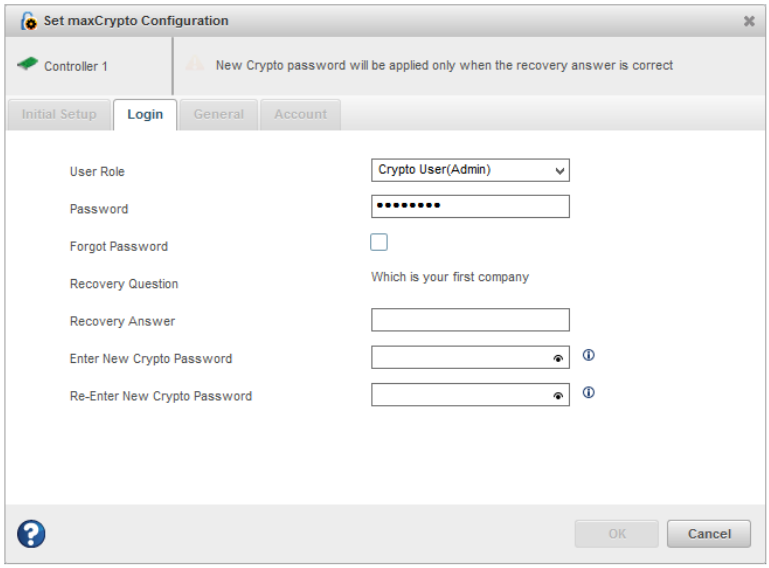


To login back in, or to login to a different account:

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**.

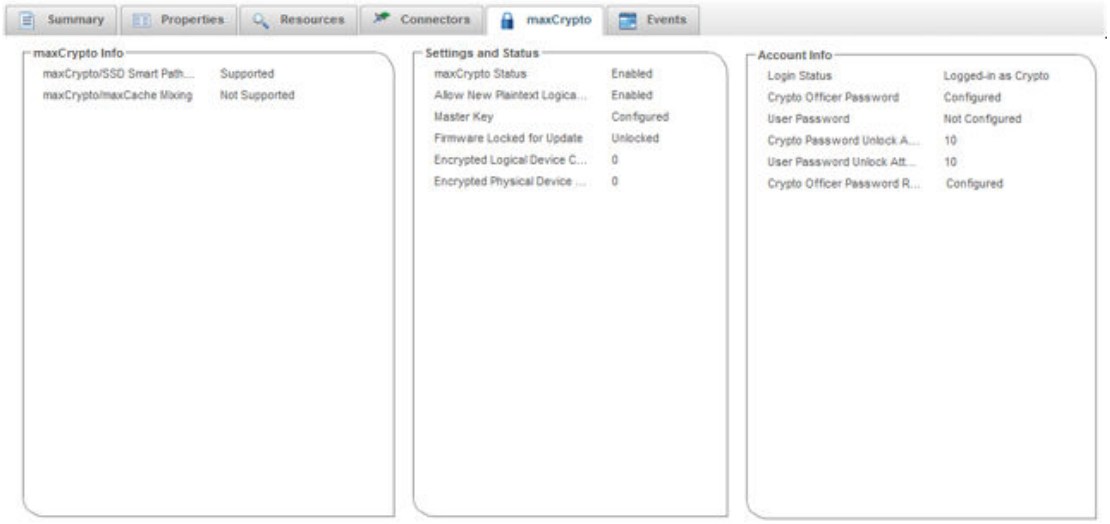
To reset the Crypto Officer password:

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**.

8.1.3 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.



Property	Description
maxCrypto Status	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.
Allow New Plaintext Volumes	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.
Master Key	After Initial setup, Master Key value is displayed as Configured.
Firmware Locked for Update	If Unlocked, firmware upgrade is enabled. If Locked, firmware upgrade is disabled.
Number of maxCrypto Logical Devices	Total count of the encrypted logical devices.
Number of maxCrypto Physical Devices	Total count of encrypted physical devices.

.....continued

Property	Description
Crypto Officer Password	After Initial setup, Crypto Officer Password will be displayed as Configured.
Login Status	If logged-in as the Crypto Officer (Admin), displays “Logged-in as Crypto”. If logged in as User, displays “Logged-in as User”. If maxCrypto session timed out, displays “Timeout”. If maxCrypto is logged-out, displays as “Not Logged In”.
User Password	If the User account is configured, displays as “Configured”; otherwise, displays as “Not Configured”.
Crypto Password Unlock Attempts Remaining	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.
User Password Unlock Attempts Remaining	Countdown of User role attempts remaining after a failed login. **Note:** After 10 failed login attempts, the User account is locked for 15 minutes.
Crypto Officer Password Recovery Parameters	Displays as “Configured” when Crypto Officer sets the password recovery question and answer. Displays as “Not Configured” when Crypto Officer has not set the password recovery question and answer.

8.2 Modifying the maxCrypto Configuration

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

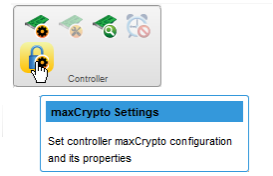
If you are logged in as the Crypto Officer, you can:

- Enable/Disable maxCrypto
- Enable/Disable new plaintext volumes
- Lock/Unlock firmware upgrade
- Change the maxCrypto master encryption key

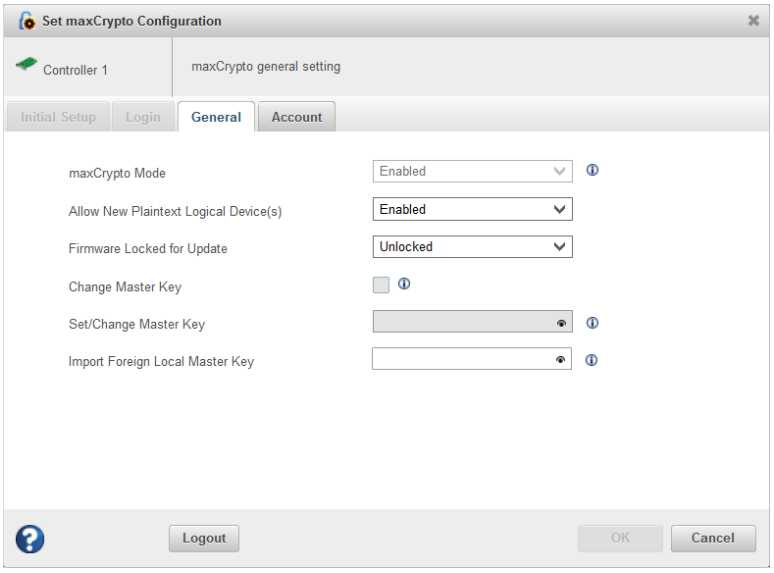
If you are logged in as the maxCrypto User, you can only Lock/Unlock firmware upgrade.

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**.



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.

     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.

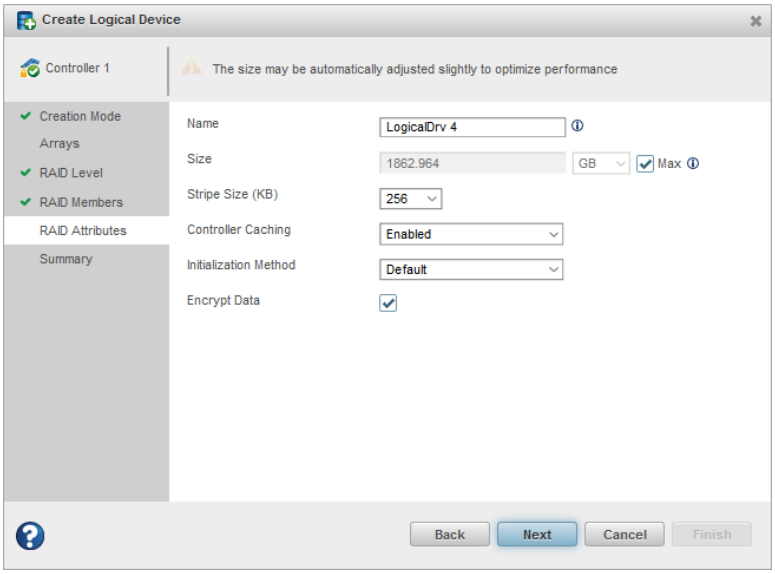
4. Click **OK**.

8.3 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 4.4 Creating Arrays and Logical Drives.

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.

© 2021 Microchip Technology Inc. and its subsidiaries



Notes:

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.

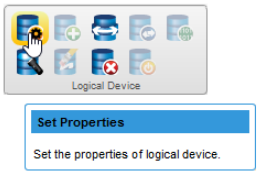
   Note: You must be logged in to maxCrypto to create plaintext volumes, even if maxCrypto status and Allow New Plaintext Volumes are both Enabled; see 8.1.2 Logging In and Logging Out.
3. If maxCrypto status is Enabled and Allow New Plaintext Volumes property is Disabled, only encrypted logical drives can be created.

8.4 Converting Plaintext Data to Encrypted Data

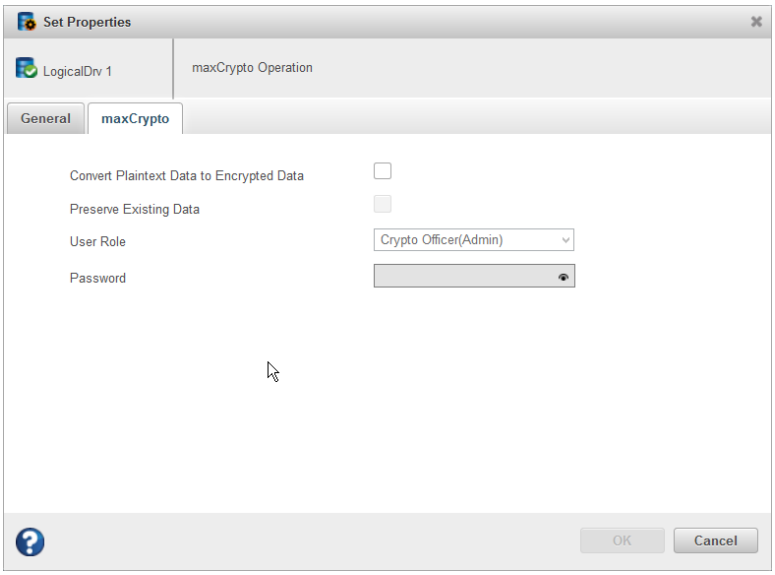
Use this operation to convert plaintext data to encrypted data. You can convert an unencrypted logical drive or all unencrypted logical drives on an array. Additionally, you can choose to preserve or discard the existing data during conversion.

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**.



Note: The User Role and Password fields are enabled only when you are not logged in to maxCrypto.

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**.

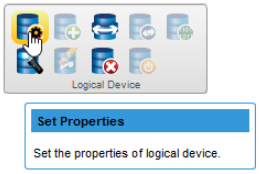
8.5 Re-Keying a Logical Drive

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.

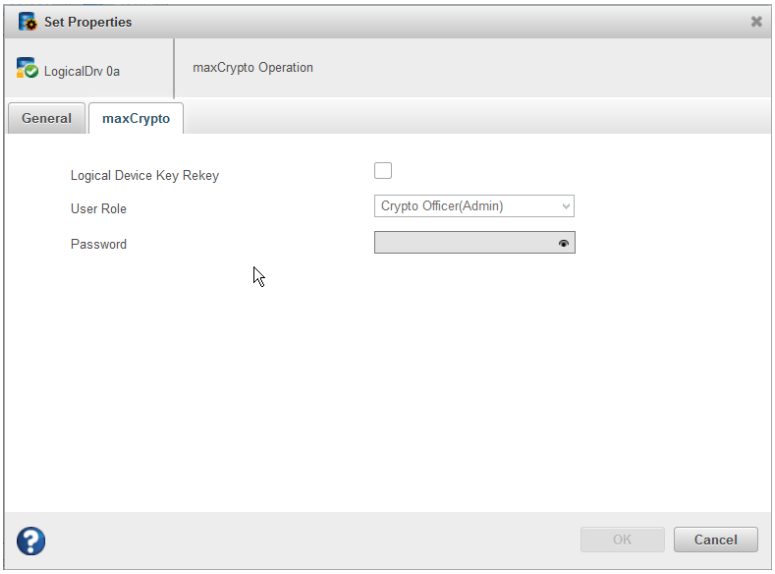
Optionally, you can re-key an array to generate a new key for all encrypted logical drives on the array.

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**.



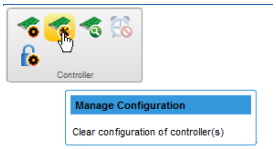
3. Click the **Logical Device(s) Key ReKey** check box.
4. Click **OK**.

8.6 Clearing the maxCrypto Configuration

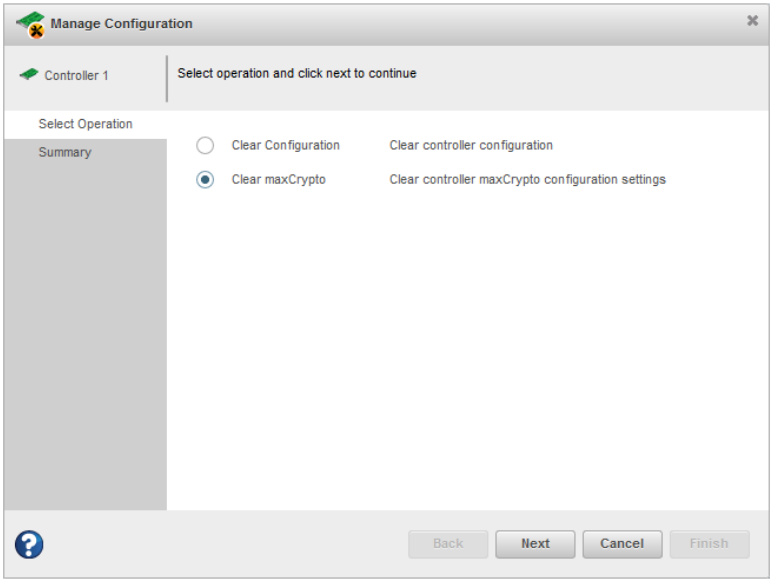
You can clear the maxCrypto configuration to restore the default maxCrypto settings. Clearing the maxCrypto configuration resets all keys, passwords, and users, including the maxCrypto Officer account and User account.
Note: To clear the maxCrypto configuration, ensure that there is no encrypted logical 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**.

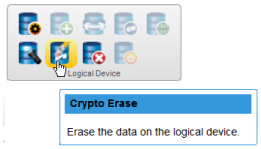
8.7 Erasing an Encrypted Logical Drive

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.

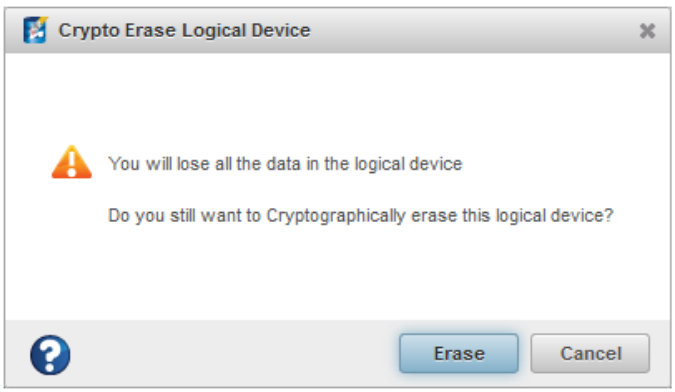
⚠ CAUTION When you cryptographically erase a logical drive, you lose all data on that drive.

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**.

8.8 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.

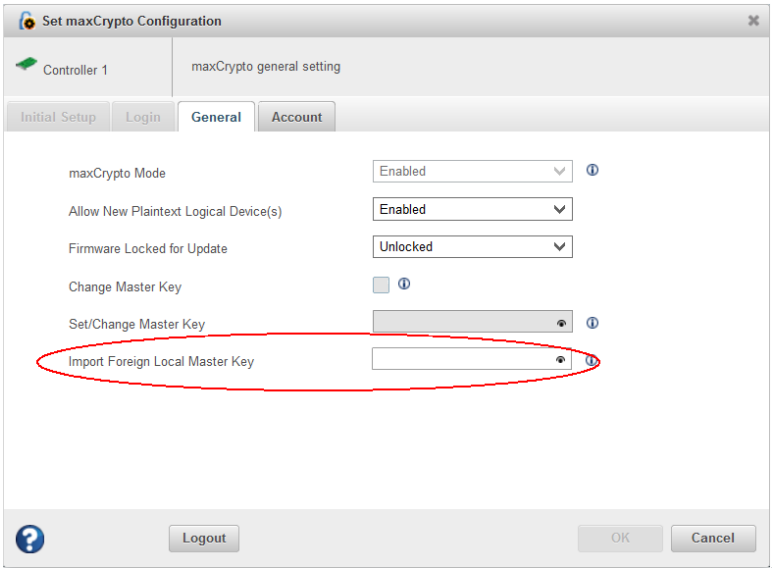
To import a foreign master key:

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**.



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**.

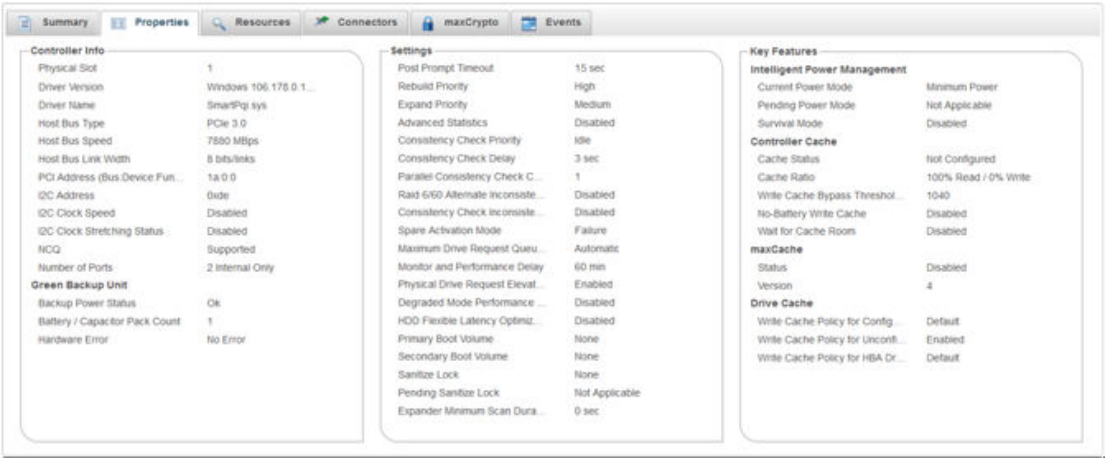
9. Maintaining Physical Devices

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

9.1 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 10.2.3 Viewing Component Status in the Storage Dashboard.



9.2 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.

To Locate...	Select...
A disk drive	Disk Drive icon: 
All disk drives on a controller	Controller icon: 
All disk drives included in an array	Array icon: 
All disk drives included in a logical drive	Logical Drive icon: 

.....continued	
To Locate...	**Select...**
All SSDs in the maxCache Device	maxCache Device icon: 

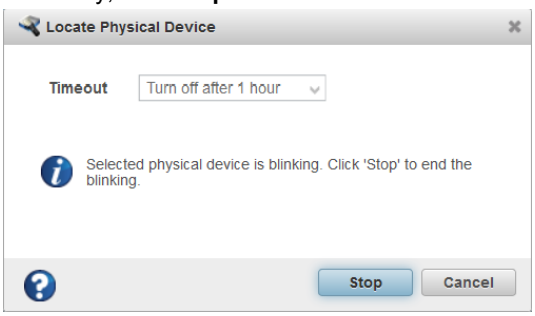
9.2.1 Locating Disk Drives

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.

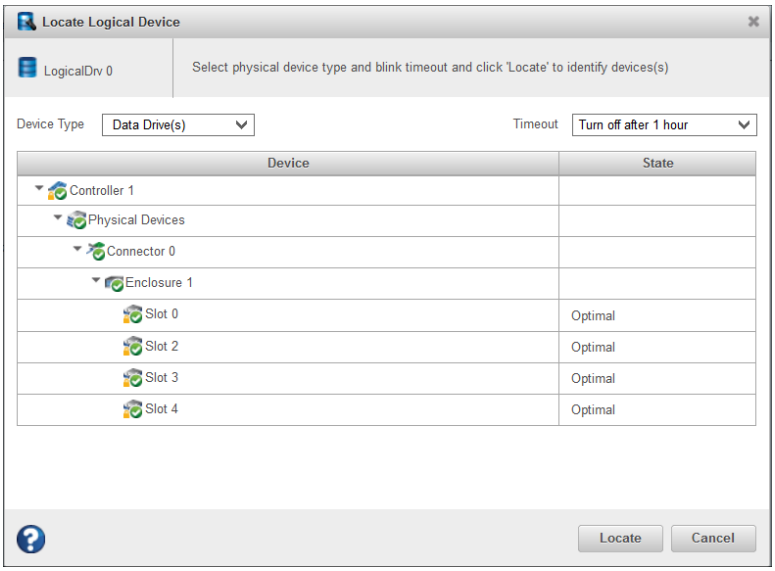
9.2.2 Locating Physical Disks in an Array or Logical Drive

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**.



   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**.



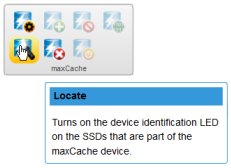
The LEDs on the disk drives begin to blink.

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.

9.2.3 Locating SSDs in the maxCache Device

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

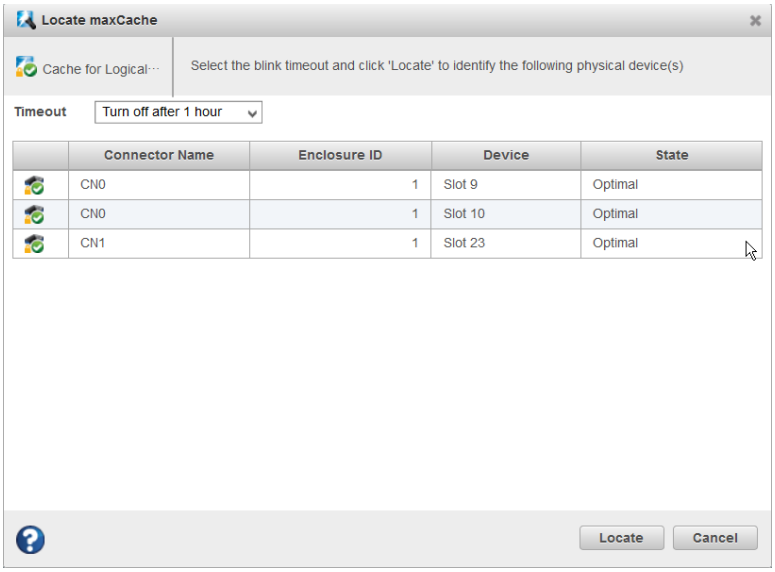
1. In the Enterprise View, select a controller; then select the maxCache Device on that controller. You can select the maxCache array or logical device.
2. On the ribbon, in the maxCache group, click **Locate**.



The Locate maxCache window opens, displaying a list SSDs comprising the maxCache Device.

3. Select the time-out period from the drop-down list: 1 hour, 4 hours, 24 hours.
4. Click the **Locate** button.

© 2021 Microchip Technology Inc. and its subsidiaries



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.

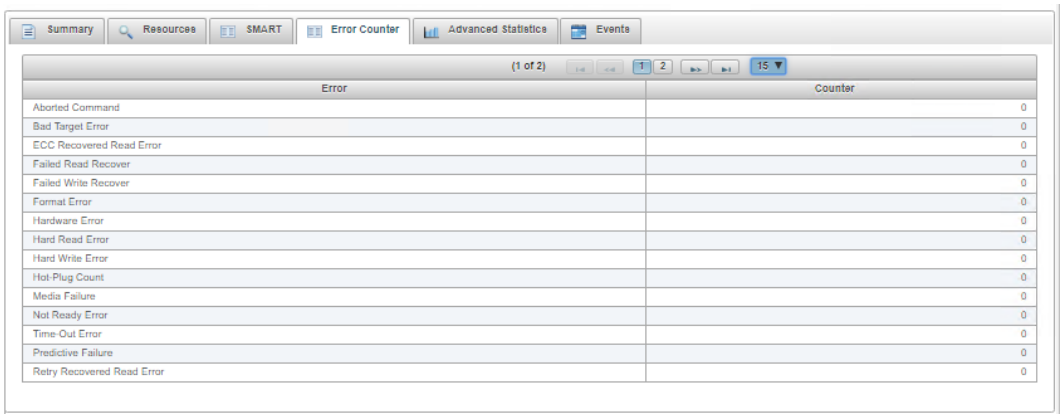
9.3 Working with Physical Device Error Counters

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.

9.3.1 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.



Error Counter	Description
Aborted Command	Number of times a drive was failed due to aborted commands that could not be retried successfully.

.....continued

Error Counter	Description
Bad Target Error	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.
ECC Recovered Read Errors	Number of ECC-corrected read errors.
Failed Read Recover	Number of times a recover of another physical drive in the logical volume failed due to a hard read error from this drive.
Failed Write Recover	Number of times a recover of this physical drive failed due to an error occurring on this drive during a write operation.
Format Error	Number of times a Format command (used when remapping defects) failed. A failed remap operation may cause the controller to fail a drive.
Hardware Error	Number of times a drive returned a bad hardware status. The drive may be failed if retries do not work.
Hard Read Error	Number of unrecoverable read errors.
Hard Write Error	Number of unrecoverable write errors.
Hot-Plug Count	Number of times this drive was hot-plugged (removed) from a box.
Media Failure	Number of times a drive was failed due to unrecoverable media errors.
Not Ready Error	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.
Other Timeouts	Timeouts other than Data ReQuest Timeouts (DRQ).
Predictive Failure	Number of times that the drive returned a predictive failure error.
Retry Recovered Read Error	Number of retry-recovered read errors.
Retry Recovered Write Error	Number of retry-recovered write errors.
SCSI Bus Fault	Number of “bus faults”, which we define as SCSI bus parity errors, overrun/ underrun conditions, etc.
Service Hours	Number of service hours since the last power cycle.
Sectors Written	Number of sectors written to media.
Sectors Read	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.

9.3.2 Clearing Error Counters from a Physical Device

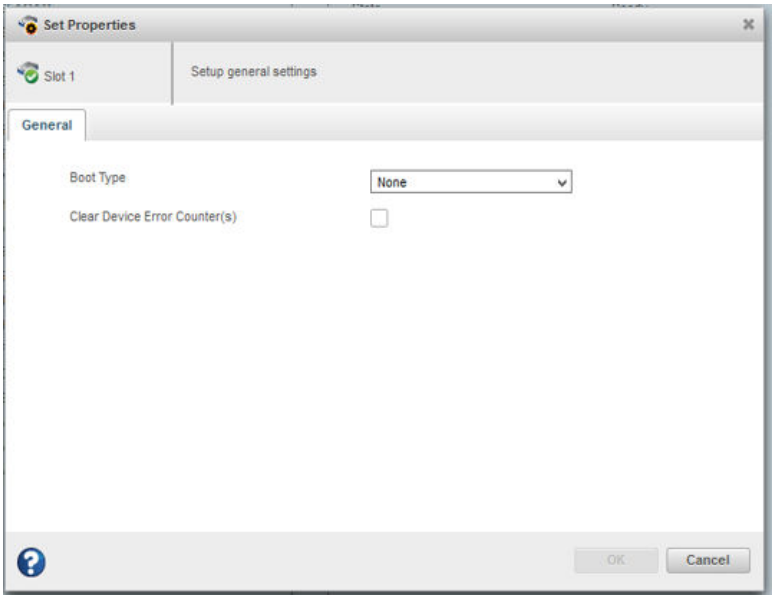
Use this option to clear the device error counters of a specific physical device.

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**.



The Set Properties window opens.



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

9.3.3 Clearing Error Counters from a Controller

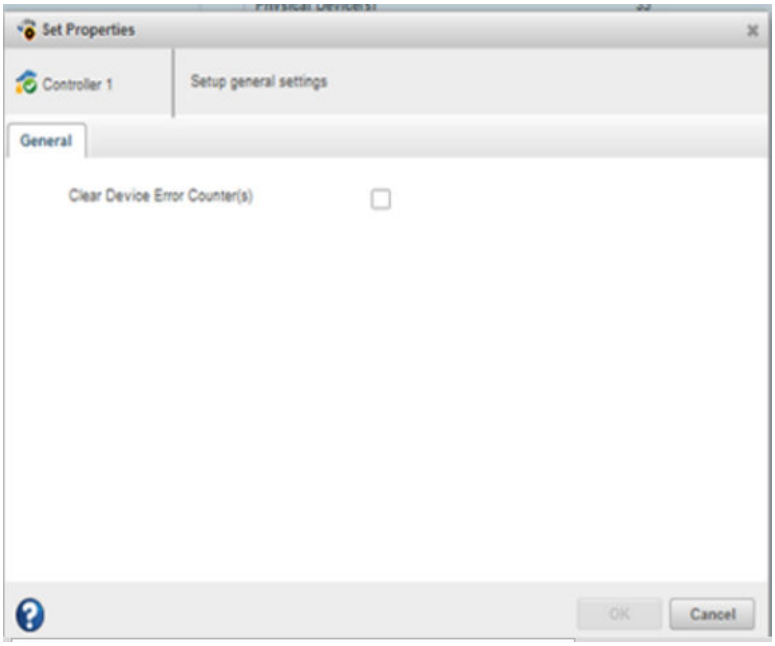
Use this option to clear the the device error counters of all the physical devices from controller.

To clear the 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**.

9.4 Refresh SED Security Status

This section explains how to refresh the security status of all the self encrypting drives. It is required if the security status of a drive is modified outside of this application.

The SED security status can be refreshed at the following two levels:

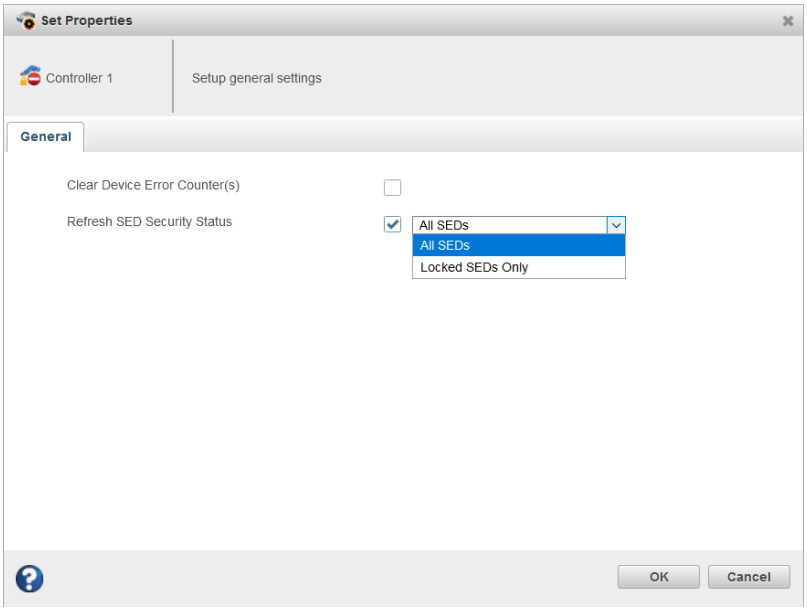
- On Controller
- On Physical Device

Perform the following steps to refresh SED security at the controller level:

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



The **Set Properties** window opens.



3. Select one of the following option from the **Refresh SED Security Status** drop-down menu:
   - All SEDs: This will refresh the SED security status for all the SED drive attached to the controller.
   - Locked SEDs Only: This will refresh the SED security status for all locked SED drive attached to the controller.
4. Click **OK**.

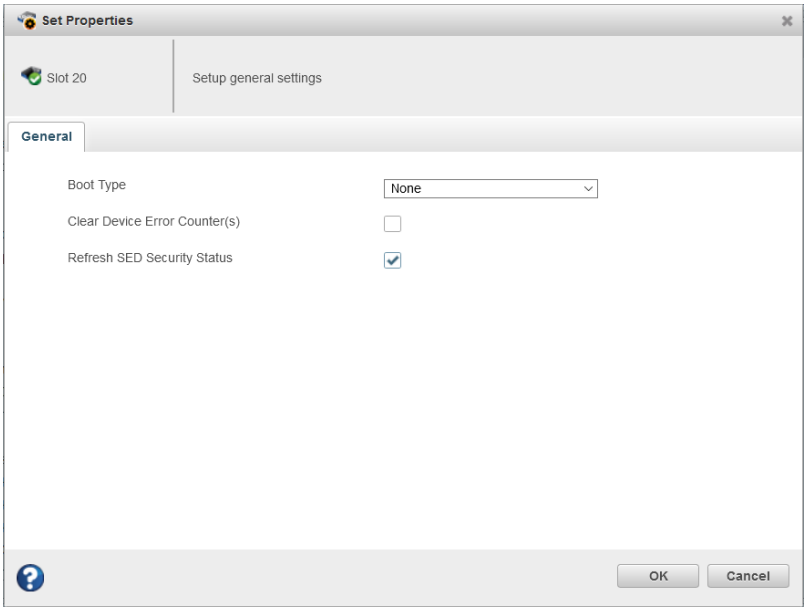
   This will refresh the SED security status for selected SED drive attached to the controller. This option will be rendered only if the selected drive has SED capability.

Perform the following steps to refresh SED security at the physical device level:

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



   The **Set Properties** window opens.



3. Select **Refresh SED Security Status** option.
4. Click **OK**.

9.5 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.

9.5.1 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 12.4 Rebuilding Logical Drives), 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 9.5.2 Setting a Disk Drive to 'Failed'.)
3. Remove and replace the disk drive with one of equal or greater size.
4. Wait for the logical drive to rebuild. (See 12.4 Rebuilding Logical Drives.)
5. Repeat these steps for each disk drive you want to replace.

9.5.2 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, *or*
- The disk drive is part of a redundant, healthy logical drive

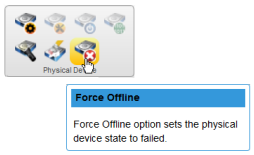
Once you force a drive offline, it can be brought online again only after power-cycling the controller.

© 2021 Microchip Technology Inc. and its subsidiaries

⚠ 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.

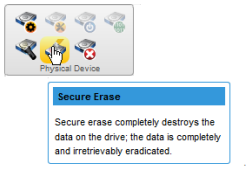
9.6 Erasing a Disk Drive

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.

9.6.1 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.

© 2021 Microchip Technology Inc. and its subsidiaries

- **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 9.6 Erasing a Disk Drive .

9.7 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.

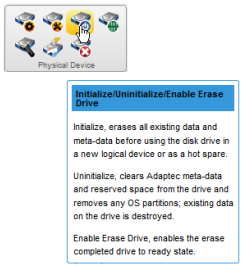
9.7.1 Uninitializing a Disk Drive

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.

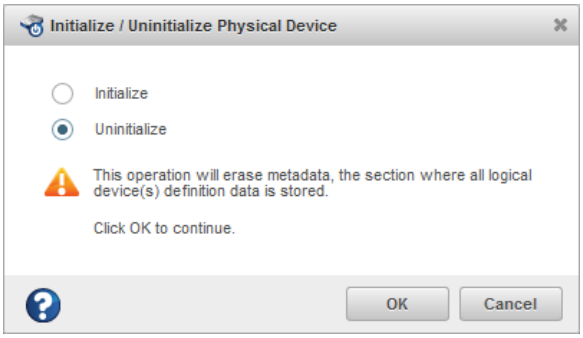
To uninitialize a disk drive:

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**.



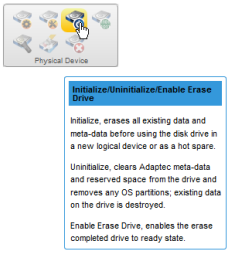
4. When prompted, click **OK** to close the Initialize/Uninitialize Device window.

9.7.2 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.

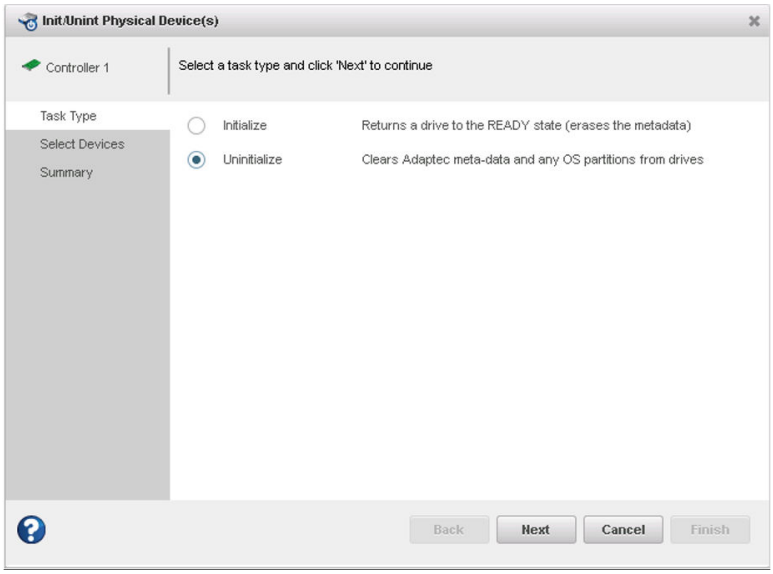
To initialize or uninitialize drives with the wizard:

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**.

9.8 Setting the Physical Drive Boot Priority

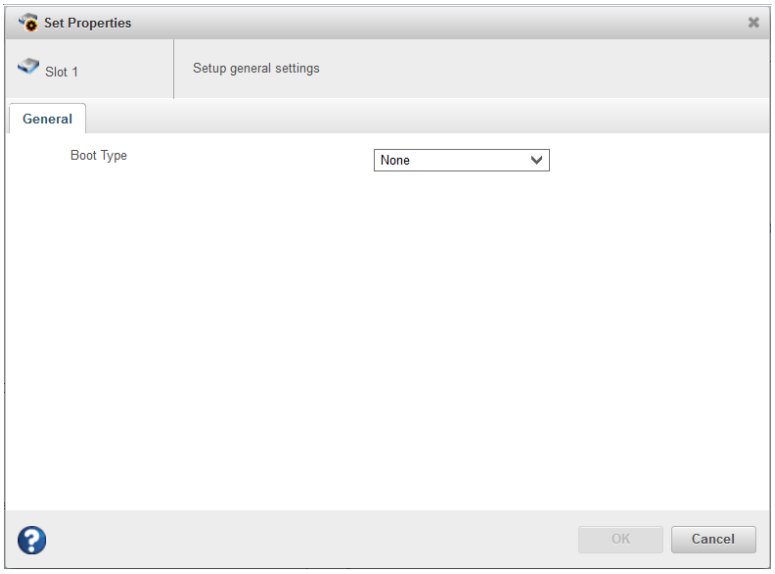
Use this option to set the boot priority of a physical device to Primary, Secondary, Primary and Secondary, or None (default). A controller can have only one physical (or logical) device as the primary or secondary boot device. When you select a new physical device as the primary/secondary boot drive,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

9.9 Working with Controllers

This section describes how to use maxView Storage Manager to manage the controllers in your storage space:

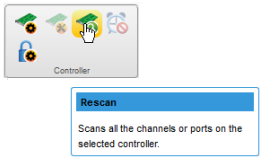
- To re-scan a controller, see 9.9.1 Rescanning a Controller.
- To optimize controller performance, see 9.9.2 Optimizing Controller Performance.
- To change the operating mode of connectors on the controller , see 9.9.3 Changing the Connector Operating Mode.

9.9.1 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.

9.9.2 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.

Option	Description
Queue Depth	Sets the max drive request queue depth for the controller. Valid values are Automatic, 2, 4, 8, 16, and 32.
Monitor and Performance Delay	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).
Elevator Sort	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.
Degraded Performance Optimization	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.
Latency	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.

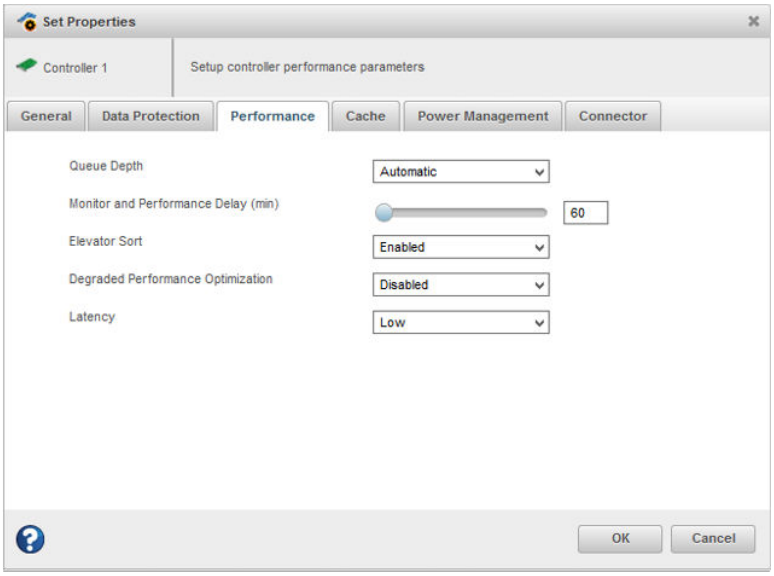
To enable/disable performance optimizations on a controller:

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**.

9.9.3 Changing the Connector Operating Mode

Use this option to change the behavior of the connectors on your 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

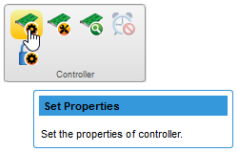
By default, products with RAID support are configured to operate in Mixed Mode. Mode options vary, depending on the configuration of logical and physical devices on the connector. For example, you cannot switch the connector to HBA mode if the connector is already configured with a RAID volume.

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

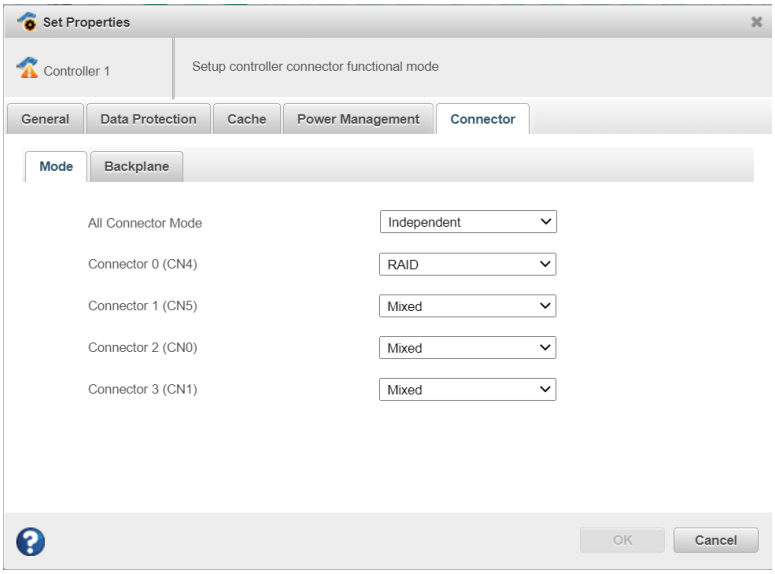
Note: Changing from Mixed Mode or HBA Mode to RAID Mode removes access to the physical drives from the operating system.

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.

9.9.4 Changing the Backplane Discovery Protocol Settings

A discovery protocol is the connector mode protocol to discover the attached backplane on the connectors of your Adaptec Smart Storage Controller. Following are the supported backplane discovery protocols in maxView:

- AutoDetect (With SAS/SATA fallback): The controller firmware attempts to automatically detect the discovery protocol of the backplane attached to the port.
- SGPIO: The controller firmware uses Serial General Purpose Input/Output (SGPIO) to communicate with the backplane attached to the port
- UBM: The controller firmware uses Unified Backplane Management (UBM) protocol to communicate with the backplane attached to the port.

© 2021 Microchip Technology Inc. and its subsidiaries

- VPP: The controller firmware uses the Virtual Pin Port (VPP) protocol to communicate with the backplane attached to the port.
- Direct-Attached Cable: The controller firmware uses the direct-attached cable protocol to communicate with direct attached drives. User needs to provide the number of targets (drives) that matches the direct attached cable's capabilities. If the number of targets is not configured correctly, target drives may not get discovered.

Note:
If the port discovery protocol is not configured correctly, some features of the backplane may not function as expected. A reboot is required for the new port discovery protocol to take effect.

Note:
In maxView, the Backplane Discovery Protocol related properties are displayed both at connector and controller level.

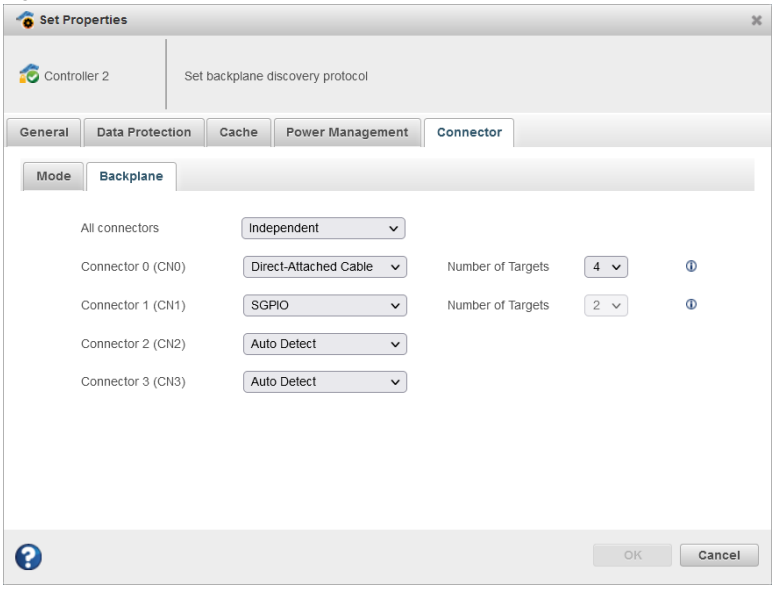
To change the backplane discovery mode protocol settings:

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 backplane setting of each of the connector to Independent, SGPIO, VPP, UBM, or Direct-Attached Cable. You can also change the backplane setting of all the connectors of that controller by selecting the mode from "All connectors" drop-down list.



The Connector tab displays only those connectors that supports the backplane discovery mode.

4. Click **OK**.
5. Reboot the server.

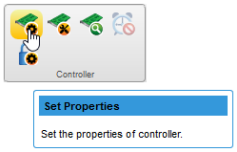
9.9.5 Changing the Expander Minimum Scan Duration Settings

Some expanders do not scan the drives on time for the firmware to discover them. Once the controller is up, the logical device may be marked as failed. To overcome this situation, the firmware has added a new configurable value of minimum scan duration (in seconds) that will force the firmware to stop and wait during discovery.
Whenever the Expander Scan Duration value is changed, it will take affect on the next power cycle. The controller waits for the specified duration and then scans/discovers the drive attached to the expander.

To change the expander minimum scan duration settings:

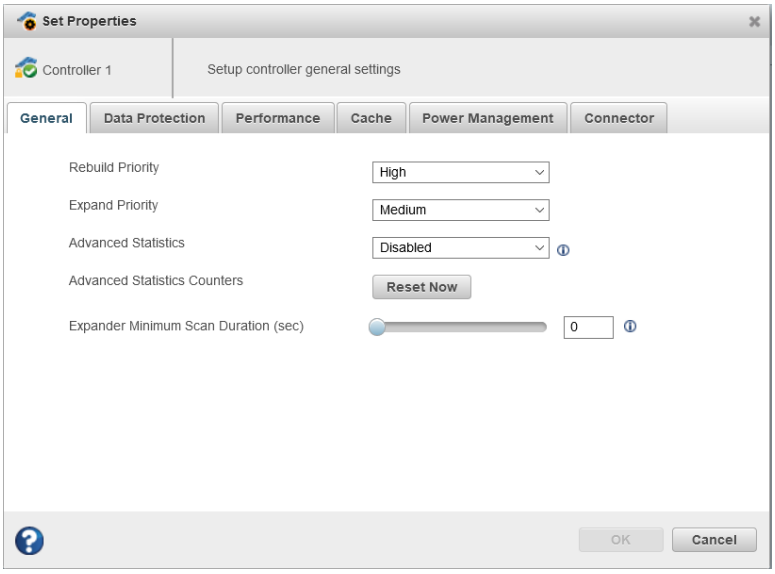
1. In the Enterprise View, select a controller.

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



The **General** tab on the Set Properties window opens.

3. To specify the waiting time for the controller, slide through the bar next to the Expander Minimum Scan Duration field.



When the Expander Minimum Scan Duration setting is changed, the power cycle warning is displayed.

4. Click **OK**.
The value of Expander Scan Duration gets displayed in the Properties tab of the controller.

9.10 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 manufactures, 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 9.10.1 Before You Begin, then follow one of these sets of instructions:

- 9.10.2 Updating the Controller Firmware
- 9.10.3 Updating the Disk Drive Firmware
- 9.10.4 Updating the Enclosure Firmware

9.10.1 Before You Begin

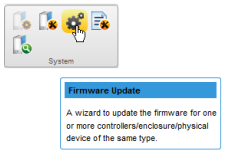
Before you begin, download the latest firmware images from www.adaptec.com, or from your vendor's support site on the World Wide Web. Controller images come in sets of one or more files and have a `.bin` file extension. Disk drive and enclosure image file names vary by manufacturer.

9.10.2 Updating the Controller Firmware

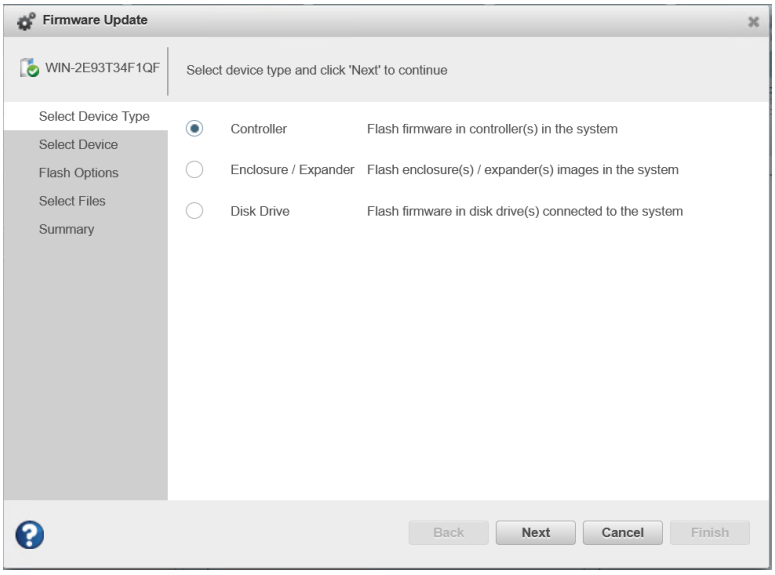
Use the Firmware Update wizard to update the firmware for one or more controllers of the same type on the local or a remote system.

To update the controller firmware:

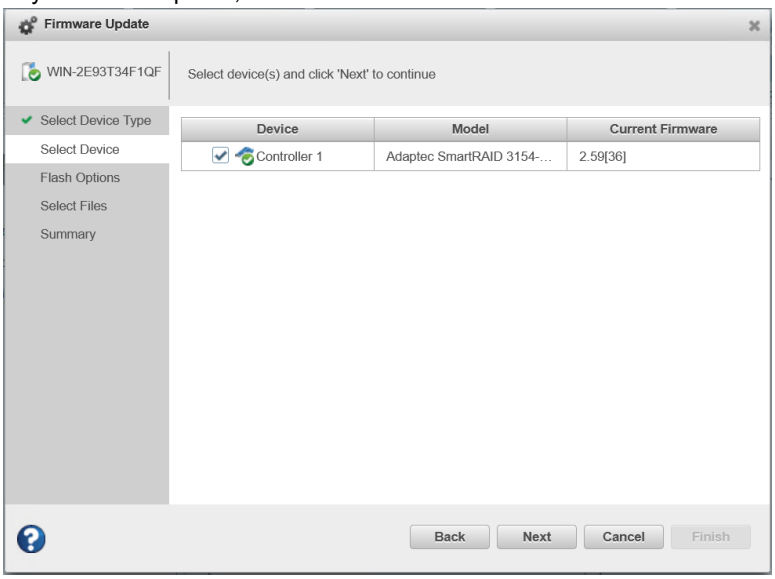
1. In the Enterprise View, select a system.
2. On the ribbon, in the System group, click **Firmware Update**.



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

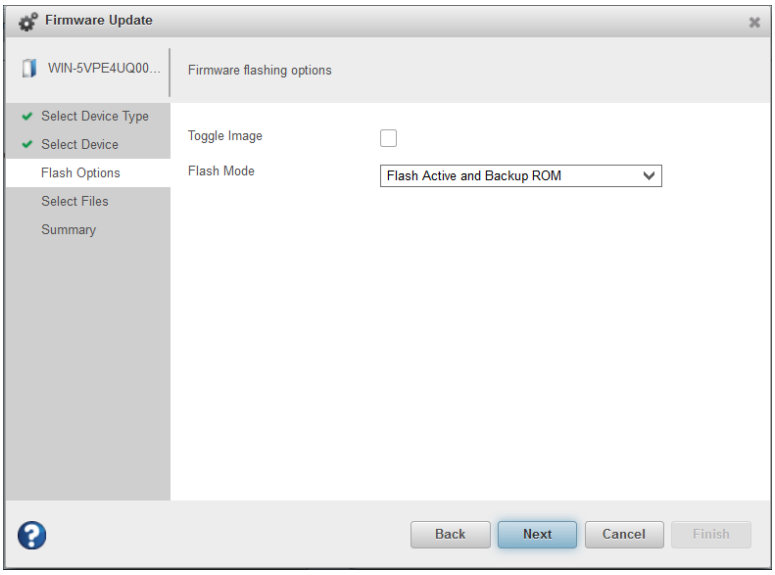


4. Select the controllers you want to update, then click **Next**.

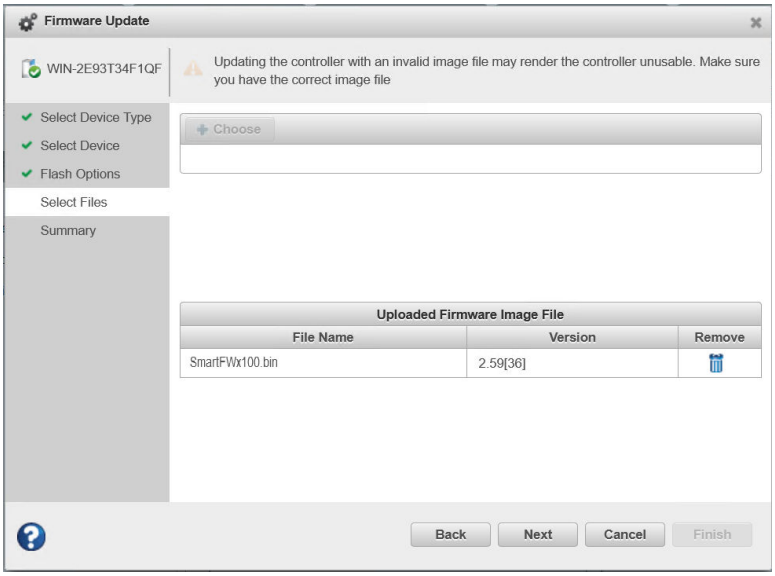


5. Select flash options for the update, then click **Next**. Choose Toggle Image to replace the active image with the backup image.

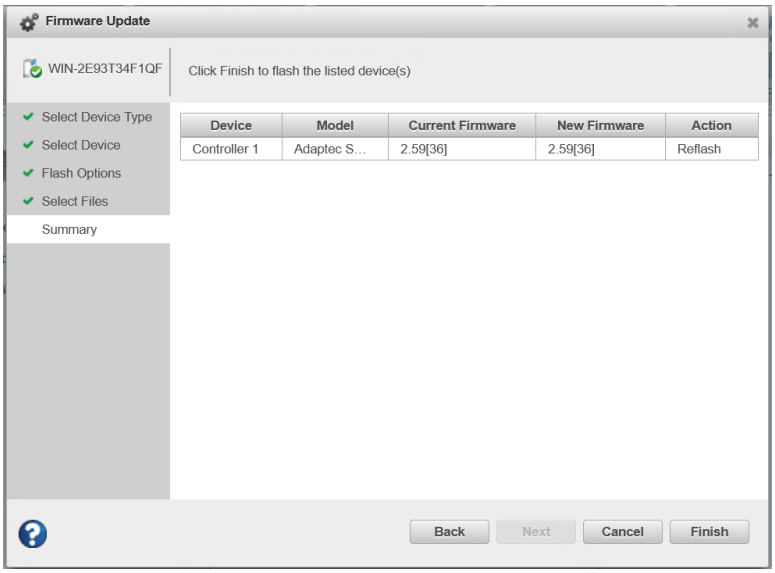
   Note: If you choose Toggle Image, Step , Select Files 6, is skipped.



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

9.10.3 Updating the Disk Drive Firmware

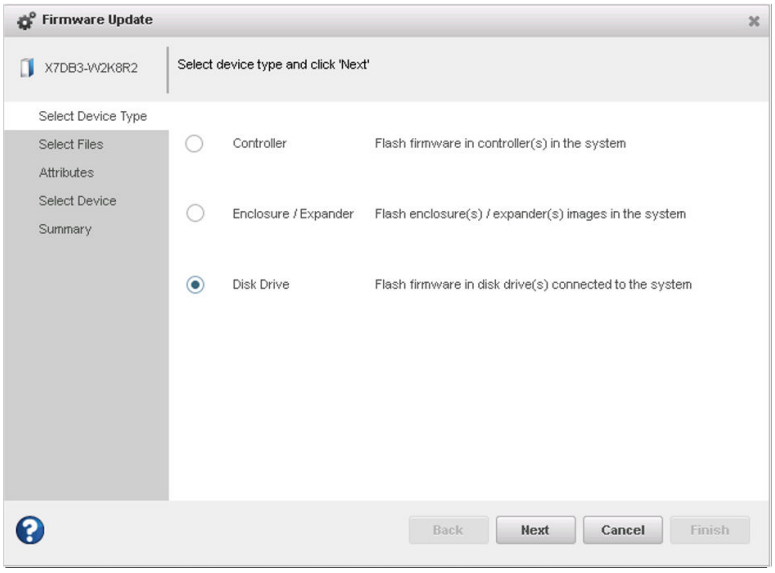
Use the Firmware Update wizard to update the firmware for one or more disk drives of the same type on the local or a remote system. The procedure is similar to updating the controller firmware (see 9.10.2 Updating the Controller Firmware).

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.

9.10.4 Updating the Enclosure Firmware

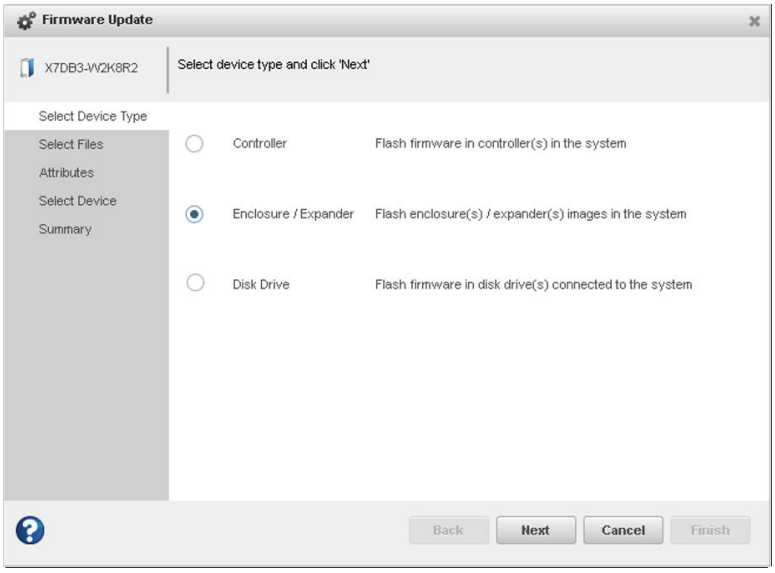
Use the Firmware Update wizard to update the firmware for one or more enclosures or expanders of the same type on the local or a remote system.

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.

10. Monitoring Status and Activity

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

10.1 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 10.2.1 Viewing Activity Status in the Event Log and 10.5 Changing an Operating System's Event Log Setting.
- **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 10.2.2 Viewing Task Status in the Task Log.
- **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 10.2.3 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 10.2.4 Viewing Storage Space Usage in Chart View.
- **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 10.3 Notifying Users by Email About Status and Activity .
- **Advanced Statistics**—You can set maxView Storage Manager to log advanced I/O and usage statistics for the RAID controllers in your system.
  See 10.4 Monitoring Advanced Statistics about Activity in Your Storage Space.
- **Audible Alarm**—A series of beeps sounds whenever a serious event occurs on your storage space.

10.2 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 10.5 Changing an Operating System's Event Log Setting.) 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.

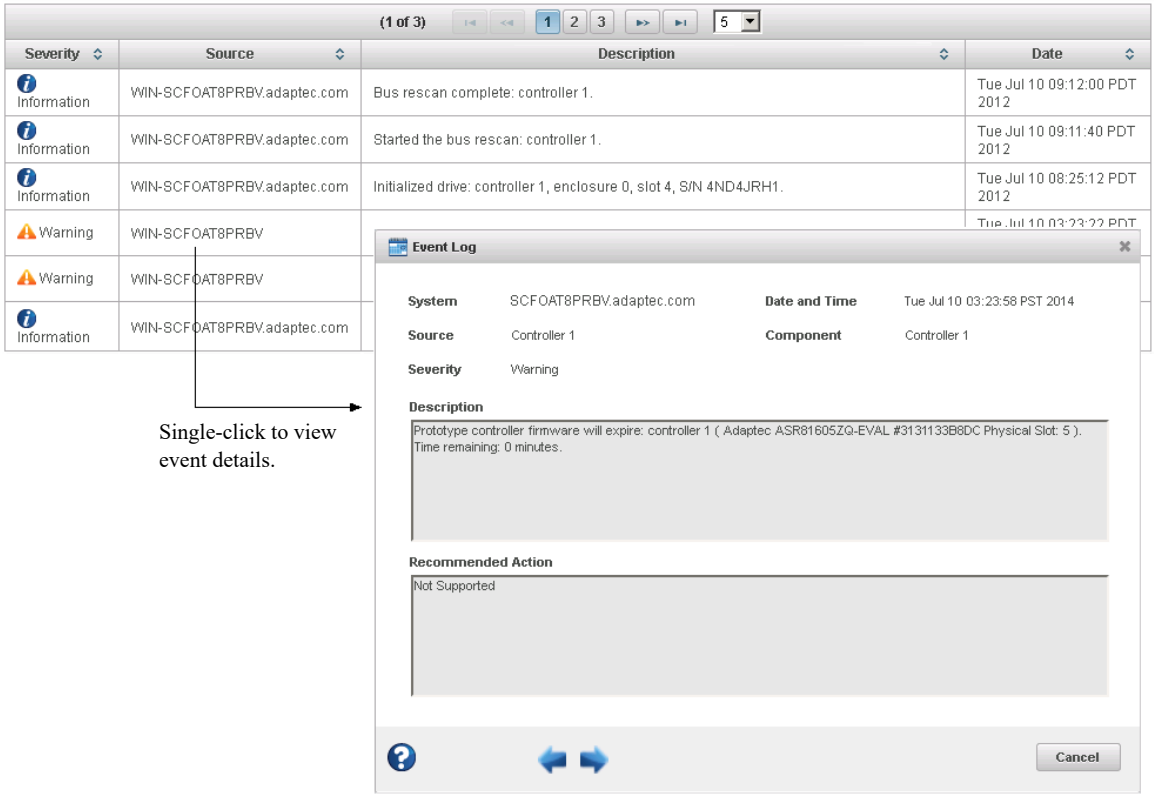
10.2.1 Viewing Activity Status in the Event Log

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 10.2.1.1 What Do the Event Status Icons Mean?) 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 10.2.3 Viewing Component Status in the Storage Dashboard).

© 2021 Microchip Technology Inc. and its subsidiaries

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.

10.2.1.1 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.

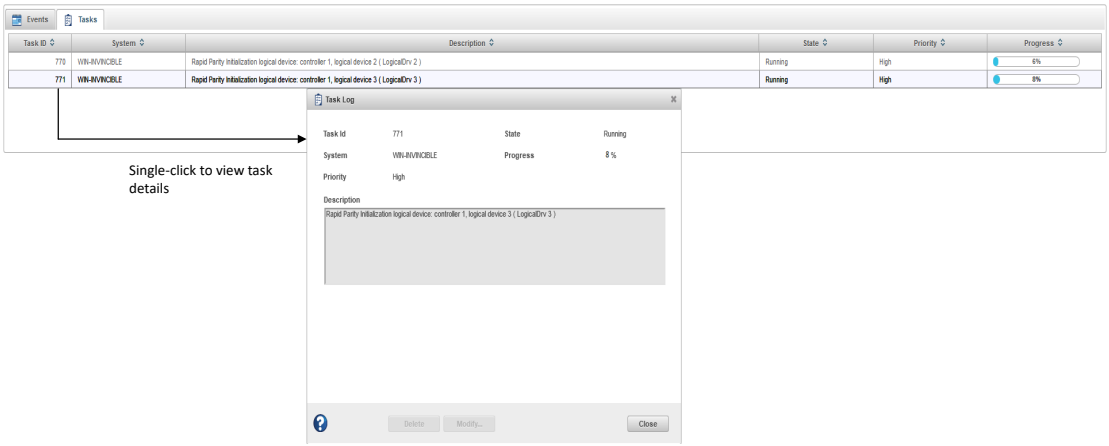
Icon	Status	Examples
	Information	The local system successfully connected to a remote system. A logical drive was created. A hot spare was deleted.
	Warning	A logical drive is in a degraded state. A disk drive is being rebuilt. A controller is not responding to an enclosure.
	Error	A controller has failed. 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 9.9 Working with Controllers for more information.

10.2.2 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.

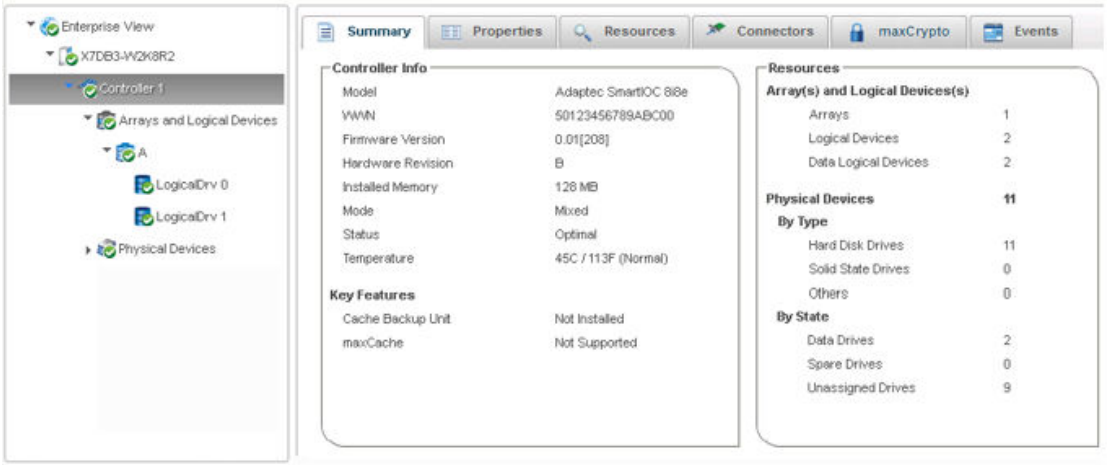


10.2.3 Viewing Component Status in the Storage Dashboard

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 10.2.1 Viewing Activity Status in the Event Log).

Note: For information about Chart View, on the right side of the Storage Dashboard, see 10.2.4 Viewing Storage Space Usage in Chart View.



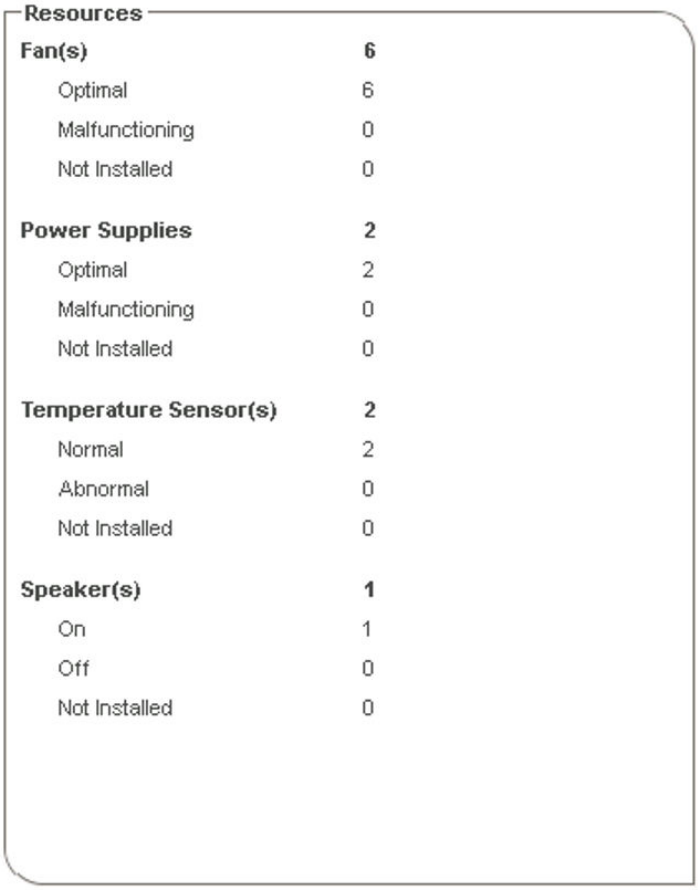
The following table lists the categories and types of information provided on the Storage Dashboard for each component in your storage space. All top-level nodes in the Enterprise View (System, Controller, Arrays, Logical Drives, Physical Devices, and so on) include a Summary tab and Events tab.

Component	Categories/Tabs	Examples
System	Summary Properties	System name and IP address Operating system Number and type of controllers Alarm status Web Server settings SMTP settings
Controller	Summary Properties Resources Connectors maxCrypto	Model, key features, manufacturing data, driver and firmware version, controller mode, and status Number of physical drives, arrays, logical drives, and status Power management features I2C address for PBSI interface (hex), I2C clock speed and clock stretching status maxCache status maxCrypto status (see 8.1.3 Checking maxCrypto Status) Health and activity of flash backup module, if present ("Green backup" status) Connector functional mode Performance optimizations and other settings Physical drive assignments by logical device (see 3.5 Revealing More Device Information)
Arrays	Summary Resources	Total size and unused size Spare rebuild mode Logical drive RAID level, size, status
Logical drives and maxCache Device	Summary Resources	Raid level, segment and group (RAID 10 only), size, mount point, status Member drives and sizes
Enclosure	Summary Resources Slots	Enclosure type, vendor, model and status Fan, power supply, and temperature status (see 10.2.3.1 Monitoring Enclosure Status) Speaker status Slot allocation and usage
Hard drives and SSDs	Summary Resources SMART Statistics	Drive type (hard drive, SSD, SMR), interface type (SAS/SATA), vendor, and model Drive state (Ready, Optimal, Hot Spare), mount point Channel number and device ID Transfer speed Drive segment allocation SMART statistics (see 10.2.3.2 Viewing SMART Statistics)

© 2021 Microchip Technology Inc. and its subsidiaries

10.2.3.1 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.



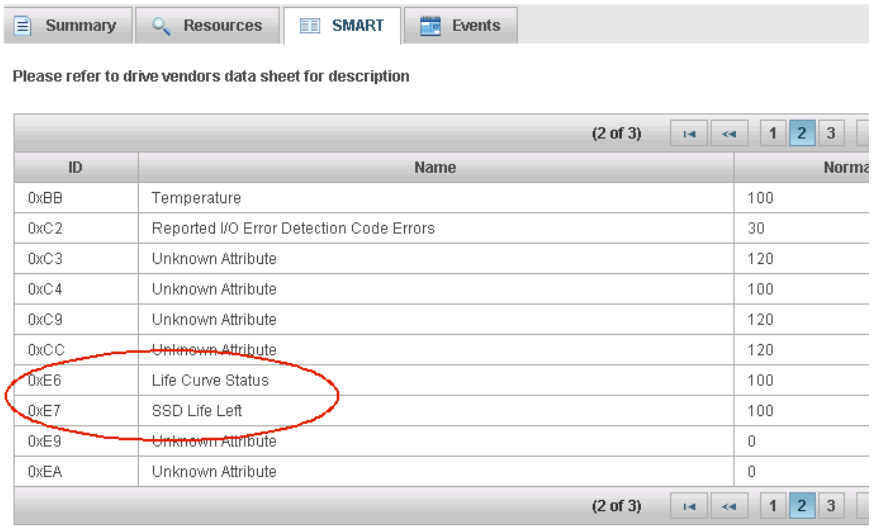
10.2.3.2 Viewing SMART Statistics

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 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.

© 2021 Microchip Technology Inc. and its subsidiaries

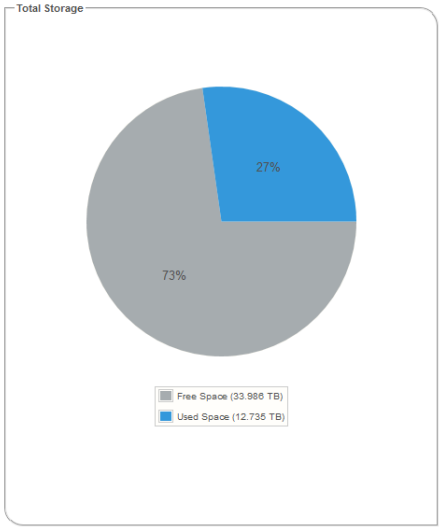
SSD wear-level and longevity indicators



10.2.4 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.



10.3 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.

© 2021 Microchip Technology Inc. and its subsidiaries

Follow the instructions in this section to:

- Set up email notifications (see 10.3.1 Setting Up Email Notifications).
- Send a test email (see 10.3.2 Sending a Test Message).
- Modify or remove an email recipient (see 10.3.3 Modifying or Removing an Email Recipient).
- Modify email server settings (see 10.3.4 Modifying Email Server Settings).
- Disable email notifications (see 10.3.5 Disabling Email Notifications)

10.3.1 Setting Up Email Notifications

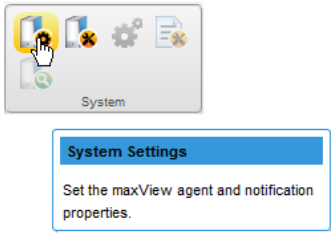
This section describes how to set up email notifications for one system. If you want to monitor multiple systems by email, you must complete the tasks in this section for each one separately.

Before you begin, note this information:

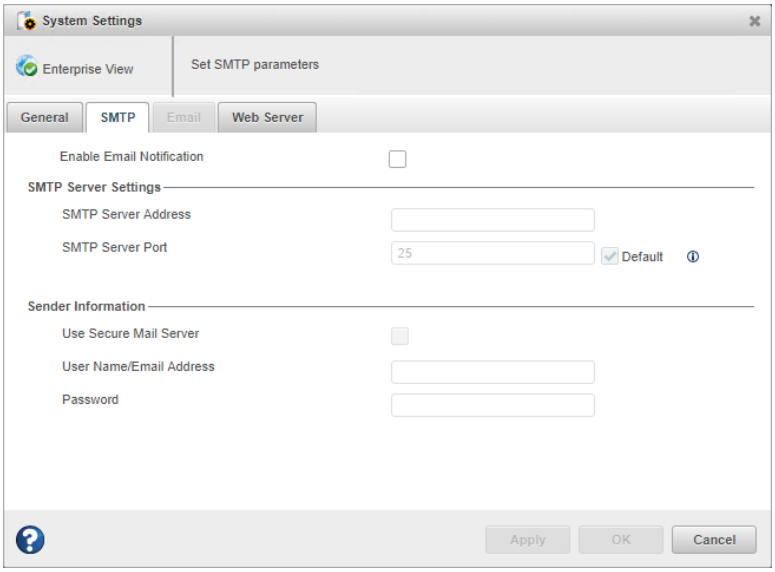
- The address of your Simple Mail Transfer Protocol (SMTP) server (host name and domain, or TCP/IP address)
- The email address of each person who will receive email notifications

To set up email notifications:

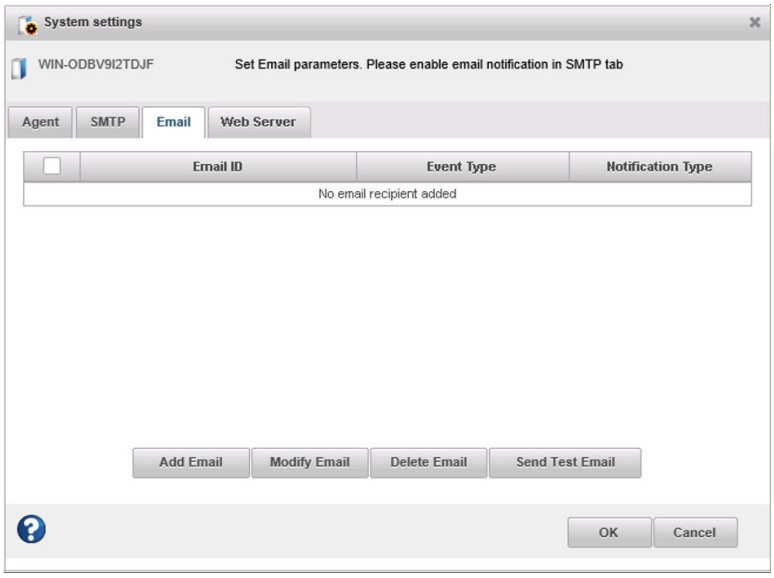
1. Select the Enterprise View node.
2. On the ribbon, in the System group, click **System Settings**.



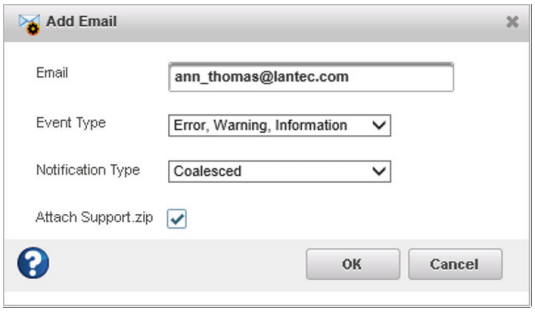
3. When the System settings window opens, click the **SMTP** tab.
4. Select **Enable Email Notifications**.
5. Enter the IP address of your SMTP server and the server's port number (or use the default port).



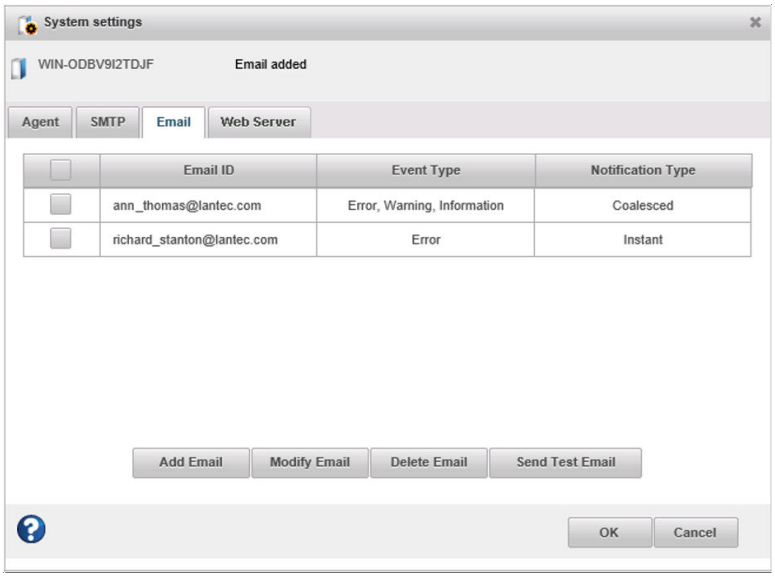
6. If authentication is enabled on your SMTP server (that is, the server requires authentication details before it will send messages to users), select **Use Secure Mail Server**, then enter the SMTP server's login credentials (username/password) in the space provided.
7. On the System settings window, 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 10.2.1.1 What Do the Event Status Icons Mean?; for more information about the support archive file, see 12.5 Creating a Support Archive File.)



Repeat this step to add more email recipients.
Each recipient appears in the Email Notifications Manager, as shown below:



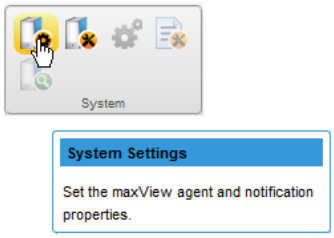
9. When you're done adding email recipients, click **OK**.
   The email recipients and your SMTP server settings are saved.
10. Repeat the steps in this section *for each system* you want to monitor with email notifications, then continue by sending test messages to all recipients (see 10.3.2 Sending a Test Message).

10.3.2 Sending a Test Message

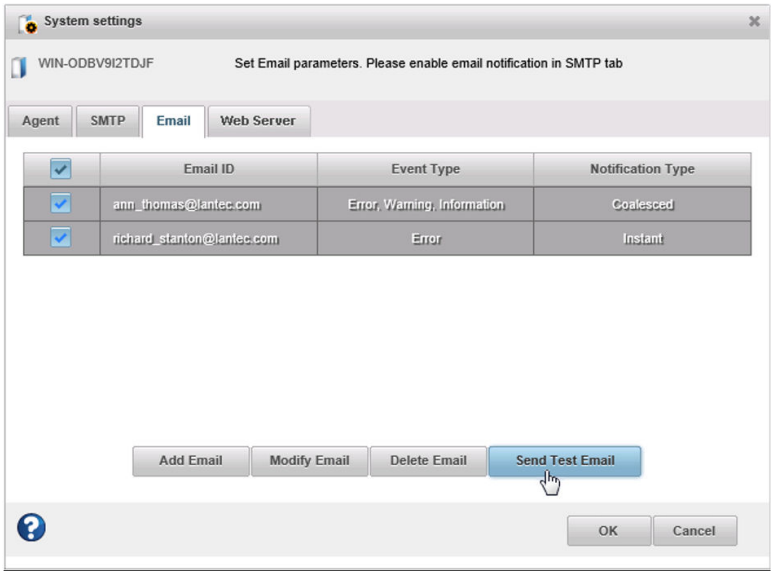
To ensure that an email recipient is receiving event notifications, you can send them a test message.

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.



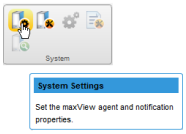
5. Click **Send Test Email**.
   If the test is successful, the email recipient(s) receive the test message. If the test fails:
   - Ensure that the recipient's email address is correct. (See 10.3.3 Modifying or Removing an Email Recipient .)
   - Ensure that your SMTP server address is correct. (See 10.3.4 Modifying Email Server Settings.)
   - Try sending the test message again.

10.3.3 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**.



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.

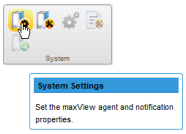
10.3.4 Modifying Email Server Settings

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.

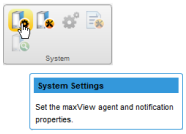
10.3.5 Disabling Email Notifications

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.

10.4 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.

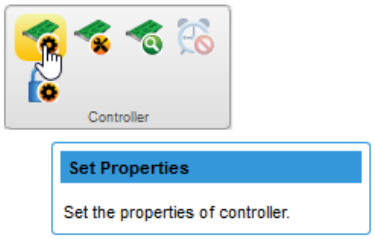
Follow the instructions in this section to:

- Enable statistics logging on a controller (see 10.4.1 Setting up Statistics Logging).
- View the advanced statistics for a controller, hard drive, SSD, logical drive, or maxCache Device (see 10.4.2 Viewing Advanced Statistics).
- Reset the statistics counters (see 10.4.3 Resetting the Statistics Counters).

10.4.1 Setting up Statistics Logging

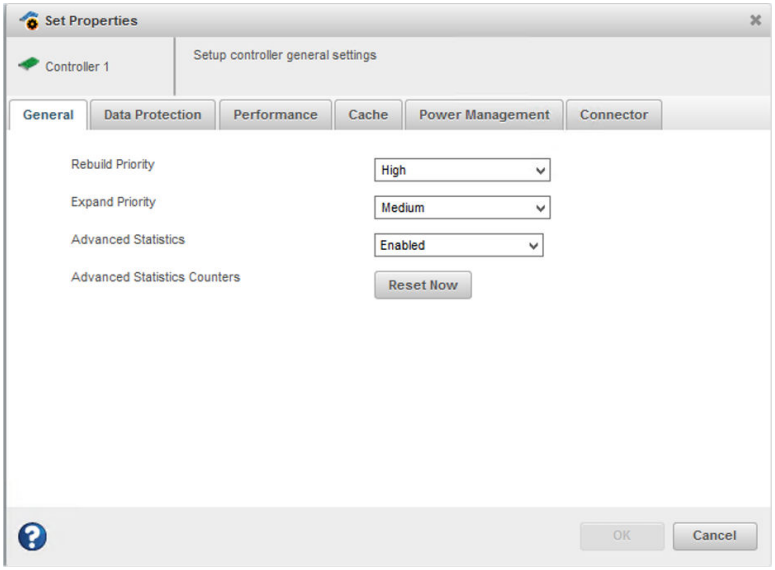
To set up statistics logging for the controllers in your storage space:

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.

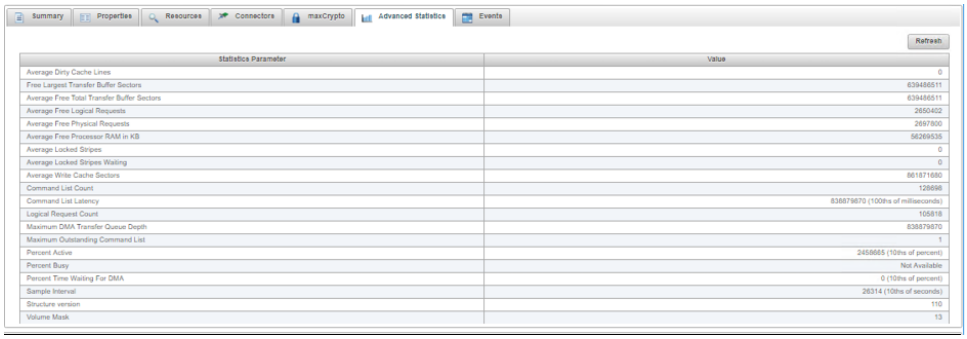
3. In the Advanced Statistics drop-down list, select `Enabled`.



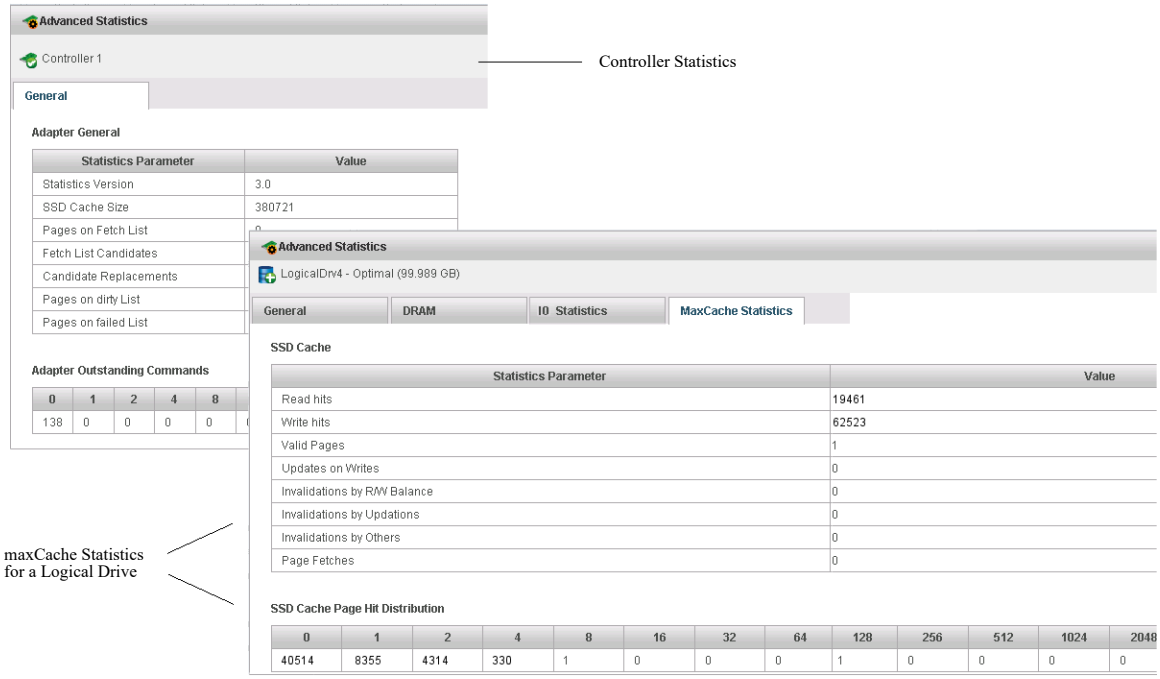
4. Click **OK**.

10.4.2 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 20. Advanced Statistics Descriptions 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.

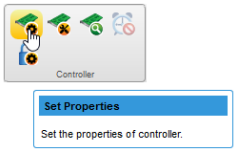


10.4.3 Resetting the Statistics Counters

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**.



The Set Properties window opens.

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



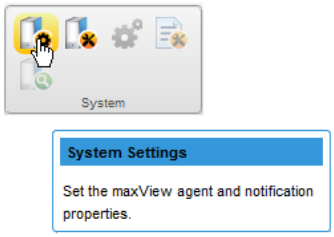
The statistics counters are reset.

10.5 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.

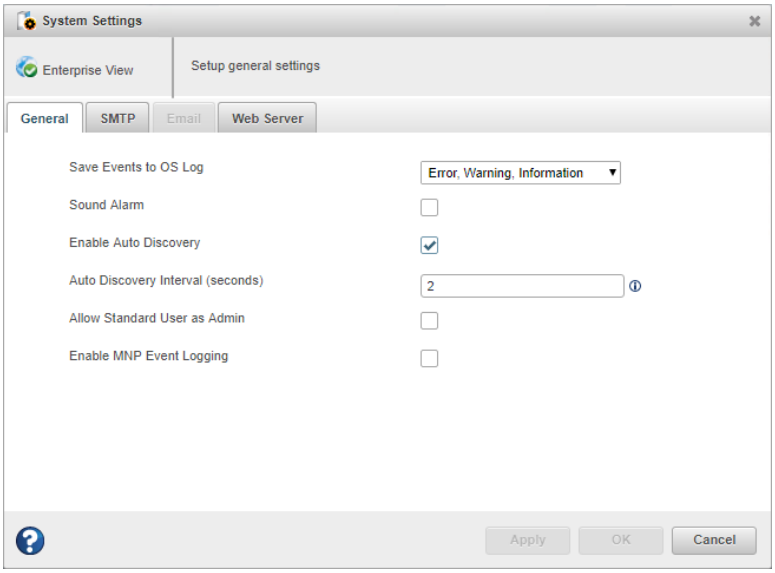
To change or disable operating system event logging on a system:

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



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.

11. 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

11.1 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 *sever 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.

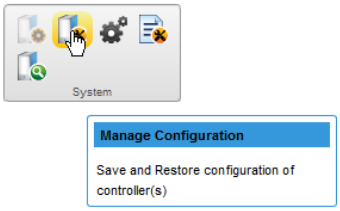
The following sections provide details on each of these steps.

11.1.1 Creating a Server Template File

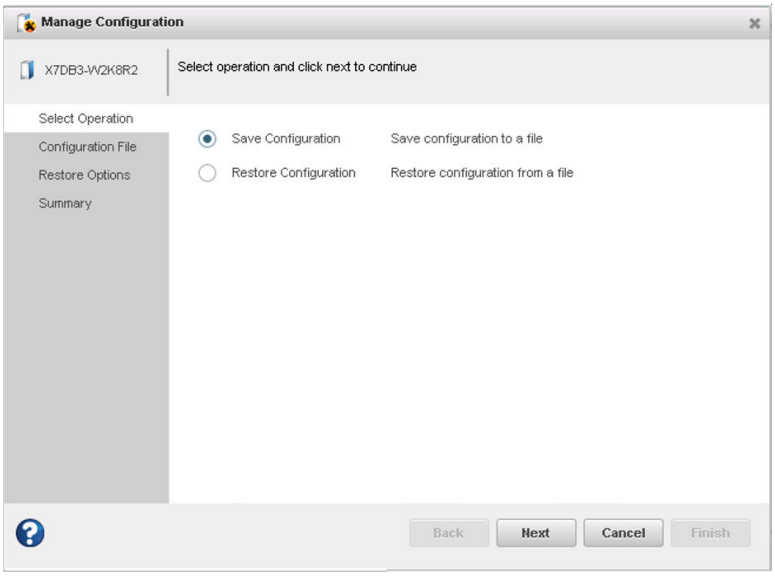
This procedure saves the configuration of a system that you want to use as a model for other servers in your storage space. It creates a server template file in XML format, which defines the controller type(s), operational settings, physical drive size, logical drive size, RAID level, and more. The default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



   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.

11.1.2 Duplicating the Server Template

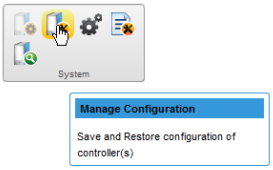
When you are ready to duplicate the server template on other systems in your storage space, you can restore the configuration from the server template file.

Keep in mind that:

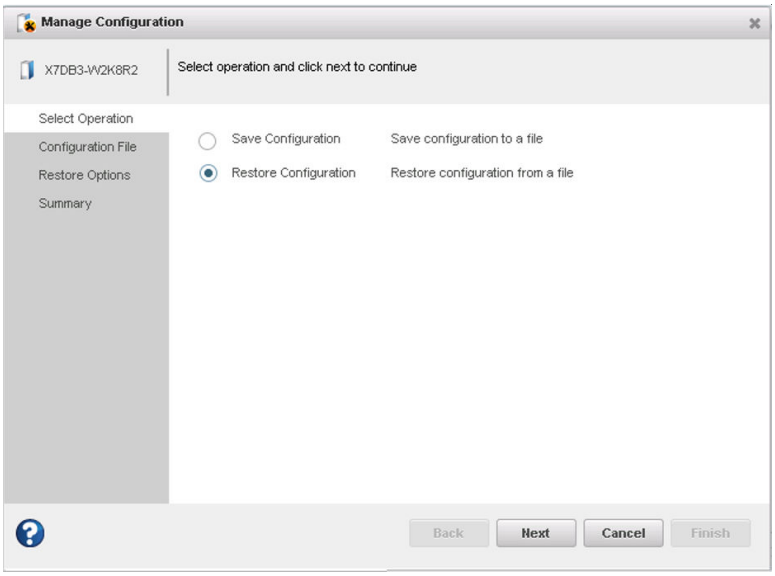
- The server template file (default, `ControllerConf.xml`) is editable. For example, you may need to change the disk drive capacity or logical drive size to accommodate the differences on each machine.
- Drives from the same vendor with slightly different capacities (147 GB vs. 150 GB, for instance) 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:

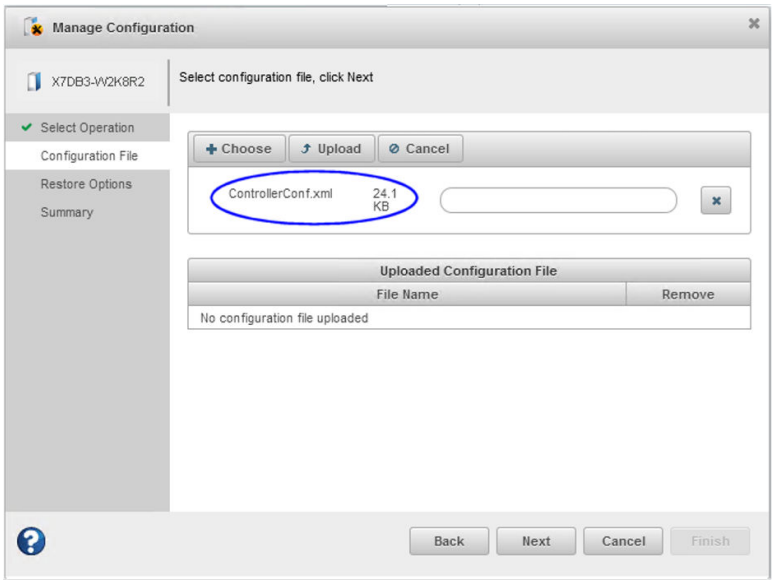
1. In the Enterprise View, select a system.
2. On the ribbon, in the System group, click **Manage Configuration**.



   The Manage Configuration wizard opens.
3. Select **Restore Configuration**, then click **Next.**

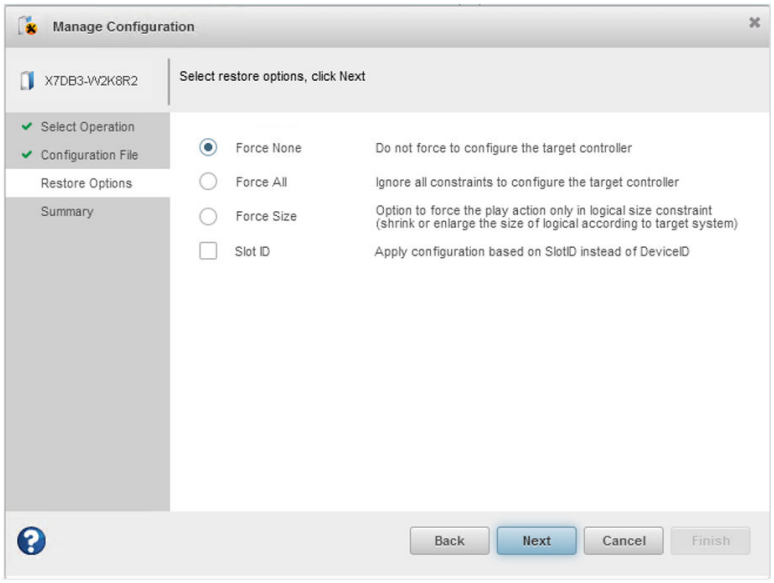


4. In the Configuration File panel, click **Choose**, navigate the file system to your server template file, then click **Open**. When the file name appears in the "selected file" area (circled in blue in figure below), click **Upload**, wait for the upload to complete, then click **Next**.



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:

Option	Description
Force All	To force deployment of all features
Force Size	To force deployment of just the logical drives

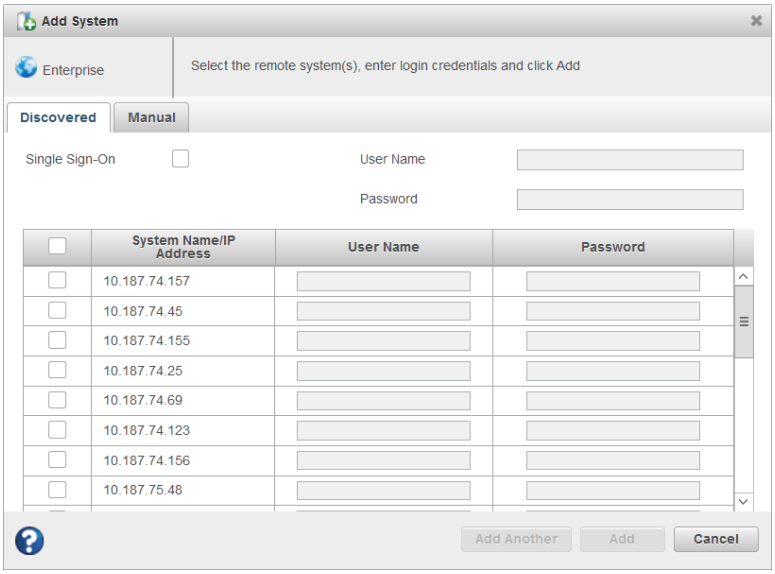


6. To apply the configuration based on SlotID rather than DeviceID, click the **Slot ID** check box.
7. Click **Next**, review the summary information, then click **Finish**.
   maxView Storage Manager duplicates the system configuration on the new controller.

11.2 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.



11.2.1 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

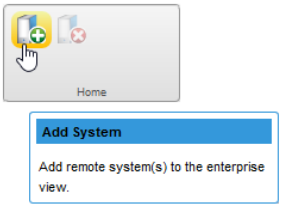
maxView Storage Manager. You can work with a remote system's controllers, disk drives, and logical drives as if they were part of your local system.
Note: The wizard adds all selected systems to the Enterprise view even if login fails on some systems. For those systems, try running the wizard again with different login credentials.

11.2.2 Manually Adding a Remote System

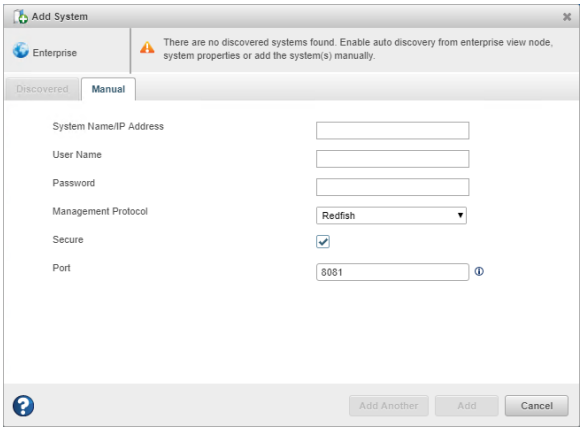
You can add a remote system manually if auto-discovery fails to find the system on your network.

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**.



   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.

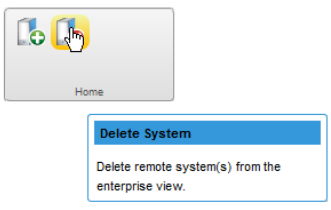
11.2.3 Removing a Remote System

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.

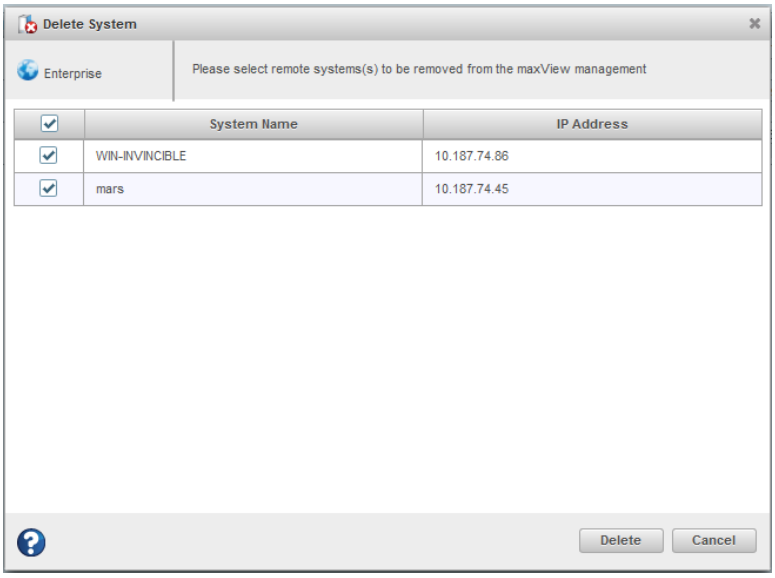
To remove a remote system:

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



   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.



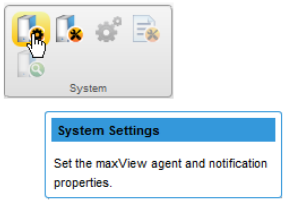
3. Click **Delete**.
   maxView Storage Manager removes the remote system(s) from the Enterprise View.

11.2.4 Changing the Auto-Discovery Settings

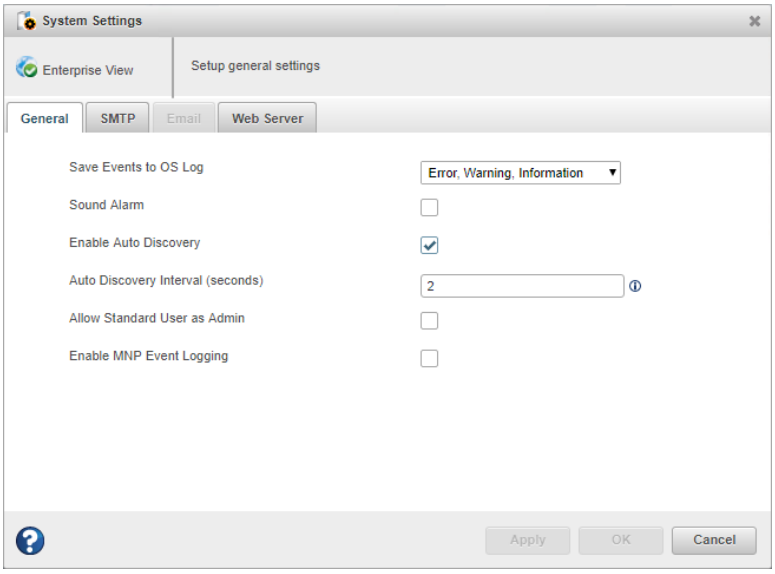
Auto-discovery, in maxView Storage Manager, is disabled by default. If enabled, the auto-discovery task runs in the background each time maxView Storage Manager is started. You can enable the auto-discovery if desired, and configure the auto-discovery settings described below.

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.

11.2.5 Importing and Exporting Remote Systems

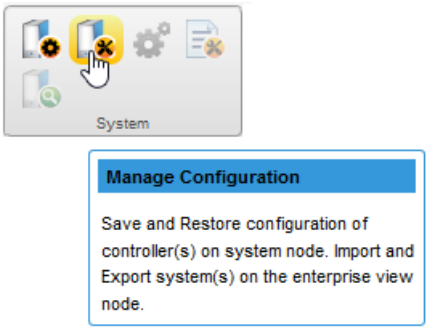
maxView provides the 'Import and Export systems' feature to add multiple systems and export the added systems in "SystemConf.json" file, which can be used later to import the added systems in maxView running on another system.

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.

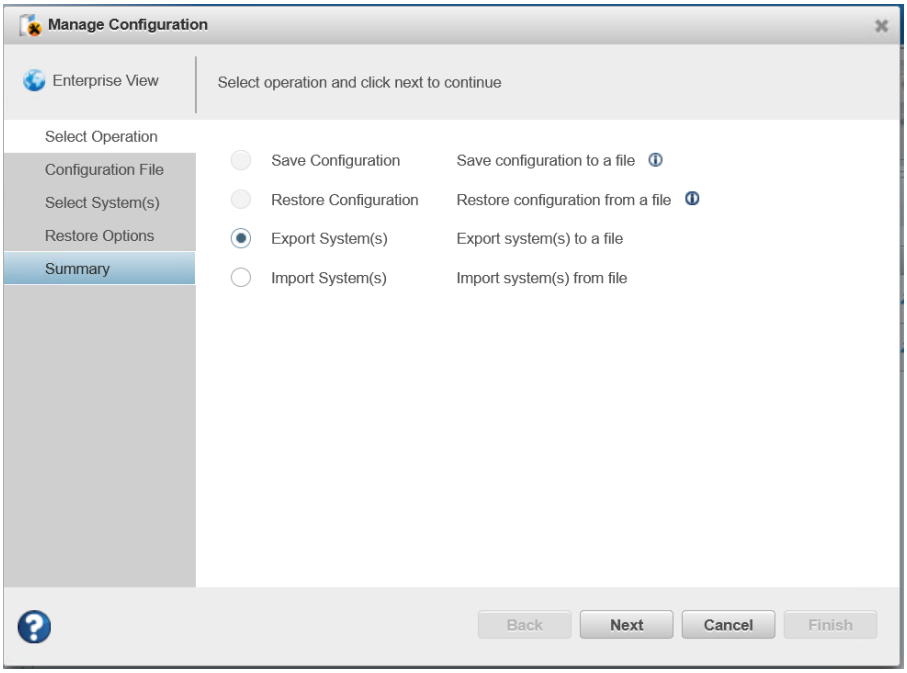
To export a system:

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

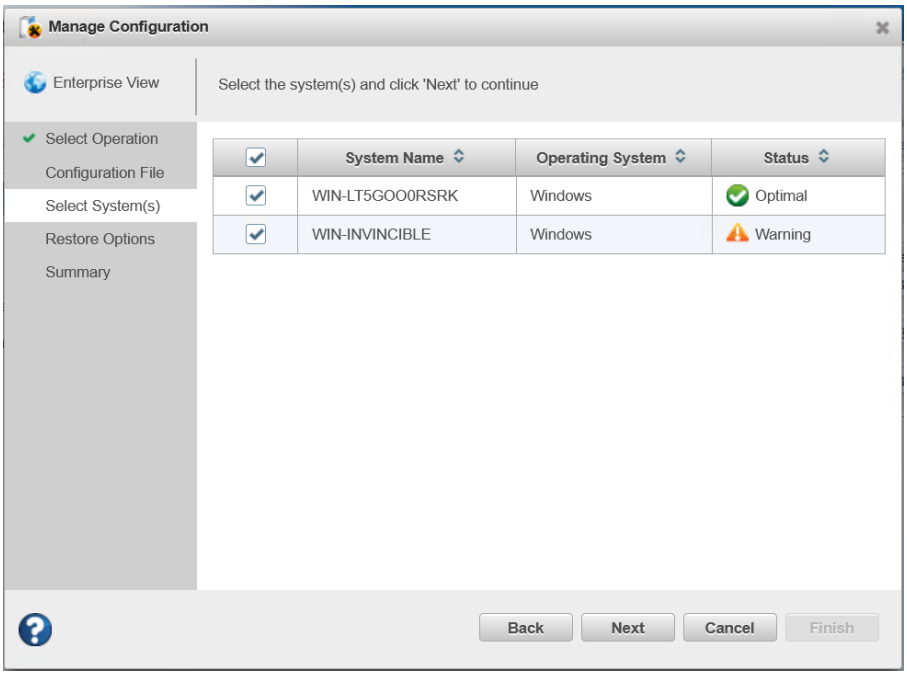


The Manage Configuration wizard opens for that system.

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.

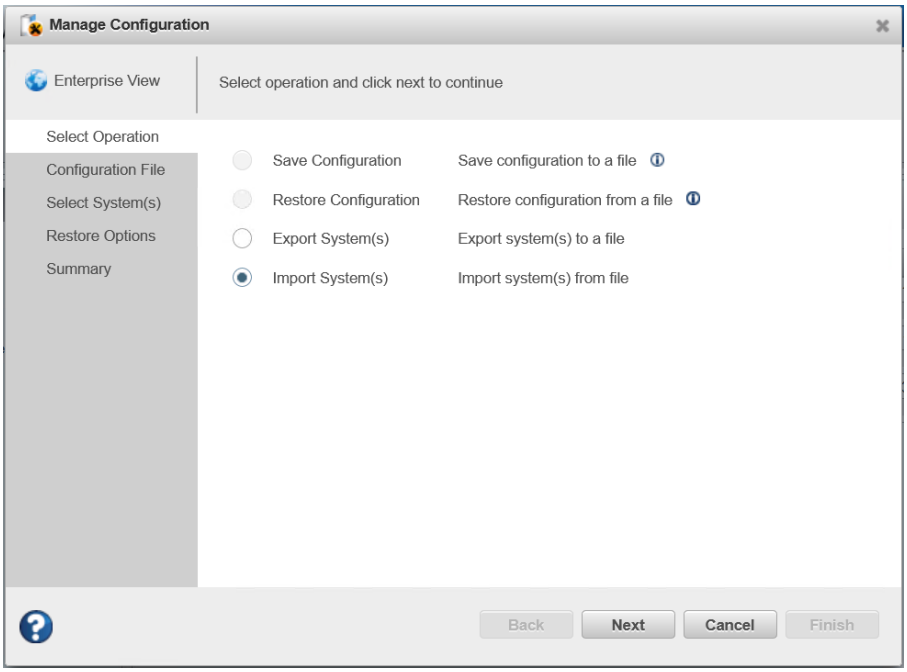
To import a system:

1. Select the Enterprise View node.

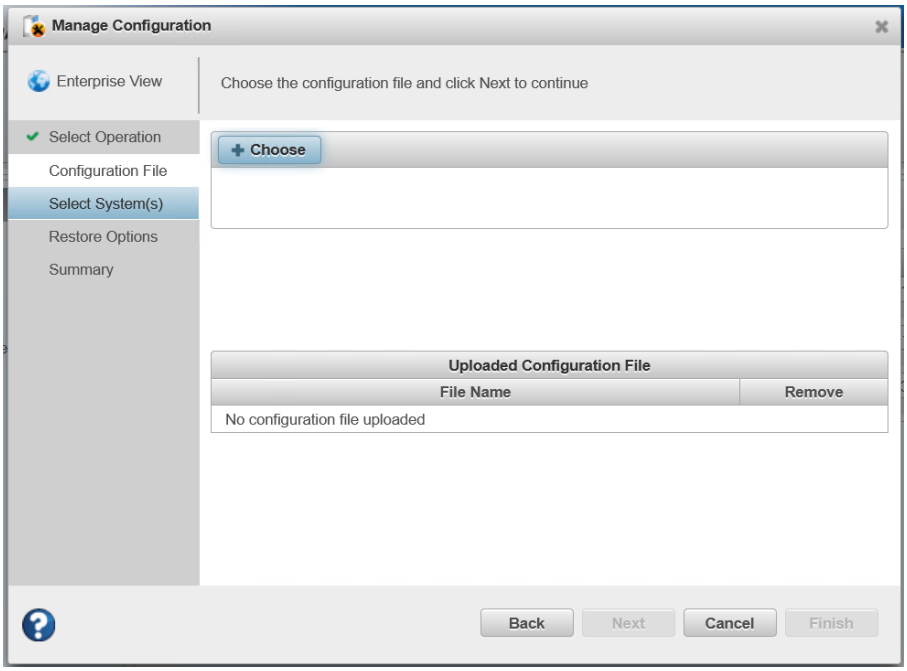
2. On the ribbon, in the System group, click **Manage Configuration**.

   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.



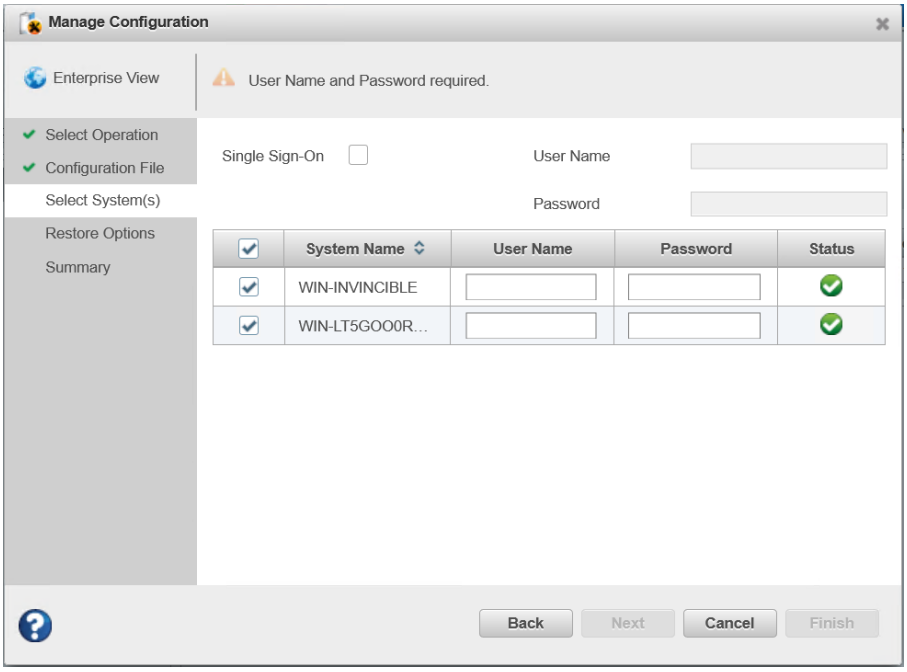
   The file gets uploaded under "**Uploaded Configuration File**" field.

5. Click **Next**.

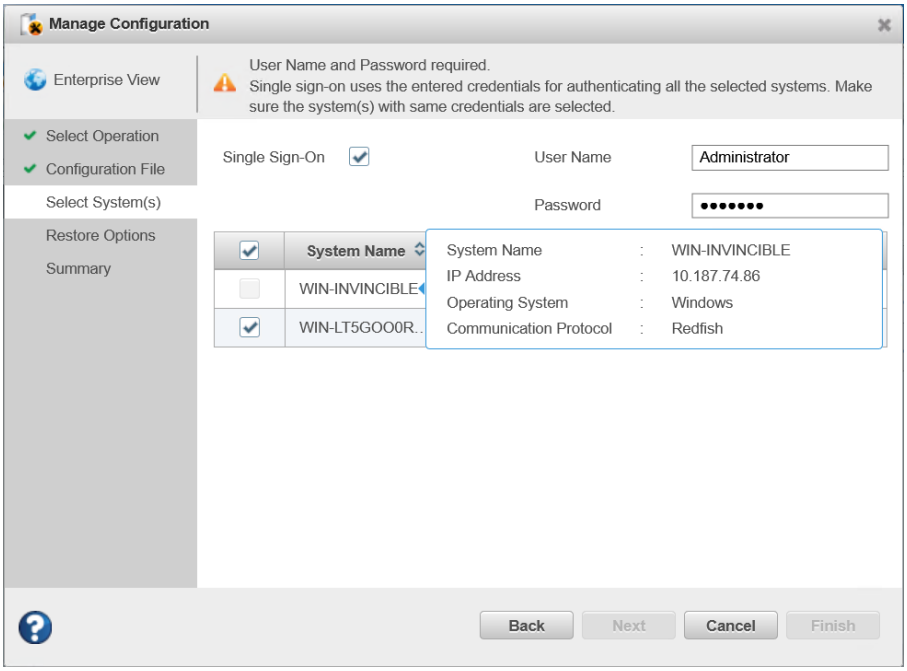
   The **Select Systems** screen appears.

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.

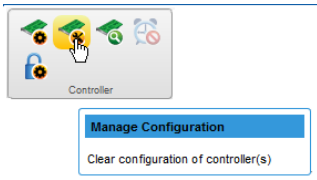
11.3 Clearing the Controller Configuration

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.

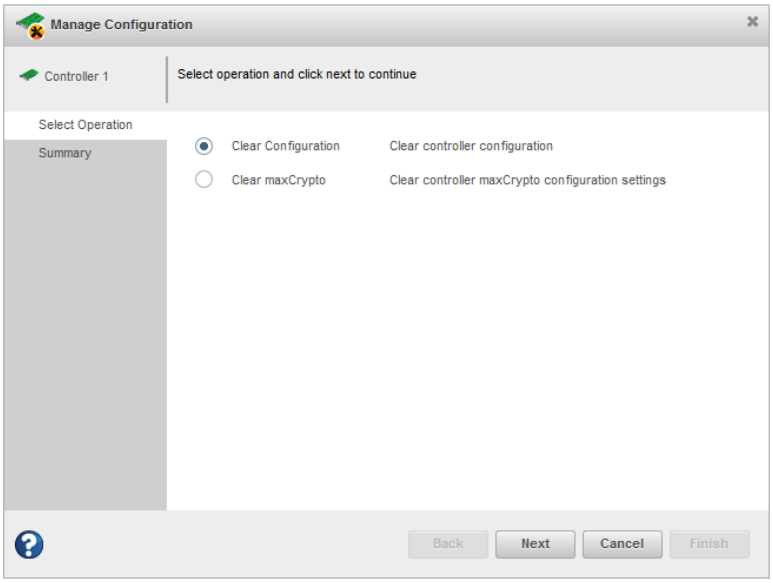
To clear the controller configuration:

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**.

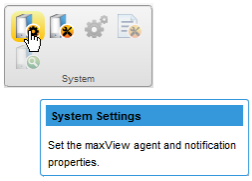
11.4 Changing the Web Server Port

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.

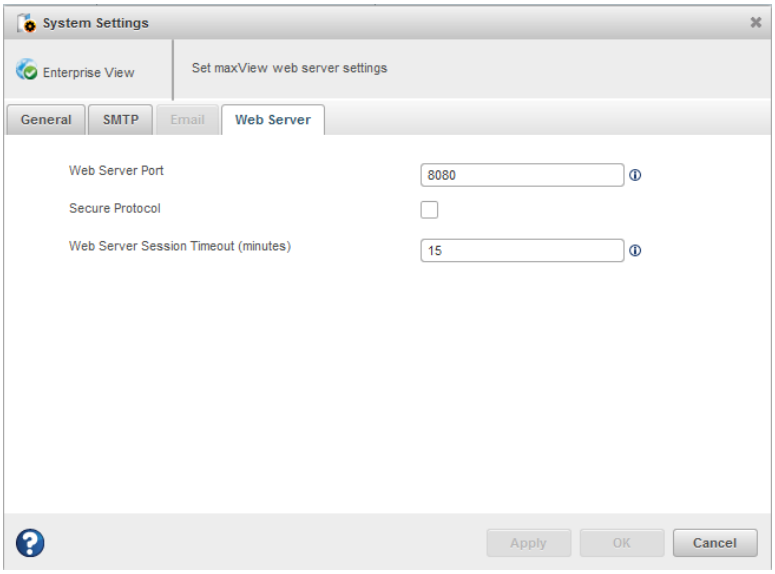
To change the Web Server port:

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

© 2021 Microchip Technology Inc. and its subsidiaries



When the System Settings window opens, click the **Web Server** tab.



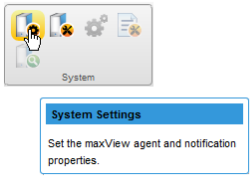
3. Enter the new Web Server port. Optionally, click **Secured Protocol** to enable/disable secure communication over https.
4. Click **Apply.**
5. Restart maxView Storage Manager.

11.5 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 3.2 Working in maxView Storage Manager). 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.

12. Solving Problems

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

12.1 General Troubleshooting Tips

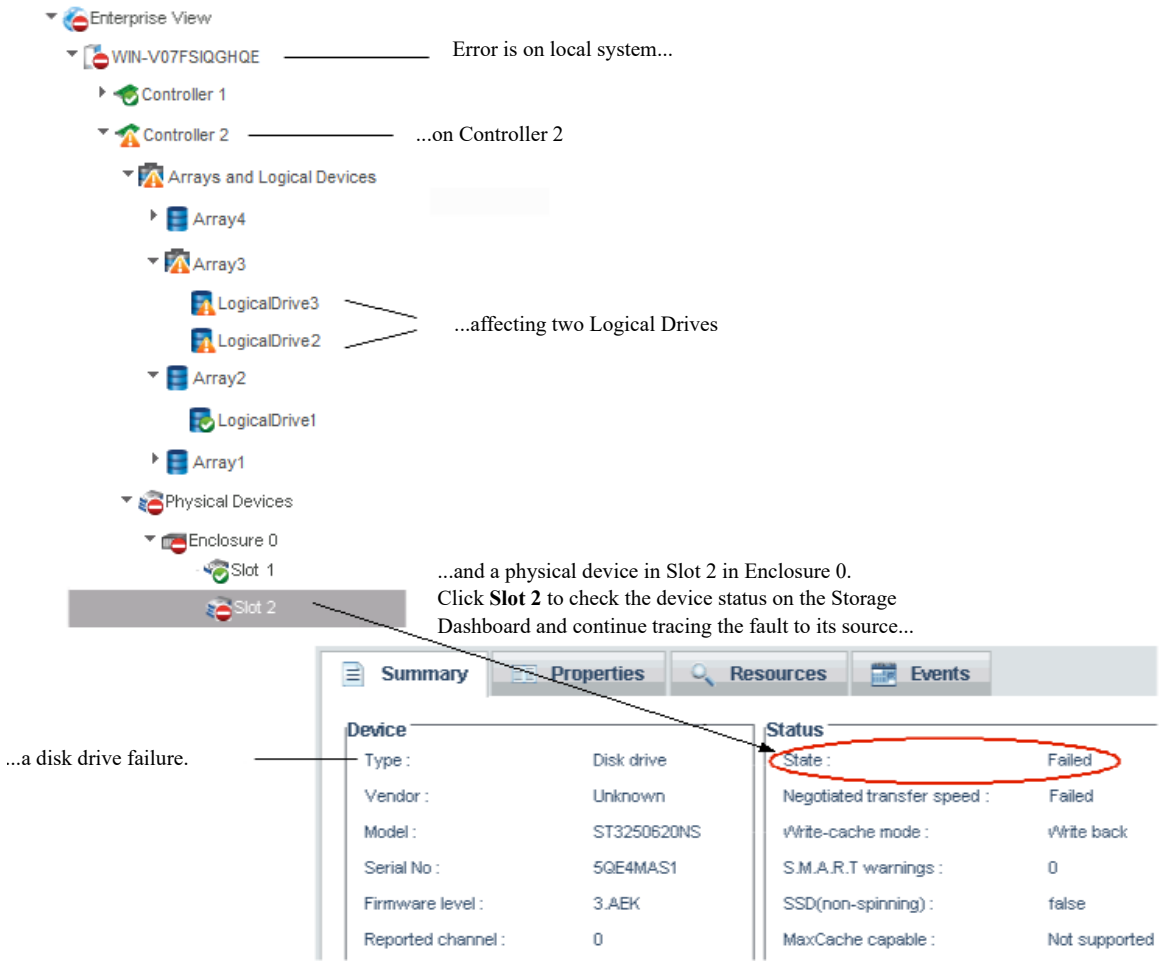
If you experience problems installing or using maxView Storage Manager, try these troubleshooting tips first:

- Ensure that all managed systems are powered on and that you are logged in to any remote systems that you want to manage. (See 4.3 Logging into Remote Systems from the Local System for more information.)
- Check all cable connections.
- Try uninstalling and reinstalling maxView Storage Manager.
- Check the Release Notes for compatibility issues and known problems.

12.2 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.



12.3 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 12.3.1 Failed Disk Drive Protected by a Hot Spare.
- If the logical drive is *not* protected by a hot spare, see Failed Disk Drive Not Protected by a Hot Spare.
- If there is a disk drive failure in more than one logical drive simultaneously, see 12.3.3 Failure in Multiple Logical Drives Simultaneously.
- If it is a RAID 0 logical drive, see 12.3.4 Disk Drive Failure in a RAID 0 Logical Drive.
- If multiple disk drives fail within the same logical drive, see 12.3.5 Forcing a Logical Drive with Multiple Drive Failures Back Online.

12.3.1 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 5. Protecting Your Data for more information about managing spares.

12.3.2 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 Drives.

12.3.3 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 Spare..

12.3.4 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".

© 2021 Microchip Technology Inc. and its subsidiaries

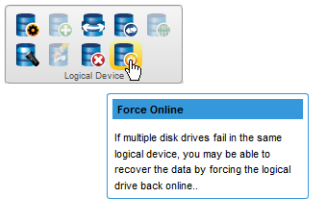
12.3.5 Forcing a Logical Drive with Multiple Drive Failures Back Online

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 12.2 Identifying a Failed or Failing Component).
2. On the ribbon, in the Logical Device group, click **Force Online**.



3. Click **Force**, then click **OK**.

12.3.6 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.

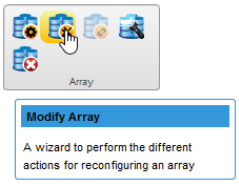
The Heal Array operation is part of the Modify Array wizard (see 6.6 Moving an Array). It is available in the wizard only if:

- 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.

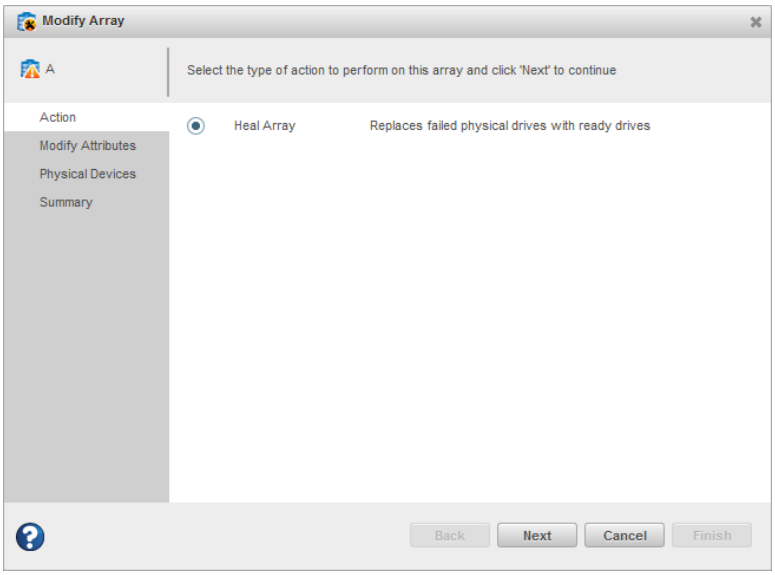
For a RAID 0 volume, the heal operation recreates the volume. For other RAID volume types, the heal operation rebuilds the volume.

To heal an array:

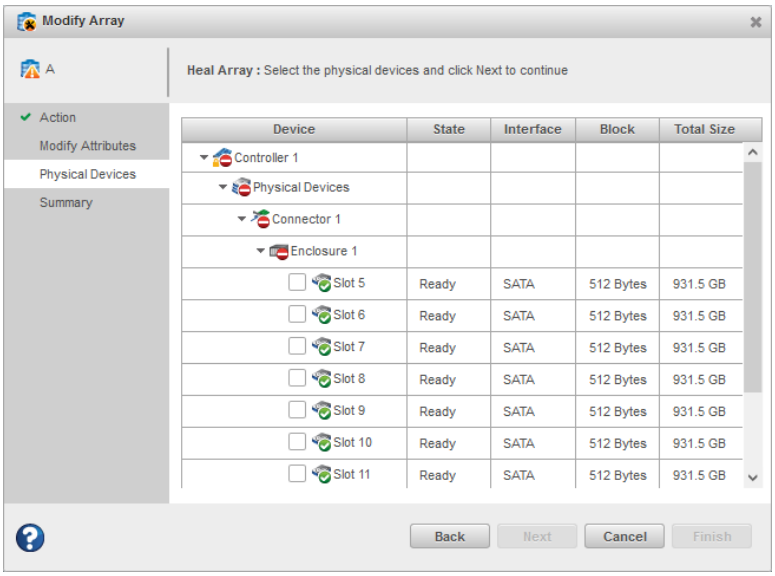
1. In the Enterprise View, select an array.
2. On the ribbon, in the Array group, click **Modify Array**.



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.



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

Note:
For details on SED support operations for healing array, see 4.6.2 Modify Array.

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

12.4 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 12.3.6 Healing an Array.

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.

© 2021 Microchip Technology Inc. and its subsidiaries

If necessary, replace the failed disk drive with a new disk drive of equal or larger size.

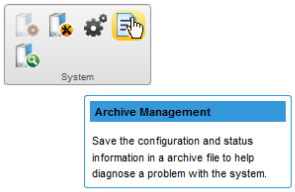
3. The controller detects the reinserted (or new) disk drive and begins to rebuild the logical drive.

12.5 Creating a Support Archive File

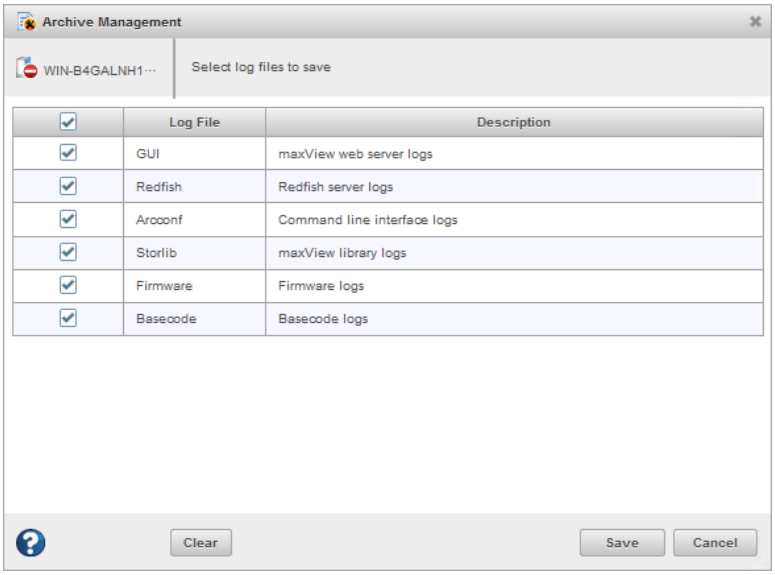
Your support representative might ask you to create a support archive file to help diagnose a problem with your system. Saved information includes device logs, drive logs, event logs, error logs, controller logs, history logs, and SMART statistics.

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.

13. 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.

13.1 Completing a Silent Installation

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

13.1.1 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 2.1.2 Download the Installation Package for details).
2. Run the silent installation from the command line:

Option	Description
Windows 64-bit	setup_asm_x64.exe /s /v"/qn <properties>"

where <*properties*> is one or more of the options listed in 13.1.1.1 Switches, Properties, and Values .

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.

13.1.1.1 Switches, Properties, and Values

This section describes the command line options for Windows silent installation. These options are not supported on Linux.

Switch or Property	Description
/s (required)	Suppress dialog boxes.
/v (required)	Pass command line parameters to the setup program.
/qn	Suppress progress bar during installation.
/qb	Show progress bar during installation.
/lv* <*path*> (optional)	Generate verbose installation log at <*path*>. Example: `/lv* c:\pmc.log`
INSTALLDIR (optional)	Specifies the installation path. If specified, the installation path must be enclosed in escaped quotation marks. Example: `INSTALLDIR=\"C:\Program Files\Adaptec\maxView Storage Manager\"` **Note:** The default installation path is "C:\Program Files\Adaptec\maxView Storage Manager".

© 2021 Microchip Technology Inc. and its subsidiaries

.....continued	
Switch or Property	**Description**
ADDLOCAL (optional)	• ALL (default)—Installs the maxView Storage Manager Console (GUI and Redfish server), and ARCCONF (CLI). If you specify ALL, do not specify any of the following values. • ARCCONF—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.

13.1.2 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 for details).
2. Run the silent installation from the command line using one of these commands (x.xx-xxxxx=version-build number):

Option	Description
Linux 64-bit	./StorMan-X.XX-XXXXX.x86_64.bin --silent

Note: Linux systems also support silent upgrade and silent removal. See 13.2 Example Command Line Installations.

13.2 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\""
```

```
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`

14. 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.

14.1 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:

```
$OutBound = @{
    DisplayName = "Maxview Outbound Rule on TCP port 34572 for SNMP Service"
    Direction = "Outbound"
    InterfaceType = "Any"
    Action =  "Allow"
    Protocol =  "TCP"
    Service = "snmp"
    Program = "$($env:systemdrive)\WINDOWS\system32\snmp.exe"
    Enabled = "TRUE"
    RemotePort = "34572"
    PolicyStore = "ConfigurableServiceStore"
}
New-NetFirewallRule @OutBound
```

   b) Inbound Rule for Port 34572:

```
$InBound = @{
    DisplayName = "Maxview Inbound Rule on TCP port 34572 for SNMP Service"
    Direction = "Inbound"
    InterfaceType = "Any"
    Action =  "Allow"
    Protocol =  "TCP"
    Service = "snmp"
    Program = "$($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:

```
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"
```

14.2 Setting Up SNMP Notifications on Linux

1. Install the Net-SNMP RPM packages:

© 2021 Microchip Technology Inc. and its subsidiaries

- net-snmp
- libsnmp15
- snmp-mibs

2. In `/etc/snmp/snmpd.conf` configuration file:
   a) Comment out the com2sec entry:

   ```
   # com2sec notConfigUser  default       public
   ```

   b) Add the following lines at the end of the file:

   ```
   rocommunity public
   trapsink localhost
   master agentx
   ```

   c) (*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
   ```

© 2021 Microchip Technology Inc.
and its subsidiaries

15. 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 3.3.3 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).

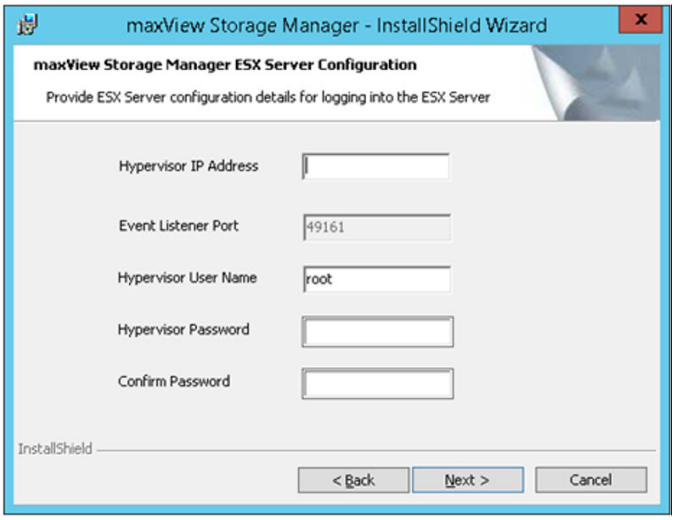
15.1 Installing the maxView Plugin for vSphere Web Client

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.

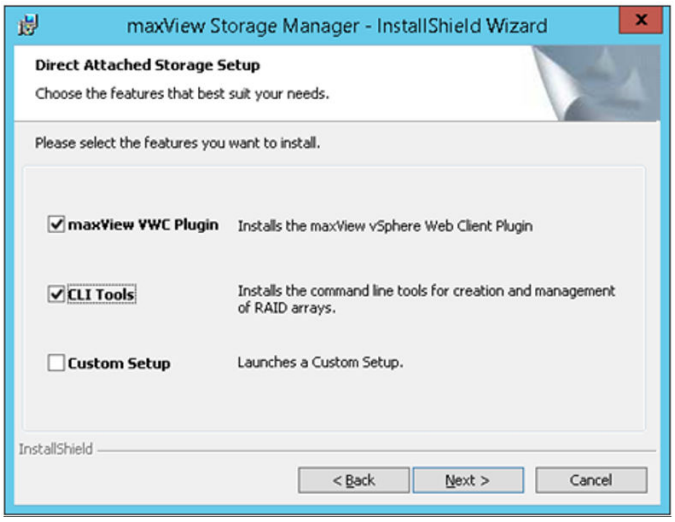
1. Download the setup program for the maxView vSphere plugin from the Web site (see Downloading the Installer Package).
2. Double-click the setup program:

Option	Description
VMware ESXi 6.0 client	setup_maxView_VWC6_Plugin_x64.exe
VMware ESXi 6.5 client	setup_maxView_VWC65_Plugin_x64.exe

   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**.

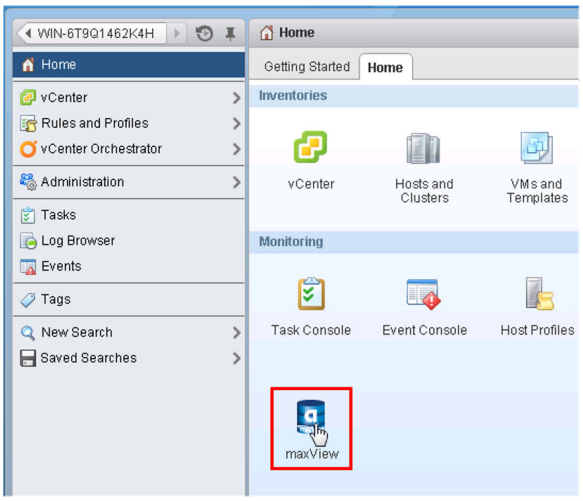


6. Click **Install** to begin the installation.

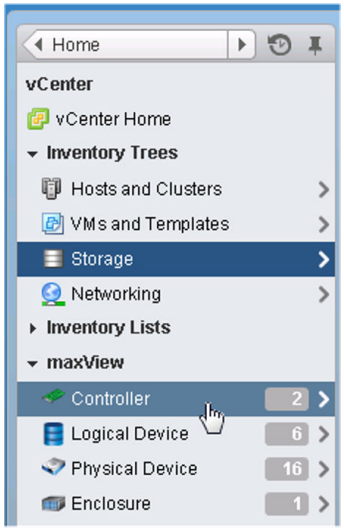
When the installation is complete, you receive a confirmation message that the plugin is installed.

15.2 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.



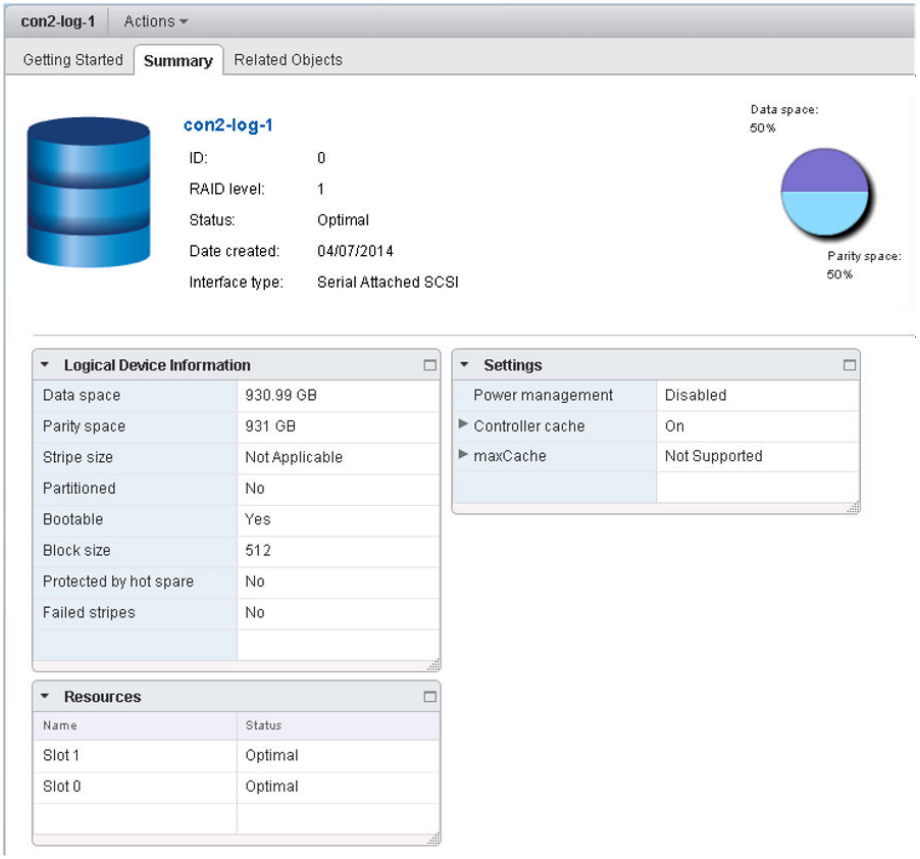
3. Alternatively, in the Navigation pane (on the left), click **vCenter**, scroll down to the maxView tree, then select a resource category, such as Controller, Logical Device, Physical Device, or Enclosure, to open the information screen for that item.



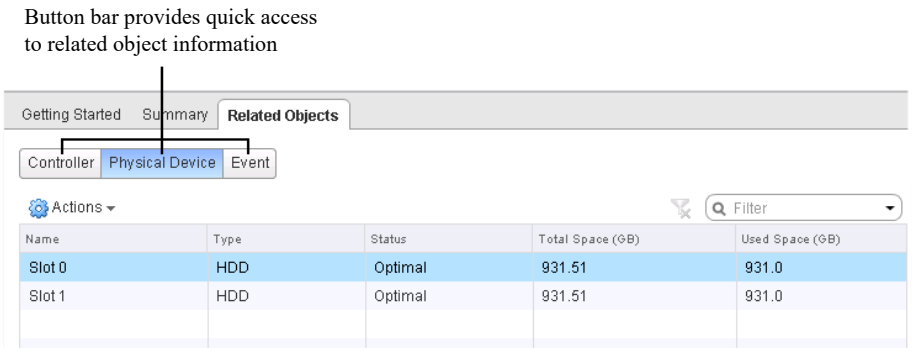
15.3 Monitoring maxView Resources in vSphere Web Client

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.

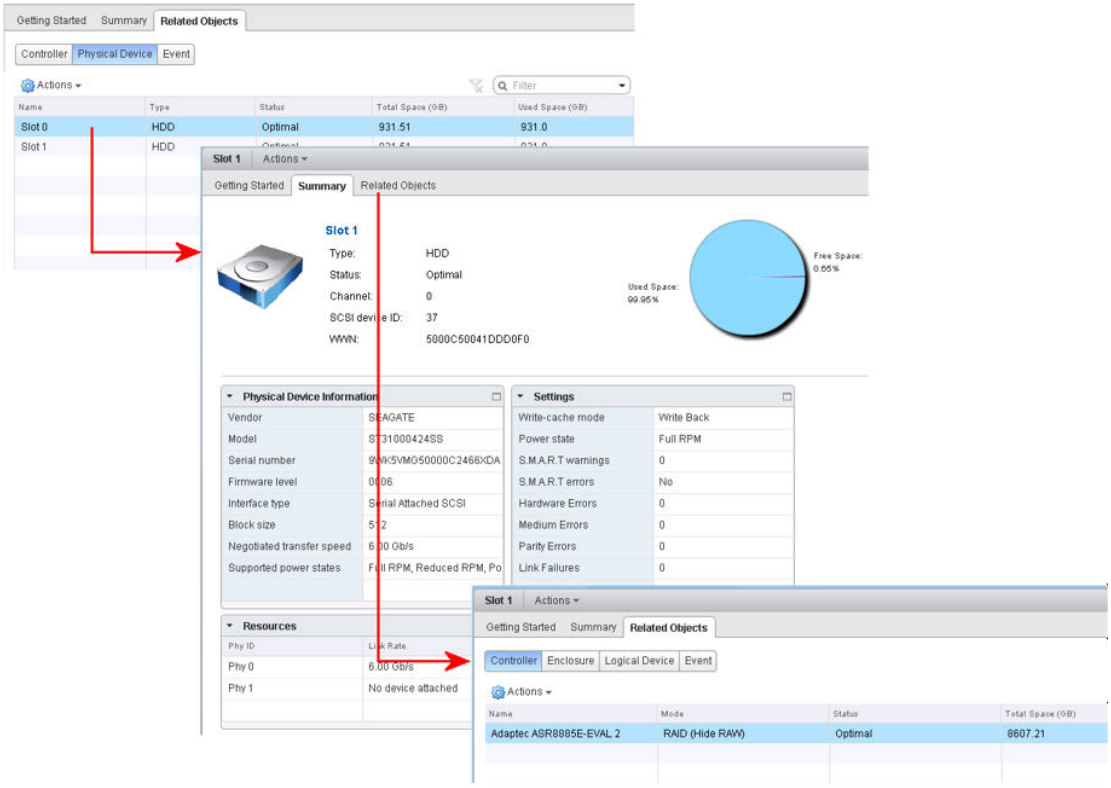
For example, the figure below shows the summary information screen for a logical drive, with expandable information fields containing general information about the logical drive, its settings, and resources. (Each expandable field has an arrow next to it.)



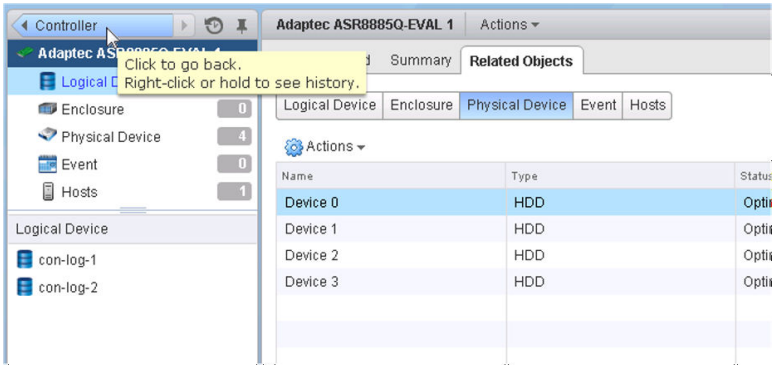
Click on the **Related Objects tab** (next to the Summary tab) to show the physical devices comprising the logical drive, the logical drive's controller, or a filtered list of events for that logical drive.



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 10.2.3 Viewing Component Status in the Storage Dashboard.

© 2021 Microchip Technology Inc. and its subsidiaries

16. Using the maxView Plugin for VMware vSphere HTML5

The maxView plugin for VMware vSphere Web Client is a monitoring tool that lets you explore your storage resources directly from the vSphere HTML client, without using maxView Storage Manager as a separate Web GUI.

16.1 Installing the maxView Plugin for vSphere HTML5 Client

Follow the instructions in this section to install the maxView vSphere Plugin HTML5 on a vCenter Server Appliance.

You need to have VMware ESXi 7 and above and vCenter Server Appliance (VCSA) 7 and above versions running on the machine before proceeding with the installation steps.

1. Create an ESXi setup and mount the `VCSA.iso` file on a machine.
2. Navigate to the following directory on the mounted file: `\vcsa-ui-installer\win32\installer.exe`
3. Double-click on the installer and follow the instructions to create a virtual machine in the ESXi machine with the VMWare Photon OS.
4. Perform either of the following two steps to install the maxView vSphere plugin:
   a. Download and install the maxView vSphere plugin from the Web site.
   b. Install the `maxView-plugin.zip` locally by coping the downloaded `maxView-plugin.zip` in `/etc/vmware-vpx/locale/ maxView-plugin.zip`.
5. Execute the following steps to install the maxView vSphere plugin.
   a. Extract the vsphere-client-sdk-7.zip provided by the VMWare.
   b. Navigate to `\html-client-sdk\tools\vCenter plugin registration\prebuilt\` location that contains the plugin registration script.
   c. Run the following command to register the plugin from the Windows machine:
      - Using Microchip Web URL (download.adaptec.com/raid/storage_manager/maxView-plugin.zip):

```
extension-registration.bat -action
                    registerPlugin --key com.pmc.maxview.maxviewvsphere -url
                    https://IP_ADDRESS/sdk --username Username --version 1.0.0
                    --vcenterServerThumbprint vcenterServerThumbprint
                    --pluginUrl
                    https://download.adaptec.com/raid/storage_manager/maxView-
plugin.zip
                    -serverThumbprint serverThumbprint
```

      - Installing the maxView-plugin.zip locally:

```
extension-registration.bat -action
                    registerPlugin --key com.pmc.maxview.maxviewvsphere -url
                    https://IP_ADDRESS/sdk --username Username --version 1.0.0
                    --vcenterServerThumbprint vcenterServerThumbprint
                    --pluginUrl https:// IP_ADDRESS
                    /catalog/maxView-plugin.zip -serverThumbprint
                    serverThumbprint
```

      Note: For more detail on the commands, check with VMWare.

      where:

      - `IP_Address` is the IP address of the vCenter Server Appliance
      - `Username` is the username of the vCenter Server Appliance
      - `vcenterServerThumbprint` is the vCenter Server Appliance SHA1 Thumbprint. To retrieve SHA1 Thumbprint, perform the following steps:
        1. Launch the vCenter Server appliance in the Web browser.
        2. Click the **Lock** icon on the address bar to get the certificate.
        3. View the SHA1 Thumbprint on the the certificate.
      - `download.adaptec.com/raid/storage_manager/maxView-plugin.zip` is where the maxView plugin is placed. Or, the IP address of the machine where `maxView_plugin.zip` is placed.

- `serverThumbprint`is required from the Microchip website.

A password is prompted. Enter the password of the vCenter Server Appliance.

d. Run the following command to de-register the plugin from Windows machine.

```
extension-registration.bat -action unregisterPlugin
          --key com.pmc.maxview.maxviewvsphere -url https://IP_ADDRESS /sdk
          --username Username --vcenterServerThumbprint
          vcenterServerThumbprint
```

Note: For more detail on the commands, check with VMWare.

where:

- `IP_Address` is the IP address of the vCenter Server Appliance
- `Username` is the username of the vCenter Server Appliance
- `vcenterServerThumbprint` is the vCenter Server Appliance SHA1 Thumbprint. Retrieve the SHA1 Thumbprint certificate as described in the preceeding step.

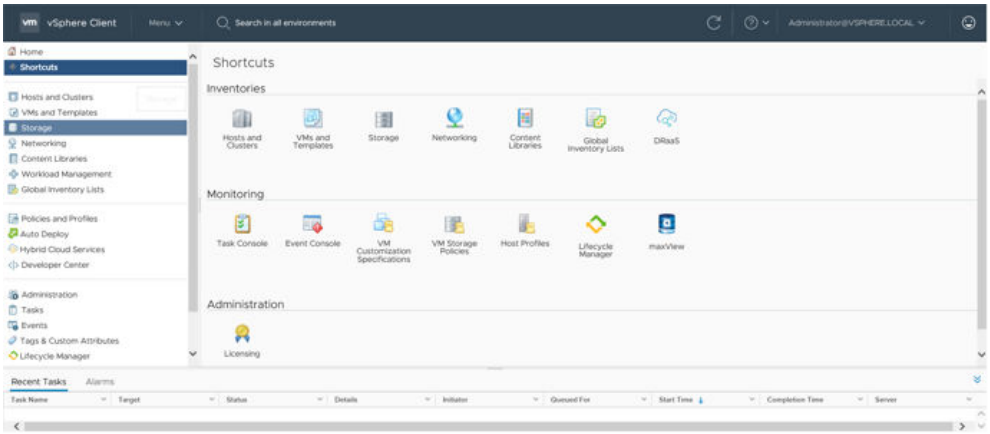
A password is prompted. Enter the password of vCenter Server Appliance.

Once the maxView vSphere plugin is registered, the maxView icon is displayed in shortcut of vCenter Server Appliance (see VCSA_IP/ui/app/shortcuts).

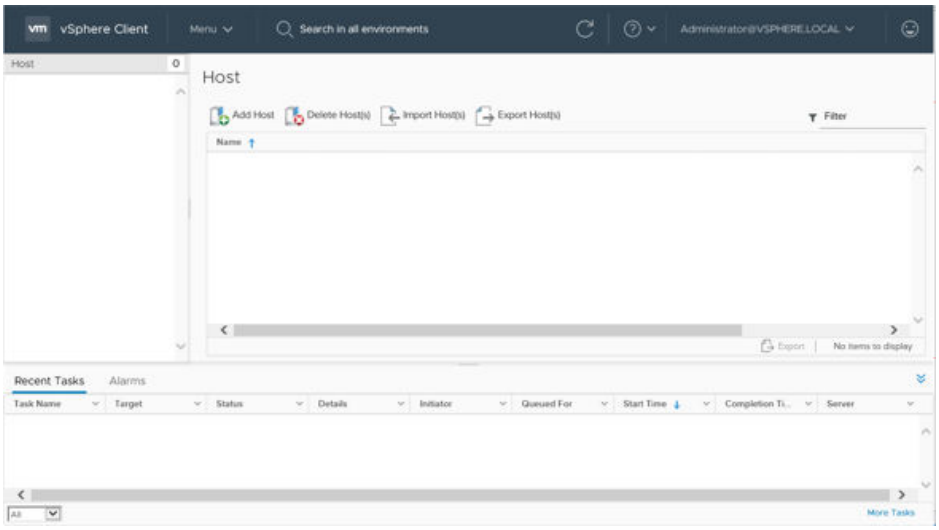
6. Click on the maxView icon to list the ESXi systems added.
   Note: Initially, none of the system are added.
7. Click on **Add system** to add the ESXi systems.
8. Add the firewall entry by using URL https://VCSA_IP: 5480. Click on the firewall and add the entry.
   Note: The configuration or events are not delivered, if the firewall is not added.

16.2 Starting the maxView Plugin for vSphere HTML Client

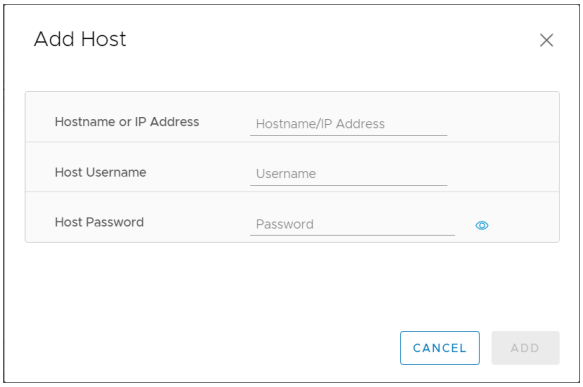
1. Launch the VMware vSphere Web Client and enter your login credentials.
2. From the menu, select the **Shortcuts** option.
3. In the Monitoring section on the vSphere client's Shortcut page screen, click the **maxView** icon; the Host information screen opens.



4. The maxView plugin loads and displays the Host list page.



5. Click on the **Add Host** icon to add and manage the ESXi host.



   The **Add Host** dialog box opens.
6. Enter the following credentials:
   a) Hostname or IP address of the ESXi Server
   b) Username and password of the ESXi Server
7. Click the **Add** button.
   The status dialog is displayed with success or failure status.
8. Click **OK**.
9. **Note:** Before adding the system, make sure to install the `arcconf` and `arc-cim-provider vibs` on the ESXi server.

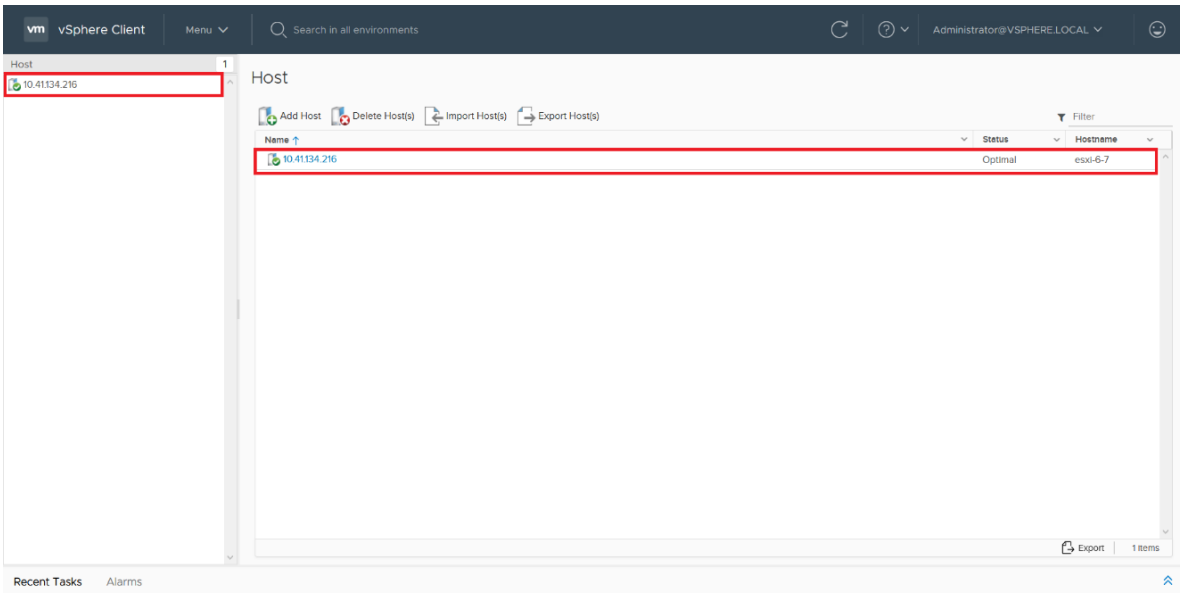
   Click on **Global Refresh** icon to display the new added system in the list.



16.3 Monitoring maxView Resources in vSphere HTML 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 following figure shows the added ESXi server.



Click on the system IP address to navigate to the two tabs listed in the following table.

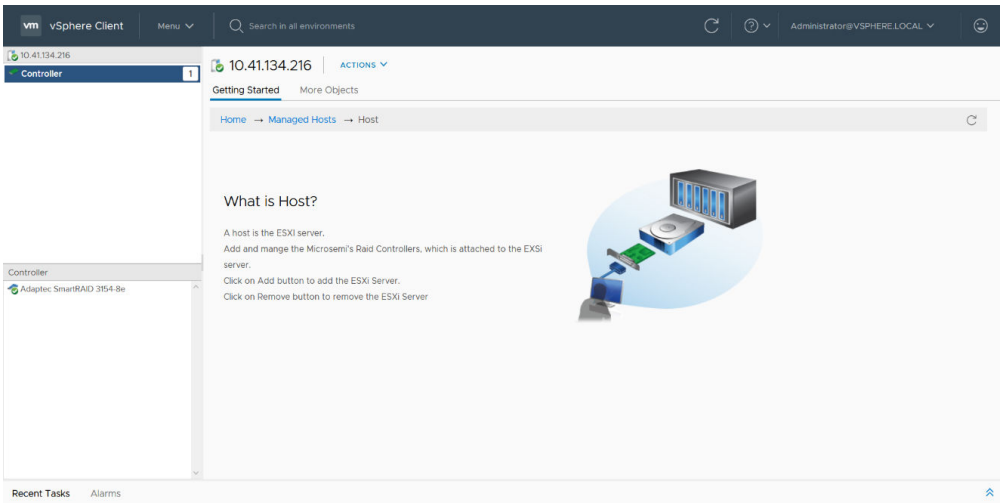


Table 16-1. Host Tab Details

Tab	Details
Getting Started	Provide details on the ESXi server
More Objects	List the controller details

16.3.1 maxView vSphere Plugin Resources

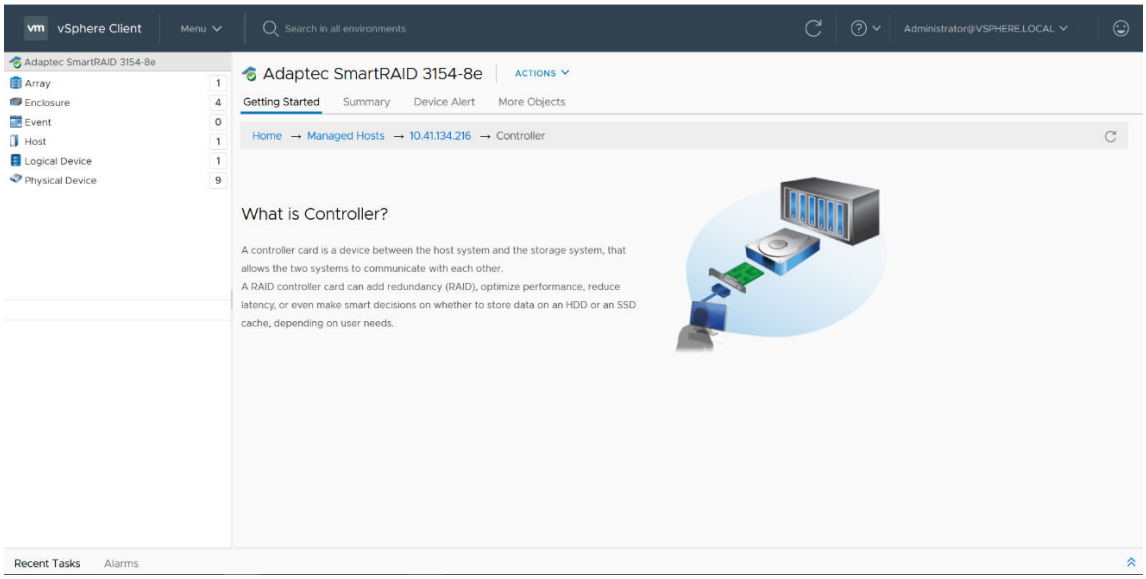
The following section describes the controller details of the maxView vSphere plugin.

The controller has the following four tabs:

- Getting Started
- Summary
- Device Alert
- More Objects (VMware specific)

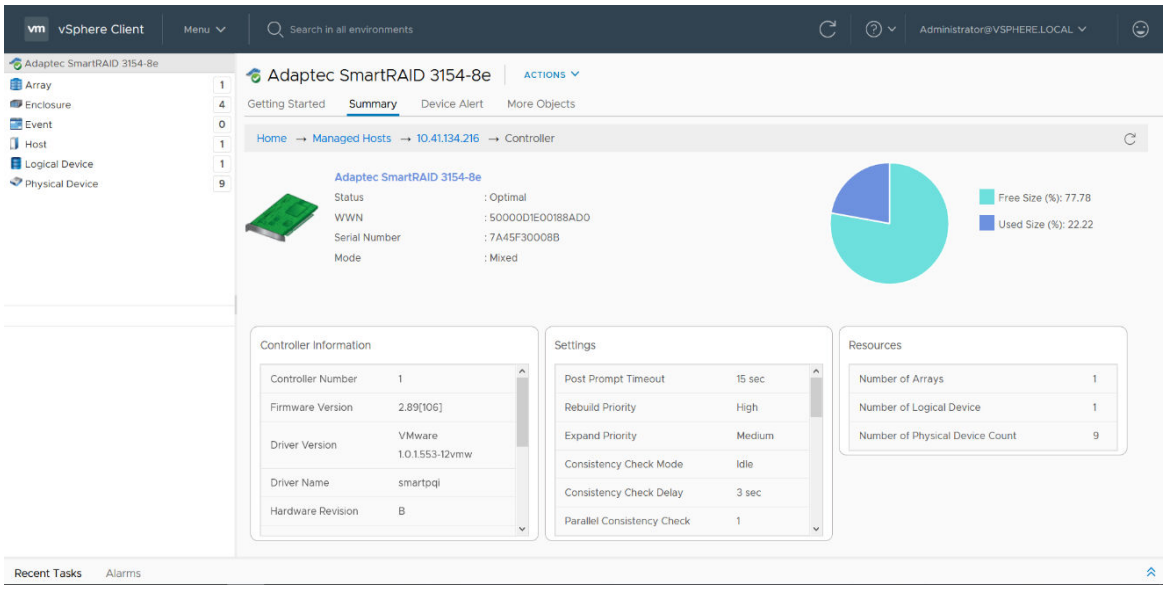
Getting Started Tab

The following figure shows the **Getting Started** tab that displays the basic information of a controller.



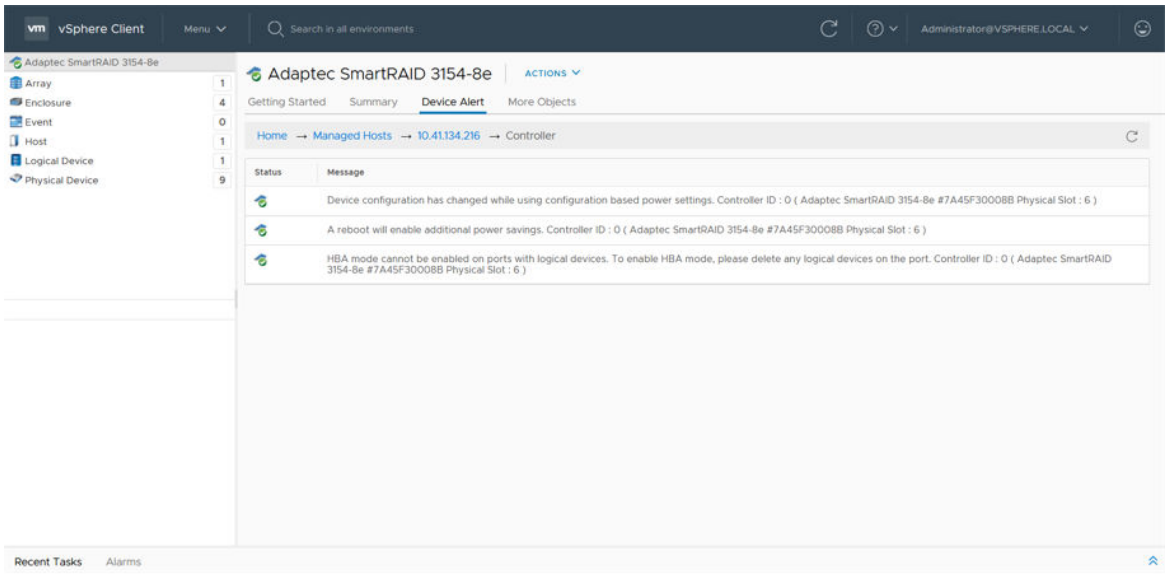
Summary Tab

The **Summary** tab displays the status and the properties of the controller.



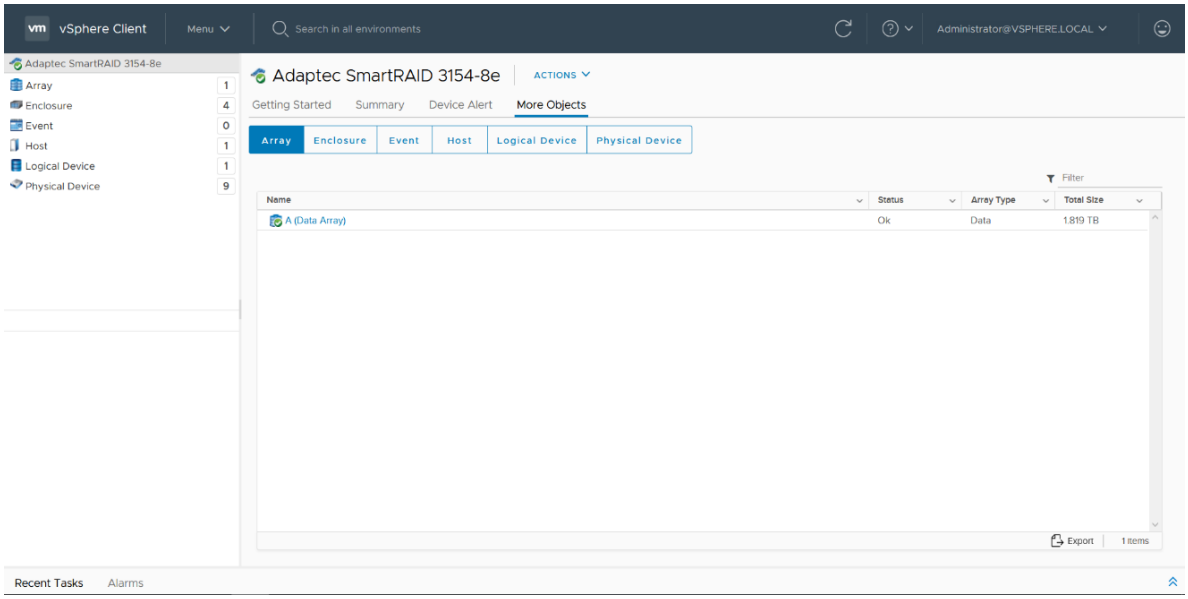
Device Alert Tab

The **Device Alert** tab display the information(s), warning(s), and errors(s) of the controller.



More Objects Tab

The **More Objects** tab is a VMware specific tab, which displays the related resources of the controller.



Note:

You can also obtain the similar details of an Array, Enclosure, Event, Logical Device, and Physical device by clicking on the respective tabs.

16.4 Import and Export Remote ESXi Systems using maxView Plugin

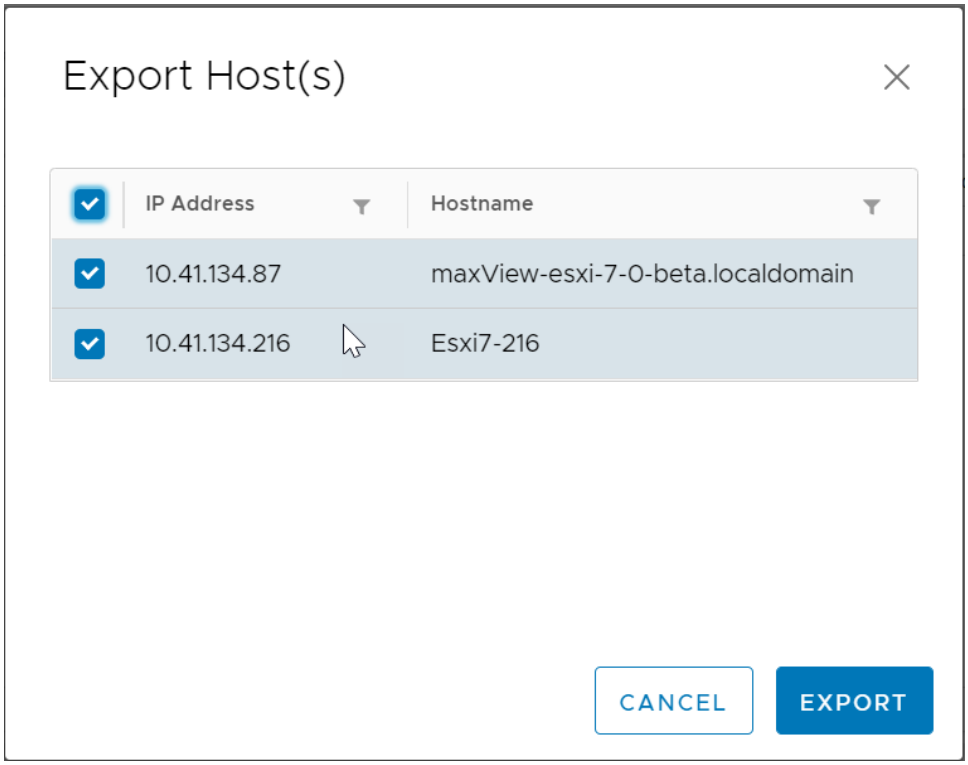
maxView plugin provides the Import and Export systems feature to add multiple systems and export the added systems in “SystemConf.json” file, which can be used later to import the added systems in maxView plugin running on another machine.

Note:

Export feature is only applicable when maxView plugin manages at least one ESXi system.

Perform the following steps to export the ESXi systems:

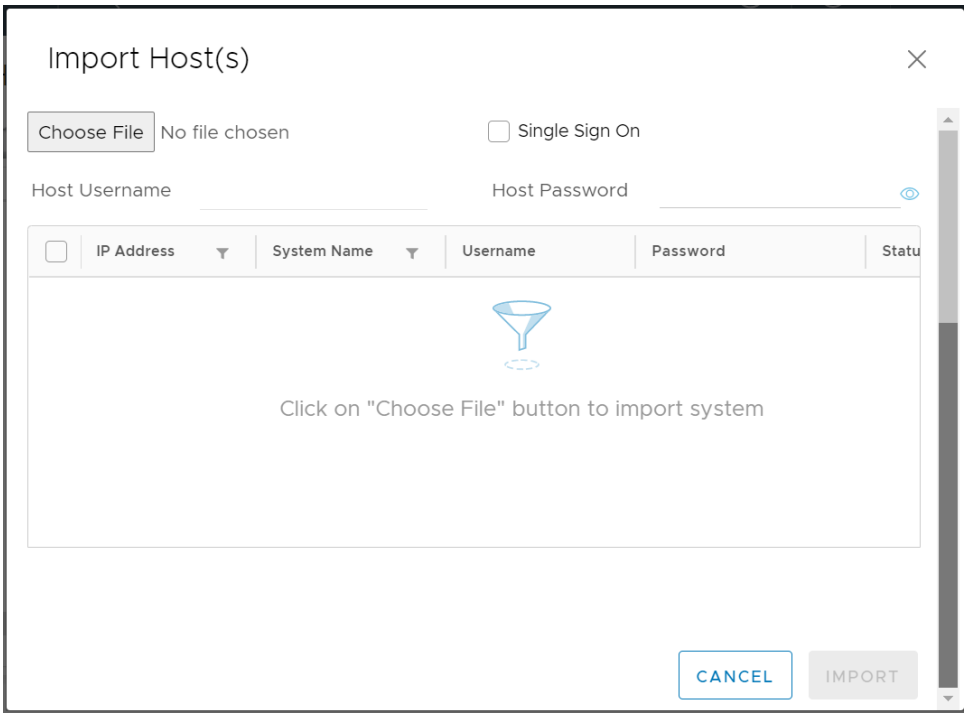
1. In the Monitoring section on the vSphere client's Shortcut page screen, click the **maxView** icon; the Host information screen appears.
2. Click on the **Export Host(s)** button.
3. Select the IP address of the system that need to be exported. Click **Export**.



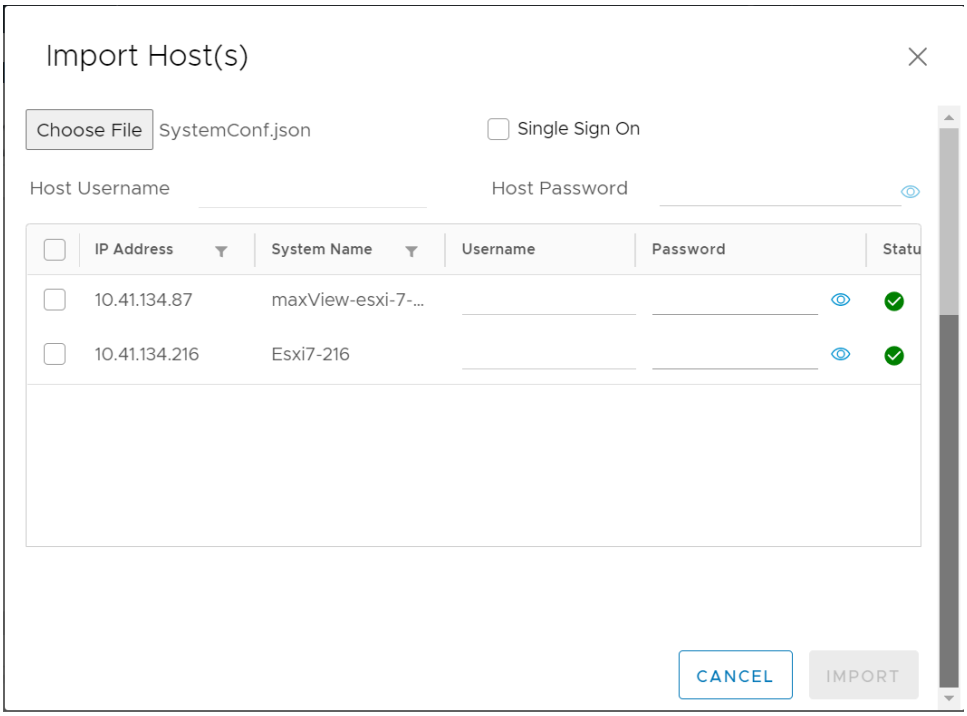
The exported systems are downloaded as "`SystemConf.json`" file in the browser download directory.

Perform the following steps to import the ESXi systems into the vSphere client:

1. Navigate to the Host screen and click the **Import** button.
   The **Import Host(s)** screen appears.

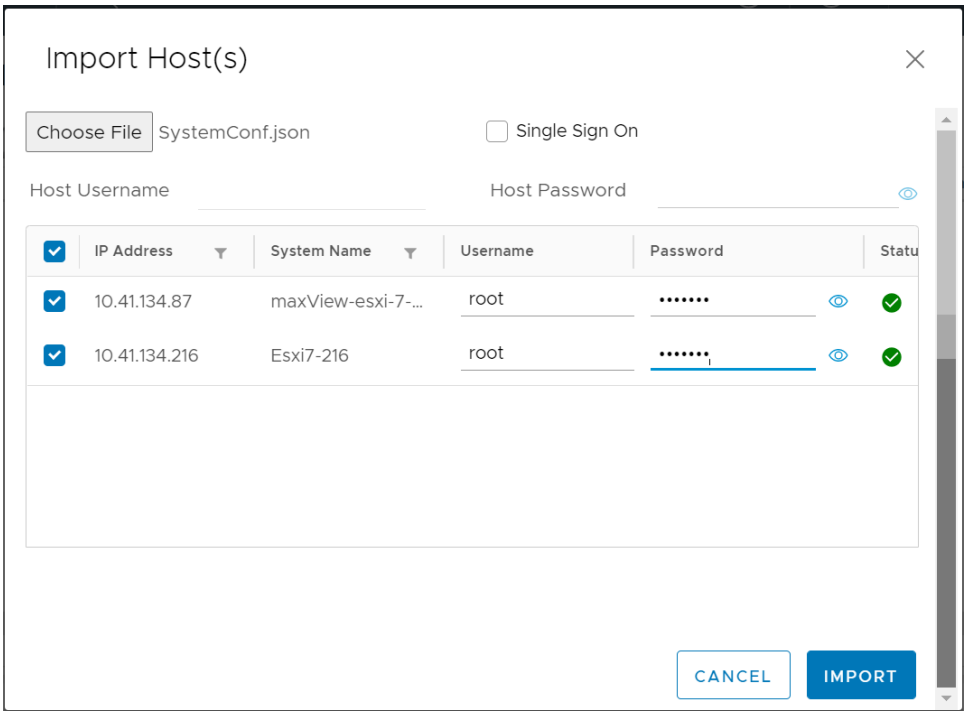


2. Click **Choose File** to specify the path of the "`SystemConf.json`" file.



3. Select the system name(s) and specify the login credentials. Select **Single Sign On** option to specify the Host Username and Host 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.

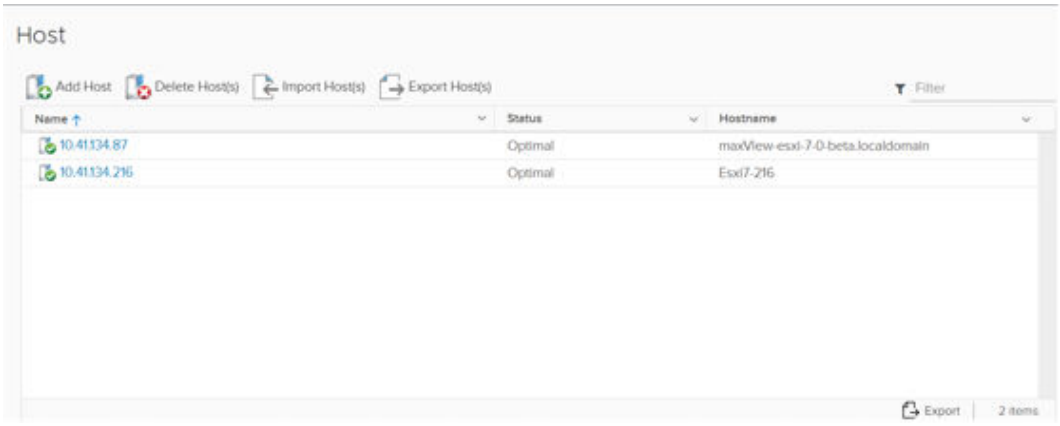


4. Click **Import**.

   A **Status** message box appears stating that the "System added successfully".

5. Click **Close** and refresh the screen.

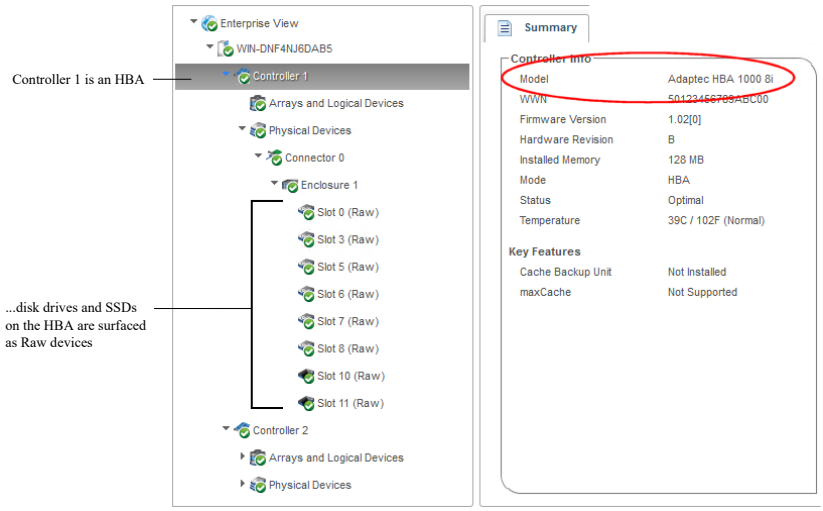
   The imported systems will appear under the Host screen.



17. Using maxView Storage Manager with HBAs and Non-RAID Mode Controllers

maxView Storage Manager allows you to manage storage resources on Microchip Adaptec Host Bus Adapters (HBAs) and RAID controllers operating in HBA mode (see 9.9.3 Changing the Connector Operating Mode). 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 Microchip 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.

Ribbon	Options for HBAs / Non-RAID Mode Controllers
System Group	Firmware Update
Controller Group	Rescan, Properties (non-RAID mode controllers only)
Array Group	None
Logical Device Group	None
Physical Devices Group	Force Offline, Uninitialize, Locate
maxCache Group	None

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 10.2.3 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 10.2.1 Viewing Activity Status in the Event Log).

The following table lists the categories and types of information provided on the Storage Dashboard for HBAs and connected devices.

Component	Categories	Examples
Controller	Summary Properties Resources Connectors	Model, WWN, key features, firmware version, controller mode, status, number and type of physical devices. 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
Physical Devices (node)	Summary	Physical drive assignments by connector, including protocol, state, free and used space
Connector	Summary	Functional mode, number of devices
Enclosure	Summary	Enclosure type, vendor, model, ID, channel, firmware version, status Fan, power supply, and temperature status (see 10.2.3.1 Monitoring Enclosure Status) Slot allocation and usage
Hard drives and SSDs	Summary Resources SMART	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 10.2.3.2 Viewing SMART Statistics)

© 2021 Microchip Technology Inc. and its subsidiaries

18. 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.

18.1 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.

RAID Level	Redundancy	Disk Drive Usage	Read Performance	Write Performance	Built-in Hot Spare	Minimum Disk Drives
RAID 0	No	100%	***	***	No	2
RAID 1	Yes	50%	**	**	No	2
RAID 1(Triple)	Yes	33%	**	**	No	3
RAID 1E	Yes	50%	**	**	No	3
RAID 10	Yes	50%	**	**	No	4
RAID 10(Triple)	Yes	33%	**	**	No	6
RAID 5	Yes	67 – 94%	***	*	No	3
RAID 50	Yes	67 – 94%	***	*	No	6
RAID 6	Yes	50 – 88%	**	*	No	4
RAID 60	Yes	50 – 88%	**	*	No	8

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.

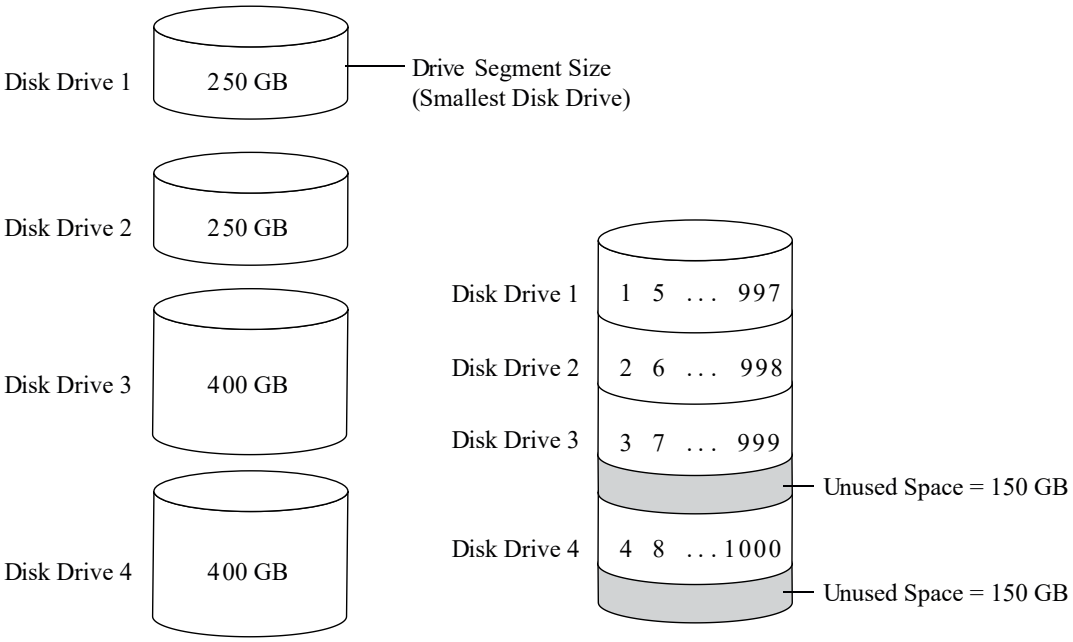
18.2 Non-redundant Logical Drives (RAID 0)

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.

© 2021 Microchip Technology Inc. and its subsidiaries

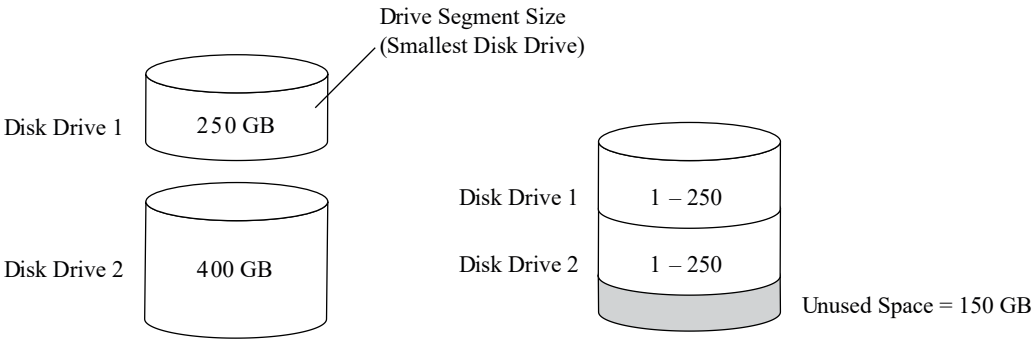


Disk Drives in Logical Drive **RAID 0 Logical Drive = 1000 GB**

18.3 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.

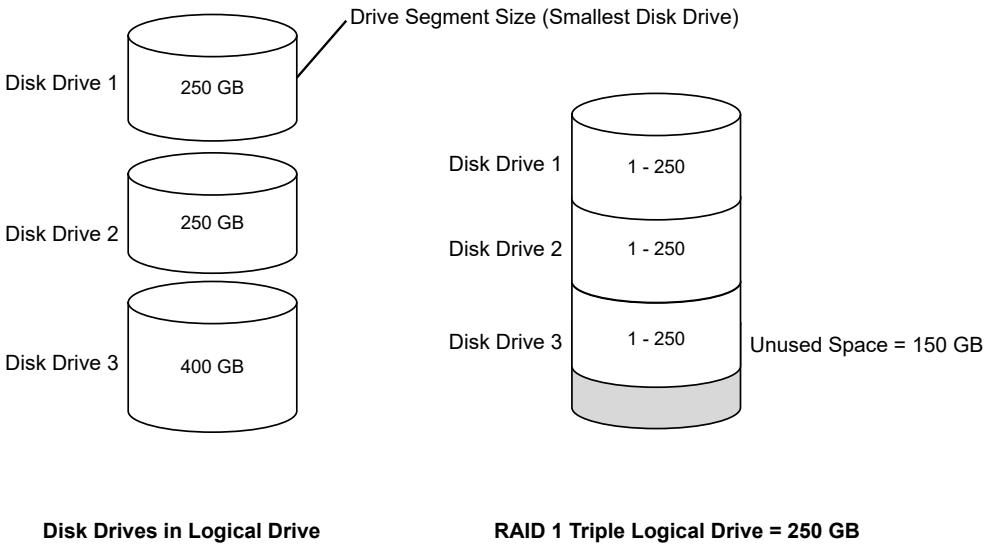


Disk Drives in Logical Drive **RAID 1 Logical Drive = 250 GB**

18.4 RAID 1 Triple Logical Drives

RAID 1 Triple 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.

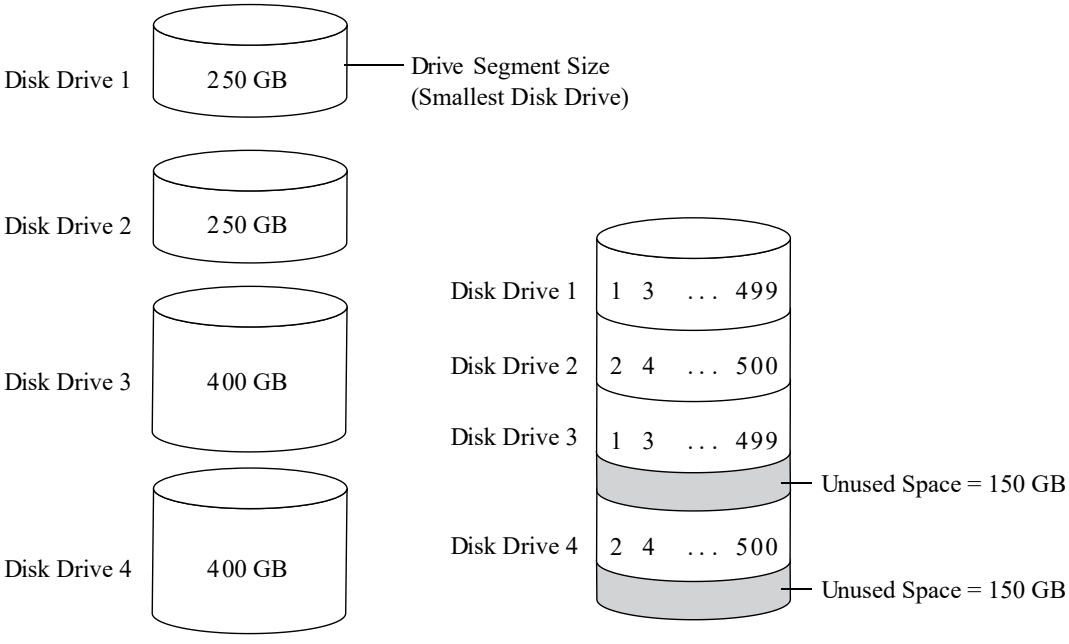


Disk Drives in Logical Drive **RAID 1 Triple Logical Drive = 250 GB**

18.5 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.

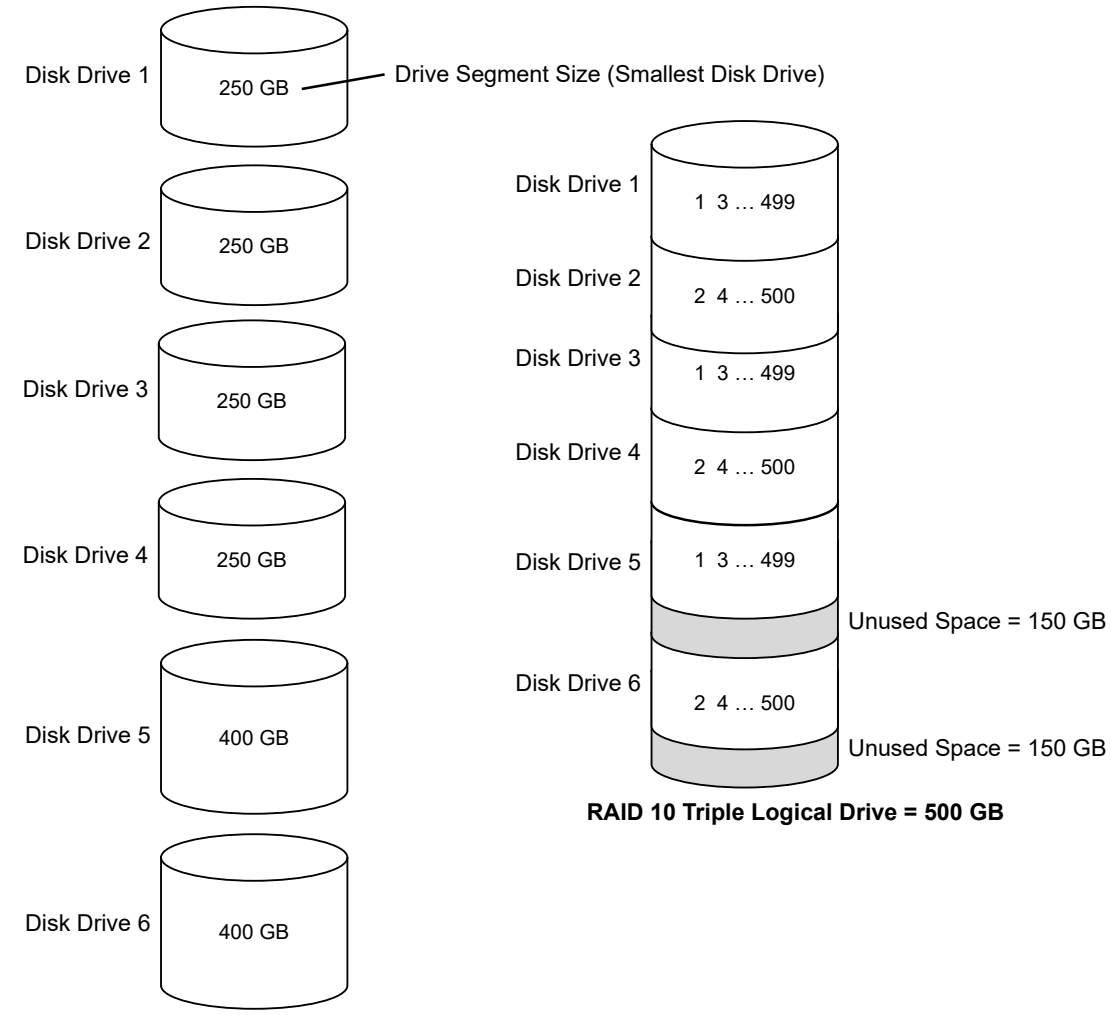


Disk Drives in Logical Drive **RAID 10 Logical Drive = 500 GB**

18.6 RAID 10 Triple Logical Drives

RAID 10 Triple 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 (Triple) drives for rapid access.

If a drive fails, the remaining drives provide backup copies of the files and normal system operations are not interrupted.



Disk Drives in Logical Drive

RAID 10 Triple Logical Drive = 500 GB

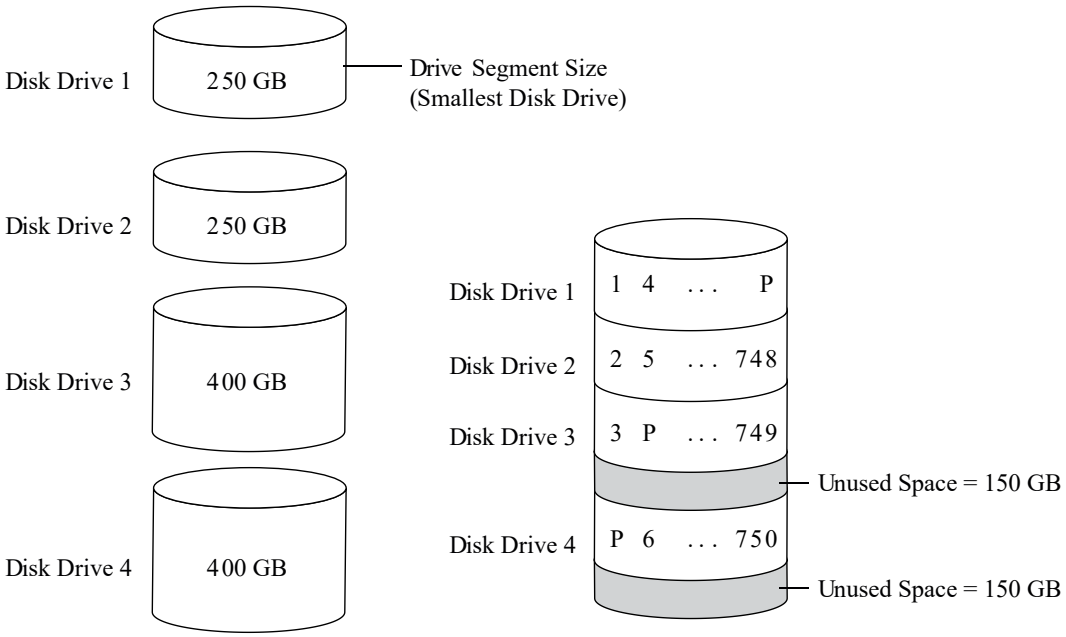
18.7 RAID 5 Logical Drives

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.

© 2021 Microchip Technology Inc.
and its subsidiaries



Disk Drives in Logical Drive **RAID 5 Logical Drive = 750 GB plus Parity**

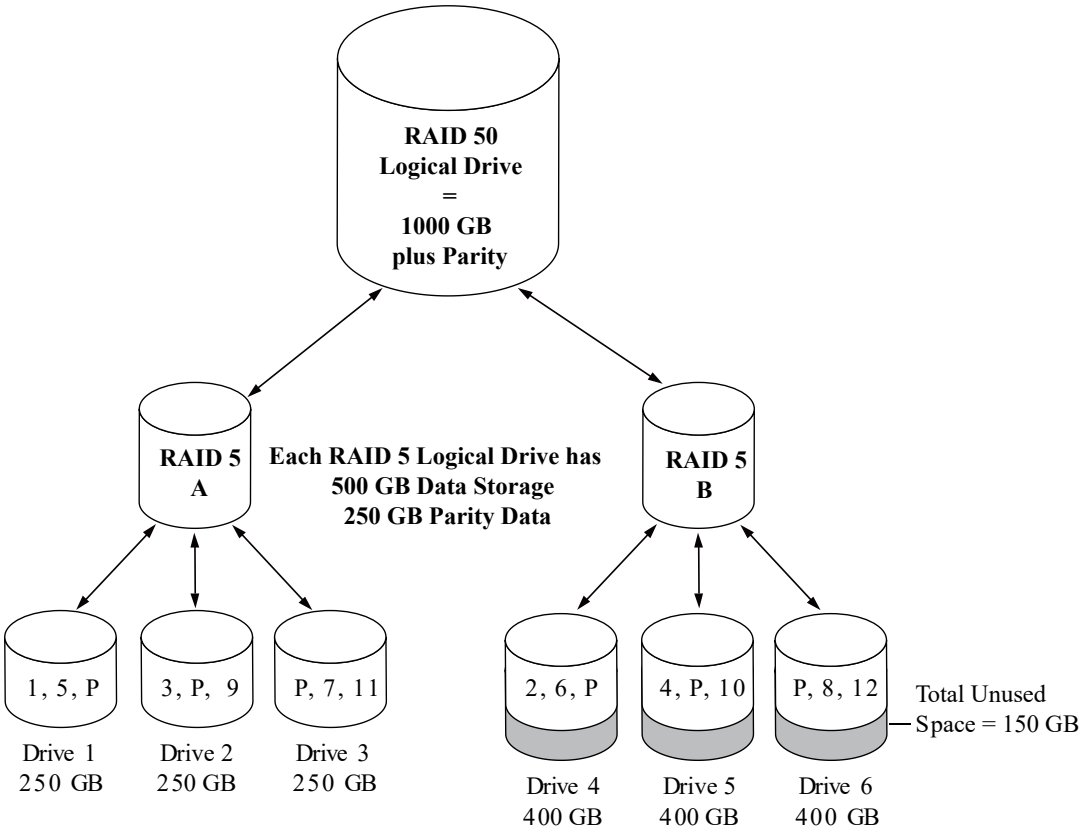
18.8 RAID 50 Logical Drive

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.



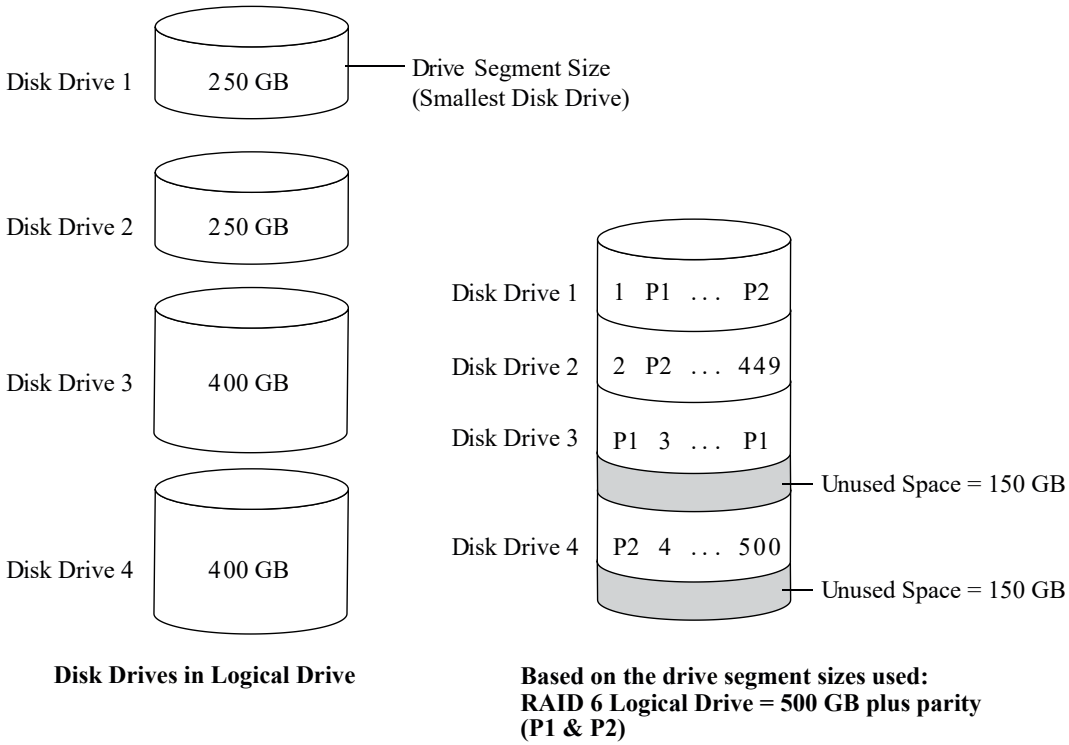
18.9 RAID 6 Logical Drives

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.

© 2021 Microchip Technology Inc.
and its subsidiaries



Disk Drives in Logical Drive

Based on the drive segment sizes used:
RAID 6 Logical Drive = 500 GB plus parity (P1 & P2)

18.10 RAID 60 Logical Drives

Similar to a RAID 50 logical drive (see RAID 50 Logical Drives), 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.

19. 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 3.3 Overview of the Main Window for more information.

Ribbon Home Icons

Icon	Description
	Remote system add
	Remote system delete

Ribbon System Icons

Icon	Description
	System settings
	Manage configuration (save/restore)
	Firmware update
	Save archive file

Ribbon Controller Icons

Icon	Description
	Controller settings
	Manage configuration (clear)
	Controller rescan
	maxCrypto settings

Ribbon Array Icons

Icon	Description
	Array settings
	Array modify
	Array split/mirror
	Array locate
	Array delete

Ribbon Logical Device Icons

Icon	Description
	Logical drive settings
	Logical drive create
	Logical drive expand/migrate
	Logical drive locate
	Logical drive delete
	Logical drive force online

Ribbon Physical Device Icons

Icon	Description
	Physical disk properties
	Assign/unassign physical disk as spare
	Force physical disk offline
	Physical disk secure erase
	Physical disk locate

Ribbon maxCache Icons

Icon	Description
	maxCache Device create
	maxCache Device set properties
	maxCache Device locate
	maxCache Device delete
	maxCache Device disable

Enterprise View Icons

Icon	Description
	Enterprise View
	Local or remote system
	Controller
	Enclosure
	Logical disk

.....continued

Icon	Description
	Logical disks
	Physical disk
	Hard disk drive
	Solid State drive
	SMR drive
	Physical disks
	Enclosure
	Connector or other physical device

Enterprise View Status Icons

Icon	Description
	Enterprise OK
	Enterprise error
	Enterprise no access
	Enterprise warning

Enterprise View System Icons

Icon	Description
	System OK
	System error
	System missing
	System no access
	System warning

Enterprise View Connector Icons

Icon	Description
	Connector OK
	Connector failed
	Connector missing
	Connector warning

© 2021 Microchip Technology Inc. and its subsidiaries

Enterprise View Controller Icons

Icon	Description
	Controller OK
	Controller failed
	Controller missing
	Controller warning
	Controller encrypted

Enterprise View Enclosure Icons

Icon	Description
	Enclosure Management OK
	Enclosure Management failed
	Enclosure missing
	Enclosure Management warning

Enterprise View Physical Disk Icons

Icon	Description
	Physical disk OK
	Physical disks OK
	Physical disks failure
	Physical disks missing
	Physical disks warning
	Physical disk encrypted

Enterprise View MaxCache Device Icons

Icon	Description
	maxCache Device error
	maxCache Device missing
	maxCache Device OK
	maxCache Device warning

Tab Icons

Icon	Description
	Summary
	Properties
	Resources
	Events
	Task
	maxCrypto

Dialog Box Icons

Icon	Description
	E-mail notification
	Chart

20. Advanced Statistics Descriptions

The following table describes the advanced statistics properties by device type.

See 10.4.2 Viewing Advanced Statistics for more information.

Table 20-1. Advanced Statistics Descriptions

Type	Property	Description	Units
Controller	Average Dirty Cache Lines	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 "dirty," so the number of dirty cache lines may exceed the number of write cache lines.	—
Controller	Free Largest Transfer Buffer Sectors	The average number of consecutive transfer buffer sectors available in the controller's internal pool.	—
Controller	Average Free Total Transfer Buffer Sectors	The average number of transfer buffer sectors available in the controller's internal pool.	—
Controller	Average Free Logical Requests	The average number of logical request structures available in the controller's internal pool.	—
Controller	Average Free Processor RAM in kB	The average amount of available processor RAM in kB available in the controller's internal pool.	—
Controller	Average Locked Stripes	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).	—
Controller	Average Locked Stripes Waiting	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.	—
Controller	Average Write Cache Sectors	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.	—
Controller	Command List Count	Number of command lists submitted by the host.	—
Controller	Command List Latency	Average command latency in hundredths of milliseconds.	Hundredths of milliseconds
Controller	Logical Request Count	Number of logical requests submitted by the host.	—
Controller	Maximum DMA Transfer Queue Depth	The maximum number of DMA transfer (WCXC bus master) requests that have been queued up at any time since performance monitoring was started.	—
Controller	Maximum Outstanding Command List	Maximum number of outstanding command lists.	—
Controller	Percent Active	Percentage of time (in tenths of a percent) that at least one logical request is outstanding, including event-notification commands.	Tenths of a percent

© 2021 Microchip Technology Inc. and its subsidiaries

.....continued

Type	Property	Description	Units
Controller	Percent Busy	Percentage of time (in percent) that the controller's CPU is not just sitting in the "idle" task. Note that background activity such as surface analysis is not considered "idle" time.	Percent
Controller	Percent Time Waiting For DMA	The percentage of time (in tenths of a percent) that the local CPU has been stalled waiting for DMA (WCXC bus master) transfers.	Tenths of a percent
Controller	Sample Interval	Time since performance monitoring was last cleared, in tenths of seconds.	Tenths of seconds
Logical Drive	Average Queue Depth	Average number of logical read and write requests queued.	—
Logical Drive	Average Read Latency	Average latency for logical read requests in hundredths of milliseconds.	Hundredths of milliseconds
Logical Drive	Average Write Latency	Average latency for logical write requests in hundredths of milliseconds.	Hundredths of milliseconds
Logical Drive	Cache Hits	Number of cache hits (host-generated logical read requests which could be serviced entirely by the cache without any disk access).	—
Logical Drive	Cache Misses	Number of cache misses.	—
Logical Drive	Coalesced Requests	Number of host requests to this volume that were coalesced by firmware.	—
Logical Drive	Flush Read Requests	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.	—
Logical Drive	Flush Write Requests	Number of flush requests issued by the cache flush task.	—
Logical Drive	Logical Reads	Number of logical read requests submitted by the host, excluding requests coalesced by firmware.	—
Logical Drive	Logical Writes	Number of logical write requests submitted by the host, excluding requests coalesced by firmware.	—
Logical Drive	Maximum Read Request Latency	Maximum latency for logical read requests to this volume in hundredths of milliseconds.	—
Logical Drive	Maximum Write Request Latency	Maximum latency for logical write requests to this volume in hundredths of milliseconds.	Hundredths of milliseconds
Logical Drive	Non-Sequential Reads	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.	—

© 2021 Microchip Technology Inc. and its subsidiaries

.....continued

Type	Property	Description	Units
Logical Drive	Non-Sequential Writes	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.	—
Logical Drive	Posted Writes	Number of host write operations that were absorbed by the posted write cache.	—
Logical Drive	Read Ahead Sector Count	Number of sectors pre-fetched.	—
Logical Drive	Sectors Flushed	Total number of sectors in all flush requests issued by the cache flush task.	—
Logical Drive	Sectors Read	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.).	—
Logical Drive	Sectors Written	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.).	—
Logical Drive	Unaligned Reads	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.	—
Logical Drive	Unaligned Writes	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.	—
Physical Drive	Average Request Latency	Average latency for physical read/write requests in hundredths of milliseconds.	Hundredths of milliseconds
Physical Drive	Maximum Queue Depth	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.	—
Physical Drive	Maximum Request Latency	Maximum latency for physical read/write requests in hundredths of milliseconds.	Hundredths of milliseconds
Physical Drive	Maximum Wait Time Between Completions	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.	Hundredths of milliseconds
Physical Drive	Read Requests	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&P, etc.).	—

© 2021 Microchip Technology Inc. and its subsidiaries

.....continued

Type	Property	Description	Units
Physical Drive	Write Requests	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&P, RIS saves, etc.).	—
Physical Drive	Aborted Commands	The number of times a drive was failed due to aborted commands that could not be retried successfully.	—
Physical Drive	Medium Errors	The number of times a drive was failed due to unrecoverable media errors.	—
Physical Drive	Parity Errors	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.	—
Physical Drive	Hardware Errors	The number of times a drive returned a bad hardware status.	—

© 2021 Microchip Technology Inc.
and its subsidiaries

21. 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 a Controller

Status	Description
Optimal	Controller is healthy.
Controller Has Incompatible Driver	The controller has the incompatible driver.
Failed	Controller is not in working condition.
Inaccessible	Controller communication failure error.
Down/Offline	Controller offline error.
Controller Lockup Error	Controller failed with a lockup error.
Missing SG Module	Controller missing module error. This controller requires that the scsi_generic (sg) module be loaded in order to be configured.
Controller Powered OFF	Controller poweroff error.
Sys PQI Driver Conflict	This controller has an incompatible driver.
Unknown	Controller unknown error.

Status Details of an Array

Status	Description
Ok	The array has all the logical device(s) in optimal state
Has Initializing Logical Device	One or more member logical device(s) has RPI in progress
Logical Devices Not Contiguous	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.
Has Failed Physical Device	Array has a bad or missing physical device
Has Failed Logical Device	One or more logical device(s) in the array has failed
Failed	A physical device or logical device in the array has failed.
Has Erasing Drive	The array currently has a drive erase operation queued, running, stopped or completed on a logical or physical device.
Spare Drive Size Too Small	The array has a spare drive assigned which is smaller than the smallest data drive in the array.
One or more logical drives undergoing or failed SED Qualification	The array has the logical device(s) with status as "SED Qualification in Progress" or "SED Qualification Failed".

Status Details of a Logical Device

© 2021 Microchip Technology Inc. and its subsidiaries

Status	Description
Optimal	The logical device is healthy and is readily accessible by the host
Queued for Expansion	The logical device is queued for expansion
Expanding	The logical device is undergoing online capacity expansion
Ready for Recovery	The logical device is queued to be recovered from a failed physical device
Recovering	The logical device is rebuilding a physical device from fault tolerant data
Wrong Drive Replaced	A wrong physical device was replaced
RPI In Progress	Rapid parity initialization is currently in progress on this logical device
RPI Queued	Rapid parity initialization is currently queued on this logical device. It will start once other progress tasks are completed.
Unsupported on The Controller	Logical device is unsupported on this controller. Host access to this volume is denied. Logical device can still be deletd/reconfigured with data loss.
Encrypted Logical Device Without Key	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.
Encryption Migration	The logical device is being migrated between plaintext and ciphertext
Encrypted Logical Device Rekeying	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.
Encrypted Logical Device With maxCrypto Off	The logical device is encrypted, exported from a foreign controller and cannot be accessed as the controller does not have encryption enabled/not configured.
Encryption Migration Requested	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.
Encrypted Logical Device Rekey Requested	The logical device is encrypted and has received a request to re-key all data with a new encryption key
Unknown	The status of logical device is unknown
Erase In Progress	The logical device is offline and has erase in progress
Ejected	The logical device is offline from being ejected. Reinstall the removed physical devices.
Not Yet Available	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.
Not Configured	The logical device is not yet configured
Interim Recovery	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.

© 2021 Microchip Technology Inc.
and its subsidiaries

.....continued	
Status	**Description**
Failed	The logical device has bad or missing physical device(s).
Disabled From SCSI ID Conflict	A conflict with an existing SCSI ID exists. Check all SCSI components to make sure they all have a unique SCSI ID.
Drive Improperly Connected	A physical device is not properly connected.
Hardware Has Overheated	A physical device temperature has crossed the threshold value.
Hardware Is Overheating	A physical device temperature is about to reach the threshold value.
Optimal(Background Parity Initialization)	Logical device is undergoing the Parity initialization in background.
Rapid Parity Initialization	Logical device is undergoing the Rapid Parity initialization and may not available until it is completed.
Offline Parity Initialization	Logical device is undergoing Offline parity initialization.
Logical Device Reconfiguring	Logical device is reconfiguring.
Plaintext Volume Rejected In Encrypting Mode	Logical device is plaintext and cannot be accessed as the controller is in encryption-only mode.
SED Qualification in Progress	This state indicates that the SED qualification is in progress.
SED Qualification Failed	This state indicates that the SED qualification is failed.

Status Details of a Physical Device

Status	Details
Ready	The physical device is readily available for RAID configuration
Optimal	The physical device is part of an array/logical device
Waiting For Rebuild	The physical device is waiting to be rebuilt
Rebuilding	The data on the physical device is being rebuilt. The physical deice will be accessible. But performance will be less than optimal during the rebuilding process.
Queued For Erase	The physical device is currently queued for erase and the will not be available for use until the erase operation is completed
Erase In Progress	The physical device is currently being erased and the will not be available for use until the erase operation is completed
Erase Completed	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.
Erase Failed	The physical device erase process is failed and the is offline. The physical device may now be brought online through the initialize operation.
Erase Aborted	The physical device is offline due to a aborted erase process

© 2021 Microchip Technology Inc. and its subsidiaries

.....continued

Status	Details
Predictive Failure	This physical device is predicted to fail soon. Backup all the data on the drive and replace the drive.
Transient Data Drive	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
Failed	The physical device is bad or missing
Failed Due To Predictive Spare Activation	The physical device has been failed by the controller after completing a predictive spare activation
Unsupported	The physical device is not supported by the controller
Not Supported	The controller firmware version does not support this physical device. Replace the physical device with the one supported by the controller.
Dedicated Hot Spare	A dedicated hot spare is assigned to one or more arrays.
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.
Raw	A physical device is in RAW state which has no or unknown file system.
Size Not Valid	Physical device size is not valid.

© 2021 Microchip Technology Inc.
and its subsidiaries

22. Display Properties of a Controller, Array, Logical Device, and a Physical Device

This section lists the display properties of a controller, array, logical device, and physical device.

Table 22-1. Controller Display Properties

Property	Tooltip Details
Model	Model of the Controller
Status	Overall status of the controller based on its resources.
Serial Number	A unique number assigned to the controller,used for identification and inventory purposes.
WWN	A World Wide Name(WWN) is an unique identifier of the controller.
Firmware Version	Active firmware version of the controller
Hardware Revision	Describes the hardware revision information about the controller.
Manufacturing Part Number	Describes the hardware part number information about the controller.
Manufacturing Spare Part Number	Describes the hardware spare part number information about the controller.
Manufacturing Wellness Log	Describes the hardware wellness log information about the controller.
Installed Memory	Size of Dynamic Random Access Memory(DRAM) installed on the controller
Cache Memory	Cache memory size on controller.
Mode	Mode of the controller on which it is operating
Pending Mode	Pending mode of the controller which will reflect on reboot.
Temperature	Current temperature of the controller
Power Consumption	Power Consumption
NVRAM Checksum Status	NVRAM Checksum Status
maxCache	The maxCache software uses a reserved logical drive comprised of SSDs only, called the maxCache device, for fast read and write caching.
maxCrypto	maxCrypto feature ensures the sensitive data is encrypted and protected by secure 256 bit AES, in-line encryption.
Physical Slot	PCI slot number to which the controller is connected.
Driver Version	Current version of driver installed on the system.
Driver Name	Driver name describes the name of the driver.
Host Bus Type	Type of host expansion bus standard.
Host Bus Speed	Speed of host expansion bus standard in MHz.
Host Bus Link Width	Speed of host expansion bus standard in MHz.

© 2021 Microchip Technology Inc.
and its subsidiaries

.....continued

Property	Tooltip Details
PCI Address (Bus:Device:Function)	PCI address describes the PCI address for the controller.
I2C Address	I2C address describes the Inter-Integrated Circuit(I2C) slave address.
I2C Clock Speed	I2C clock speed describes the Inter-Integrated Circuit(I2C) clock speed.
I2C Clock Stretching Status	I2C stretching status describes the Inter-Integrated Circuit(I2C) clock status.
NCQ	Native Command Queuing, or NCQ, lets SATA disk drives arrange commands into the most efficient order for optimum performance.
Number of Ports	Number of ports describes number of internal and external ports of the controller.
Backup Power Status	Status of battery backup unit.
Battery / Capacitor Pack Count	Number of battery pack connected to controller
Hardware Error	Hardware error type occurred on battery backup unit
Post Prompt Timeout	Post prompt timeout describes the F1/F2 POST prompt timeout for the controller during system boot.
Rebuild Priority	Rebuild priority 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, rebuilding occurs for half of the time, and normal system operations occur for the rest of the time. At the medium high setting, rebuilding is given a higher priority over normal system operations. At the high setting, the rebuild takes precedence over all other system operations.
Expand Priority	Expand Priority setting determines the urgency with which the controller treats an internal command to expand an array. At the low setting level, normal system operations take priority over an array expansion. At the medium setting, expansion occurs for half of the time, and normal system operations occur for the rest of the time. At the high setting, the expansion takes precedence over all other system operations.
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, including virtual volumes and the maxCache Container.
Consistency Check Priority	Consistency Check Mode is an automatic background process that ensures that you can recover data if a drive failure occurs. The scanning process checks physical drives in fault-tolerant logical drives for bad sectors and it also verifies the consistency of parity data if applicable. The available modes are disable, high, or idle. The idle mode must also specify a delay value.

© 2021 Microchip Technology Inc.
and its subsidiaries

.....continued

Property	Tooltip Details
Consistency Check Delay	Consistency Check Delay determines the time interval for which a controller must be inactive before a consistency check is started on the physical drives that are connected to it. The value can be between 0 and 30 to specify the duration of the delay in seconds. A value of 0 disables the scan.
Parallel Consistency Check Count	Parallel consistency check count describes the number of logical devices on which the controller will perform consistency check in parallel.
Raid 6/60 Alternate Inconsistency Repair Policy	RAID 6/60 alternate inconsistency repair policy searches for a single inconsistent strip and repairs the strip on that one drive only.
Consistency Check Inconsistency Notify	Consistency Check Inconsistency Notify property enables the event notification messages and serial debug log messages for mirrored volumes.
Spare Activation Mode	Spare activation mode feature enables the controller firmware to activate a spare drive. The firmware starts rebuilding a spare drive only when a data drive fails when the mode is Failure. With the predictive failure activation mode, rebuilding can begin before the drive fails when a data drive reports a predictive failure (SMART) status which will reduce the likelihood of data loss that could occur if an additional drive fails.
Maximum Drive Request Queue Depth	Queue Depth controls the behavior of the cache write queue. This option is used to tune controller performance for video applications. The valid values are 2, 4, 8, 16, 32, or Automatic.
Monitor and Performance Delay	MNP Delay option controls the behavior of the controller Monitor and Performance Analysis Delay and is expressed in values ranging from 0 to 1440. This option is primarily used to tune controller performance for video applications.
Physical Drive Request Elevator Sort	Elevator Sort option controls the behavior of the controller cache write Elevator sort algorithm. This option is used to tune controller performance for video applications. The possible options are Enable or Disable.
Degraded Mode Performance Optimization	Degraded Mode Performance Optimization setting applies to RAID 5/RAID 50/RAID 6/RAID 60 logical devices in degraded mode only. Enabling this setting directs the controller to attempt to improve performance of large read requests by buffering physical drive requests. Disabling this feature forces the controller to read from the same drives multiple times. This option is used to tune controller performance for video applications. The possible options are Enable or Disable.

© 2021 Microchip Technology Inc.
and its subsidiaries

.....continued

Property	Tooltip Details
HDD Flexible Latency Optimization	Latency describes Flexible Latency Schedule (FLS) setting. Flexible Latency Scheduler (FLS) is a controller option where the controller can re-prioritize I/O requests to prevent some requests to HDDs from timing out. Under normal operation (when FLS is disabled, or in controllers that don\u2019t support FLS), the controller will sort incoming requests in order to minimize the amount of travel for the HDD\u2019s read heads (Elevator Sort). This strategy works well for workloads that access sequential data, or workloads that require multiple requests from localized sectors in the drive. For highly random workloads, such as transaction processing, some requests will end up on the wrong side of the disk platter and, due to their high latency, will be marked as timed out. When FLS is enabled, it will detect these high-latency requests and apply a cutoff value, after which it will suspend elevator sorting and service the request right away.
Primary Boot Volume	Primary Boot Volume describes which logical device or physical device is the primary boot volume on the current controller.
Secondary Boot Volume	Secondary Boot Volume describes which logical device or physical device is the secondary boot volume on the current controller.
Sanitize Lock	Set the sanitize lock policy of the controller. This policy will be applied to all SATA physical devices that support the feature. 1. None : No freeze lock or anti-freeze lock commands are sent to any physical device. 2. Freeze : Supported physical devices are freeze locked and sanitize is not allowed. 3. Anti-Freeze : Supported physical devices are anti-freeze locked and freezing the physical devices is not allowed.
Pending Sanitize Lock	Sanitize lock is in pending state, reboot the system and require all physical devices to be power cycled or hot-plugged for the lock state to be applied to the physical devices.
Expander Minimum Scan Duration	Controller waits for the specified seconds to scans/discover the drives attached to the expander on the next power cycle. Set this to a non-zero value if some devices do not appear in the topology after controller boot or rescan requests.
Intelligent Power Management	
Current Power Mode	Power mode setting determines controller static settings based on work load. MINIMUM POWER: Set static settings to lowest possible. Reduce dynamically based on workload. MAXIMUM PERFORMANCE : Set static settings to highest possible. Do not reduce dynamically.
Pending Power Mode	Power mode setting determines controller static settings based on work load before system reboot. MINIMUM POWER: Set static settings to lowest possible. Reduce dynamically based on workload. MAXIMUM PERFORMANCE : Set static settings to highest possible. Do not reduce dynamically.

© 2021 Microchip Technology Inc. and its subsidiaries

.....continued

Property	Tooltip Details
Survival Mode	Enabling survival mode allows the controller to throttle back dynamic power settings to their minimums when temperatures exceed the warning threshold. This allows the server to continue running in more situations, but performance may decrease.
Controller Cache	
Cache Status	Determines the preservation status of the cache module.
Cache Ratio	The controller cache ratio setting determines the controller ability to adjust the amount of memory for read-ahead cache versus write cache.
Write Cache Bypass Threshold (KB)	All writes larger than the specified value will bypass the write cache and be written directly to the disk for non-parity RAID volumes.
No-Battery Write Cache	No-Battery Write Cache setting decides the controller to enable write cache when no battery is present or when the battery fails. Values are Enable or Disable.
Wait for Cache Room	Wait for Cache Room setting causes the controller to always wait for room in the read/write cache when full instead of automatically bypassing it in favor of higher performance.
maxCache	
Status	maxCache support status on controller.
Version	maxCache version
Drive Cache	
Write Cache Policy for Configured Drives	This option allows to configure the write cache policy on a controller. Setting to default allows the controller to optimize the drive write cache policy of those drives. Enabling drive write cache can increase write performance but risks losing the data in the cache on sudden power loss. Setting the policy to “unchanged” means that the controller will make no changes to the drive’s default power-on write cache policy.
Write Cache Policy for Unconfigured Drives	This option allows to configure the write cache policy on a controller. Setting to default for unconfigured drives uses the drive's existing write cache policy. Enabling drive write cache can increase write performance but risks losing the data in the cache on sudden power loss.
Write Cache Policy for HBA Drives	This option allows to configure the write cache policy on a controller. Setting to default uses the drive's existing write cache policy. Enabling drive write cache can increase write performance but risks losing the data in the cache on sudden power loss.

Table 22-2. Array Display Properties

Property	Tooltip Details
ID	ID describes unique array identifier within the controller.
Name	Name describes unique name of array

.....continued

Property	Tooltip Details
Status	Status of array is based on health of member disk drives.
Device Type	Type describes the type of the array such as data array, backup array etc.
Interface Type	Disk drives which are the member of array can have interface type such SAS, SATA, SAS SSD and SATA SSD. The interface type of array is based on the member disk drives interface type.
Total Size	Total usable size is the total space available in the array for creating logical device.
Used Size	The total disk space used by the logical device(s) on the given array.
Unused Size	Unused size is the free space available to create new logical device to store the data.
Member Device(s) Block Size	Block size indicates the maximum size of data block on disk drives which are member of array (can be 512 Bytes or 4K).
Transformation Status	Transformation status indicates whether the array is transforming or not.
Protected by Hot Spare	Protected by Hot Spare indicates whether the array is protected by Hot Spare.
Spare Rebuild Mode	Spare rebuild mode describes the spare type for the array. It can be "dedicated" or "auto replace" if the array is valid.
SSD I/O Bypass	SSD I/O Bypass enables an optimized data path to high performance solid state drives. The optimized path bypasses the controllers RAID processing components and sends I/O directly to the drives.
Member Logical Device(s)	Number of logical device(s) present in the array.
Member Physical Device(s)	Number of physical device(s) used to create the array.
Spare Drive(s)	Number of spare drives associated to this array. If a drive fails in the array, the controller automatically rebuilds the data onto the spare drive.

Table 22-3. Logical Device Display Properties

Property	Tooltip Details
ID	Describes unique ID of logical device listed.
RAID Level	RAID level on which the logical device has been created.
Device Type	Drive type indicates the type of logical device like data and etc.
Interface Type	Disk drive which are RAID member of logical device can have interface type such SAS or SATA will also reflect as interface type of logical device. A logical drive can be combination of SAS and SATA interface.
Data Space	Data space is where actual data is striped across the disk drives.

© 2021 Microchip Technology Inc. and its subsidiaries

.....continued

Property	Tooltip Details
Stripe Size	Stripe size is the amount of data (in KB) written to one disk drive, before moving to the next disk drive in the logical device. Stripe size options vary, depending on your controller and RAID level.
Full Stripe Size	Full stripe size refers to the combined size of all the strips across all physical drives, excluding parity-only drives.
Member Device(s) Block Size	Maximum size of data block on disk drives which are RAID member of logical device (can be 512 Bytes or 4K).
Volume Unique Identifier	The logical device unique identifier.
Heads	Heads indicates the pre-defined space set aside for RAID redundant information on a logical device.
Sectors Per Track	Sectors Per Track specifies the number of sectors that are to comprise each track.
Cylinders	Cylinders indicates the set of all of tracks of equal diameter in a logical device.
Status	Status of logical device based on health of RAID members of logical device.
Name	Logical device name can be of maximum 64 characters and it should contain only ASCII characters
Disk Name	Name of the logical disk drive
OS Location	Operating system location of the logical disk drive
Mounted	Mount points describes the Operating system device names of the logical device.
Controller Caching	This option toggles the controller cache preservation state. When enabled, the system preserves the controller's cache to prevent data loss in the event of a system failures like power loss or shutdown
Acceleration Method	Logical Device Acceleration Method indicates whether caching for logical device enabled through controller cache. Defaults to enable.
Boot Type	A bootable logical device is a logical device that the system can attempt to boot from after a system power-on. A controller can have up to two bootable logical device, where one is a primary boot logical device and the other a secondary boot logical device. When the system looks at a controller for a boot logical device, it will first attempt to boot from a primary boot logical device, and if that fails, then it will attempt to boot from a secondary boot logical device.
Protected by Hot Spare	Protected by Hot Spare indicates whether the logical device is protected by Hot Spare.
maxCrypto	
Encrypted	Indicate user whether the logical device is encrypted or not.
maxCache	

.....continued	
Property	**Tooltip Details**
State	State of the associated maxCache logical device.
Write Cache Policy	The current write cache policy used by the associated maxCache for data write operations. This will indicate whether the posted write operations to this logical device, are transferred via the write cache memory.
Write Cache Policy Preferred	The write cache policy preferred by the user for data write operations to this logical device.
Write Cache Policy Status	The status of current write cache policy used by the associated maxCache.

Table 22-4. Physical Device Display Properties

Property	Tooltip Details
Vendor	Physical device manufacturer name.
Model	Product model name of the physical device.
Serial Number	Serial number of physical device.
Interface Type	Interface type supported by the physical device.
Total Size	Total data storage capacity of the physical device.
Block Size	Maximum size of data block on disk drives which are RAID member of logical device (can be 512 Bytes or 4K).
Physical Block Size	Physical block size is the unit of data that can be physically read or write to the disk.
Rotational Speed	Indicates the rotational speed of the physical device.
Device Type	Type of physical device such as "hard disk drive", "solid state drive" or "shingled magnetic recording hard disk drive".
Firmware Level	Firmware version of the physical device.
WWN	Reported world wide name provided by manufacturer.
Unique ID	ID to uniquely identify the physical device.
Reported Channel	The channel to which the physical device is connected.
Reported SCSI Device ID	The SCSI ID for a physicals device reported by controller.
NCQ Supported	Specifies whether this physical device supports native command queuing.
NCQ Status	Indicates whether the native command queuing is enabled/disabled on this physical device.
Sanitize Erase	Specifies whether the sanitize erase is supported by this physical device.

© 2021 Microchip Technology Inc. and its subsidiaries

.....continued

Property	Tooltip Details
Sanitize Lock Freeze	Specifies whether the sanitize lock freeze is supported by this physical device.
Sanitize Lock Anti-Freeze	Specifies whether the sanitize lock anti-freeze is supported by this physical device.
Encryption Capability	A SED (or Self-Encrypting Drive) is a type of hard drive that automatically and continuously encrypts the data on the drive without any user interaction.
State	Current state of physical device based on the operations done on it.
Negotiated Transfer Speed	Negotiated data transfer rate of selected physical device.
Configuration Type	Determines the presence/type of logical devices of which this physical device is a part of.
SED Security Status	Current status of Self-Encrypting Drive (SED).
SED Qualification Status	The current status of the SED qualification.
Boot Type	A bootable physical device is a physical device that the system can attempt to boot from after a system power-on. A controller can have up to two bootable physical device, where one is a primary boot physical device and the other a secondary boot physical device. When the system looks at a controller for a boot physical device, it will first attempt to boot from a primary boot physical device, and if that fails, then it will attempt to boot from a secondary boot physical device.
Exposed to OS	Indicates whether the physical device is exposed to the operating system.
Disk Name	Name of the physical disk drive
OS Location	Operating system location of the physical disk drive
Partitioned	Partition describes that the physical device is exposed to operating system or not. The drive must be partitioned and formatted for storing data.
Mounted	Mount point(s) describes the operating system device names of the physical device.
Has Stale RIS Data	Specifies whether the physical device has stale RIS data.
S.M.A.R.T. Error	Any SMART error reported on physical device.
Current Temperature	Current temperature of the physical device.
Maximum Temperature	The maximum temperature reported by the physical device.
Threshold Temperature	The threshold temperature value of the physical device.
Encrypted Drive	Indicates whether this physical device is a part of any encrypted logical device.
Negotiated Physical Link Rate	Negotiated Physical Link Rate

© 2021 Microchip Technology Inc.
and its subsidiaries

.....continued	
Property	**Tooltip Details**
Negotiated Logical Link Rate	Negotiated Logical Link Rate
Maximum Link Rate	Maximum Link Rate
Last Known Reason for Failure	Indicates last known failure occurred on this device.

© 2021 Microchip Technology Inc.
and its subsidiaries

23. maxView Video Tutorials

The following table provides the list of maxView video tutorials, their descriptions, and the web links to access them online.

Table 23-1. maxView Video Tutorials

S.No	Topic	Details	Links
1	maxView Remote System Management for Adaptec® RAID Adapters and Host Bus Adapters	This video shows how to remotely view, monitor, and configure all Adaptec® SAS/SATA RAID adapters and Host Bus Adapters (HBAs) in your storage infrastructure with Adaptec® maxView Storage Manager.	https://youtu.be/Wzcnz9KuL0U
2	How to flash firmware using Adaptec® maxView Storage Manager	This video provides step-by-step instructions to flash firmware on Adaptec® SAS/SATA RAID adapters and Host Bus Adapters (HBAs) using maxView Storage Manager.	https://www.youtube.com/watch?v=9xPTgZASiSc
3	Export and Import Remote Systems Using maxView Storage Manager	This video provides instructions on how to import and /or export remote systems from your network using the Adaptec® maxView Storage Manager user interface	https://www.youtube.com/watch?v=Nu-Il4eidIM&feature=youtu.be&ab_channel=MicrochipTechnology
4	How to Diagnose Errors using Adaptec® maxView Storage Manager	This video allows users to quickly identify, isolate, review and fix errors using an intuitive, browser-based software application. maxView Storage Manager can be used locally or remotely across storage platforms featuring Adaptec® storage adapters and popular third-party vendor solutions that have integrated remote management.	https://www.youtube.com/watch?v=2ffI3Lm5LEE

© 2021 Microchip Technology Inc. and its subsidiaries

.....continued

S.No	Topic	Details	Links
5	How to Force a Logical Drive with Multiple Drive Failures Back Online	In our previous video on How to Diagnose Errors using Adaptec® maxView Storage Manager, you have already learned how to identify a failed or failing component using maxView Storage Manager. This video focuses on how to force a logical drive, with multiple drive failures, back online using maxView storage manager to try and recover lost data.	https://youtu.be/pRNBd39UXdw

© 2021 Microchip Technology Inc. and its subsidiaries

24. Revision History

Revision	Date	Description
A	10/2021	The following is a summary of changes in revision A of this document: • The document was updated to latest Microchip template. • The document number was changed from PMC-2153109 to DS00004219A. • Added section Installing on VMware 7.x and Uninstalling from VMware 7.x.

© 2021 Microchip Technology Inc. and its subsidiaries

The Microchip Website

Microchip provides online support via our website at www.microchip.com/. This website is used to make files and information easily available to customers. Some of the content available includes:

- **Product Support** – Data sheets and errata, application notes and sample programs, design resources, user's guides and hardware support documents, latest software releases and archived software
- **General Technical Support** – Frequently Asked Questions (FAQs), technical support requests, online discussion groups, Microchip design partner program member listing
- **Business of Microchip** – Product selector and ordering guides, latest Microchip press releases, listing of seminars and events, listings of Microchip sales offices, distributors and factory representatives

Product Change Notification Service

Microchip's product change notification service helps keep customers current on Microchip products. Subscribers will receive email notification whenever there are changes, updates, revisions or errata related to a specified product family or development tool of interest.

To register, go to www.microchip.com/pcn and follow the registration instructions.

Customer Support

Users of Microchip products can receive assistance through several channels:

- Distributor or Representative
- Local Sales Office
- Embedded Solutions Engineer (ESE)
- Technical Support

Customers should contact their distributor, representative or ESE for support. Local sales offices are also available to help customers. A listing of sales offices and locations is included in this document.

Technical support is available through the website at: www.microchip.com/support

Microchip Devices Code Protection Feature

Note the following details of the code protection feature on Microchip products:

- Microchip products meet the specifications contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is secure when used in the intended manner, within operating specifications, and under normal conditions.
- Microchip values and aggressively protects its intellectual property rights. Attempts to breach the code protection features of Microchip product is strictly prohibited and may violate the Digital Millennium Copyright Act.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of its code. Code protection does not mean that we are guaranteeing the product is "unbreakable". Code protection is constantly evolving. Microchip is committed to continuously improving the code protection features of our products.

Legal Notice

This publication and the information herein may be used only with Microchip products, including to design, test, and integrate Microchip products with your application. Use of this information in any other manner violates these terms. Information regarding device applications is provided only for your convenience and may be superseded by updates. It is your responsibility to ensure that your application meets with your specifications. Contact your local Microchip sales office for additional support or, obtain additional support at www.microchip.com/en-us/support/design-help/client-support-services.

THIS INFORMATION IS PROVIDED BY MICROCHIP "AS IS". MICROCHIP MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WHETHER EXPRESS OR IMPLIED, WRITTEN OR ORAL, STATUTORY OR OTHERWISE, RELATED TO THE INFORMATION INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE, OR WARRANTIES RELATED TO ITS CONDITION, QUALITY, OR PERFORMANCE.

IN NO EVENT WILL MICROCHIP BE LIABLE FOR ANY INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, OR CONSEQUENTIAL LOSS, DAMAGE, COST, OR EXPENSE OF ANY KIND WHATSOEVER RELATED TO THE INFORMATION OR ITS USE, HOWEVER CAUSED, EVEN IF MICROCHIP HAS BEEN ADVISED OF THE POSSIBILITY OR THE DAMAGES ARE FORESEEABLE. TO THE FULLEST EXTENT ALLOWED BY LAW, MICROCHIP'S TOTAL LIABILITY ON ALL CLAIMS IN ANY WAY RELATED TO THE INFORMATION OR ITS USE WILL NOT EXCEED THE AMOUNT OF FEES, IF ANY, THAT YOU HAVE PAID DIRECTLY TO MICROCHIP FOR THE INFORMATION.

Use of Microchip devices in life support and/or safety applications is entirely at the buyer's risk, and the buyer agrees to defend, indemnify and hold harmless Microchip from any and all damages, claims, suits, or expenses resulting from such use. No licenses are conveyed, implicitly or otherwise, under any Microchip intellectual property rights unless otherwise stated.

Trademarks

The Microchip name and logo, the Microchip logo, Adaptec, AnyRate, AVR, AVR logo, AVR Freaks, BesTime, BitCloud, CryptoMemory, CryptoRF, dsPIC, flexPWR, HELDO, IGLOO, JukeBlox, KeeLoq, Kleer, LANCheck, LinkMD, maXStylus, maXTouch, MediaLB, megaAVR, Microsemi, Microsemi logo, MOST, MOST logo, MPLAB, OptoLyzer, PIC, picoPower, PICSTART, PIC32 logo, PolarFire, Prochip Designer, QTouch, SAM-BA, SenGenuity, SpyNIC, SST, SST Logo, SuperFlash, Symmetricom, SyncServer, Tachyon, TimeSource, tinyAVR, UNI/O, Vectron, and XMEGA are registered trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

AgileSwitch, APT, ClockWorks, The Embedded Control Solutions Company, EtherSynch, Flashtec, Hyper Speed Control, HyperLight Load, IntelliMOS, Libero, motorBench, mTouch, Powermite 3, Precision Edge, ProASIC, ProASIC Plus, ProASIC Plus logo, Quiet- Wire, SmartFusion, SyncWorld, Temux, TimeCesium, TimeHub, TimePictra, TimeProvider, TrueTime, WinPath, and ZL are registered trademarks of Microchip Technology Incorporated in the U.S.A.

Adjacent Key Suppression, AKS, Analog-for-the-Digital Age, Any Capacitor, AnyIn, AnyOut, Augmented Switching, BlueSky, BodyCom, CodeGuard, CryptoAuthentication, CryptoAutomotive, CryptoCompanion, CryptoController, dsPICDEM, dsPICDEM.net, Dynamic Average Matching, DAM, ECAN, Espresso T1S, EtherGREEN, GridTime, IdealBridge, In-Circuit Serial Programming, ICSP, INICnet, Intelligent Paralleling, Inter-Chip Connectivity, JitterBlocker, Knob-on-Display, maxCrypto, maxView, memBrain, Mindi, MiWi, MPASM, MPF, MPLAB Certified logo, MPLIB, MPLINK, MultiTRAK, NetDetach, NVM Express, NVMe, Omniscient Code Generation, PICDEM, PICDEM.net, PICkit, PICtail, PowerSmart, PureSilicon, QMatrix, REAL ICE, Ripple Blocker, RTAX, RTG4, SAM-ICE, Serial Quad I/O, simpleMAP, SimpliPHY, SmartBuffer, SmartHLS, SMART-I.S., storClad, SQI, SuperSwitcher, SuperSwitcher II, Switchtec, SynchroPHY, Total Endurance, TSHARC, USBCheck, VariSense, VectorBlox, VeriPHY, ViewSpan, WiperLock, XpressConnect, and ZENA are trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

SQTP is a service mark of Microchip Technology Incorporated in the U.S.A.

The Adaptec logo, Frequency on Demand, Silicon Storage Technology, Symmcom, and Trusted Time are registered trademarks of Microchip Technology Inc. in other countries.

GestIC is a registered trademark of Microchip Technology Germany II GmbH & Co. KG, a subsidiary of Microchip Technology Inc., in other countries.

All other trademarks mentioned herein are property of their respective companies.

© 2021, Microchip Technology Incorporated and its subsidiaries. All Rights Reserved.

ISBN: 978-1-5224-9130-9

Quality Management System

For information regarding Microchip's Quality Management Systems, please visit www.microchip.com/quality.

Worldwide Sales and Service

AMERICAS	ASIA/PACIFIC	ASIA/PACIFIC	EUROPE
Corporate Office 2355 West Chandler Blvd. Chandler, AZ 85224-6199 Tel: 480-792-7200 Fax: 480-792-7277 Technical Support: www.microchip.com/support Web Address: www.microchip.com **Atlanta** Duluth, GA Tel: 678-957-9614 Fax: 678-957-1455 **Austin, TX** Tel: 512-257-3370 **Boston** Westborough, MA Tel: 774-760-0087 Fax: 774-760-0088 **Chicago** Itasca, IL Tel: 630-285-0071 Fax: 630-285-0075 **Dallas** Addison, TX Tel: 972-818-7423 Fax: 972-818-2924 **Detroit** Novi, MI Tel: 248-848-4000 **Houston, TX** Tel: 281-894-5983 **Indianapolis** Noblesville, IN Tel: 317-773-8323 Fax: 317-773-5453 Tel: 317-536-2380 **Los Angeles** Mission Viejo, CA Tel: 949-462-9523 Fax: 949-462-9608 Tel: 951-273-7800 **Raleigh, NC** Tel: 919-844-7510 **New York, NY** Tel: 631-435-6000 **San Jose, CA** Tel: 408-735-9110 Tel: 408-436-4270 **Canada - Toronto** Tel: 905-695-1980 Fax: 905-695-2078	**Australia - Sydney** Tel: 61-2-9868-6733 **China - Beijing** Tel: 86-10-8569-7000 **China - Chengdu** Tel: 86-28-8665-5511 **China - Chongqing** Tel: 86-23-8980-9588 **China - Dongguan** Tel: 86-769-8702-9880 **China - Guangzhou** Tel: 86-20-8755-8029 **China - Hangzhou** Tel: 86-571-8792-8115 **China - Hong Kong SAR** Tel: 852-2943-5100 **China - Nanjing** Tel: 86-25-8473-2460 **China - Qingdao** Tel: 86-532-8502-7355 **China - Shanghai** Tel: 86-21-3326-8000 **China - Shenyang** Tel: 86-24-2334-2829 **China - Shenzhen** Tel: 86-755-8864-2200 **China - Suzhou** Tel: 86-186-6233-1526 **China - Wuhan** Tel: 86-27-5980-5300 **China - Xian** Tel: 86-29-8833-7252 **China - Xiamen** Tel: 86-592-2388138 **China - Zhuhai** Tel: 86-756-3210040	**India - Bangalore** Tel: 91-80-3090-4444 **India - New Delhi** Tel: 91-11-4160-8631 **India - Pune** Tel: 91-20-4121-0141 **Japan - Osaka** Tel: 81-6-6152-7160 **Japan - Tokyo** Tel: 81-3-6880- 3770 **Korea - Daegu** Tel: 82-53-744-4301 **Korea - Seoul** Tel: 82-2-554-7200 **Malaysia - Kuala Lumpur** Tel: 60-3-7651-7906 **Malaysia - Penang** Tel: 60-4-227-8870 **Philippines - Manila** Tel: 63-2-634-9065 **Singapore** Tel: 65-6334-8870 **Taiwan - Hsin Chu** Tel: 886-3-577-8366 **Taiwan - Kaohsiung** Tel: 886-7-213-7830 **Taiwan - Taipei** Tel: 886-2-2508-8600 **Thailand - Bangkok** Tel: 66-2-694-1351 **Vietnam - Ho Chi Minh** Tel: 84-28-5448-2100	**Austria - Wels** Tel: 43-7242-2244-39 Fax: 43-7242-2244-393 **Denmark - Copenhagen** Tel: 45-4485-5910 Fax: 45-4485-2829 **Finland - Espoo** Tel: 358-9-4520-820 **France - Paris** Tel: 33-1-69-53-63-20 Fax: 33-1-69-30-90-79 **Germany - Garching** Tel: 49-8931-9700 **Germany - Haan** Tel: 49-2129-3766400 **Germany - Heilbronn** Tel: 49-7131-72400 **Germany - Karlsruhe** Tel: 49-721-625370 **Germany - Munich** Tel: 49-89-627-144-0 Fax: 49-89-627-144-44 **Germany - Rosenheim** Tel: 49-8031-354-560 **Israel - Ra'anana** Tel: 972-9-744-7705 **Italy - Milan** Tel: 39-0331-742611 Fax: 39-0331-466781 **Italy - Padova** Tel: 39-049-7625286 **Netherlands - Drunen** Tel: 31-416-690399 Fax: 31-416-690340 **Norway - Trondheim** Tel: 47-72884388 **Poland - Warsaw** Tel: 48-22-3325737 **Romania - Bucharest** Tel: 40-21-407-87-50 **Spain - Madrid** Tel: 34-91-708-08-90 Fax: 34-91-708-08-91 **Sweden - Gothenberg** Tel: 46-31-704-60-40 **Sweden - Stockholm** Tel: 46-8-5090-4654 **UK - Wokingham** Tel: 44-118-921-5800 Fax: 44-118-921-5820

© 2021 Microchip Technology Inc.
and its subsidiaries