

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



# Table of Contents

1.	About this Guide.....	6
1.1.	What You Need to Know Before You Begin.....	6
1.2.	Terminology Used in this Guide.....	6
1.3.	How to Find More Information.....	7
2.	Introduction to maxView Storage Manager.....	8
2.1.	Getting Started.....	8
2.2.	About maxView Storage Manager.....	8
2.3.	System Requirements.....	8
2.4.	Browser Support.....	9
2.5.	Typical Storage Space Configurations.....	9
3.	Installing maxView Storage Manager.....	12
3.1.	Before You Begin the Installation.....	12
3.2.	Installing on Windows.....	12
3.3.	Installing on Red Hat, Citrix XenServer, CentOS, or SuSE Linux.....	14
3.4.	Installing on Debian or Ubuntu Linux.....	14
3.5.	Installing on VMware 7.x and ESXi 8.x.....	15
3.6.	Running maxView™ Storage Manager from a Bootable USB Image.....	16
3.7.	Uninstalling maxView Storage Manager.....	17
4.	Exploring maxView Storage Manager.....	19
4.1.	Starting maxView Storage Manager and Logging In .....	19
4.2.	Working in maxView Storage Manager.....	19
4.3.	Overview of the Main Window.....	20
4.4.	Checking System Status from the Main Window.....	24
4.5.	Revealing More Device Information .....	25
4.6.	Getting Help.....	26
4.7.	Logging Out of maxView Storage Manager.....	26
5.	Building Your Storage Space.....	27
5.1.	Overview.....	27
5.2.	Choosing a Management System.....	27
5.3.	Logging into Remote Systems from the Local System.....	28
5.4.	Creating Arrays and Logical Drives.....	29
5.5.	Controller Support for 4K Drives.....	37
5.6.	Controller Support for SED.....	43
6.	Protecting Your Data.....	48
6.1.	Dedicated Spare or Auto-Replace Spare?.....	48
6.2.	Hot Spare Limitations.....	48
6.3.	Assigning a Dedicated Hot Spare.....	48
6.4.	Assigning an Auto-Replace Hot Spare.....	50
6.5.	Removing a Hot Spare.....	52
6.6.	Setting the Spare Activation Mode .....	54
6.7.	Controller Sanitize Lock Freeze/Anti-Freeze .....	55
7.	Modifying Your Storage Space.....	59

7.1.	Understanding Arrays and Logical Drives.....	59
7.2.	Creating and Modifying Logical Drives.....	59
7.3.	Enabling Background Consistency Check.....	60
7.4.	Optimizing Logical Drive Performance.....	61
7.5.	Moving a Logical Drive.....	64
7.6.	Moving an Array.....	66
7.7.	Modifying an Array.....	67
7.8.	Working with Mirrored Arrays.....	69
7.9.	Changing the RAID Level of a Logical Drive.....	71
7.10.	Increasing the Capacity of a Logical Drive.....	72
7.11.	Changing the Logical Drive Rebuild Priority.....	73
7.12.	Renaming a Logical Drive.....	74
7.13.	Deleting an Array or Logical Drive .....	74
7.14.	Maintaining an Energy-Efficient Storage Space .....	75
8.	Working with maxCache Devices.....	77
8.1.	maxCache Limitations.....	77
8.2.	Creating a maxCache Device.....	77
8.3.	Changing the Write Cache Mode .....	79
8.4.	Deleting the maxCache Device.....	79
8.5.	Analyzing maxCache Performance .....	80
9.	Working with maxCrypto™ Devices.....	81
9.1.	maxCrypto Initial Setup .....	81
9.2.	Modifying the maxCrypto Configuration .....	87
9.3.	Creating an Encrypted Logical Drive.....	89
9.4.	Converting Plaintext Data to Encrypted Data.....	89
9.5.	Re-Keying a Logical Drive .....	90
9.6.	Clearing the maxCrypto Configuration .....	91
9.7.	Erasing an Encrypted Logical Drive.....	92
9.8.	Importing a Foreign Master Key .....	93
9.9.	Volatile Key.....	94
10.	Working with Self Encrypting Drive (SED) Based Encryption.....	95
10.1.	Self Encrypting Drive (SED) Initial Setup.....	96
10.2.	SED Based Encryption Settings.....	98
10.3.	Physical Device Self Encrypting Drives (SEDs) Properties.....	104
10.4.	Controller Level Operation on Self Encrypting Drives (SEDs).....	105
10.5.	Physical Device Level Operation on Self Encrypting Drives (SEDs).....	106
10.6.	Creating Logical Device.....	108
10.7.	Assigning Spares at the Array Level.....	110
10.8.	Assigning Spares at the Physical Device Level.....	111
10.9.	Creating maxCache.....	112
10.10.	Moving a Logical Drive.....	115
10.11.	Moving an Array.....	119
10.12.	Modifying an Array.....	123
10.13.	Importing Foreign Array.....	123
11.	Working with Security Protocol and Data Model (SPDM).....	125
11.1.	Security Protocol and Data Model (SPDM) Properties.....	125

11.2.	SPDM Security Settings.....	127
11.3.	Get Certificate Chain.....	127
11.4.	Import Certificate Chain.....	128
11.5.	Invalidate Slot.....	128
12.	Maintaining Physical Devices.....	130
12.1.	Viewing Device Properties.....	130
12.2.	Multi Actuator Drives.....	130
12.3.	Locating Drives in Your Storage Space.....	131
12.4.	Working with Physical Device Error Counters.....	134
12.5.	Refresh SED Security Status.....	137
12.6.	Working with Failed or Failing Disk Drives.....	138
12.7.	Erasing a Disk Drive .....	139
12.8.	Initializing and Uninitializing Disk Drives.....	140
12.9.	Setting the Physical Drive Boot Priority.....	142
12.10.	Working with Controllers.....	143
12.11.	Updating Controller, Enclosure, Backplane, and Disk Drive Firmware.....	151
13.	Monitoring Status and Activity.....	159
13.1.	Monitoring Options.....	159
13.2.	Checking Status from the Main Window .....	159
13.3.	Notifying Users by Email About Status and Activity .....	165
13.4.	Changing an Operating System's Event Log Setting.....	171
14.	Managing Your Storage Space.....	172
14.1.	Deploying Servers .....	172
14.2.	Managing Remote Systems.....	175
14.3.	Clearing the Controller Configuration.....	182
14.4.	Changing the Web Server Port.....	182
14.5.	Granting Standard Users Admin Privilege.....	183
15.	Solving Problems.....	185
15.1.	General Troubleshooting Tips.....	185
15.2.	Identifying a Failed or Failing Component.....	185
15.3.	Recovering from a Disk Drive Failure.....	186
15.4.	Rebuilding Logical Drives.....	188
15.5.	Creating a Support Archive File.....	189
16.	Silent Installation on Windows and Linux.....	190
16.1.	Completing a Silent Installation.....	190
16.2.	Example Command Line Installations.....	191
17.	Configuring SNMP Notifications on Windows and Linux.....	192
17.1.	Setting Up SNMP Notifications on Windows.....	192
17.2.	Setting Up SNMP Notifications on Linux.....	192
18.	Using the maxView Plugin for VMware vSphere 7 HTML5.....	194
18.1.	Installing the maxView Plugin for vSphere 7 HTML5 Client.....	194
18.2.	Starting the maxView Plugin for vSphere 7 HTML Client.....	195
18.3.	Monitoring maxView Resources in vSphere 7 HTML Client.....	197
18.4.	Import and Export Remote ESXi Systems using maxView Plugin in vSphere 7 HTML Client.....	200



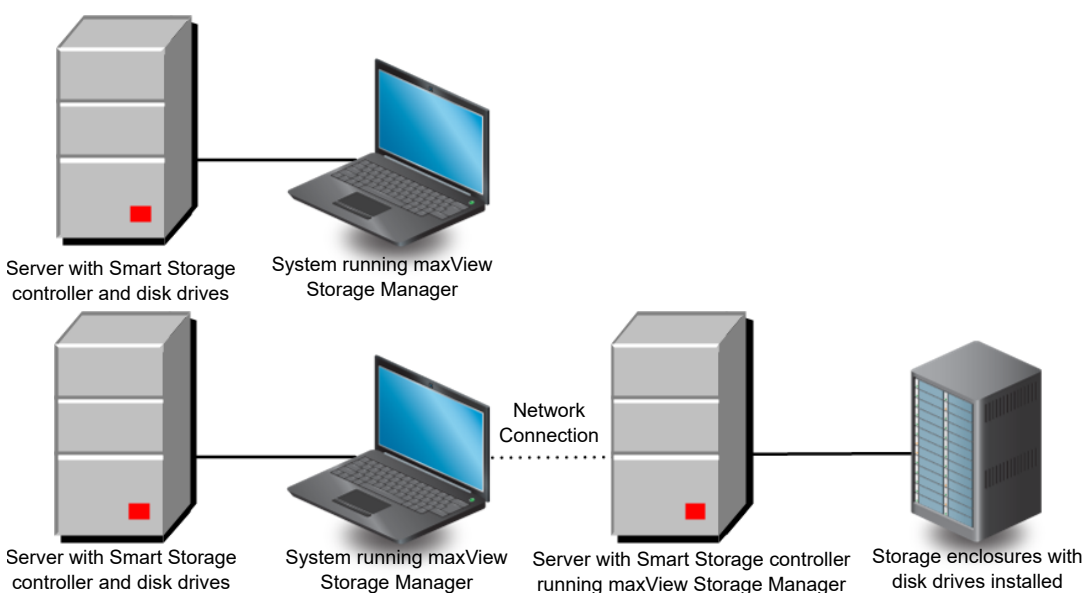
19. Using the maxView Plugin for VMware vSphere 8 HTML5.....	204
19.1. Installing the maxView Plugin for vSphere 8 HTML5 Client.....	204
19.2. Starting the maxView Plugin for vSphere 8 HTML Client.....	205
19.3. Monitoring maxView Resources in vSphere 8 HTML Client.....	206
19.4. Import and Export Remote ESXi Systems using maxView Plugin in vSphere 8 HTML Client.....	208
20. Using maxView Storage Manager with HBAs and Non-RAID Mode Controllers.....	212
21. Selecting the Best RAID Level.....	214
21.1. Comparing RAID Levels.....	214
21.2. Non-redundant Logical Drives (RAID 0).....	214
21.3. RAID 1 Logical Drives .....	215
21.4. RAID 1 Triple Logical Drives.....	215
21.5. RAID 10 Logical Drives.....	216
21.6. RAID 10 Triple Logical Drives.....	216
21.7. RAID 5 Logical Drives.....	217
21.8. RAID 50 Logical Drive.....	218
21.9. RAID 6 Logical Drives.....	219
21.10. RAID 60 Logical Drives.....	220
22. Icons At-a-Glance.....	221
23. Smart Controller Device Status.....	225
24. Display Properties of a Controller, Array, Logical Device, and a Physical Device.....	228
25. maxView Video Tutorials.....	237
26. Revision History.....	238
Microchip Information.....	240
The Microchip Website.....	240
Product Change Notification Service.....	240
Customer Support.....	240
Microchip Devices Code Protection Feature.....	240
Legal Notice.....	240
Trademarks.....	241
Quality Management System.....	242
Worldwide Sales and Service.....	243

## 1. 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 [1.3. How to Find More Information](#).



### 1.1 What You Need to Know Before You Begin

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

If you are using maxView Storage Manager as part of a complex storage system, with multiple servers, enclosures and 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).

### 1.2 Terminology Used in this Guide

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

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

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

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

### 1.3 How to Find More Information

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

## 2. Introduction to maxView Storage Manager

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

### 2.1 Getting Started

The first part of this guide provides the information needed 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 [3. Installing maxView Storage Manager](#)).

**Step 3:** Start maxView Storage Manager and explore its graphical user interface (see [4. Exploring maxView Storage Manager](#)).

**Step 4:** Build your storage space (see [5. Building Your Storage Space](#)).

### 2.2 About maxView Storage Manager

maxView Storage Manager is a browser-based software application that helps you build a storage space for your data, using Microchip 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 [2.4. 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 Redfish server on others.

#### 2.2.1 About maxView Redfish Server

The maxView 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 Redfish Server is installed automatically with the maxView Storage Manager.

#### 2.2.2 About the maxView Storage Manager Web Server

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

### 2.3 System Requirements

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

- PC-compatible computer with Intel Pentium processor, or equivalent

- At least 4 GB of RAM
- 350 MB of free disk drive space
- 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.

## 2.4 Browser Support

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

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

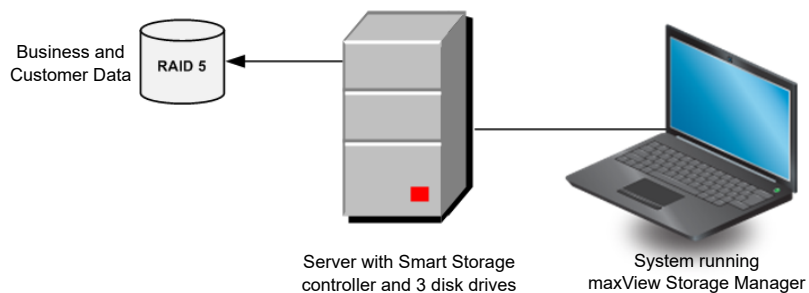
**Note:** The ideal resolution for the best view of the maxView Storage Manager is 1920 x 1080 ppi. The recommended display scaling setting and browser zoom setting is 100%.

## 2.5 Typical Storage Space Configurations

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

### 2.5.1 A Simple Storage Space

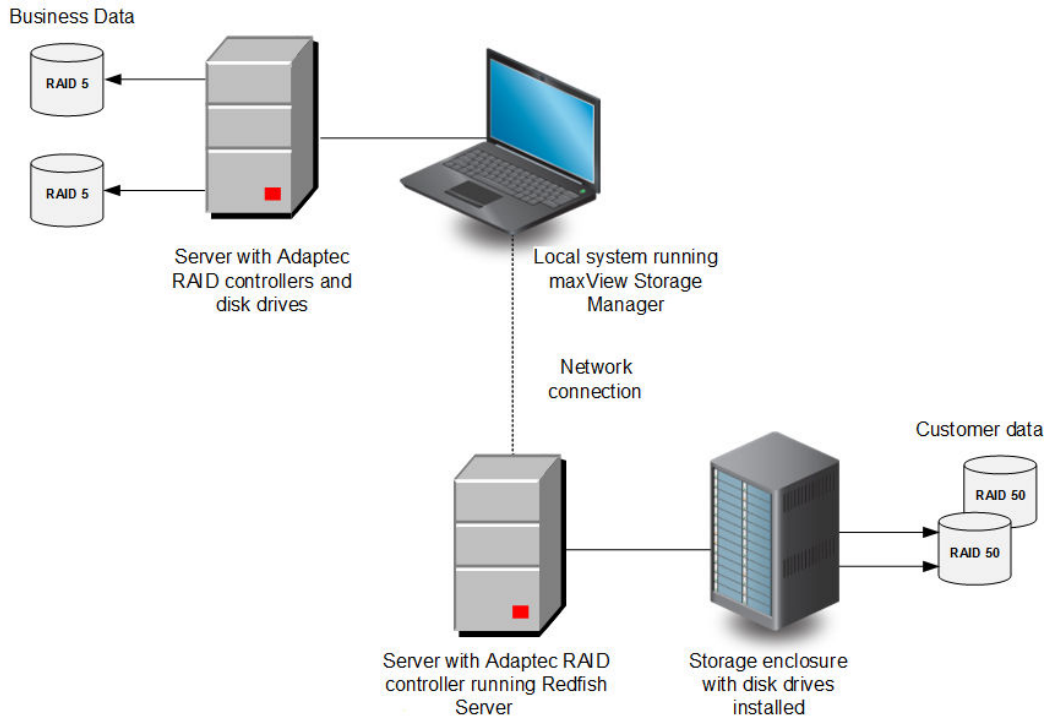
This example shows a simple storage space that might be appropriate for a small business. This storage space includes one RAID controller and three disk drives installed in a server. For data protection, the disk drives have been used to build a RAID 5 logical drive.



### 2.5.2 An Advanced Storage Space

This example shows how you can grow your storage space as the requirements of your application change. On the first server, segments from each disk drive have been used to build two RAID 5

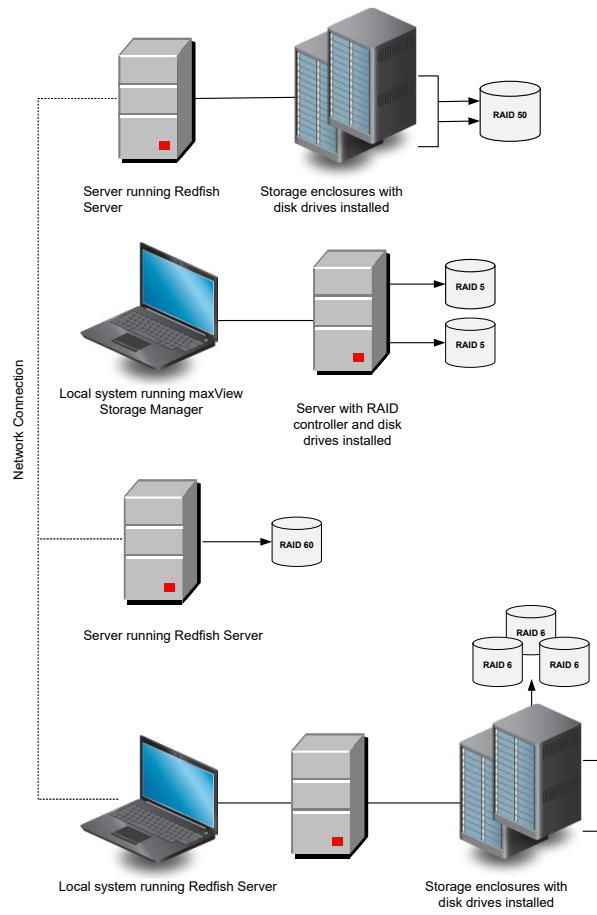
logical drives. A second server connected to two 12-disk enclosures has been added. The Administrator of this storage space can create and modify logical drives and monitor both controllers, disk drives, and enclosures from a single system running the maxView Storage Manager GUI.



### 2.5.3 Continuing to Grow Your Storage Space

For more advanced applications, such as high-volume transaction processing in a "cloud" or data center environment, maxView Storage Manager helps you grow your storage space to include multiple controllers, storage enclosures, and disk drives in multiple locations.

In this example, multiple systems, servers, disk drives, and enclosures have been added to the storage space. The Administrator can create and modify logical drives and monitor all the controllers, enclosures, and disk drives in the storage space from any system running the maxView Storage Manager GUI.



## 3. Installing maxView Storage Manager

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

### 3.1 Before You Begin the Installation

Complete the following steps before you begin the installation.

#### 3.1.1 Gather Installation Information

Prepare the following information:

- Redfish Server port number: The default port is recommended (8081). If the default port is not available, another port number will be automatically assigned. For more information on the Redfish Server, see [2.2.1. About maxView 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 [2.2.2. 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 [3.7. Uninstalling maxView Storage Manager](#) for details.

#### 3.1.1.1 Check Network Configuration

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

- Ensure that the system is configured with an IP address.
- Ensure that the OS hostname is as 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.

#### 3.1.2 Download the Installation Package

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

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

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

## 3.2 Installing on Windows

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

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

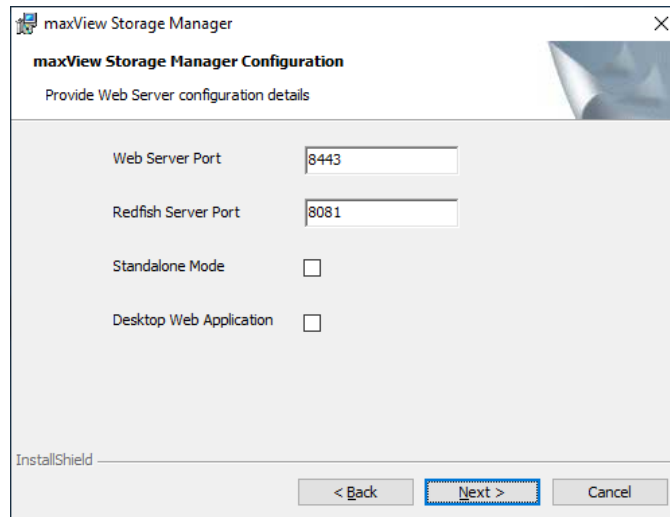


1. Open Windows Explorer or My Computer, then change to the directory where the Windows installer package is located (see 3.1.2. [Download the Installation Package](#) for details).
2. Double click the setup program for your operating system version:

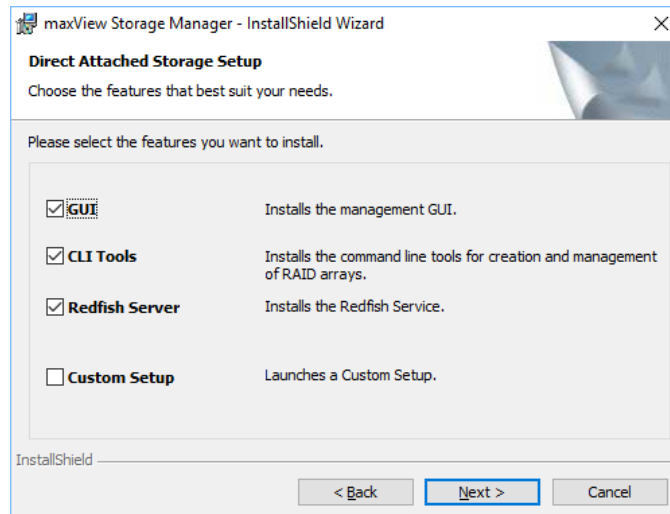
Option	Description
Windows 64-bit	setup_asm_x64.exe

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. To *install* maxView in desktop web application mode, select the **Desktop Web Application** check box.  
**Note:** In Desktop Web Application mode, there are no services installed. The remote system management from the GUI is disabled.
8. 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.
9. Ensure that **GUI and/or Redfish Server** is selected. Optionally, select **CLI Tools**. Click **Next**.



10. Click **Install** to begin the installation.
11. Repeat these steps to install maxView Storage Manager on every Windows system that will be part of your storage space.

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

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

This section describes how to install maxView Storage Manager on systems running Red Hat Linux, CentOS, XenServer, or SuSE Linux. For a list of supported Linux operating systems, see [2.3. System Requirements](#).

1. Open a shell window, then change to the directory where the Linux installer package is located (see [3.1.2. 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	<code>./StorMan-X.XX-XXXXX.x86_64.bin</code>

3. When prompted for configuration details, enter one of the following:  
 Desktop Web Application Mode: [default: No]  
**Note:** Desktop web application mode does not install the services. It *disables* remote system management from the GUI.  
 Standalone Mode: [default: No]  
**Note:** Standalone Mode *disables* remote system management from the GUI. maxView Storage Manager displays the system name as "localhost", and events as "127.0.0.1/localhost".
4. Repeat these steps to install maxView Storage Manager on every Linux system that will be part of your storage space.  
 When the installation completes a confirmation message is displayed and the maxView Storage Manager icon is placed on your desktop.

### 3.4 Installing on Debian or Ubuntu Linux

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

1. Open a shell window, then change to the directory where the Linux installer package is located (see [3.1.2. 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

- 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".  
Desktop Web Application Mode: [default: No]  
**Note:** Desktop web application mode does not install the services. It *disables* the remote system management from the GUI.
- Repeat these steps to install maxView Storage Manager on every Debian and Ubuntu Linux system that will be part of your storage space.
- 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.

### 3.5 Installing on VMware 7.x and ESXi 8.x

Use the following procedure to install the .zip 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.

- Copy the following files from the installer download location to the /tmp directory on your local ESXi.
  - AdaptecArccconf\_x.xx.xxxxx-MIS.x.x.x.xxxxxxxx\_xxxxxxxx.zip
  - AdaptecRedfish\_x.xx.xxxxx-MIS.x.x.x.xxxxxxxx\_xxxxxxxx.zip

The AdaptecArccconf\_x.xx.xxxxx-MIS.x.x.x.xxxxxxxx\_xxxxxxxx.zip is for command line communication. The AdaptecRedfish\_x.xx.xxxxx-MIS.x.x.x.xxxxxxxx\_xxxxxxxx.zip is for remote management communication
- Check for existing installation of ARCCONF.  

```
esxcli software vib list | grep arccconf
```
- Remove the existing ARCCONF package.  

```
esxcli software vib remove -n arccconf
```

  
When the package is removed, you receive the message "Reboot Required: true."
- Check for an existing installation of adaptecredfishserver.  

```
esxcli software vib list | grep adaptecredfishserver
```
- Remove the existing adaptecredfishserver package.  

```
esxcli software vib remove -n adaptecredfishserver
```

  
When the package is removed, you receive the message "Reboot Required: true."
- Set the installation acceptance level to VMwareAccepted:  

```
esxcli software acceptance set --level=VMwareAccepted
```
- Install the ARCCONF package.  

```
esxcli software vib install -d /tmp/AdaptecArccconf_x.xx.xxxxx-MIS.x.x.x.xxxxxxxx_xxxxxxxx.zip
```

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

```
esxcli software vib install -d /tmp/AdaptecRedfish_x.xx.xxxxxx-
MIS.x.x.x.xxxxxxxx_xxxxxxxx.zip
```

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

9. To add a remote system, see [14.2. Managing Remote Systems](#).
10. Execute the following command in ESXI 8.x to permit the write access to root user in order to add system and perform operations from maxView GUI.
 

```
esxcli daemon entitlement add -r -w -p root
```

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

**Note:** There are specific `arcconf` and `adaptecraidfishserver` packages for each VMware versions. Use the appropriate package for installation.

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

Running maxView Storage Manager from a *bootable USB image* allows you to configure your controller before installing 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 installing 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 [storage.microsemi.com/en-us/support/](http://storage.microsemi.com/en-us/support/) 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 arconf** 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 [5.4. Creating Arrays and Logical Drives](#).

While loading the BootUSB image, if you get the "NMI watchdog: BUG soft lockup - cpu#0 stuck for 22s!" error message then execute one of the following step in the "GNU GRUB" bootloader screen:

1. Perform the boot operation using the Troubleshoot --> Start Mscv\_Boot\_usb<Build Number> in basic graphics mode.
2. Manually set "nomodeset" by selecting 'e' command and add "nomodeset" in 'linuxefi' line.

## 3.7 Uninstalling maxView Storage Manager

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

### 3.7.1 Uninstalling from Windows

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

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

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

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

### 3.7.3 Uninstalling from Ubuntu Linux

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

1. Type the command `dpkg -r StorMan`
2. Type the command to uninstall maxView after the upgrade `export maxView_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.

### 3.7.4 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 arconf`  
`esxcli software vib list | grep adaptecredfishserver`
3. Remove the arconf package:  
`esxcli software vib remove -n arconf`
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.

## 4. Exploring maxView Storage Manager

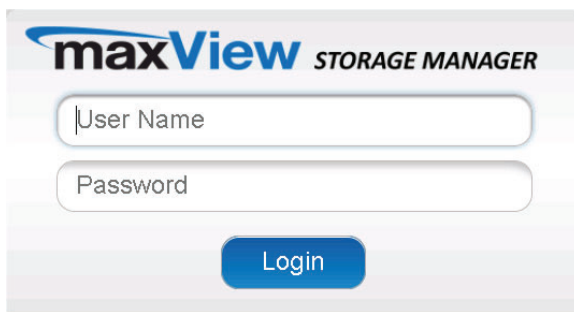
This section familiarizes you with the main features of the maxView Storage Manager graphical user interface. It describes how to start and login to maxView Storage Manager. It also explains how to get help and log out of maxView Storage Manager when you are finished working with the application.

### 4.1 Starting maxView Storage Manager and Logging In

The procedure for starting and logging in to maxView Storage Manager is the same for all operating systems with a graphical desktop. You can login as the Administrator, with full management-level access to your storage space, or as a Standard user, with restricted access to your storage space (see [4.2. 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.

### 4.2 Working in maxView Storage Manager

You can perform most tasks in maxView Storage Manager by:

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

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

**Note:** maxView Storage Manager allows you to give Standard users Administrator privileges. For details, see [14.5. 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

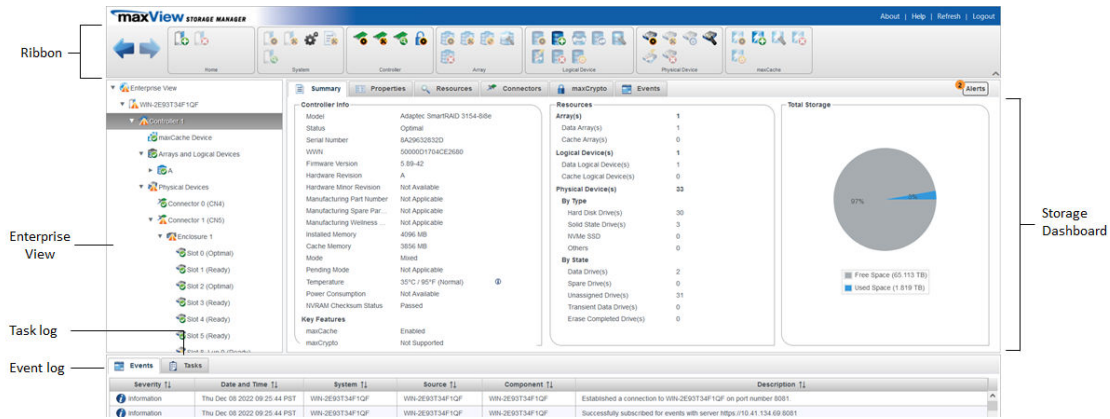
.....continued	
Standard users can:	Standard users can't:
Identify physical devices, logical devices, and enclosures	Delete arrays and logical drives
Silence alarms	Perform data migrations
View component properties on the Storage Dashboard	Clear the controller configuration

### 4.3 Overview of the Main Window

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

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

In example below, a controller is selected in the Enterprise View, and the right panel displays the Storage Dashboard for the controller, with a chart view of its storage space.



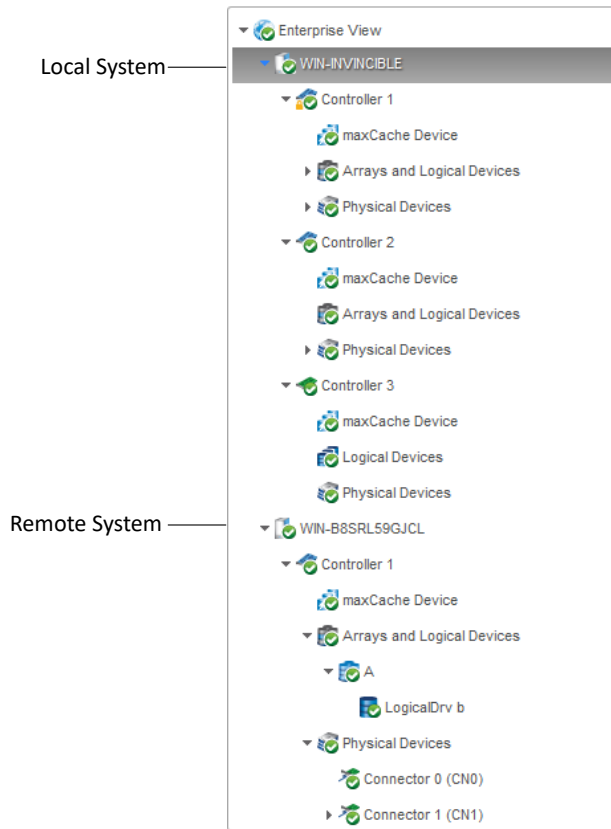
You can resize the panels and scroll horizontally or vertically as needed, to view more or less information.

#### 4.3.1 The Enterprise View

The Enterprise View is an expandable “tree” that shows the physical and logical components of your storage space. The Enterprise View lists the local system (the system you’re working on) and any remote systems that you have logged in to from the local system. (See 5.2.1. ‘Local’ or ‘Remote’? for more information.) It also lists the *maxCache Devices* in your system.

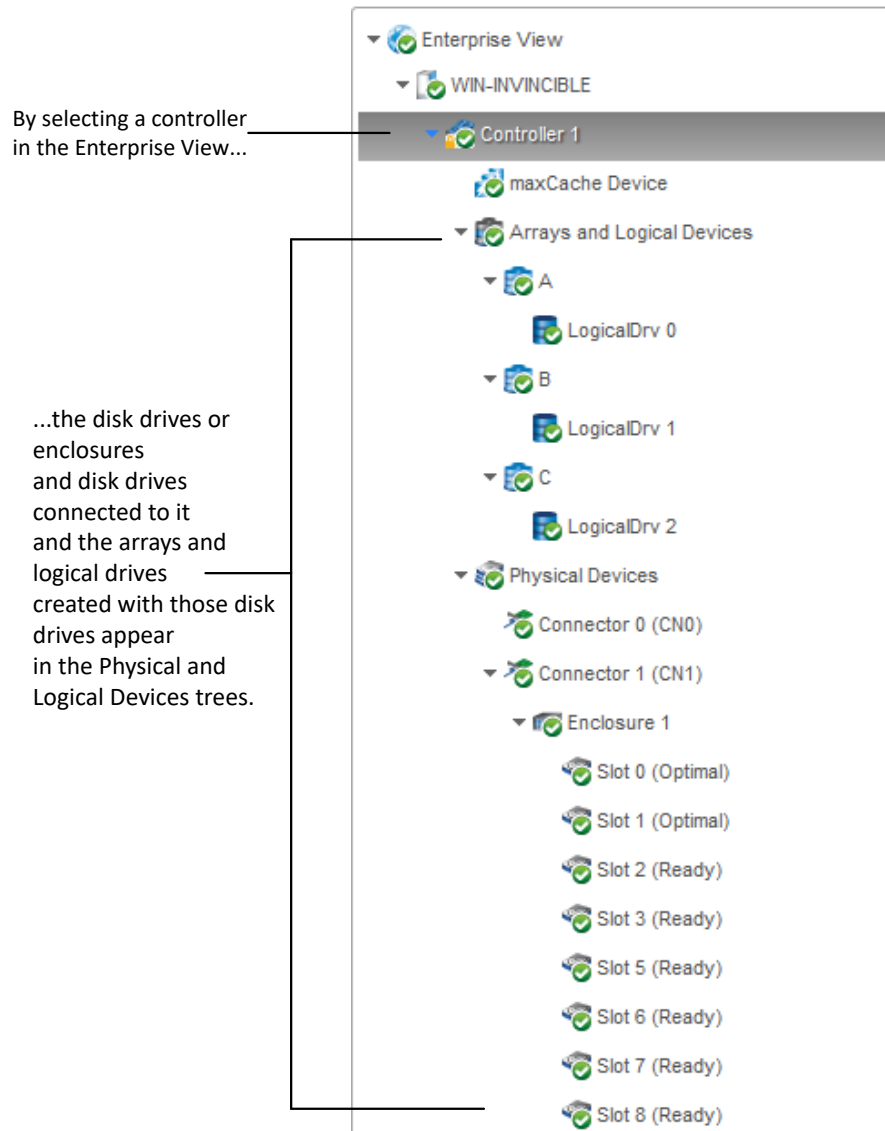
**Note:** maxCache is not supported on all Adaptec Smart Storage Controllers. See the Readme for more information. For more information about maxCache, see 8. Working with maxCache Devices.





Expand a system in the Enterprise View to see its controllers, arrays, logical drives (“devices”), physical drives, enclosures, backplanes, and maxCache devices.

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









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

#### 4.3.1.1 What do the Enterprise View Icons Mean?

Icon	Description
	System with controller and directly attached disk drives or enclosures
	Controller
	Enclosure
	Logical drive (encrypted) <sup>1</sup>

<sup>1</sup> A lock in the Enterprise View means that the device is encrypted. For more information, see [9. Working with maxCrypto™ Devices.](#)

.....continued

Icon	Description
	maxCache Device (healthy) <sup>2</sup>
	Array (healthy)
	Hard disk drive
	Solid State Drive (SSD)
	SMR (Shingled Magnetic Recording) drive <sup>3</sup>
	Connector or other physical device

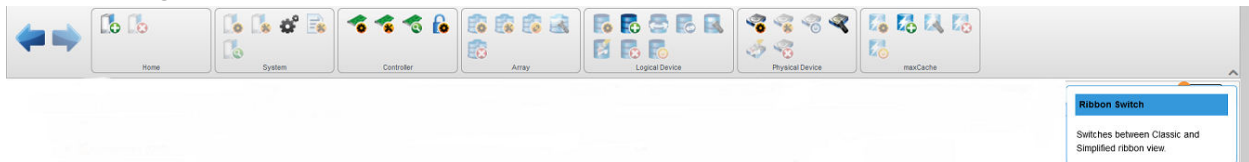
### 4.3.2 The Ribbon

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

There are two formats of ribbon view available:

- Classic Ribbon View
- Simplified Ribbon View

The following screenshot shows the **Classic Ribbon View**:



The classic 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 [14.2. Managing Remote Systems](#)). Active options on the ribbon vary, depending on which type of component is selected in the Enterprise View.

For instance, if a controller is selected in the Enterprise View, the following 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 an array is selected 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.

The following image shows the **Simplified Ribbon View**:



<sup>2</sup> A green check mark in the Enterprise View means that the device is healthy with no problems or issues. For more information, see [15.2. Identifying a Failed or Failing Component](#).

<sup>3</sup> Not supported on all controllers. See the Readme for more information.

The icon highlighted on the top right corner is used to switch between Classic view and Simplified View.

For instance, if a controller is selected in the Enterprise view, only the applicable ribbon icon is visible and activated.

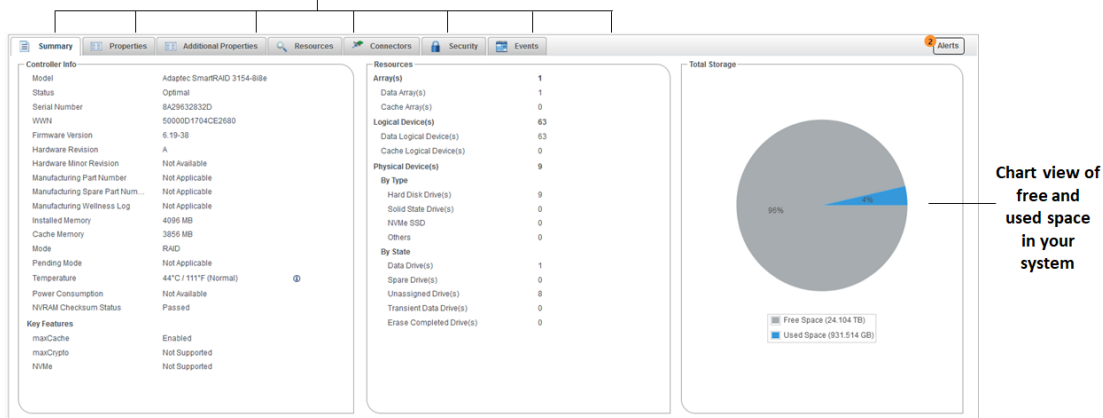
**Note:** You can switch between Classic View and Simplified View at any time.

For a description of the icons on the ribbon, see [22. Icons At-a-Glance](#).

### 4.3.3 The Storage Dashboard

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

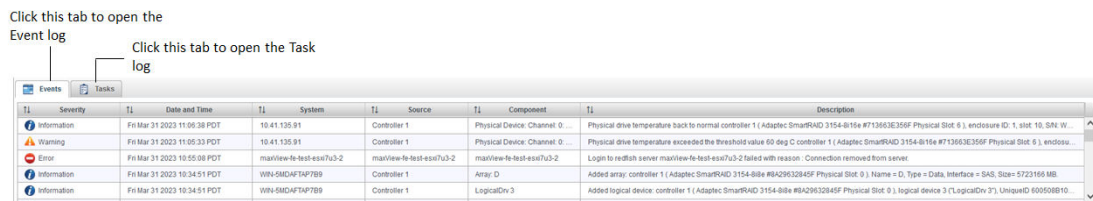
Tabs provide quick access to component information



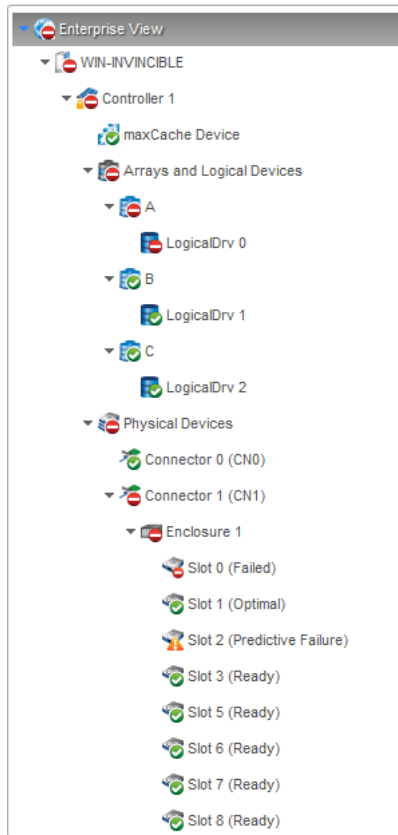
For more information about the types of information provided on the Storage Dashboard for each component in your storage space, see [13.2.3. Viewing Component Status in the Storage Dashboard](#); also see [4.5. Revealing More Device Information](#).

## 4.4 Checking System Status from the Main Window

maxView Storage Manager includes an Event Log and Task Log for at-a-glance status and activity information for all managed systems. The Event Log provides status information and messages about activity (or *events*) occurring in your storage space. The Task Log provides information about current processes in your storage space, such as rebuilding a logical device. Single-click any event or task to see more information in an easier-to-read format.



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 [15.2. 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 [13.2.3.2. Monitoring Enclosure Status](#)).

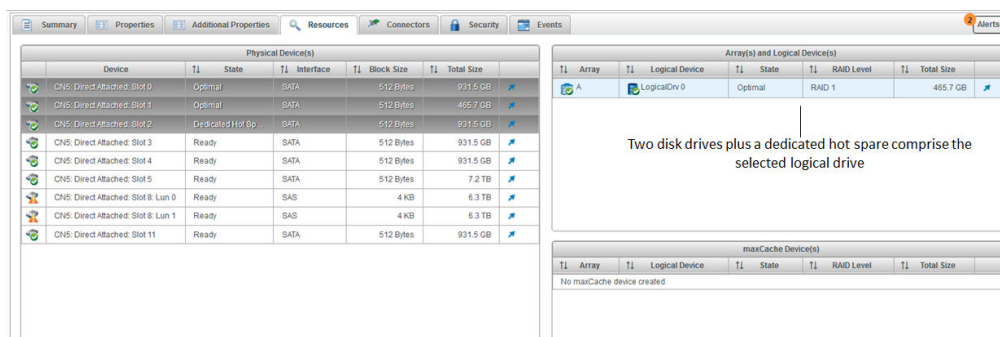
For more information about checking status from the main window, see [Monitoring Status and Activity](#).

#### 4.5 Revealing More Device Information

Reveal more information about disk drive, array, and logical drive usage in the 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. The following figure shows that clicking on a logical drive displays its member disk drives and spares; similarly, clicking on a physical disk displays which array (if any) it belongs to. In the following figure, the disk in Slot 1 and Slot 2 belongs to Array A.

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



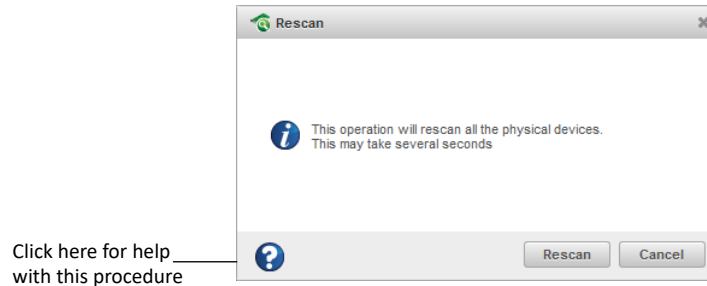
## 4.6 Getting Help

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

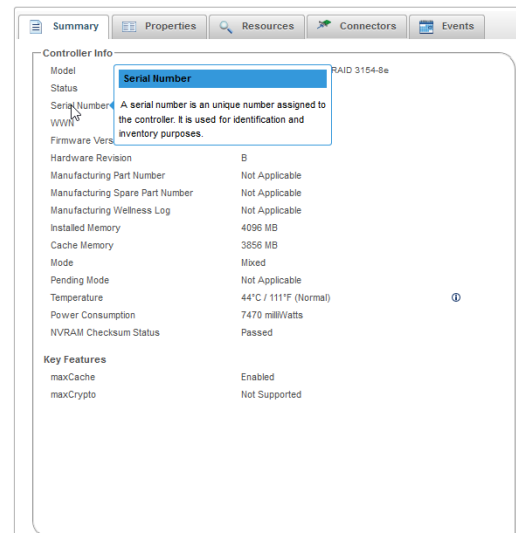
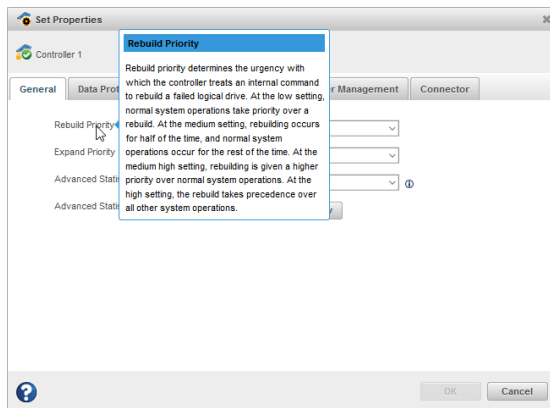
To open the online help, click the **Help** button at the upper-right corner of the main window.



For help with a dialog box or wizard, click the question-mark icon, in the lower corner of the dialog box, for help with that specific procedure.



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



## 4.7 Logging Out of maxView Storage Manager

To log out of maxView Storage Manager:

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



You are logged out of maxView Storage Manager and the main window is closed.

## 5. Building Your Storage Space

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

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

### 5.1 Overview

To build your storage space, complete these steps:

1. Choose at least one management system (see [Choosing a Management System](#)).
2. Start and log in to maxView Storage Manager on the management system (see [4.1. Starting maxView Storage Manager and Logging In](#)).
3. Log in to all other systems from the management system (see [5.3. Logging into Remote Systems from the Local System](#)).
4. Create arrays and logical drives for all systems in your storage space (see [5.4. 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 [7. Modifying Your Storage Space](#).

### 5.2 Choosing a Management System

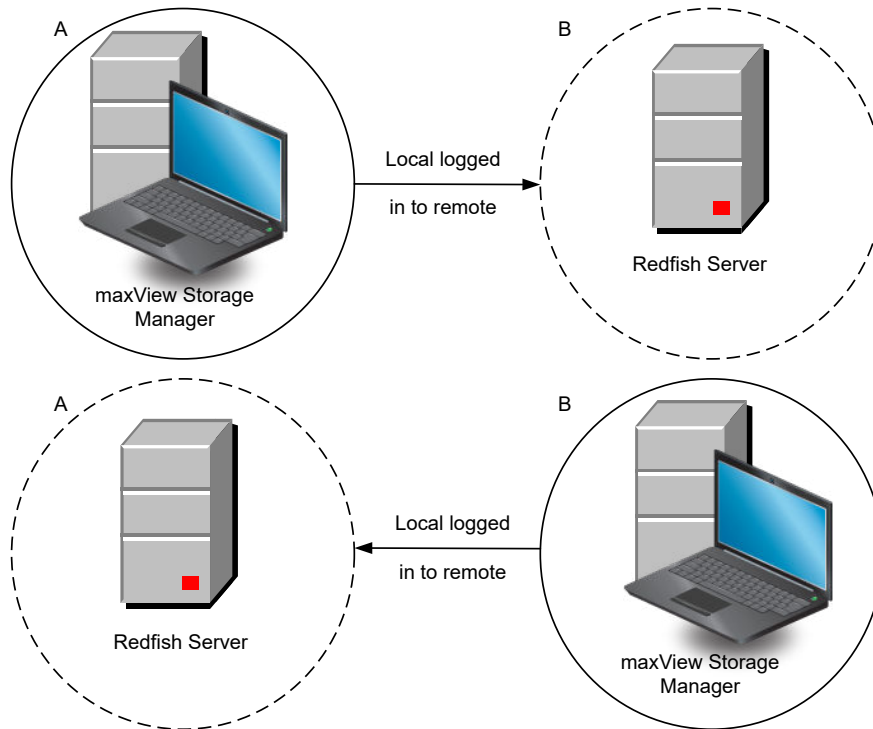
Designate at least one system as a *management system* from which you will manage the storage on all systems in your storage space.

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

#### 5.2.1 'Local' or 'Remote'?

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

For the purposes of this guide, the 'local system' is the management system.



### 5.2.2 Logging in on the Local System

To log in on the local system, see [4.1. Starting maxView Storage Manager and Logging In](#).

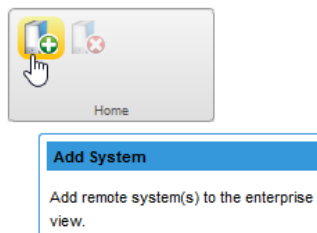
### 5.3 Logging into Remote Systems from the Local System

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

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

To log in to a remote system:

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



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

**Note:**

The list of discovered systems appear only when Auto Discovery option is enabled in maxView. For more details on how to change the auto-discovery settings, see [14.2.4. 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](#).

## 5.4 Creating Arrays and Logical Drives

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

- Create logical drive on new array—Helps you set the RAID level for the logical drive, group disk drives and SSDs, determine logical drive size and other advanced settings.  
For instructions, see [5.4.1. 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 [5.4.2. Creating a Logical Drive on an Existing Array](#).

If maxCrypto is enabled, you can create encrypted or plaintext volumes. (For more information, see [9. 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<sup>4</sup> and SMR DM drives for all RAID levels. However, mixing SMR and PMR<sup>5</sup> 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.

<sup>4</sup> SMR: Shingled Magnetic Recording. HA: Host Aware (backward compatible with standard HDD).  
DM: Device Managed (backward compatible with standard HDD).

<sup>5</sup> PMR: Perpendicular Magnetic Recording; standard HDD recording technology.

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

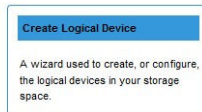
An array must be created before creating a logical drive. Use the **On New Array** configuration method to step through the process of creating a logical drive on a new array, setting the RAID level, and configuring other settings.

To create a logical drive on an existing array, see [5.4.2. Creating a Logical Drive on an Existing Array](#).

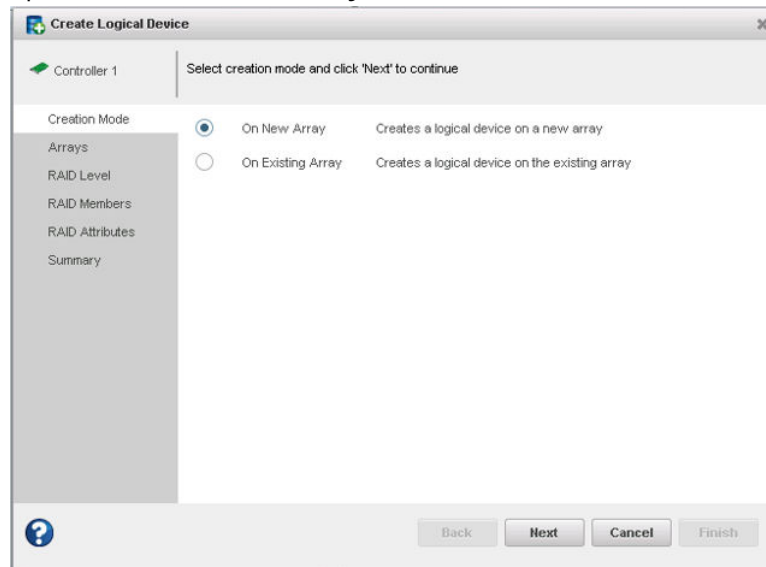
By default, maxView Storage Manager uses all available disk space to maximize the capacity of a new logical drive.

To create a logical drive on a new array:

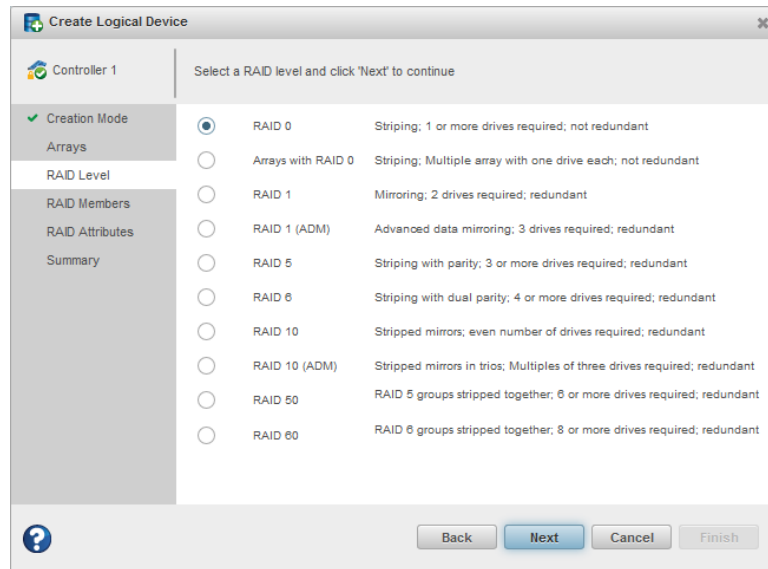
1. In the Enterprise View, select a system, then select a controller on that system.
2. On the ribbon, in the Logical Device group, click **Create Logical Device**.



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

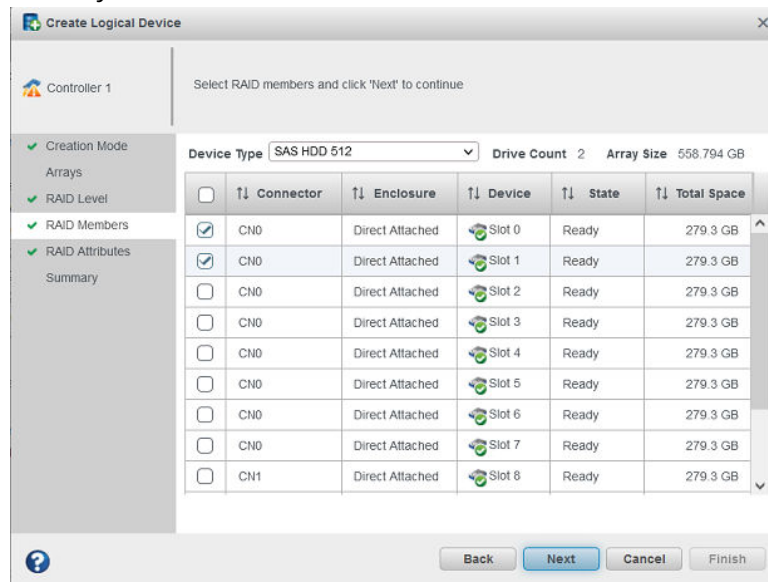


4. Select a RAID level for the logical drive, then click **Next**.



**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 [5.6.1. Create Logical Device](#).

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

The size may be automatically adjusted slightly to optimize performance

Controller 1

Creation Mode

Arrays

RAID Level

RAID Members

RAID Attributes

Summary

Name: LogicalDrv 0

Size: 10 GB Max

Stripe Size (KB): 256

Controller Caching: Enabled

Initialization Method: Default

Encrypt Data:

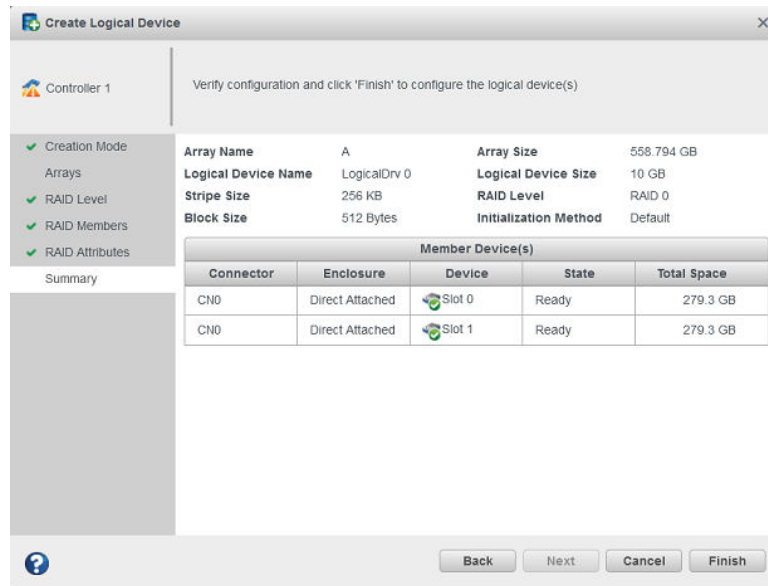
Back Next Cancel Finish

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 [9. Working with maxCrypto™ Devices](#))
7. Click **Next**, then review the array and logical drive settings.  
This example shows a RAID 0 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 [5.4.3. Partitioning and Formatting Your Logical Drives](#).

#### 5.4.2 Creating a Logical Drive on an Existing Array

After creating an array, continue to build the 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 [5.4.1. 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:

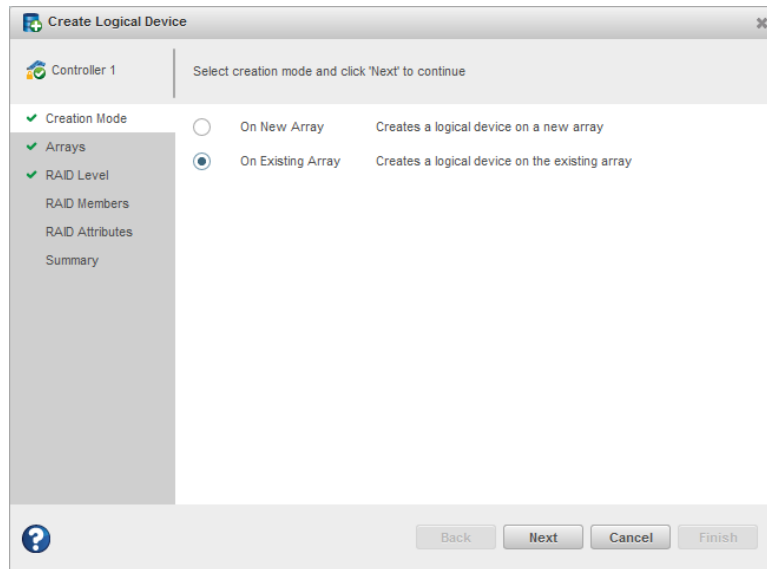
Logical drives can be added/created by selecting the existing array from the Enterprise view.

To create a logical drive on an existing array:

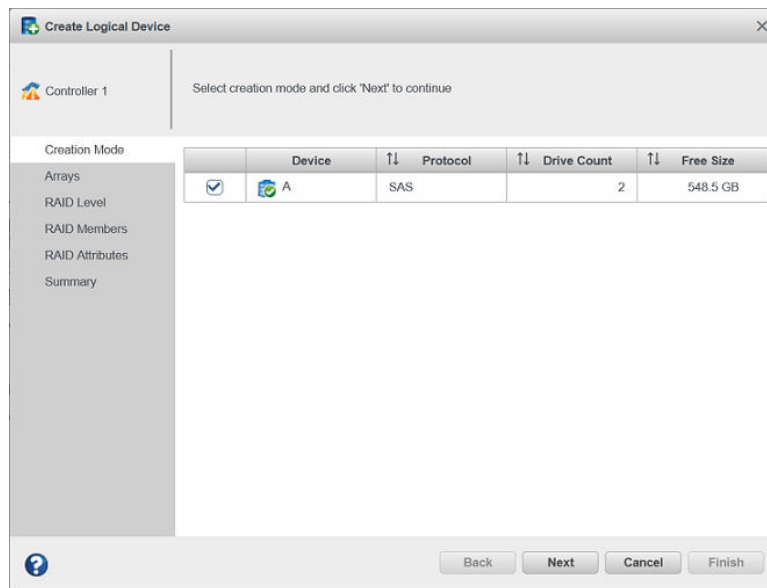
1. In the Enterprise View, select a system, then select a controller on that system.
2. On the ribbon, in the Logical Device group, click **Create Logical Device**.



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



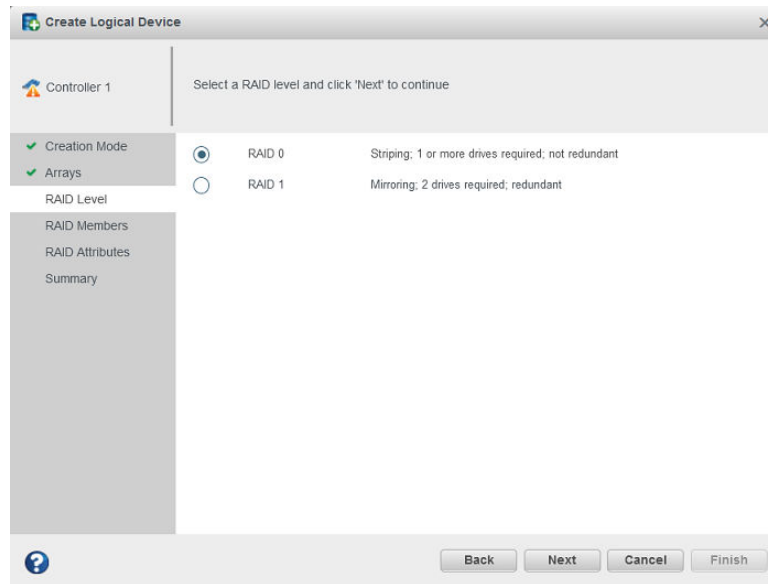
4. Select the array on which to create the logical drive, then click **Next**.



**Note:**

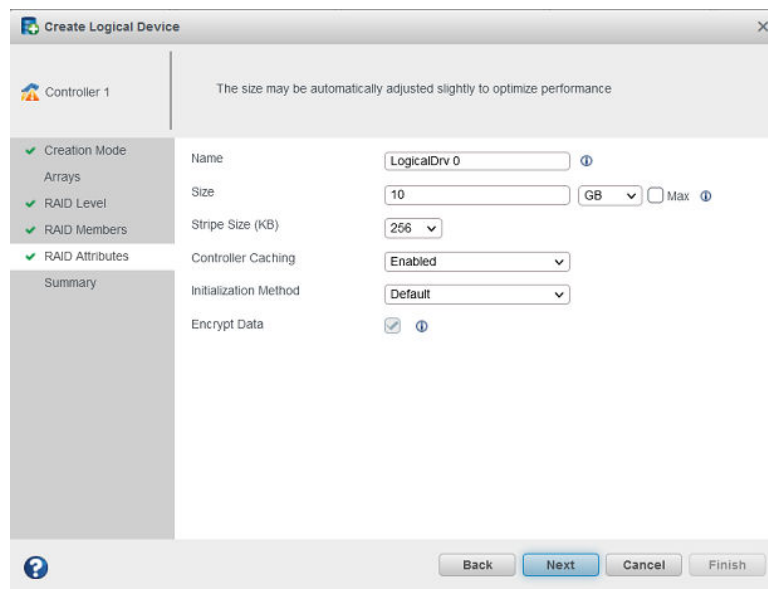
For details on SED support operations on an existing array while creating a logical device, see [5.6.1. Create Logical Device](#).

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:

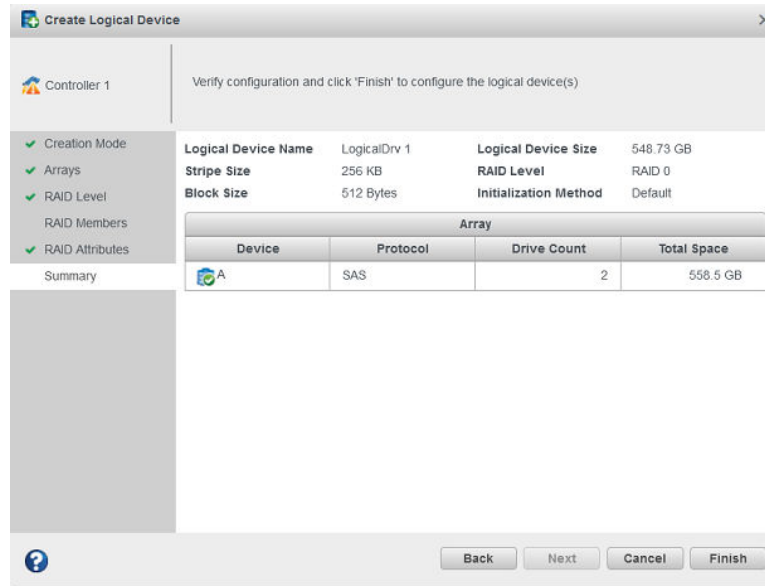
- Enter a name for the logical drive. Names can include any combination of letters, numbers, and spaces.
- Set the size and unit of measure for the logical drive. (By default, a new logical drive uses all available disk space.)
- Change the stripe size—the amount of data, in bytes, written per disk in 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 [9. Working with maxCrypto™ Devices](#))
7. Click **Next**, then review the array and logical drive settings.

This example shows a RAID 0 logical drive 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 [5.4.3. Partitioning and Formatting Your Logical Drives](#).

### 5.4.3 Partitioning and Formatting Your Logical Drives

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

**Note:** Logical drives that have not been partitioned and formatted cannot be used to store data.

Refer to your operating system documentation for more information.

### 5.4.4 Creating Logical Drives on Other Systems in Your Storage Space

If maxView Storage Manager and Microchip Smart Storage controllers are installed 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*



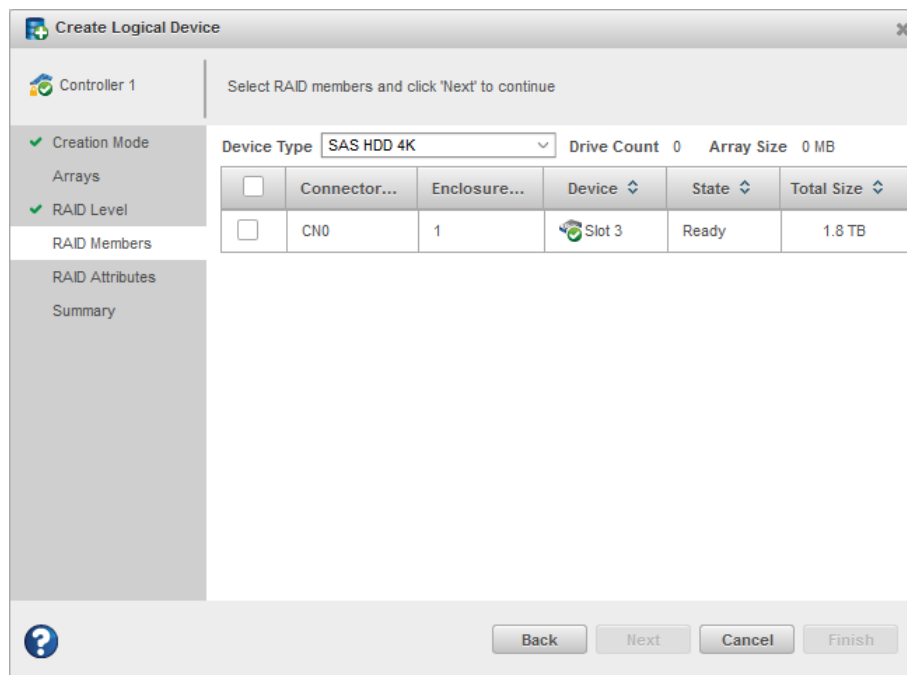
- From your *local* system (the system you're working on), log in to all other systems in your storage space as *remote* systems (see [Logging into Remote Systems](#)), then repeat the steps to create logical drives on new or existing arrays, *or*
- From your local system, create a *server template file* and deploy the configuration to the remote systems in your storage space (see [Deploying Servers](#)).

## 5.5 Controller Support for 4K Drives

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

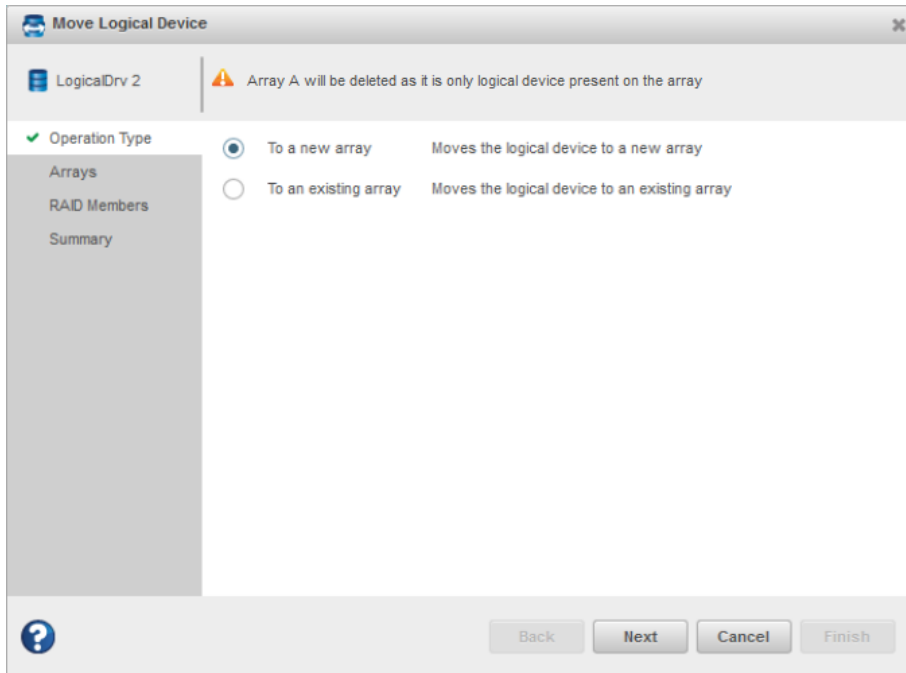
### 5.5.1 Creating a Logical Drive

A logical drive is created using 4K drives. 512-byte drives cannot be mixed with 4K drives. This can be done by selecting the **Device Type** as HDD SATA 4K or HDD SAS 4K. This will ensure that only HDD SATA 4K or HDD SAS 4K devices are displayed.

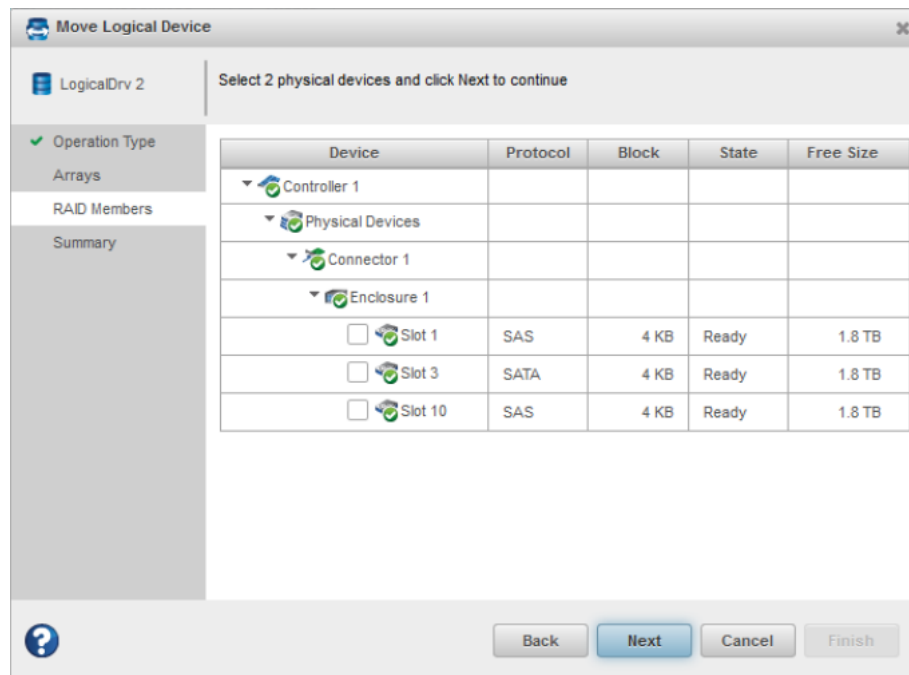


## 5.5.2 Moving a Logical Drive

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.

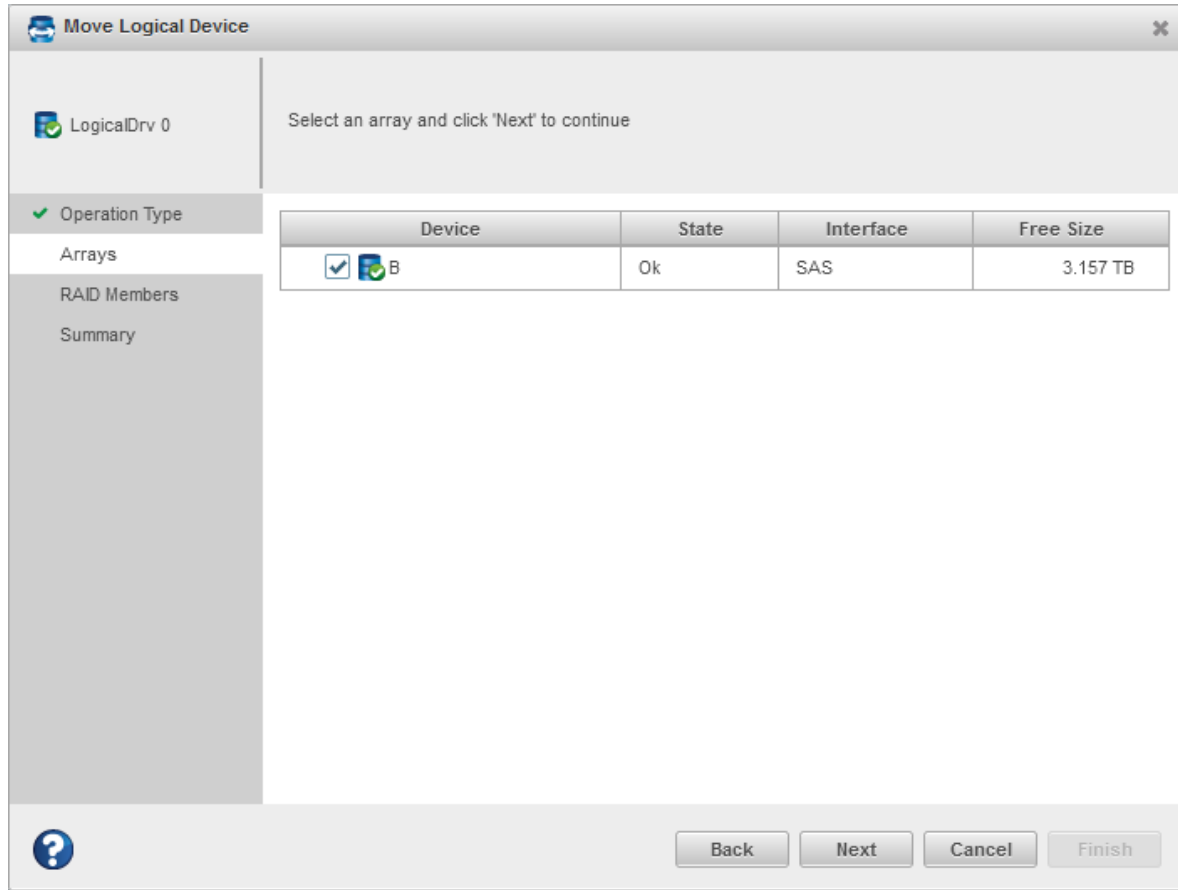


- Moving to a new array: all SATA and SAS 4K drives that are available to move to a new array are listed.



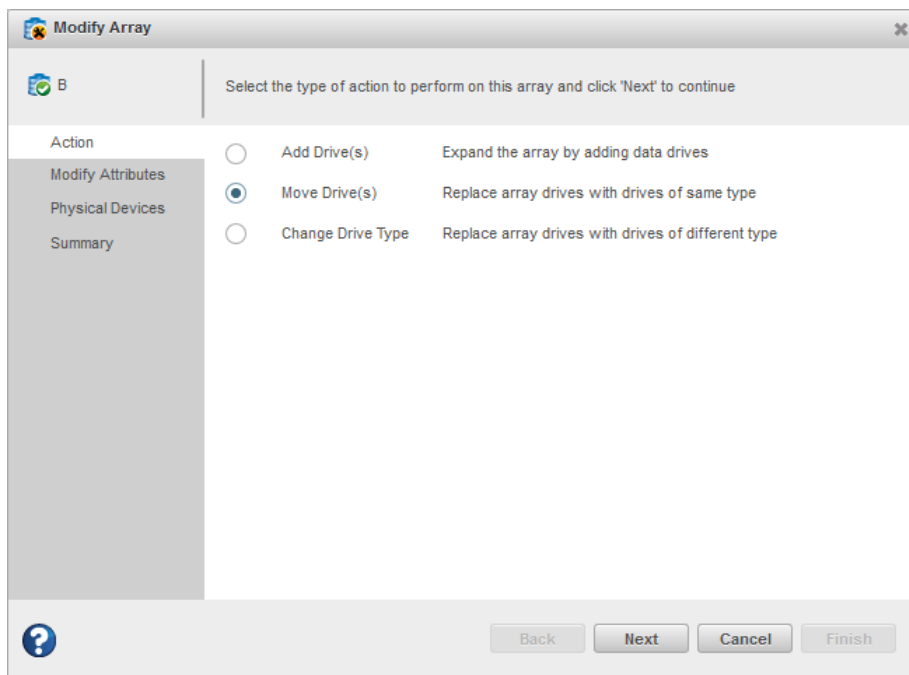
- Moving to an existing array: if the logical device has already been created in a different array using 4K drives, then the option will move a logical device to the existing array of the same block size SAS/SATA 4K drives. Only arrays created using 4K drives will be listed (512-byte arrays will not

be listed).

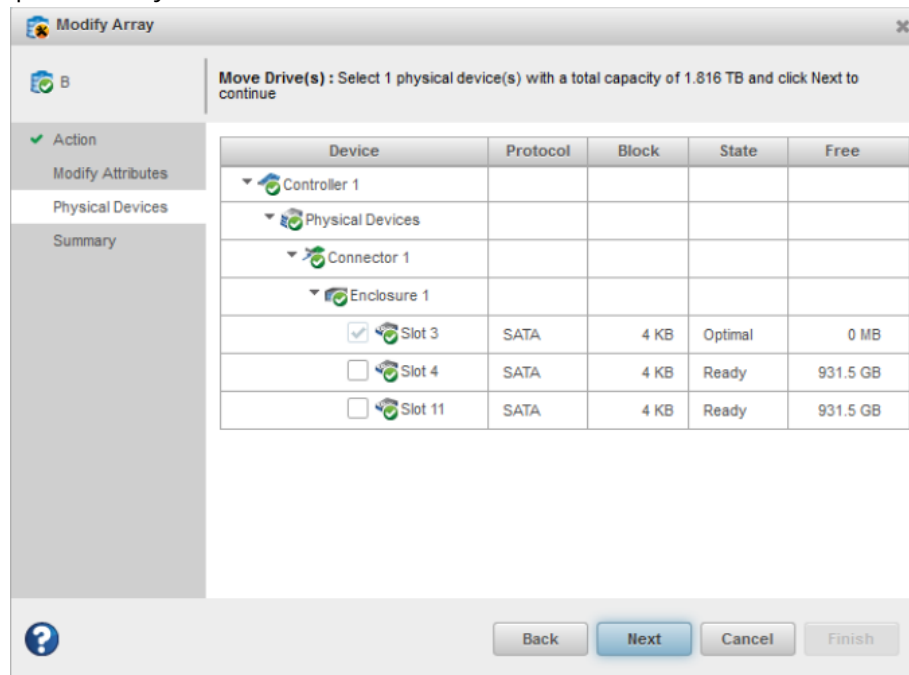


### 5.5.3 Modifying a Logical Drive

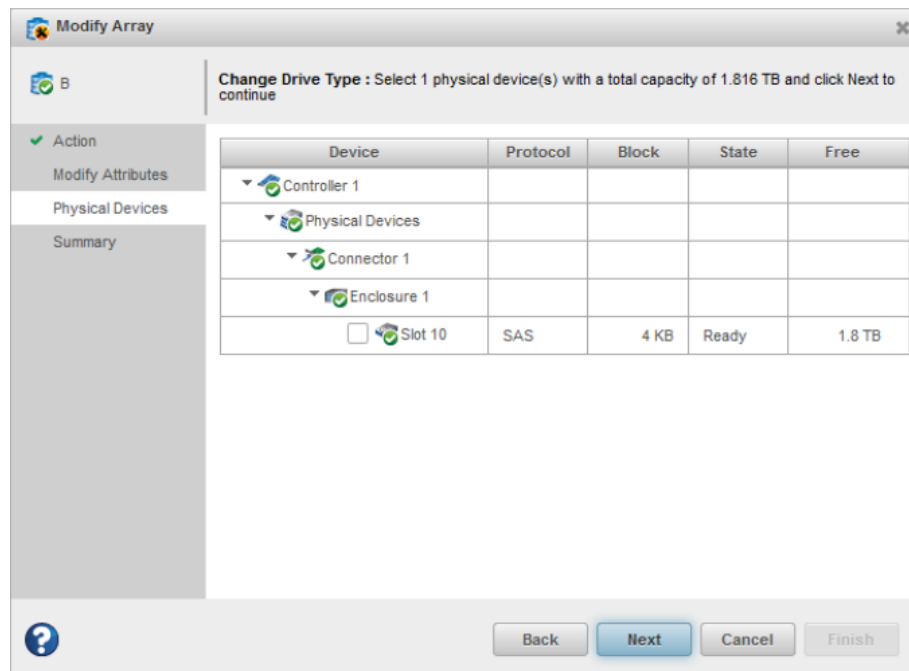
Arrays created using 4K drives can be modified.



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

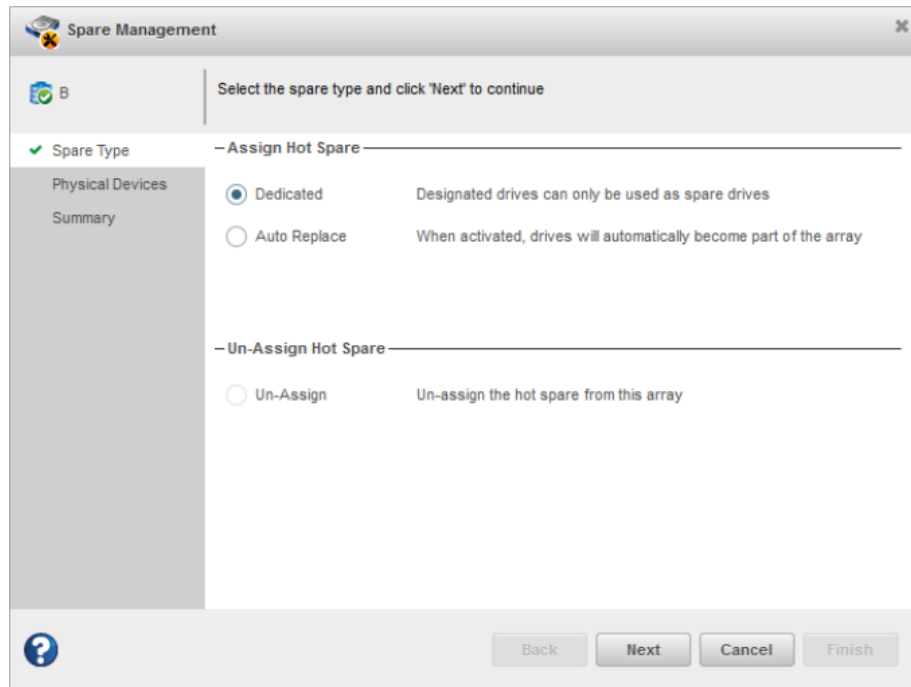


- Changing drive types: Changing the drive interface type from SAS to SATA or from SATA to SAS. For example, if an array is created using 4K SAS drives, you can change the drive type to 4K SATA drives only.

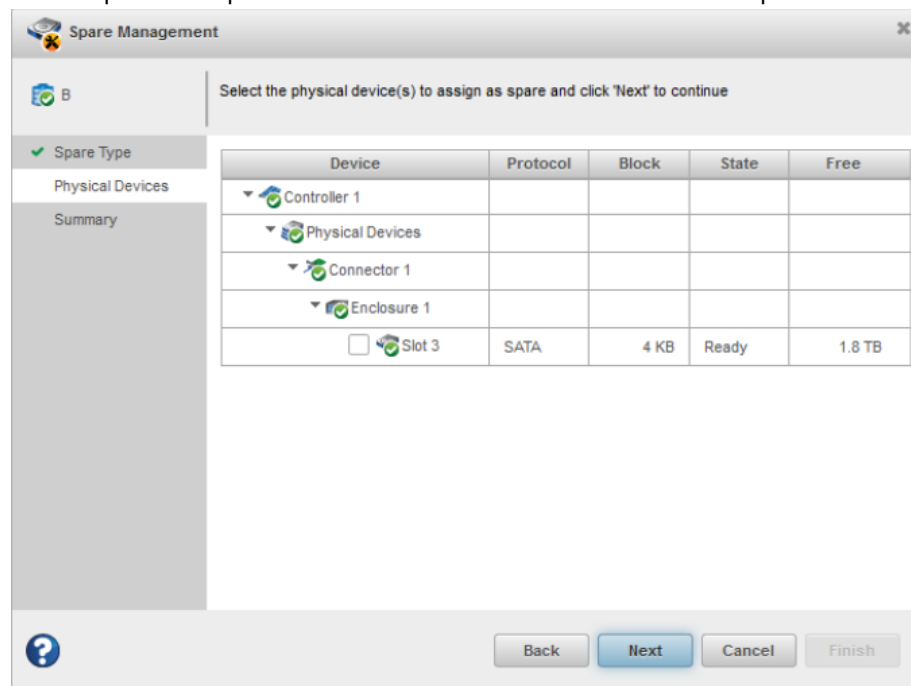


#### 5.5.4 Assigning Spares at the Array Level

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

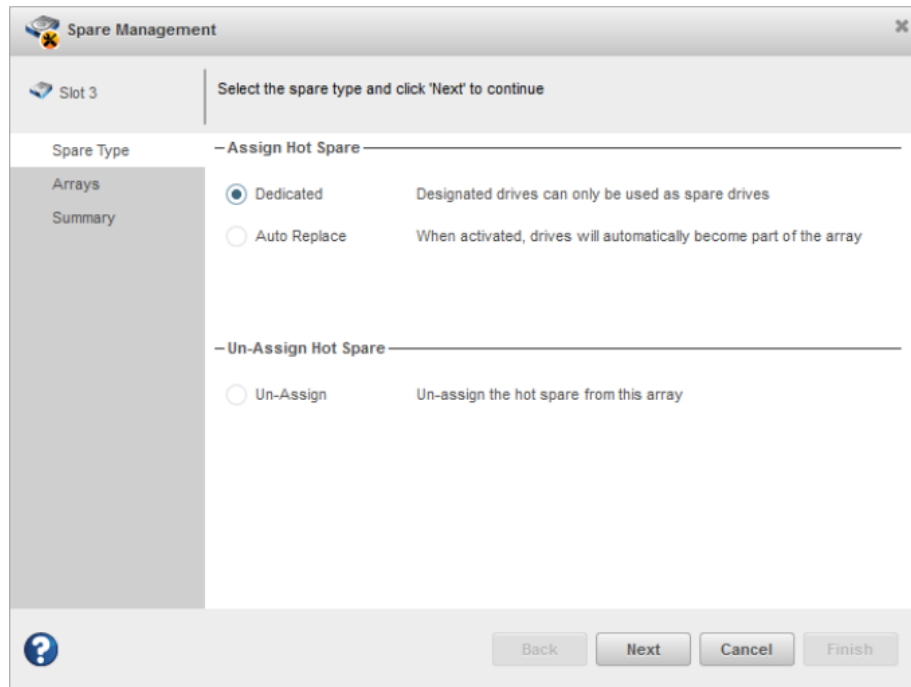


1. Dedicated Hot Spare: If the array/logical device is created using 4K SATA drives, then only the 4K SATA devices can be assigned as spares.
2. Auto Replace Hot Spare: The process is the same as the Dedicated Hot Spare.

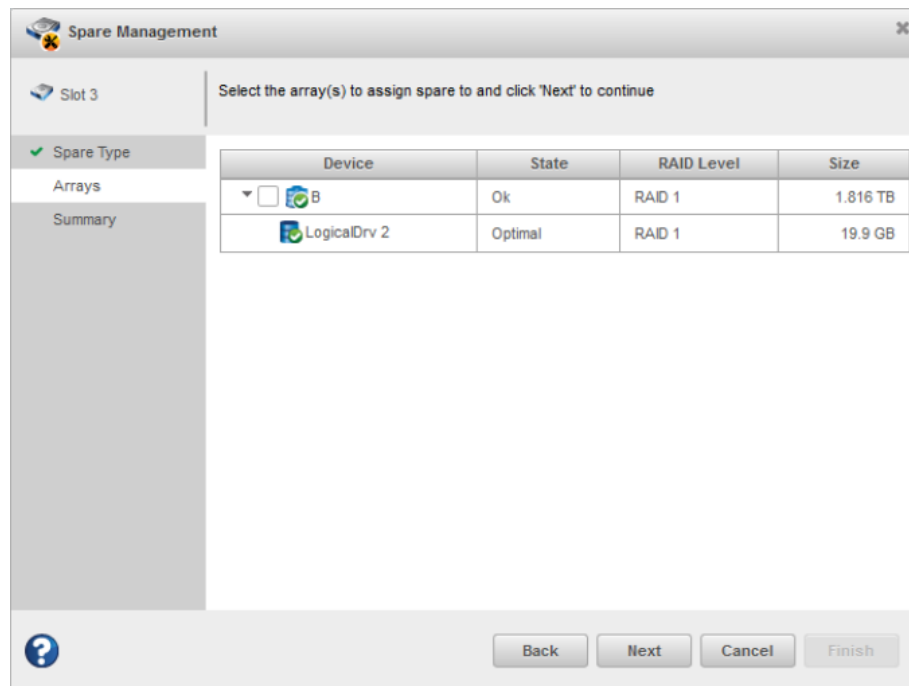


### 5.5.5 Assigning Spares at the Physical Device Level

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.

## 5.6 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 status, logical device status, physical device's SED security status, and SED qualification status.

### 5.6.1 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 must 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

### 5.6.2 Modify Array Add Drives

When the Array status is OK, adding the SED drives to the array is not allowed based on the physical device SED security status and SED qualification status:

SED Security Status	SED Qualification Status
Locked	Not Applicable
Not Applicable	Failed Locking Enabled
Not Applicable	Failed Range Length Set

When the Array status is OK, adding the SED drives to the array is not allowed based on the physical device Original Factory State (OFS) and SED ownership status.

Original Factory State (OFS)	SED Ownership Status
False	Otherwise Owned
False	MCHP Owned, Foreign
False	Otherwise Owned, Foreign

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

Array Status
One or more logical drives undergoing or failed SED qualification
Has Logical Drive with Foreign SED

#### 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 physical device SED security status and SED qualification status:

SED Security Status	SED Qualification Status
Locked	Not Applicable
Not Applicable	Failed Locking Enabled
Not Applicable	Failed Range Length Set

When the Array status is OK, adding the SED drives to the array is not allowed based on the physical device Original Factory State (OFS) and SED ownership status:

Original Factory State (OFS)	SED Ownership Status
False	Otherwise Owned
False	MCHP Owned, Foreign
False	Otherwise Owned, Foreign

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

Array Status
One or more logical drives undergoing or failed SED qualification
Has logical drive with foreign SED

### 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
Locked	Not Applicable
Not Applicable	Failed Locking Enabled
Not Applicable	Failed Range Length Set

When the Array status is OK, adding the SED drives to the array is not allowed based on the physical device Original Factory State (OFS) and SED ownership status:

Original Factory State (OFS)	SED Ownership Status
False	Otherwise Owned
False	MCHP Owned, Foreign
False	Otherwise Owned, Foreign

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

Array Status
One or more logical drives undergoing or failed SED qualification
Has Logical Drive with Foreign SED

### 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
Locked	Not Applicable
Not Applicable	Failed Locking Enabled
Not Applicable	Failed Range Length Set

When the Array status is OK, adding the SED drives to the array is not allowed based on the physical device Original Factory State (OFS) and SED ownership status:

Original Factory State (OFS)	SED Ownership Status
False	Otherwise Owned
False	MCHP Owned, Foreign
False	Otherwise Owned, Foreign

Modify Array ribbon icon should be disabled on the following Array status:

Array Status
Has Logical Drive with Foreign SED

### 5.6.3 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
Locked	Not Applicable
Not Applicable	Failed Locking Enabled
Not Applicable	Failed Range Length Set

When the Array status is OK, adding the SED drives to the array is not allowed based on the physical device Original Factory State (OFS) and SED ownership status:

Original Factory State (OFS)	SED Ownership Status
False	Otherwise Owned
False	MCHP Owned, Foreign
False	Otherwise Owned, Foreign

#### 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
One or more logical drives undergoing or failed SED qualification
Has Logical Drive with Foreign SED

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

Logical Device Status
SED Qual Failed
SED Qual In Progress
SED Locked

## 5.6.4 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
Locked	Not Applicable
Not Applicable	Failed Locking Enabled
Not Applicable	Failed Range Length Set

When the Array status is OK, adding the SED drives to the array is not allowed based on the physical device Original Factory State (OFS) and SED ownership status:

Original Factory State (OFS)	SED Ownership Status
False	Otherwise Owned
False	MCHP Owned, Foreign
False	Otherwise Owned, Foreign

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

Array Status
One or more logical drives undergoing or failed SED qualification
Has Logical Drive with Foreign SED

Spare Management ribbon icon should be disabled on the following Array status:

Array Status
Has Logical Drive with Foreign SED

## 5.6.5 maxCache

### On Existing Array

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

Array Status
One or more logical drives undergoing or failed SED qualification
Has Logical Drive with Foreign SED

Create maxCache operation on existing cache array should be blocked when the target Array has the following status:

Cache Array SED Encryption Status	Logical Device SED Encryption Status
Encrypted=True	Encrypted=False
Encrypted=False	Encrypted=True

### 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
Locked	Not Applicable
Not Applicable	Failed Locking Enabled
Not Applicable	Failed Range Length Set

When the Array status is OK, adding the SED drives to the array is not allowed based on the physical device Original Factory State (OFS) and SED ownership status:

Original Factory State (OFS)	SED Ownership Status
False	Otherwise Owned
False	MCHP Owned, Foreign
False	Otherwise Owned, Foreign

## 6. Protecting Your Data

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

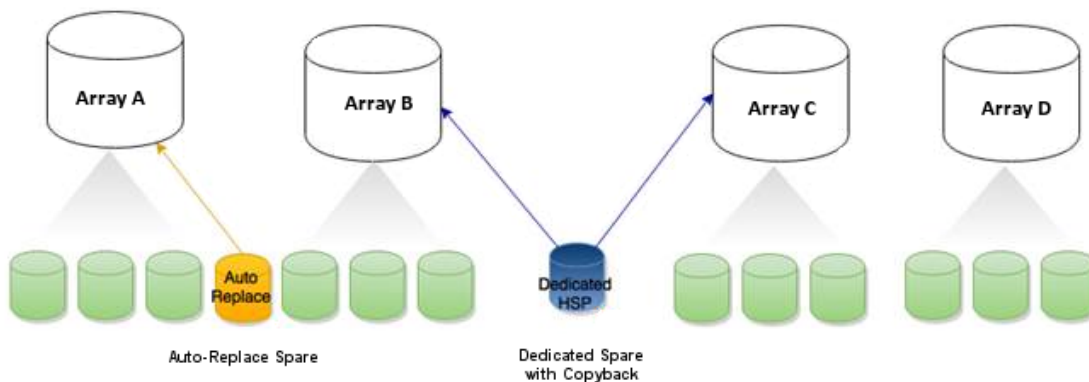
A *hot spare* is a disk drive or SSD (Solid State Drive) that automatically replaces any failed drive in a logical drive, and can subsequently be used to rebuild that logical drive. (For more information, see [15.3. Recovering from a Disk Drive Failure.](#))

### 6.1 Dedicated Spare or Auto-Replace Spare?

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

After using a dedicated hot spare to rebuild a failed logical drive, data is moved back to its original location, using a process called *copyback*, once the controller detects that the failed drive has been replaced. Once the data is copied back, the hot spare becomes available again. You must create an array before you can assign a dedicated hot spare to protect it. To assign a dedicated hot spare, see [6.3. 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 [6.4. Assigning an Auto-Replace Hot Spare.](#)



### 6.2 Hot Spare Limitations

- Hot spares protect redundant logical drives only. To protect non-redundant logical drives, set the spare activation mode of the controller to predictive activation.
- You cannot create a hot spare from a disk drive that is already part of an array.
- You should select a disk drive that is at least as big as the smallest disk drive in the array that it might replace.
- You must designate a SAS hot spare drive for an array comprised of SAS disk drives, and a SATA hot spare drive for an array comprised of SATA disk drives.
- You can designate a SMR HA<sup>6</sup> or SMR DM drive for all hot spare types. A SMR drive cannot protect a PMR<sup>7</sup> drive, or vice-versa.

### 6.3 Assigning a Dedicated Hot Spare

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

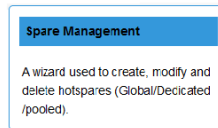
<sup>6</sup> SMR: Shingled Magnetic Recording. HA: Host Aware (backward compatible with standard HDD). DM: Device Managed (backward compatible with standard HDD).

<sup>7</sup> PMR: Perpendicular Magnetic Recording; standard HDD recording technology.

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

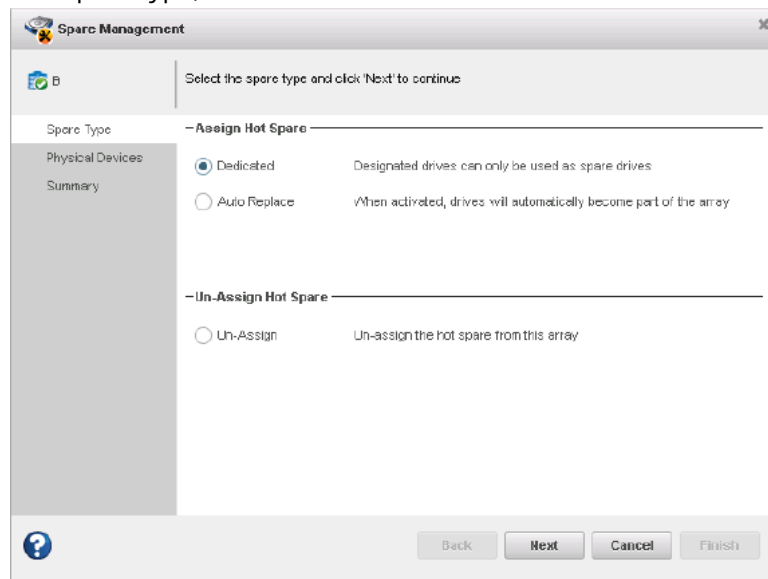
To assign a dedicated spare:

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

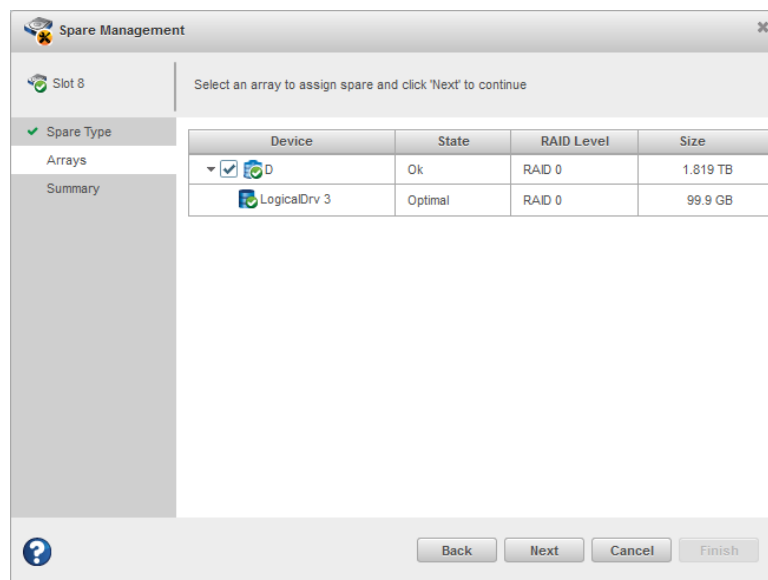


The Spare Management wizard opens.

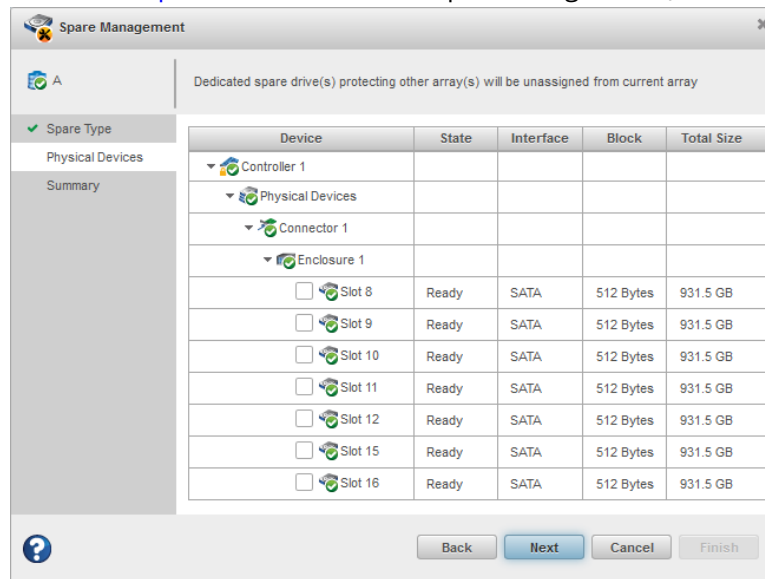
3. Select the **Dedicated** spare type, then click **Next**.



4. If you selected a physical drive in the Enterprise view, select the arrays you want to protect with a dedicated spare, then click **Next**.



- 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 5.6.4. [Spare Management](#). (See 6.2. [Hot Spare Limitations](#) for help selecting drives.)



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

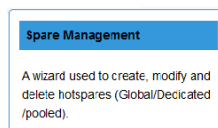
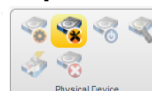
## 6.4 Assigning an Auto-Replace Hot Spare

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

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

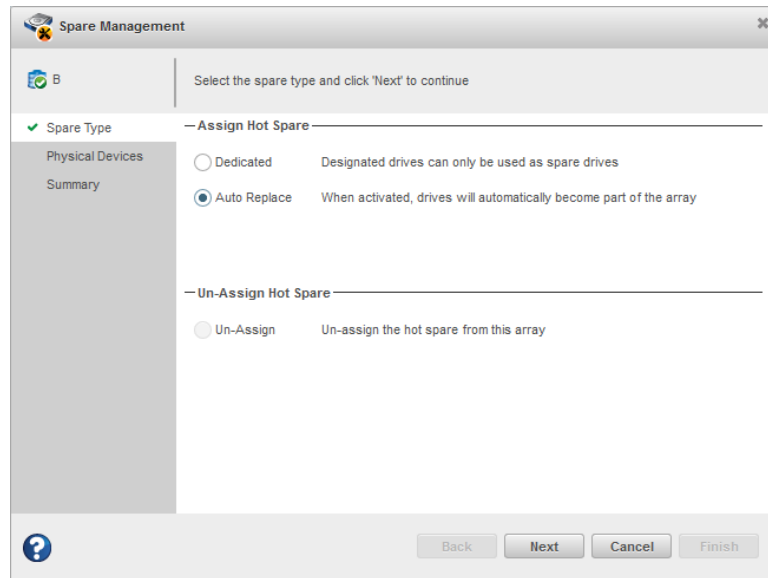
- In the Enterprise View, select an array on that controller.
 

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

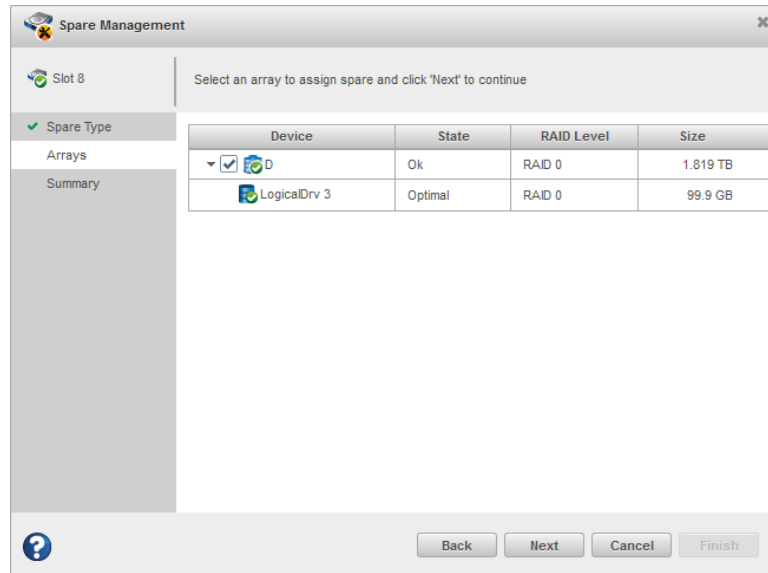


The Spare Management wizard opens.

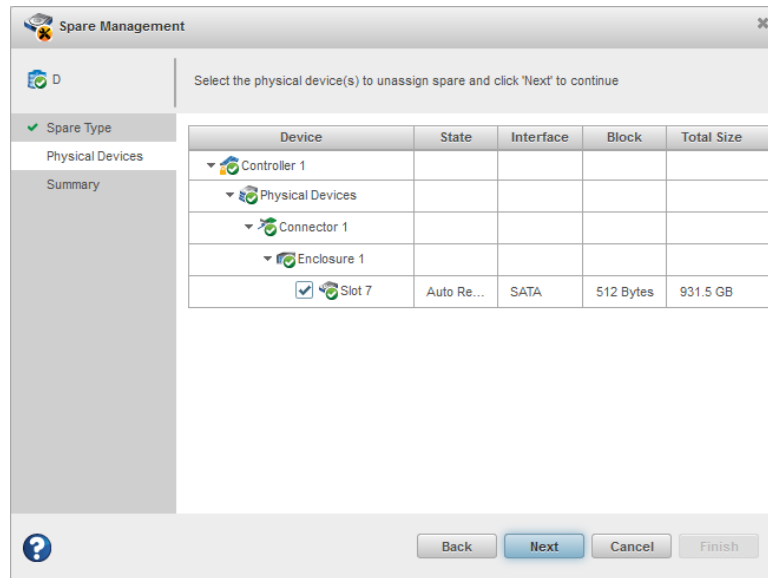
- Select the **Auto-Replace** spare type, then click **Next**.



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 [5.6.4. Spare Management](#). (See [6.2. Hot Spare Limitations](#) for help selecting drives.)



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

## 6.5 Removing a Hot Spare

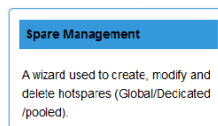
You can remove a dedicated or auto-replace hot spare from an array. Removing the last hot spare from an array returns the drive to the Ready state.

You may want to remove a hot spare to:

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

To remove a hot spare:

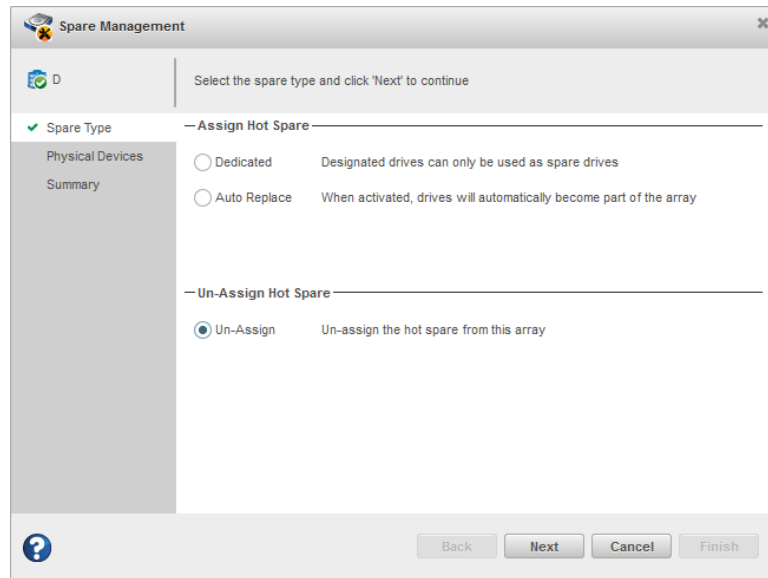
1. In the Enterprise View, select an array or an existing hot spare drive.
2. On the ribbon, in the Physical Device group, click **Spare Management**.



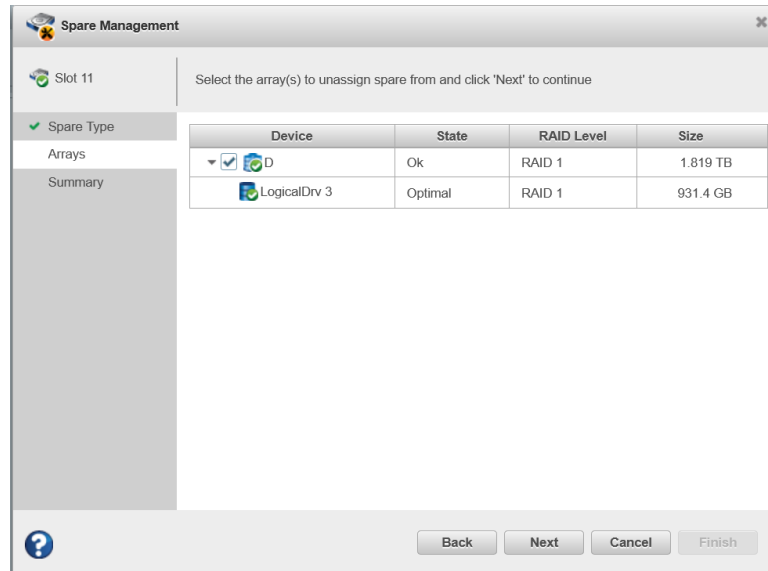
The Spare Management wizard opens.

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

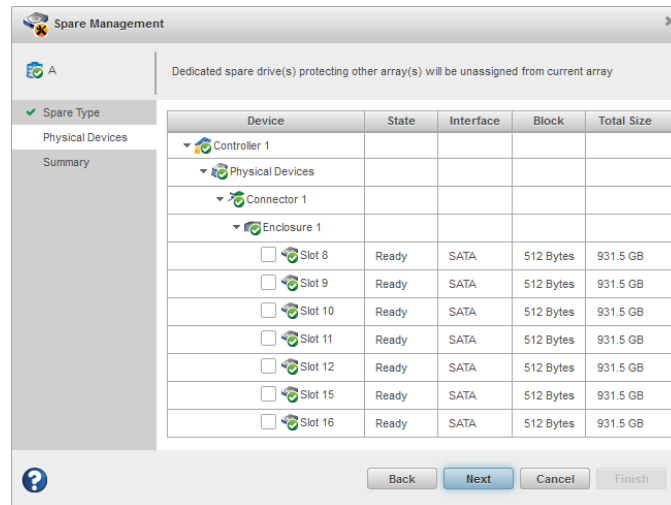




- If you selected a hot spare in the Enterprise view, select the array(s) from which to remove the spare, then click **Next**.



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



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

## 6.6 Setting the Spare Activation Mode

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

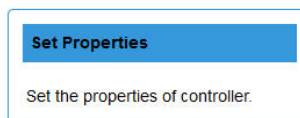
- A data drive fails; this is the default mode.
- A data drive reports a predictive failure (SMART) status.

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

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

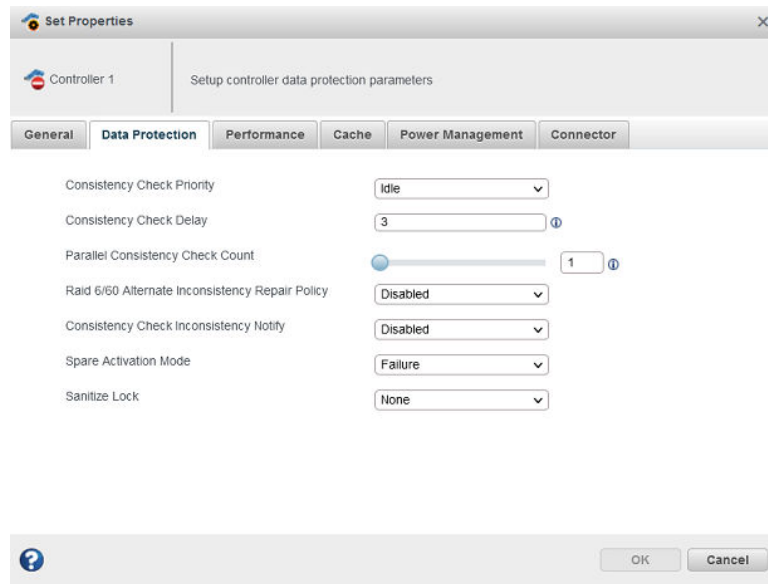
To set the spare activation mode:

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



The Set Properties window opens.

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



## 6.7 Controller Sanitize Lock Freeze/Anti-Freeze

The Sanitize Lock Freeze/Anti-Freeze feature provides the controller level of sanitize lock, which helps prevent accidental erasing of 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 data on the disk.

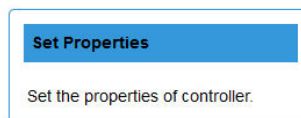
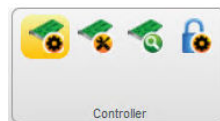
The sanitize lock feature has three options:

- Freeze: Prevents any sanitize erase operations to be performed
- Anti-Freeze: Locks the freeze command and enables any sanitize erase operation to be performed
- None: Enables any sanitize erase operation to be performed

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

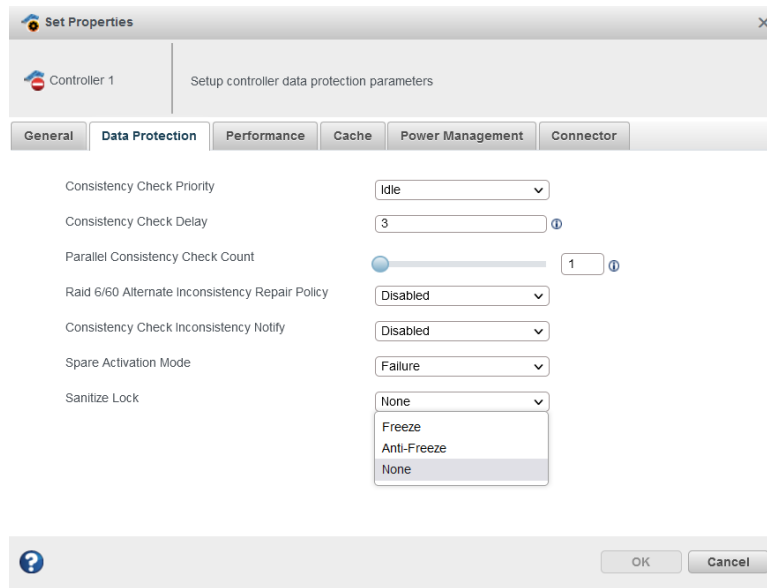
To set the Sanitize Lock:

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



The Set Properties window opens.

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



**Note:**

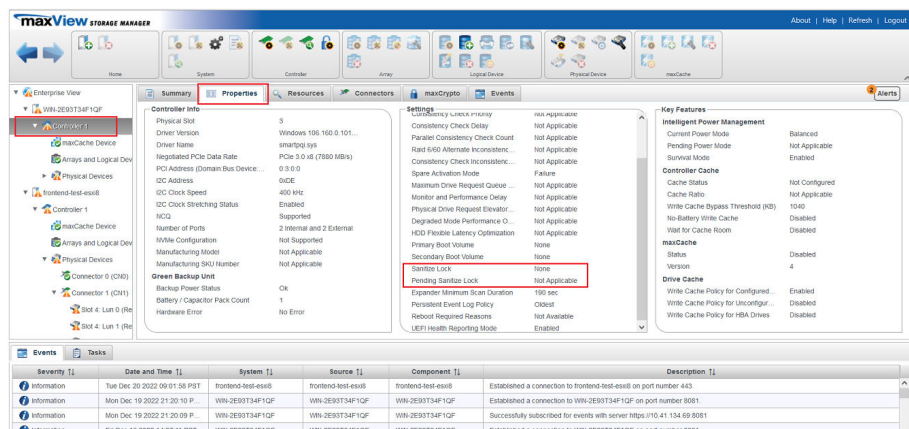
If the Sanitize Lock is set to any value other than **None**, the following warning message will be displayed in the menu header:

*Changing the Sanitize Lock will require a reboot to apply the new state to the controller, and require all physical devices to be power cycled or hot-plugged for the lock state to be applied to the physical devices.*

5. Click **OK**.

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

The properties of the Sanitize Lock feature are displayed in the controller node properties tab as shown in the following screen capture.



The Sanitize Lock property will display the current setting in which the controller is operating.

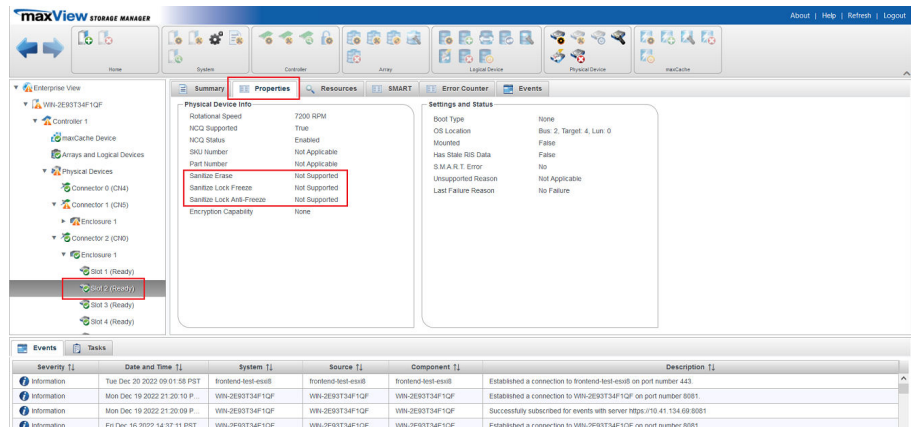
When the Sanitize Lock property is changed in the Set Properties dialog, the pending Sanitize Lock property will show the changed value.

When the machine is rebooted, the pending Sanitize Lock value will be "Not Applicable", and the Sanitize Lock value will be set to the previous pending Sanitize Lock value.

**6.7.2 Physical Device Sanitize Lock Freeze/Anti-Freeze**

This feature is supported only on SATA drives that are connected to the controller. If the drive supports the Sanitize Lock Freeze feature, it may or may not support the Sanitize Lock Anti-freeze.

Based on the support bit on the drive, the Sanitize Lock policy can be set from the controller and it will be applied on the drives that support Sanitize Freeze/Anti-Freeze.



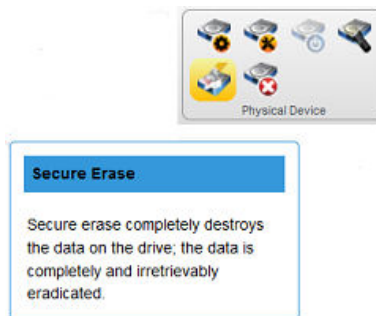
The Sanitize Lock property is dependent upon the following conditions:

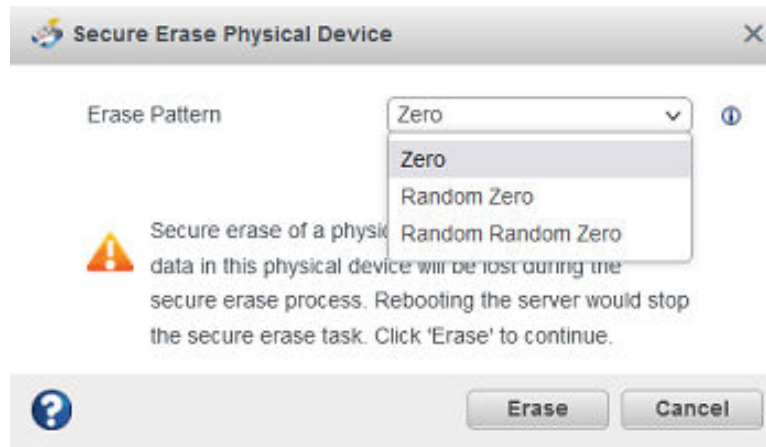
- If the drive does not support Sanitize Erase, the Sanitize Lock property is not displayed.
- If the drive supports Sanitize Erase but does not support Freeze/Anti-Freeze, then the Sanitize Lock property will be listed as "Not Applicable".
- If the controller Sanitize Lock is in the Freeze state, then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

### 6.7.3 Secure Erase Pattern

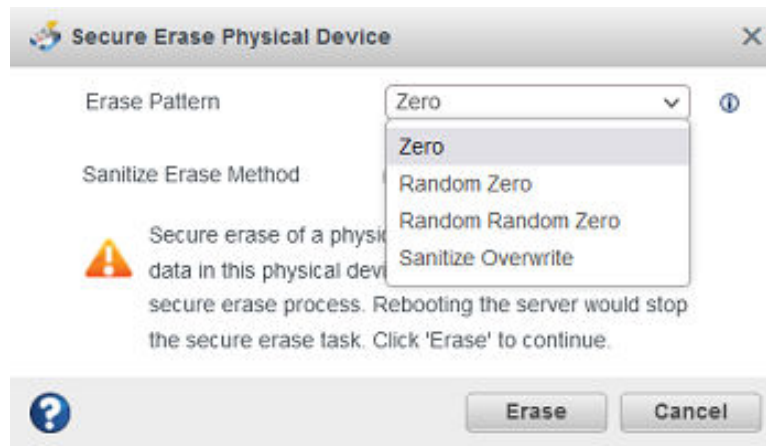
If the drive or controller Sanitize Lock is in the freeze state, then all the Sanitize Erase patterns will not be listed when you click on the Secure Erase ribbon icon in the physical device ribbon group.





Only three secure erases can be performed.

If the drive and controller Sanitize Lock is in Anti-Freeze or None states, then the Sanitize Erase pattern will be listed.



**Note:** When you perform the Sanitize Erase operation, it sets the controller Sanitize Lock to freeze, and reboots the system, the drive will remember the percentage completion for the Sanitize Secure Erase after the reboot. The freeze state will be applied only after the Sanitize Erase is completed and the sanitize erase operation cannot be stopped.

## 7. Modifying Your Storage Space

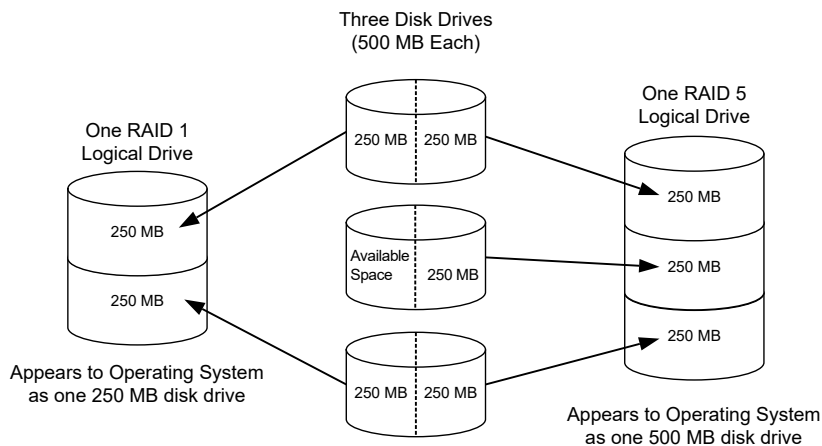
This section provides additional scenarios for creating and modifying arrays and logical drives. It explains how to check your logical drives for bad or inconsistent data; optimize controller and logical drive performance; move arrays and logical drives; and perform advanced operations, such as creating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

### 7.1 Understanding Arrays and Logical Drives

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

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

You can include the same disk drive in two different logical drives by using just a portion of the space on the disk drive in each, as shown in the following figure.



Disk drive space that has been assigned to a logical drive is called a *segment*. A segment can include all or just a portion of a disk drive's space. A disk drive with one segment is part of one logical drive, a disk drive with two segments is part of two logical drives, and so on. When a logical drive is deleted, the segments that comprised it revert to available space (or *free segments*).

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

Protect your logical drives by assigning one or more hot spares to them. (See [6. Protecting Your Data](#) for more information.)

### 7.2 Creating and Modifying Logical Drives

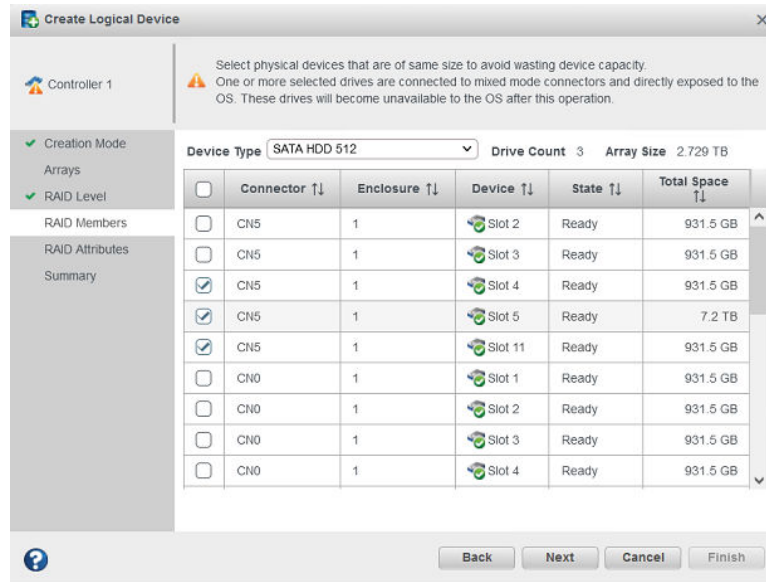
For basic instructions for creating logical drives, see [5. Building Your Storage Space](#). To create a logical drive from different-sized disk drives, see [7.2.1. Including Different-sized Disk Drives in a Logical Drive](#)

#### 7.2.1 Including Different-sized Disk Drives in a Logical Drive

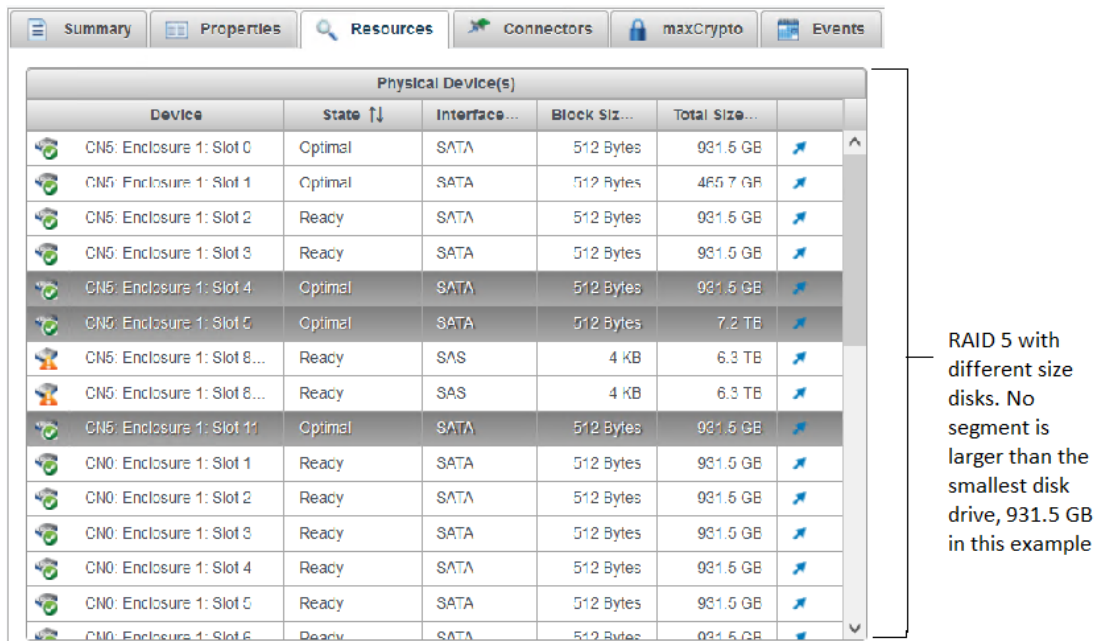
You can combine disk drives of different sizes in the same logical drive. If the logical drive includes redundancy, however, the size of each segment can be no larger than the size of the smallest disk drive. (See [Selecting the Best RAID Level](#) for more information about redundancy.)

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

To create a logical drive with disk drives of different sizes, follow the instructions in [5.4.1. 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.



### 7.3 Enabling Background Consistency Check

When background consistency check is enabled, maxView Storage Manager continually and automatically checks your logical drives for bad or inconsistent data, and then fixes any problems. Enabling consistency check ensures that you can recover data if a logical drive fails. The scanning process checks physical drives in fault-tolerant logical drives for bad sectors. It also verifies the

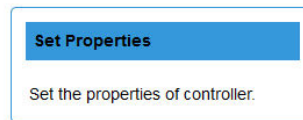
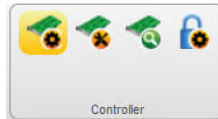


consistency of parity data, if applicable. The available modes are High, Disabled, and Idle. On selecting the Idle mode, you must also specify a delay value and parallel scan count.

When enabled, the consistency check will perform a background check on logical drives every 14 days from the time the last check was completed. However, the factors that may extend this time duration includes the priority mode, parallel count, number of logical devices, and host I/O activity.

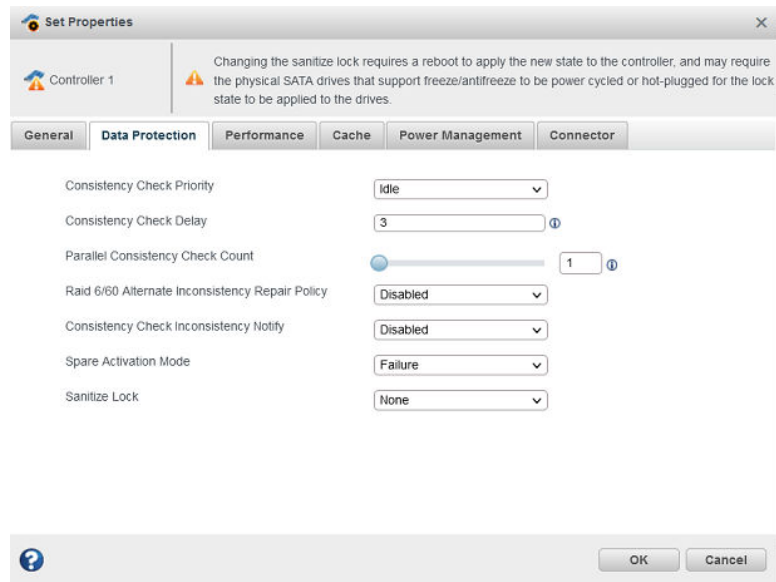
To enable or disable background consistency check:

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 Priority 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 0 value disables the scan. The default value is 3.
  - **Parallel Consistency Check Count**—Number of logical drives on which the controller will perform the consistency check in parallel.
6. Click **OK**.

## 7.4 Optimizing Logical Drive Performance


This section describes how to enable controller cache optimizations and SSD I/O bypass acceleration to improve I/O throughput on the logical drives in your storage space. Cache optimizations are

applied independently on a per controller or per logical drive basis. You can apply I/O bypass acceleration on arrays comprised of SSDs only.

### 7.4.1 Enabling Cache Optimizations

Use this option to enable the following cache optimizations on the controllers in your storage space. Apply cache optimizations independently as per controller or per logical drive basis.

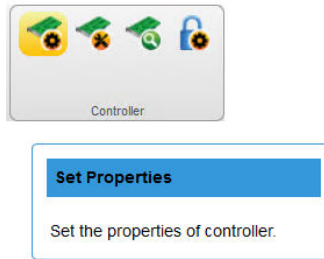
**Note:** You cannot use controller caching and maxCache caching concurrently. Controller caching is available only if maxCache is not enabled on the controller. For more information about maxCache, see [8. Working with maxCache Devices](#).

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. The property is applicable only for the non-parity logical drives. The valid threshold size is between 16 KB and 1040 KB and the value must be a multiple of 16 KB.
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.
Recover Cache Module	Recovers the failed cache module.
Global Physical Devices Write Cache Policy	<p>Sets the write cache policy for the physical drives on the controller.</p> <div style="border: 1px solid black; padding: 2px; display: inline-block; background-color: yellow;">  <b>CAUTION</b> </div> <p>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.</p>
Drive Write Cache Policy for Configured Drives	<p>Sets the write cache policy for the configured physical devices on the controller</p> <ul style="list-style-type: none"> <li>• Default: Allows the controller to control the drive write cache policy of all configured physical devices.</li> <li>• 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.</li> <li>• Disabled: The drive write cache for the physical devices will be disabled by the controller.</li> <li>• Unchanged: Sets the physical devices factory default policy for all configured drives.</li> </ul>
Drive Write Cache Policy for Unconfigured Drives	<p>Sets the write cache policy for the unconfigured physical devices on the controller</p> <ul style="list-style-type: none"> <li>• Default: The controller does not modify the drive write cache of the physical devices.</li> <li>• 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.</li> <li>• Disabled: The drive write cache for the physical devices will be disabled by the controller.</li> </ul>
Drive Write Cache Policy for HBA Drives	<p>Sets the write cache policy for the HBA physical devices on the controller</p> <ul style="list-style-type: none"> <li>• Default: The controller does not modify the drive write cache of the physical devices.</li> <li>• 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.</li> <li>• Disabled: The drive write cache for the physical devices will be disabled by the controller.</li> </ul>

To enable cache optimizations on a controller:

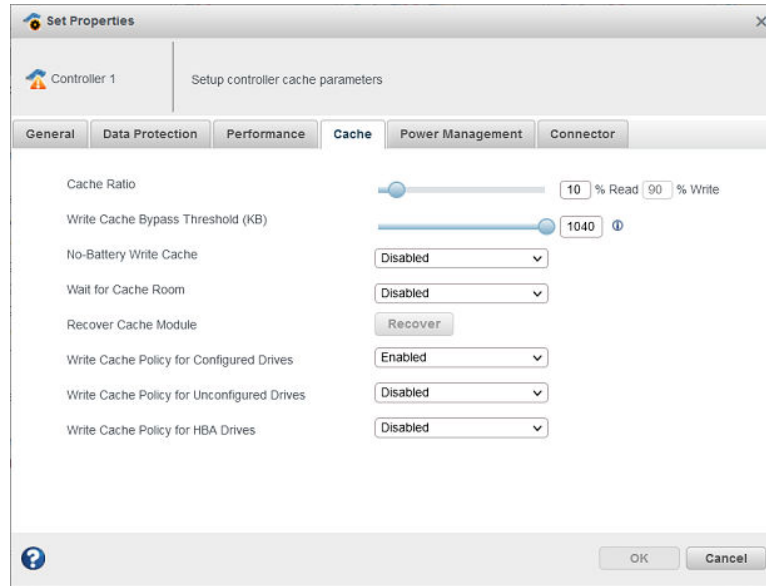
1. In the Enterprise View, select a controller.

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



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

- Adjust cache settings, as needed.



- Click **OK**.

#### 7.4.1.1 Enabling Cache Optimization for a Logical Drive

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

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

#### 7.4.2 Enabling SSD I/O Bypass

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

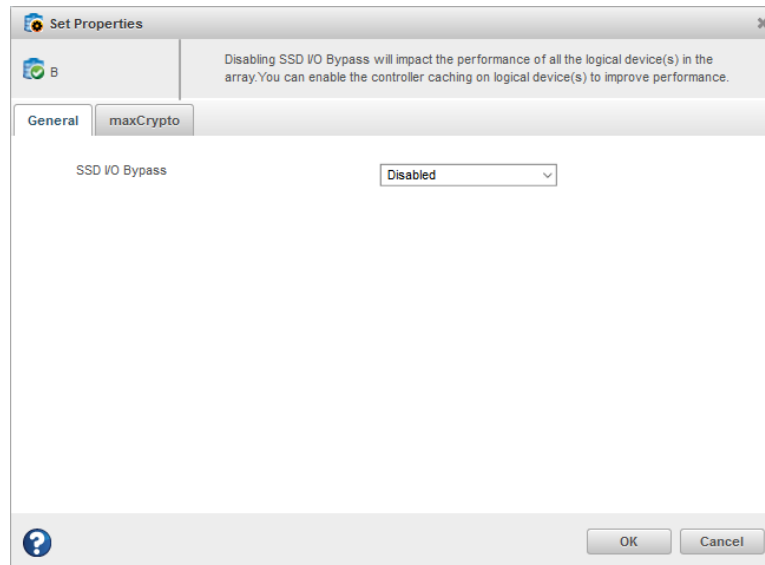
To enable I/O Bypass acceleration:

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



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

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



- Click **OK**.

## 7.5 Moving a Logical Drive

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

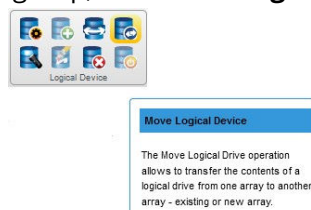
- Move Logical Drive To a New Array
- Move Logical Drive To an Existing Array

If you move the logical drive to a new array, the array is created automatically. If you move the logical drive to an existing array, it must have sufficient space and member disk drives to store the logical drive data and accommodate the RAID level; for example, three drives, minimum, for a RAID 5.

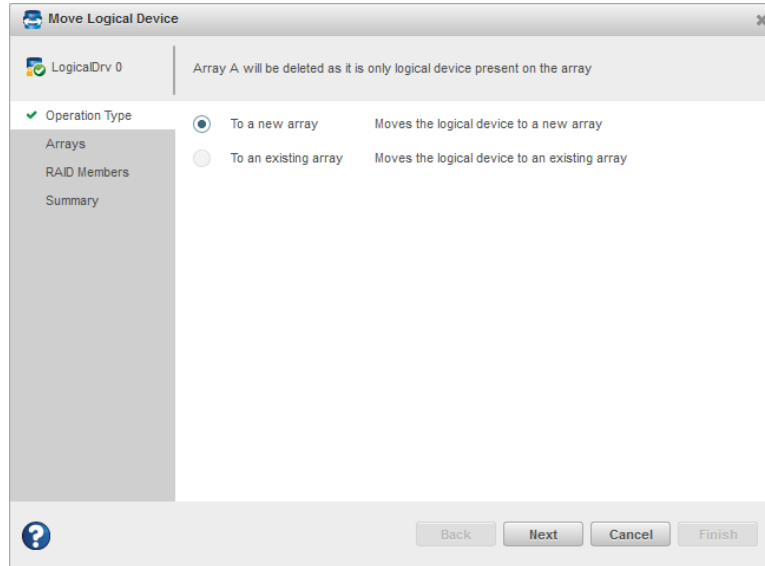
**Note:** Moving a logical drive can be a time-consuming process. All data in the logical drive is moved onto the new or existing array, and the controller continues to service I/O requests to other logical drives.

To move a logical drive:

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



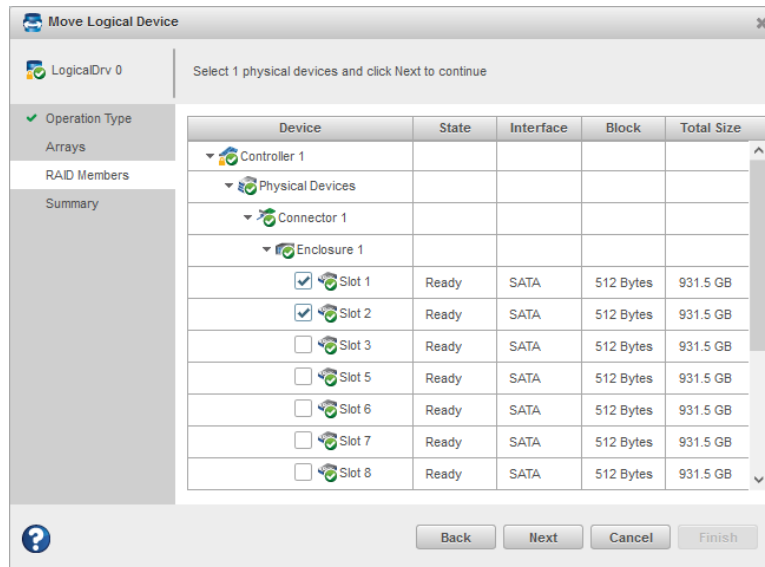
- When the wizard opens, select **To New Array** or **To Existing Array**, then click **Next**.



**Note:**

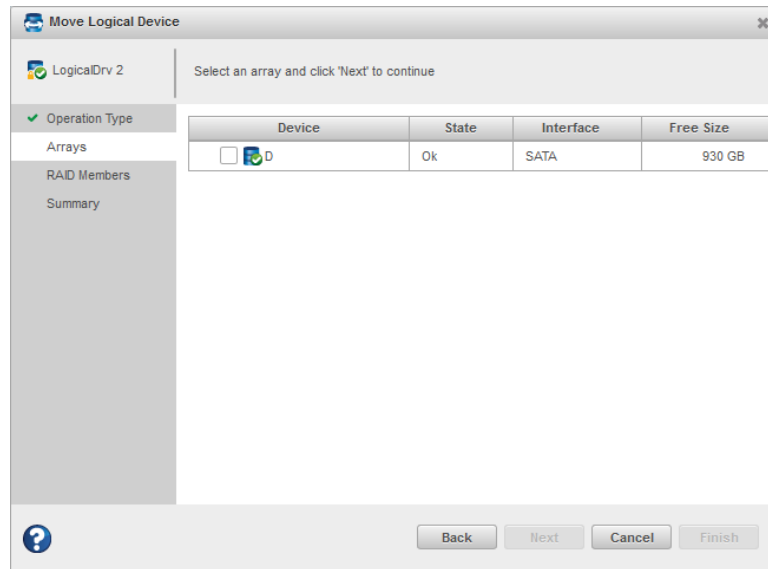
For details on SED support operations on moving a logical device, see [5.6.3. Move Logical Device](#).

- 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.

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



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

## 7.6 Moving an Array

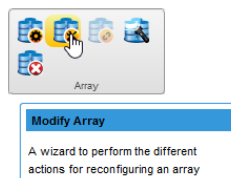
You can move an array by replacing its physical drives with drives of the same type or different type. For example, you can replace SAS drives in the array with other SAS drives, or replace SAS drives with SATA drives. You cannot combine drive types in the same array; however, if you choose to replace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

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

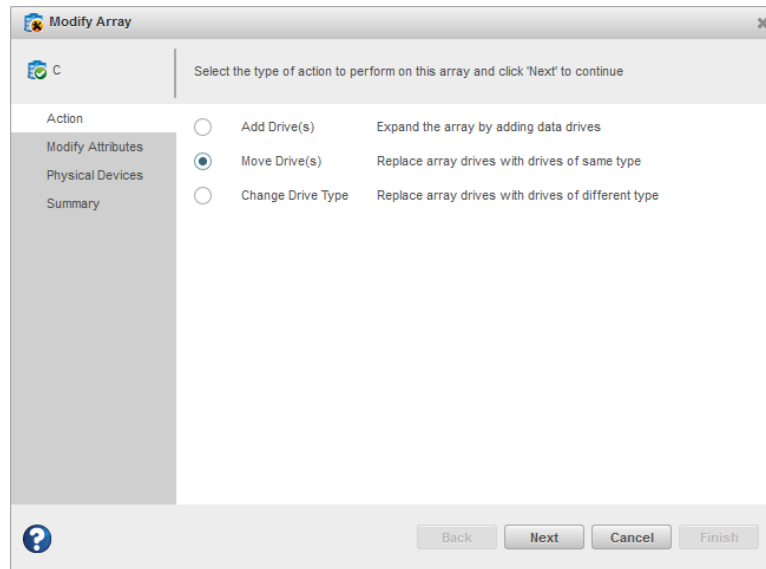
**Note:** Moving an array can be a time-consuming process. All data in each logical drive is copied to the replacement drives, and the controller continues to service I/O requests to other logical drives.

To move an array:

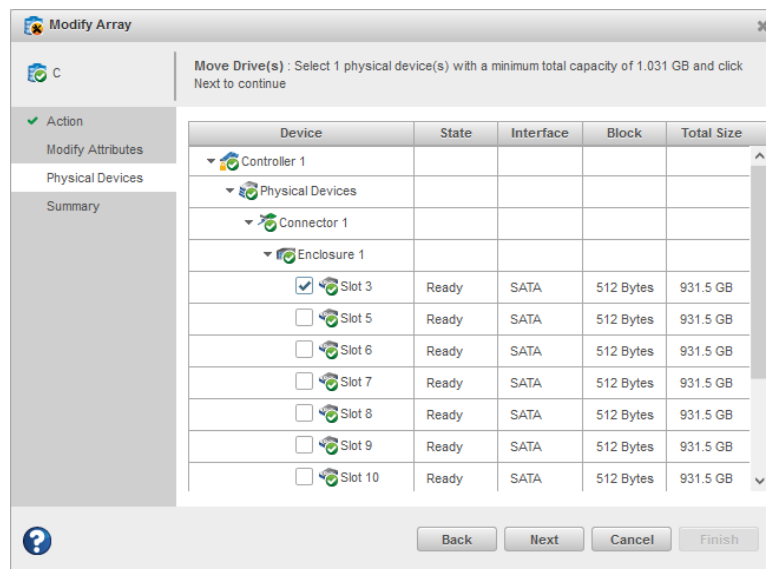
- In the Enterprise View, select an array.
- On the ribbon, in the Array group, click **Modify Array**.



- 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 [5.6.2. Modify Array](#).

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

## 7.7 Modifying an Array

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

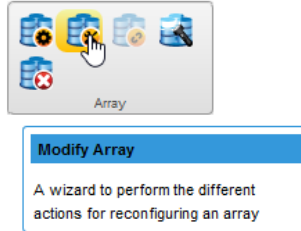
- Add Drives to an Array
- Remove Drives from an Array

If you add the logical drives, you are expanding the array by adding the data drives. You can shrink the array by removing one or more drives by selecting the remove drives option. While removing

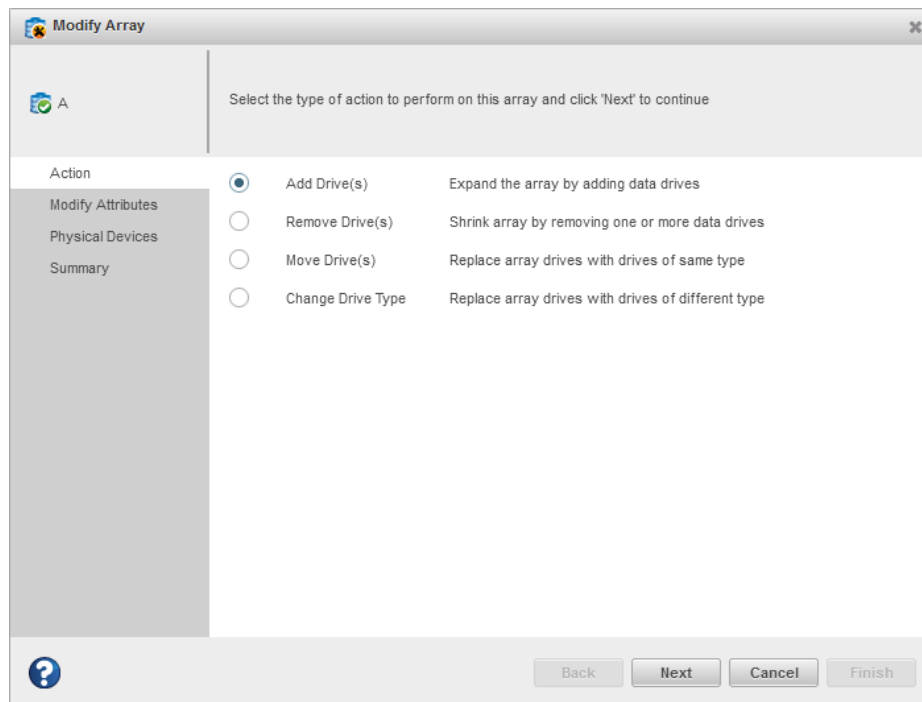
the physical drives from the array, the drives are in transient state and are not available until the operation completes.

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**.

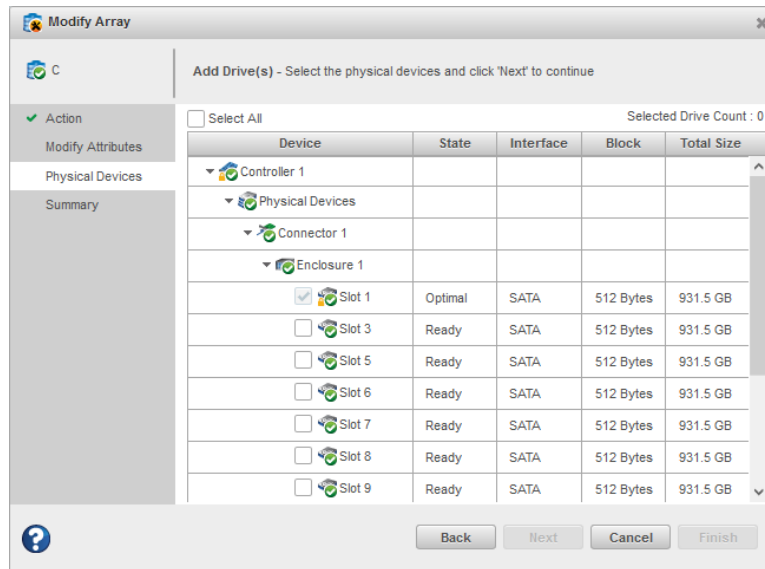


3. When the wizard opens, select **Add Drive(s)** or **Remove Drive(s)**, then click **Next**.



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 [5.6.2. Modify Array](#).

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

## 7.8 Working with Mirrored Arrays

maxView Storage Manager allows you to split a mirrored array and then recombine it. This process entails splitting a RAID 1, RAID 1(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.

### 7.8.1 Creating a Split Mirror Backup

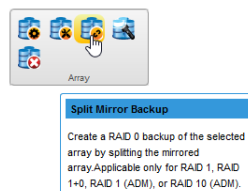
Use this option to split a mirrored array, consisting of one or more RAID 1, RAID 1(Triple), RAID 10, or RAID 10(Triple) logical drives, into two arrays: a primary array and a backup array, with these characteristics:

- 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 [7.8.2. 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**.



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

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

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

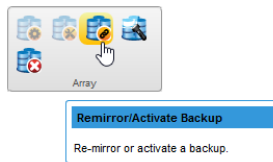
You can also reactivate the split mirror backup. This option makes the backup array fully accessible to the operating system. maxView Storage Manager removes the "Split Mirror Set Backup" designation and re-designates it as a Data Array.

To re-mirror, roll back, or reactivate a split mirror backup:

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

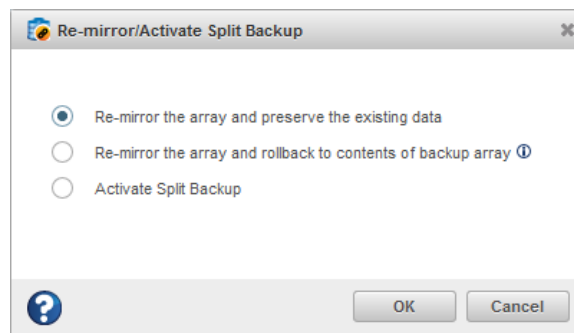
**Note:** Use the Summary tab on the Storage Dashboard to verify the array type.

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



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.



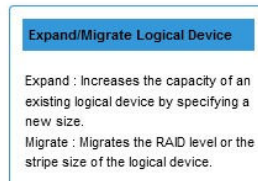
4. Click **OK**.

## 7.9 Changing the RAID Level of a Logical Drive

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

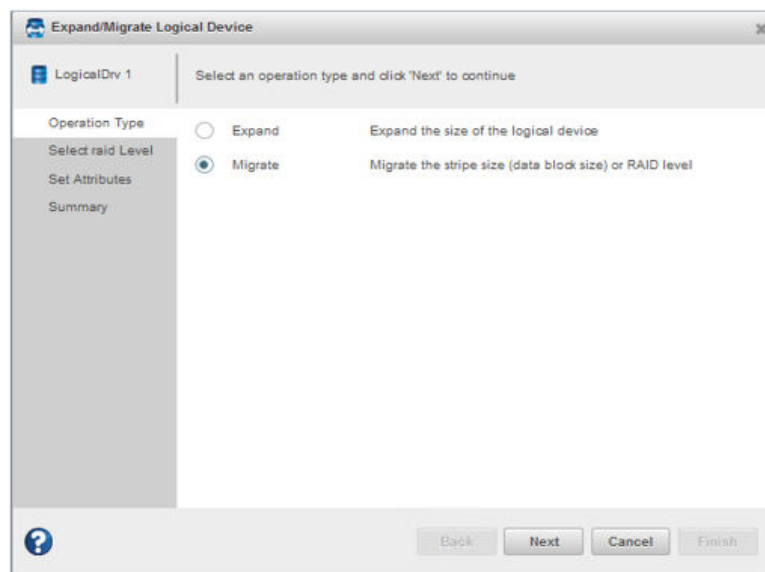
To change the RAID level of a logical drive:

1. In the Enterprise View, select a controller, then select the logical drive that you want to migrate.
2. On the ribbon, in the Logical Device group, click **Expand/Migrate**.

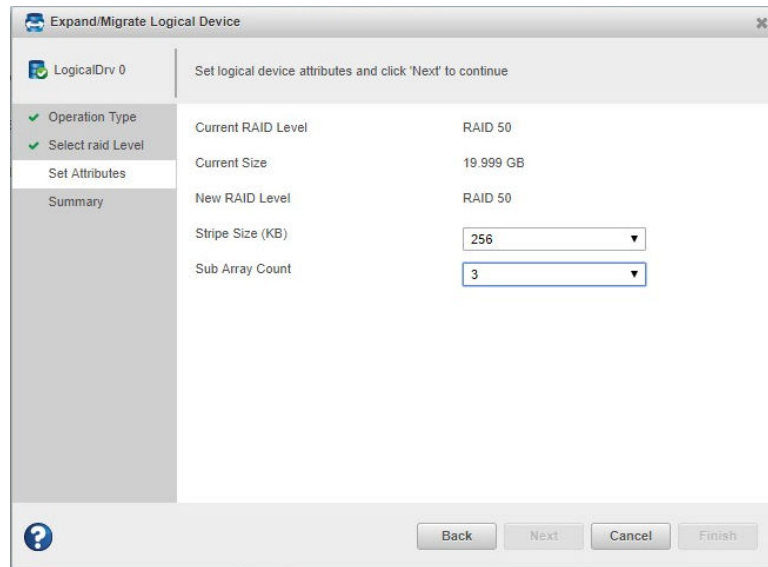


The Expand/Migrate Logical Device wizard opens.

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



4. Select a new RAID level, then click **Next**. Only valid RAID level options are offered.
5. Select the sub array count for RAID 50 and RAID 60.



6. Select the logical drive stripe size from the drop-down list.  
**Note:** The default stripe size usually provides the best performance.
7. Click **Next**.
8. Review the summary of logical drive settings. To make changes, click **Back**.
9. Click **Finish**.  
The logical drive is reconfigured and migrates to the new RAID level.

## 7.10 Increasing the Capacity of a Logical Drive

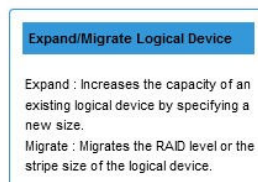
You can add more disk drive space, or *expand*, a logical drive, to increase its capacity.

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

**Note:** You can expand a logical drive only into the free space of the host array. To add physical drives in an array, see [7.7. Modifying an Array](#)

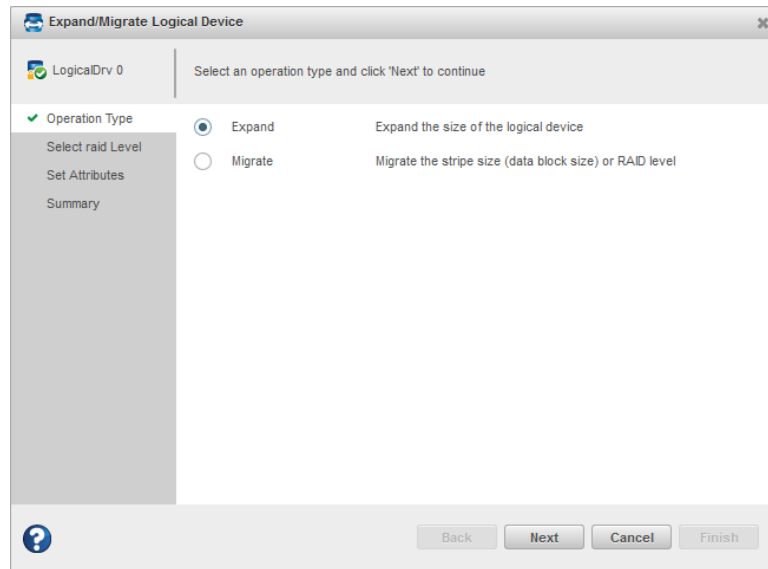
To increase the capacity of a logical drive:

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.

## 7.11 Changing the Logical Drive Rebuild Priority

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

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

If the logical drive is part of an array with an online spare, rebuilding begins automatically when drive failure occurs. If the array does not have an online spare, rebuilding begins when the failed physical drive is replaced. For more information, see [15.4. Rebuilding Logical Drives](#).

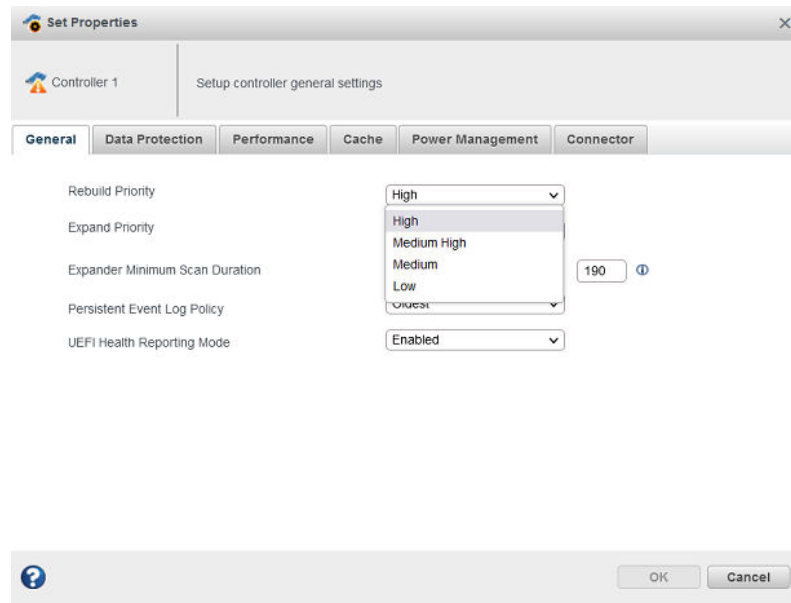
To change the rebuild priority:

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.



4. Click **OK**.

## 7.12 Renaming a Logical Drive

To change the name of a logical drive:

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



The Set Properties window opens.

3. In the Logical Device Name field, type the new name, then click **OK**. Names can include any combination of letters, numbers, and spaces.  
maxView Storage Manager updates the logical drive name and displays the new name in the Enterprise View.

## 7.13 Deleting an Array or Logical Drive

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



**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**.



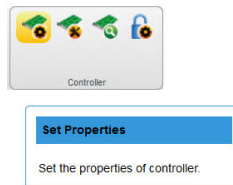
- When prompted to continue, click **Delete** to delete the array or logical drive.  
**Note:** If a deleted logical drive is the only logical in the array, the array itself is also deleted.

### 7.14 Maintaining an Energy-Efficient Storage Space

The power management options in maxVIEW Storage Manager control the power profile of the physical drives on a controller. They offer a balance between maximum performance and minimum power usage. To ensure continued operations when temperature thresholds are exceeded, you can enable Survival mode to throttle dynamic power settings to their minimum values. Spares created to protect an array are underutilized till the array state becomes degraded owing to drive failures. To achieve power efficiency gain, the inactive spares can be spun down.

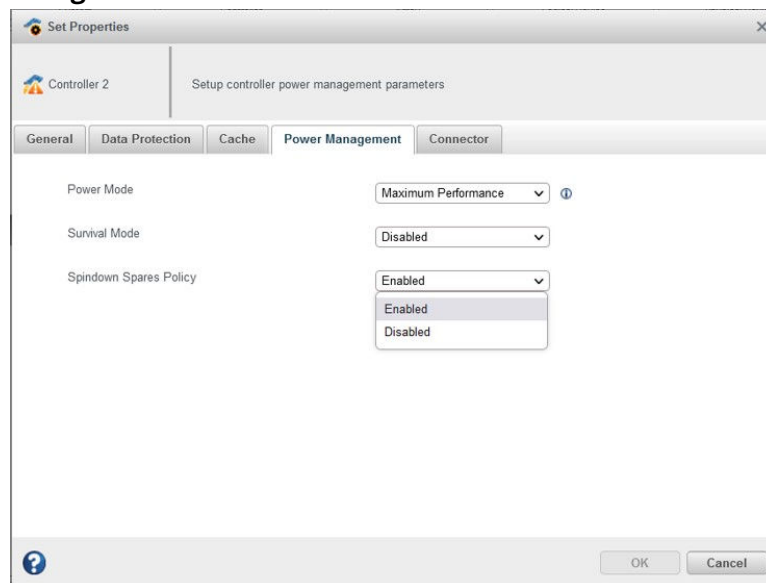
To set the power management options for a controller:

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



The Set Properties window opens.

- Click the **Power Management** tab.



- In the Power Mode drop-down list, select:
  - Balanced—Set static settings based on configuration and reduce dynamically based on workload.
  - 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.

**Note:** Some controller(s) do not support Balanced and Minimum Power mode.

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. In the Spindown Spares Policy drop-down list, select:

- Enabled—Allows the inactive spares to spin down.
- Disabled—Disables the inactive spares from spinning down.

7. Click **OK**.



## 8. 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.

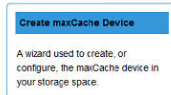
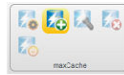
### 8.1 maxCache Limitations

- 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

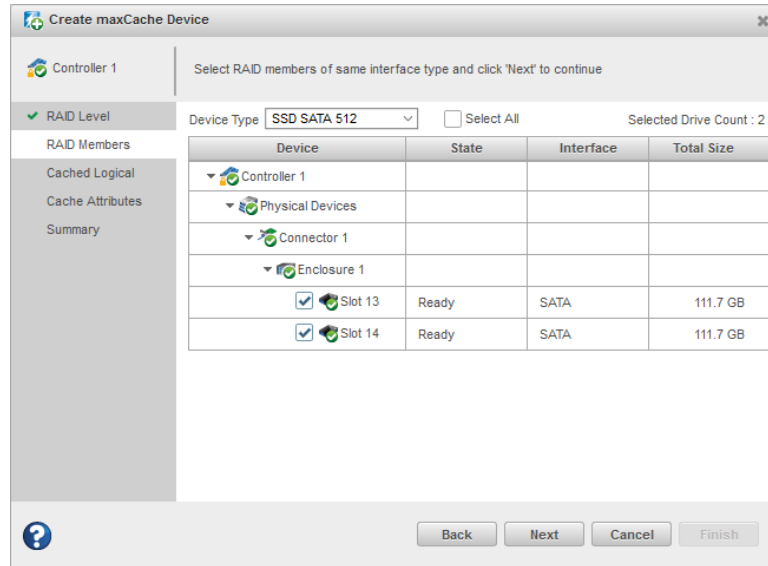
### 8.2 Creating a maxCache Device

To create a maxCache Device:

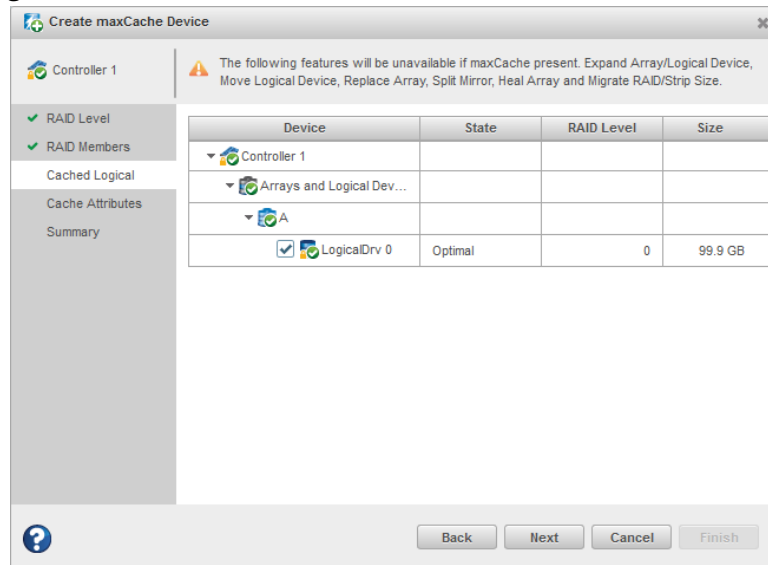
1. In the Enterprise View, select a system, then select a controller on that system. You can also create a maxCache device by selecting a logical device node.
2. On the ribbon, in the maxCache group, click **Create maxCache**.



- 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.
- 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 [5.6.5. maxCache](#).



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



- (Optional) In the Cache Attributes panel, customize the maxCache Device settings. You can:
  - Set a smaller logical drive size. (By default, the maxCache Device uses up to the maxSize of the data logical drive.)
  - Set the write cache mode to Write-Back (default) or Write-Through.

- Select the Cache Line Size. The Cache Line Size impacts the cache performance and the maximum size selected. To create a large size maxCache you need to select the larger cache line size supported by that controller.
7. Click **Next**, then review the logical drive settings.
  8. Click **Finish**, then click **OK**.  
maxView Storage Manager updates the configuration, then adds an array and logical device to the maxCache Device tree in the Enterprise View.

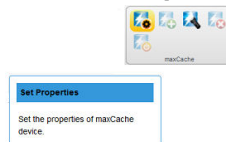
### 8.3 Changing the Write Cache Mode

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

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

To change the maxCache write cache mode:

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

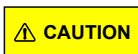


The Set Properties window opens.

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

### 8.4 Deleting the maxCache Device

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



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

#### Note:

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

To delete the maxCache Device:

1. In the Enterprise View, select a controller, then select the maxCache Device.
2. On the ribbon, in the maxCache group, click **Delete**.



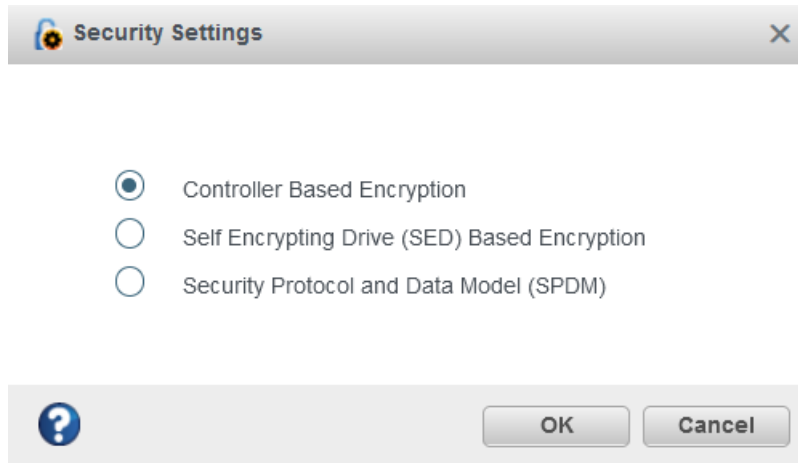
3. When prompted, click **Delete**, then click **OK**. Click **Cancel** to cancel the action.

## 8.5 Analyzing maxCache Performance

maxView Storage Manager provides advanced usage statistics about the maxCache Devices on your 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.

## 9. 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.

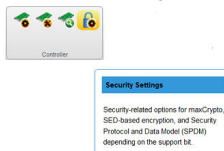
**Note:** Encryption of non-RAID volumes (such as physical, raw, or pass-through devices) is not supported. Consequently, HBAs and controllers operating in HBA Mode do not support maxCrypto.

### 9.1 maxCrypto Initial Setup

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

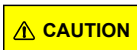
To setup maxCrypto:

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



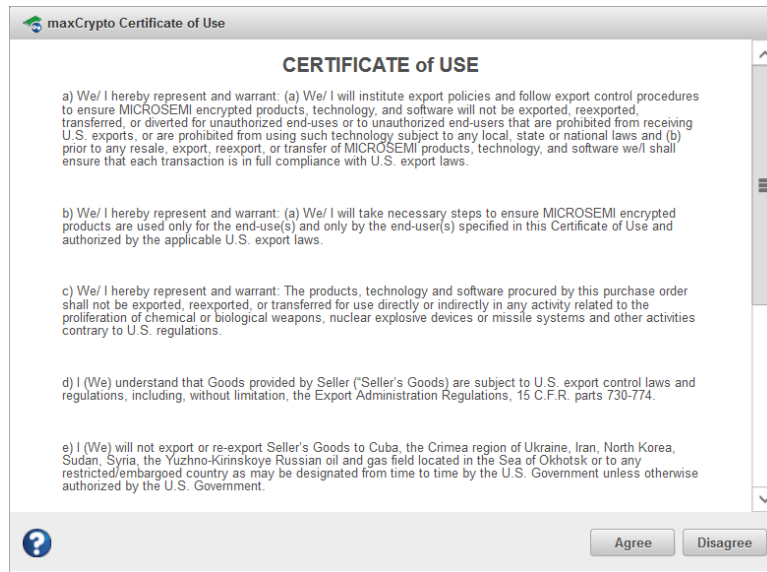
The **Set maxCrypto Configuration** window opens; the **Initial Setup** tab is selected, by default.

3. In the Key Management Mode drop-down, select `Local` to configure the local key management mode, where encryption keys are locally generated using the Master Key. Select `Remote` to configure remote key management mode, where encryption keys are generated and stored on a remote key server. A reboot is needed to take effect.  
**Note:** For Remote key management mode, you need to configure the KMS server using pre-boot.
4. In the maxCrypto Mode drop-down, select `Enabled` to activate maxCrypto. Select `Disabled` to deactivate maxCrypto.
5. 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.
6. 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.

7. 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 (`#,!,@,...`).
8. In the Re-Enter Crypto Password field, re-enter the Crypto Officer password.
9. Click **OK**.
10. When the maxCrypto Certificate of Use window opens, click **Agree** to complete the maxCrypto activation.



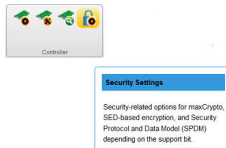
### 9.1.1 Managing maxCrypto Accounts

After initial setup is complete, the Crypto Officer account is logged in, by default. The Crypto Officer can perform all account management operations, including configuring the standard User account, changing passwords, and enabling password recovery options. The user account has the ability to perform a limited number of maxCrypto operations, as described in the following table.

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
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 **Security Settings**.



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

The screenshot shows the 'Set maxCrypto Configuration' window with the 'Account' tab selected. The 'User Role' dropdown is set to 'Crypto Officer/Admin'. The 'Enter New Password' and 'Re-Enter New Password' fields contain masked characters. The 'Set/Change Password Recovery Question' field contains 'What is your first company?' and the 'Set/Change Password Recovery Answer' field contains 'My first company is Microsem'. At the bottom, there are 'Logout', 'OK', and 'Cancel' buttons.

3. In the User Role drop-down, select the `Crypto Officer` or `User` account.
4. In the Enter New Password field, enter the password for the account.  
The password is a 8-16 character string, comprising all printable ASCII characters. It must include at least one uppercase character, one lowercase character, one numeric, and one special character (#,!,@,...).
- Note:** The first time you enable the User account, this entry defines the initial login credentials for the account. For an existing account, this entry changes the login credentials.
5. In the Re-Enter New Password field, re-enter the password for the user account.
6. For the `Crypto Officer` account, set/change the password recovery question and answer:
  - a) In the Set/Change Password Recovery Question field, enter a recovery question for a forgotten password.
  - b) In the Set/Change Password Recovery Answer field, enter the answer to the recovery question.
- Note:** Password recovery is available only for the `Crypto Officer`. The recovery question/answer fields are deactivated for the `User` account.
7. Click **OK**.

### 9.1.2 Logging In and Logging Out

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

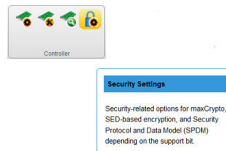
After initial setup is complete, the `Crypto Officer` account is logged in, by default.

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



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

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



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

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

To reset the Crypto Officer password:

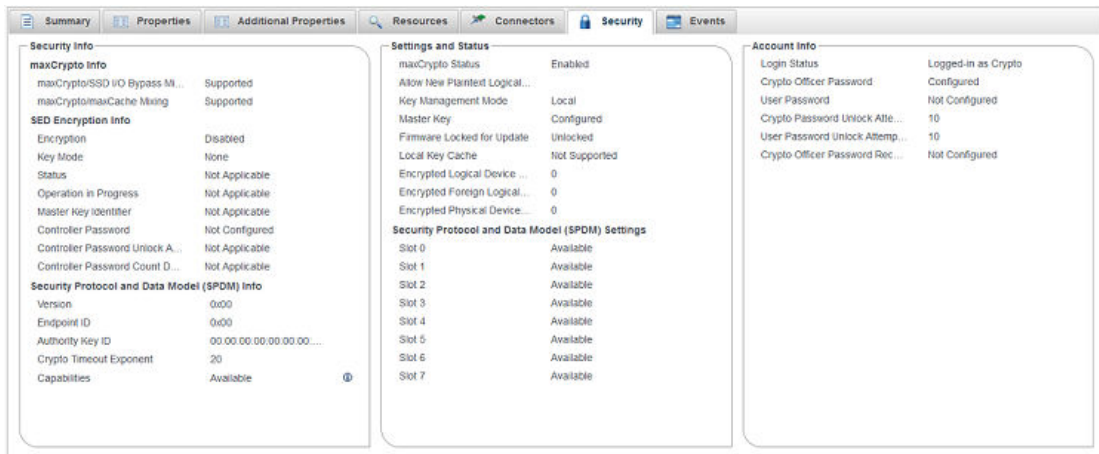
1. In the Login tab, select the `Crypto Officer` user role, as described above.
2. Click **Forgot Password**.
3. In the Recovery Answer field, enter the answer to the recovery question.
4. Enter a new password for the `Crypto Officer` account.

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

5. Re-enter the new `Crypto Officer` password.
6. Click **OK**.

### 9.1.3 Checking maxCrypto Status

To check the maxCrypto status, select a controller in the Enterprise view, then click the **Security 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.
Key Management Mode	Local key management mode is where encryption keys are locally generated using the Master Key. Remote key management mode is where encryption keys are generated and stored on a remote key server. For remote mode to take effect, a reboot is required.
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.
Local Key Cache	Encryption keys are stored in a cache locally to allow access to encrypted logical device(s) when the remote key server is offline. <b>Note:</b> This only applies when maxCrypto is operating in Remote Key Management Mode.
Attempts Remaining Before Clearing Local Key Cache	Number of attempts to access the key manager before deleting the local key cache store. When local key cache is disabled, this setting does not have any effect.
Retry Interval In Minutes	Time in minutes between attempts to reach the key manager and validate the key cache. When local key cache is disabled, this setting does not have any effect.

.....continued	
Property	Description
Number of maxCrypto Logical Devices	Total count of the encrypted logical devices.
Number of maxCrypto Physical Devices	Total count of encrypted physical devices.
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. <b>Note:</b> 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. <b>Note:</b> 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.

## 9.2 Modifying the maxCrypto Configuration

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

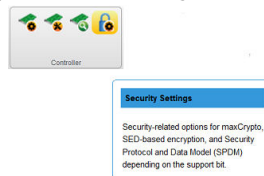
If you are logged in as the Crypto Officer, you can:

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

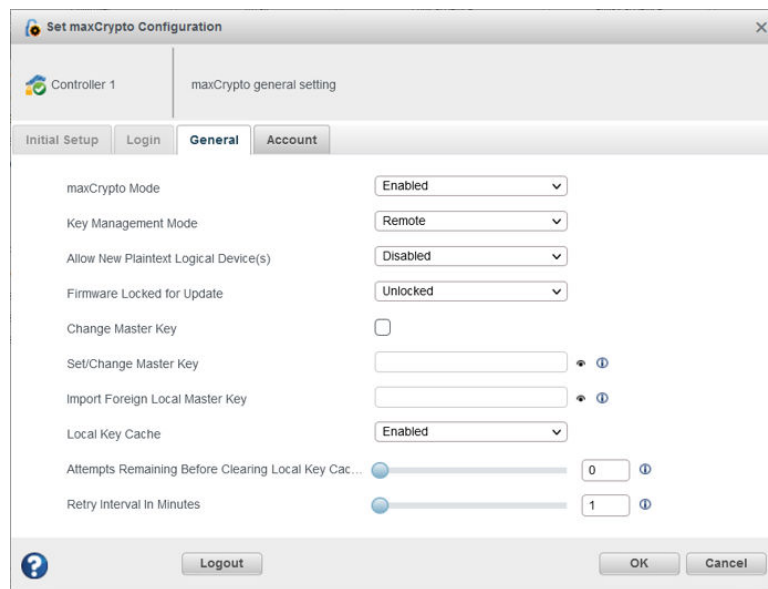
If you are logged in as the maxCrypto User, you can only Lock/Unlock firmware upgrade.

To modify the maxCrypto configuration:

1. In the Enterprise View, select a system, then select a controller on that system.
2. On the ribbon, in the Controller group, click **Security 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 Key Management Mode drop-down, select `Local` to configure the local key management mode, where encryption keys are locally generated using the master key. Select `Remote` to configure remote key management mode, where encryption keys are generated and stored on a remote key server. For remote key management mode, reboot is needed to take effect. To change between Local to Remote or Remote to Local, a master key is required. **Note:** For Remote key management mode, you need to configure the KMS server using Preboot.

**Note:** When changing the key management mode, all the other operations in this dialog will be disabled.

- 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.

---

- In the Local Key Cache, select `Enabled` to store the keys in the cache locally to allow access to encrypted logical device(s) when the remote key server is offline. Select `Disabled` to remove the local keys from the cache. When Local Key Cache is enabled:
  - The **Attempts Remaining Before Clearing Local Key Cache** field also gets enabled to specify the number of attempts to access the key manager before deleting the local key cache store.

- The **Retry Interval In Minutes** also gets enabled to specify the time in minutes between attempts to reach the key manager and validate the key cache.

4. Click **OK**.

### 9.3 Creating an Encrypted Logical Drive

Use the Create Logical Device wizard to create encrypted and plaintext logical drives on an existing array or a new array. See [5.4. 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.

#### 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 [9.1.2. 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.

### 9.4 Converting Plaintext Data to Encrypted Data

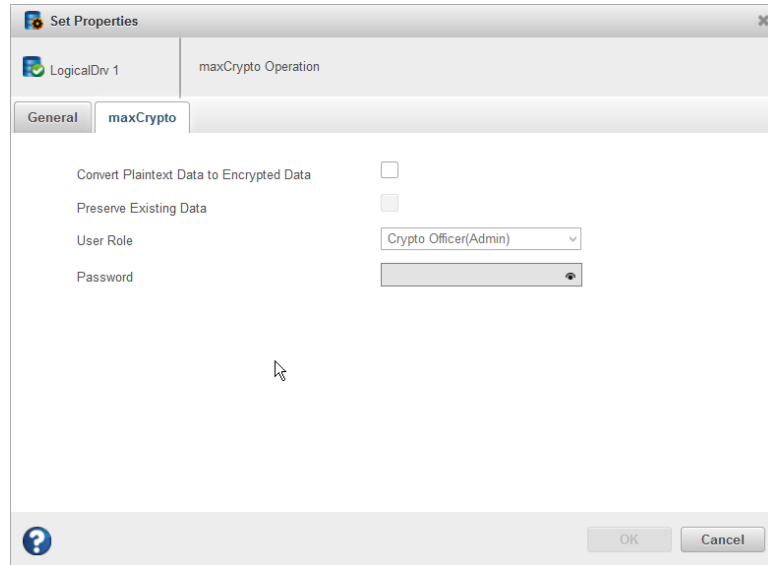
Use this operation to convert plaintext data to encrypted data. You can convert an unencrypted logical drive or all unencrypted logical drives on an array. Additionally, you can choose to preserve or discard the existing data during conversion.

To convert plaintext data:

1. In the Enterprise View, select a controller, then select a plaintext (unencrypted) logical drive or an array.
2. On the ribbon, in the Logical Device group or Array group, click **Set Properties**.



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



**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**.

## 9.5 Re-Keying a Logical Drive

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

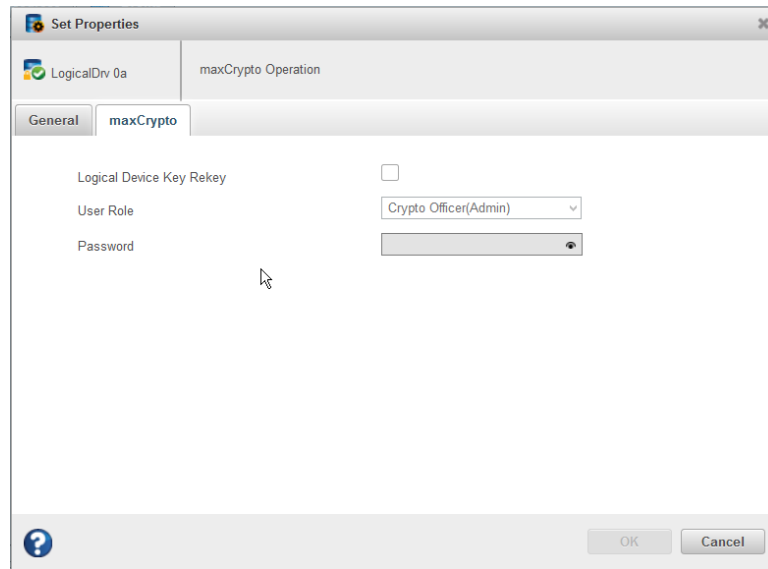
Optionally, you can re-key an array to generate a new key for all encrypted logical drives on the array.

To re-key a logical drive:

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



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



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

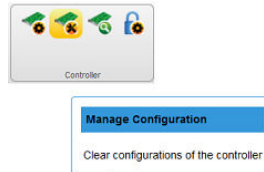
## 9.6 Clearing the maxCrypto Configuration

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

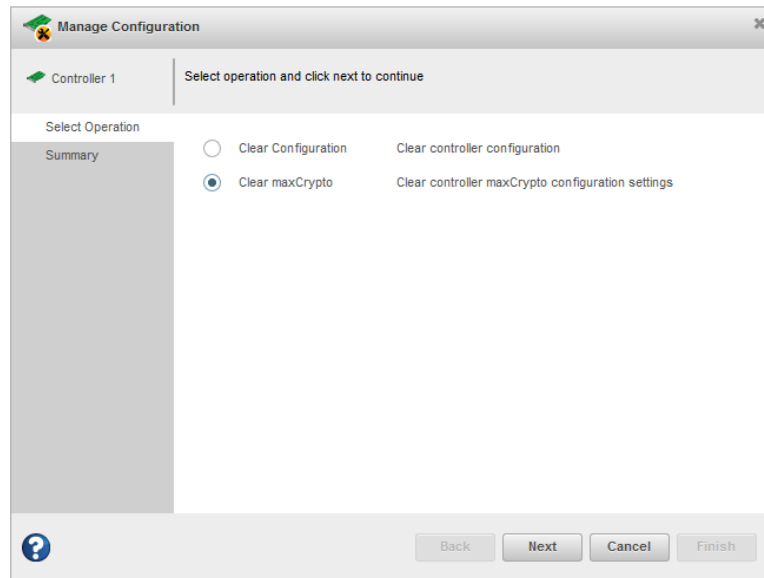
**Note:** To clear the maxCrypto configuration, ensure that there is no encrypted logical drive available in your storage space.

To clear the maxCrypto configuration:

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



The Manage Configuration wizard opens.



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

## 9.7 Erasing an Encrypted Logical Drive

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

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

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

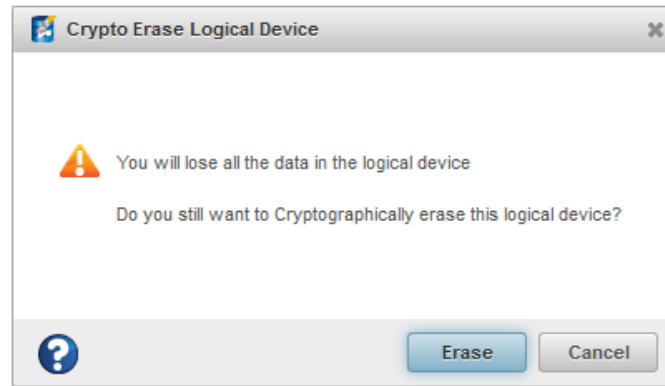
To cryptographically erase a logical drive:

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



The Crypto Erase Logical Device window opens.





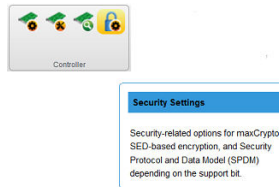
3. Click **Erase**.

## 9.8 Importing a Foreign Master Key

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

To import a foreign master key:

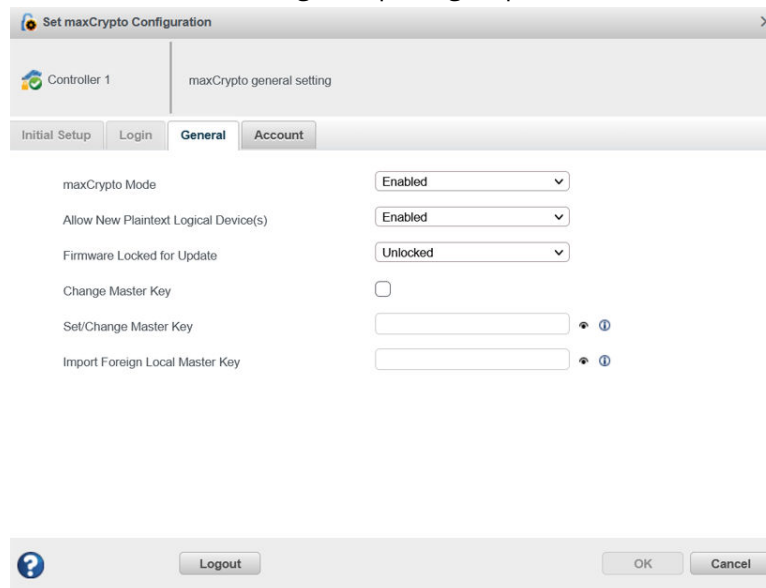
1. In the Enterprise View, select a system, then select a controller on that system.
2. On the ribbon, in the Controller group, click **Security Settings**.



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**.

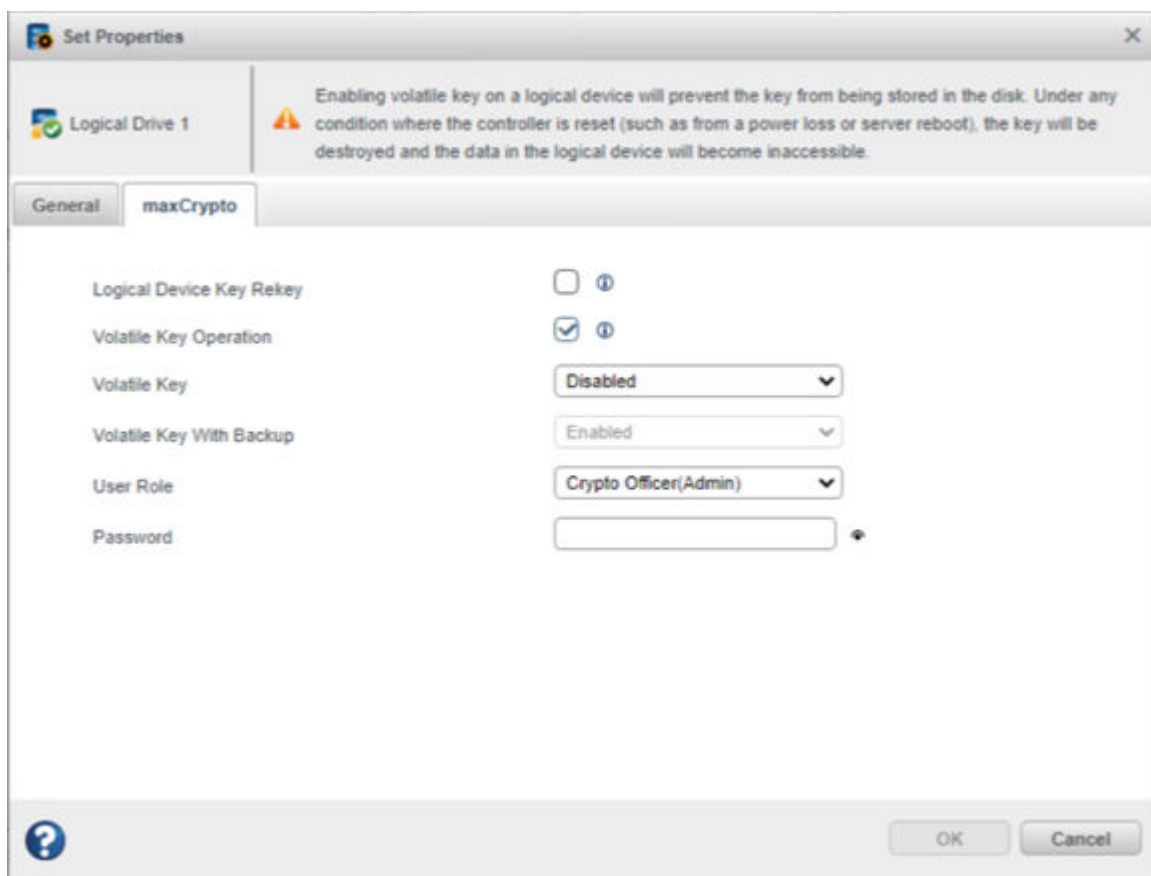
## 9.9 Volatile Key

Volatile key is supported only when maxCrypto is operating in Remote Key Management Mode and the logical device is encrypted. Data keys are stored in volatile memory instead of disk. This provides stronger data protection, but it can also cause the data to be inaccessible during power loss when the volatile key is not backed-up.

Once **Volatile Key With Backup** option is enabled, the data key will be backed up to remote key manager when enabling the volatile key. You have an option to restore the key from the remote key manager. If disabled, the data key will not be backed up to remote key manager.



**WARNING** Enabling volatile key on a logical device prevents the key from being stored in the disk. Under any condition where the controller is reset (such as from a power loss or server reboot), the key gets destroyed and the data in the logical device becomes inaccessible. There is no method available to recover the volatile key or access the data on the logical device.

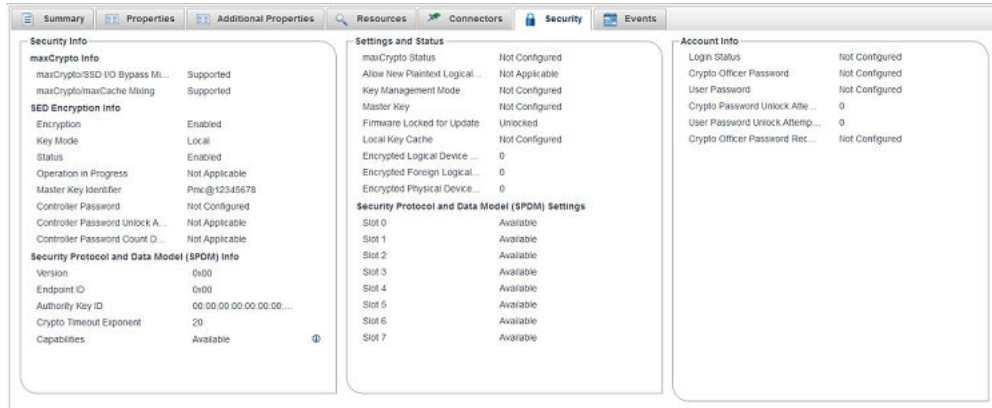


## 10. Working with Self Encrypting Drive (SED) Based Encryption

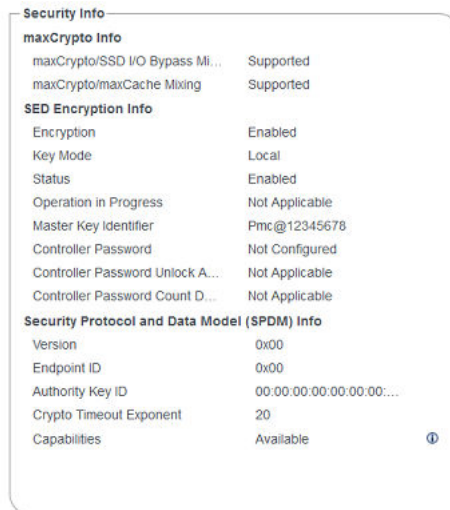
Self Encrypting Drive (SED) based Encryption provides the capability to manage all the SEDs connected to the controller by using only one active pin called the **Master Key**. The controller keeps the master key in NVRAM. When the controller boots, the master key is read from NVRAM and applied to all the attached controller owned SEDs.

The following images show that the controller supports both maxCrypto and Managed SED. It also shows the properties of maxCrypto and Self Encrypting Drive (SED) before configuration.

Click the controller node, and select **Security** tab. The **Security Info > SED Encryption Info** displays the properties of SED based encryption.



If the controller supports only Managed SED, click the controller node, and then click the **Security** tab. The **SED Encryption Info** panel displays the properties of SED based encryption.

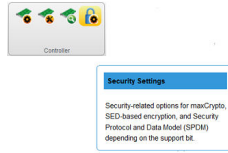


**Note:** Initially, most of the values are "Not Applicable" before configuring SED based encryption.

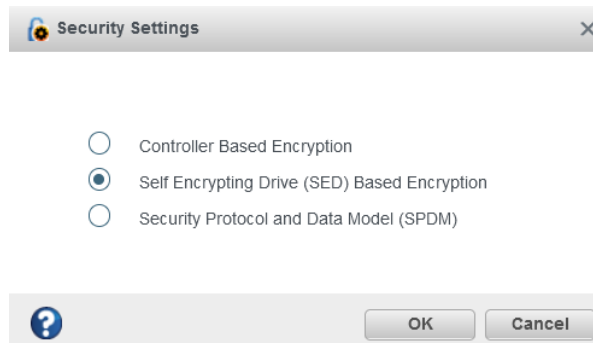
## 10.1 Self Encrypting Drive (SED) Initial Setup

Perform the following steps to configure the Self Encrypting Drive (SED) based encryption.

1. In the Enterprise View, select a controller.
2. On the ribbon, in the Controller group, select the **Security** settings.



3. Click the Security Settings ribbon icon to open a dialog based on the following criteria.
  - If the controller only supports maxCrypto. For more details, see [9. Working with maxCrypto™ Devices](#).
  - If the controller only supports Managed SED. For more details, see [10. Working with Self Encrypting Drive \(SED\) Based Encryption](#).
  - If the controller only supports SPDM. For more details, see [11. Working with Security Protocol and Data Model \(SPDM\)](#).
  - If the controller supports **maxCrypto**, **Managed SED**, and **Security Protocol and Data Model (SPDM)** but neither are configured, perform the following steps for SED Initial Setup.
    - i. Click the Security Settings ribbon icon to display the **Security Settings** dialog box.



- ii. Select **Self Encrypting Drive (SED) Based Encryption** option and then click OK. The Self Encrypting Drive (SED) Based Encryption dialog box appears, which is explained further in this section.

4. Select the Initial Setup tab to do the initial configuration of the SED based encryption settings.
  - a. **Key Management Mode:** This property manages the master key based on the mode. Currently, maxView supports both Local and Remote key management mode. For Remote key mode, you need to configure the KMS server using pre-boot.
  - b. **Master Key:** This property is used to set the unique key.
    - It must consist of all the printable ASCII characters and length should be 8-32 characters long
    - It must consist of at least one uppercase character
    - It must consist of at least one lowercase character
    - It must consist of at least one number
    - It must consist of at least one special character (#, @, \$...)
 The Master Key should be remembered or stored manually. There is no option to retrieve it; however, you can reset the Master Key.
 

**Note:** This field is applicable only for Local Mode and is disabled in Remote Mode.
  - c. **Re-Enter Master Key:** This should match to the entered master key.
 

**Note:** This field is applicable only for Local Mode.
  - d. **Master Key Identifier:** Master key identifier is a hint that helps to remember master key. It is optional and must be between 0 and 32 character long and should contain only ASCII characters.
 

**Note:** This field is applicable only for Local Mode and is disabled in Remote Mode.
  - e. **Set Controller Password:** The Controller Password is an optional setting. Check the **Set Controller Password** check box to enable the controller password during initial setup.
  - f. **Controller Password:** This is for additional security. If a controller password is set, all SED physical and logical devices are offline at the boot time. Enter the controller password to

bring the SED devices online. It is recommended to use the same controller password for all encrypted controllers in the server.

When enabled, the controller does not use the master key to unlock any SEDs until the password is supplied and validated.

**Note:** This field is applicable only for Local Mode and is disabled in Remote Mode.

- g. **Re-Enter Controller Password:** This must match to the entered controller password.

**Note:** This field is applicable only for Local Mode and is disabled in Remote Mode.

5. Click OK.

**Note:** For Remote key management mode configuration, a manual reboot is required to take effect. The status of the Encryption Status will be "Enabled, Waiting on Master Key" and most of the operation is not allowed until the system reboots.

The following message is displayed when the Set Controller Password is selected:

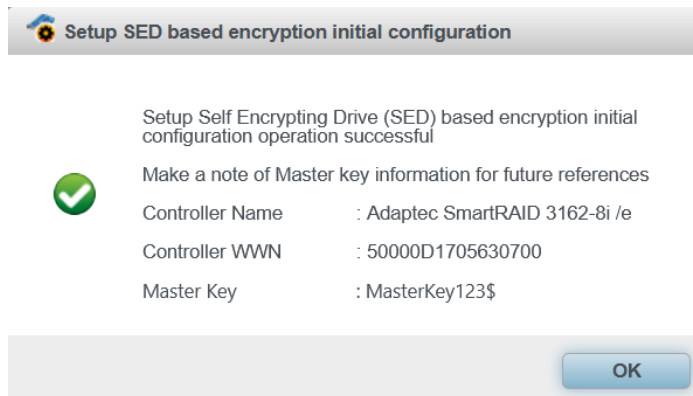
*Please record the Master Key. There is no way for recovering or displaying the Master Key once the value is set. Failure to provide the Master Key may result in encrypted data being inaccessible.*

Once user select the **Set Controller Password**, the following message gets displayed:

*If a controller password is set, all encrypted logical device will be offline at boot time. The user must enter the controller password to bring the encrypted logical device online. It is recommended to use the same controller password for all encrypted controllers in the server.*

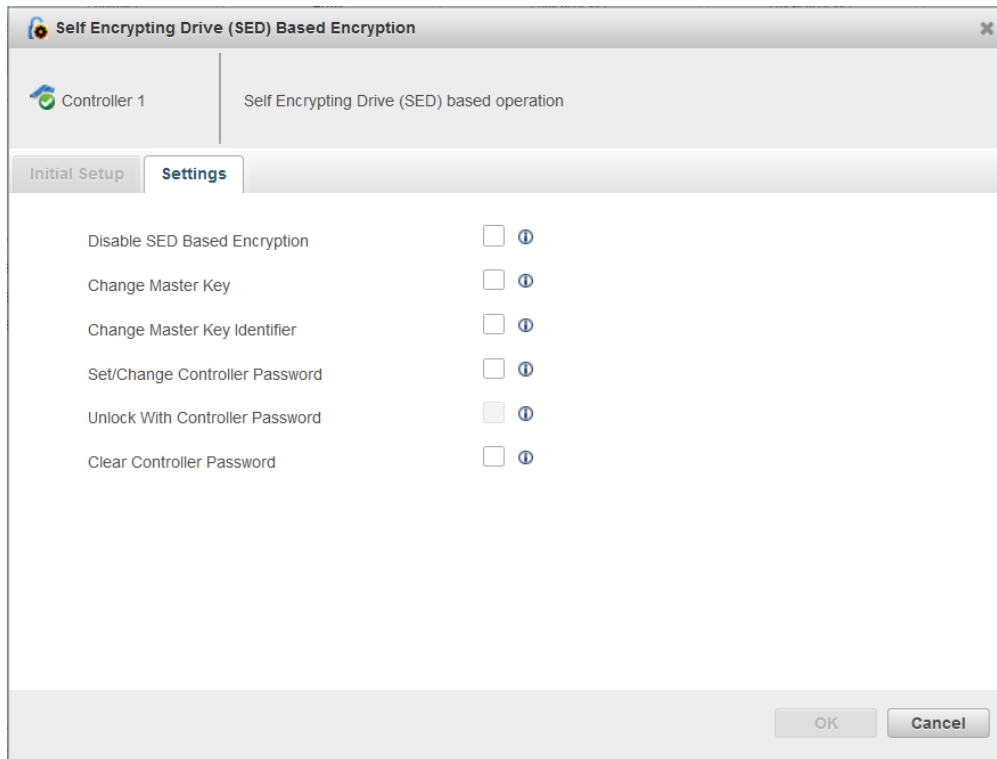
After the successful completion, the status dialog gets displayed with the Controller and Master Key details.

**Note:** This dialog box is applicable only for Local Key Management Mode.



## 10.2 SED Based Encryption Settings

This tab provide the options to perform the SED based encryption operations. Only one operation can be performed at a time.



Following is the list of operations:

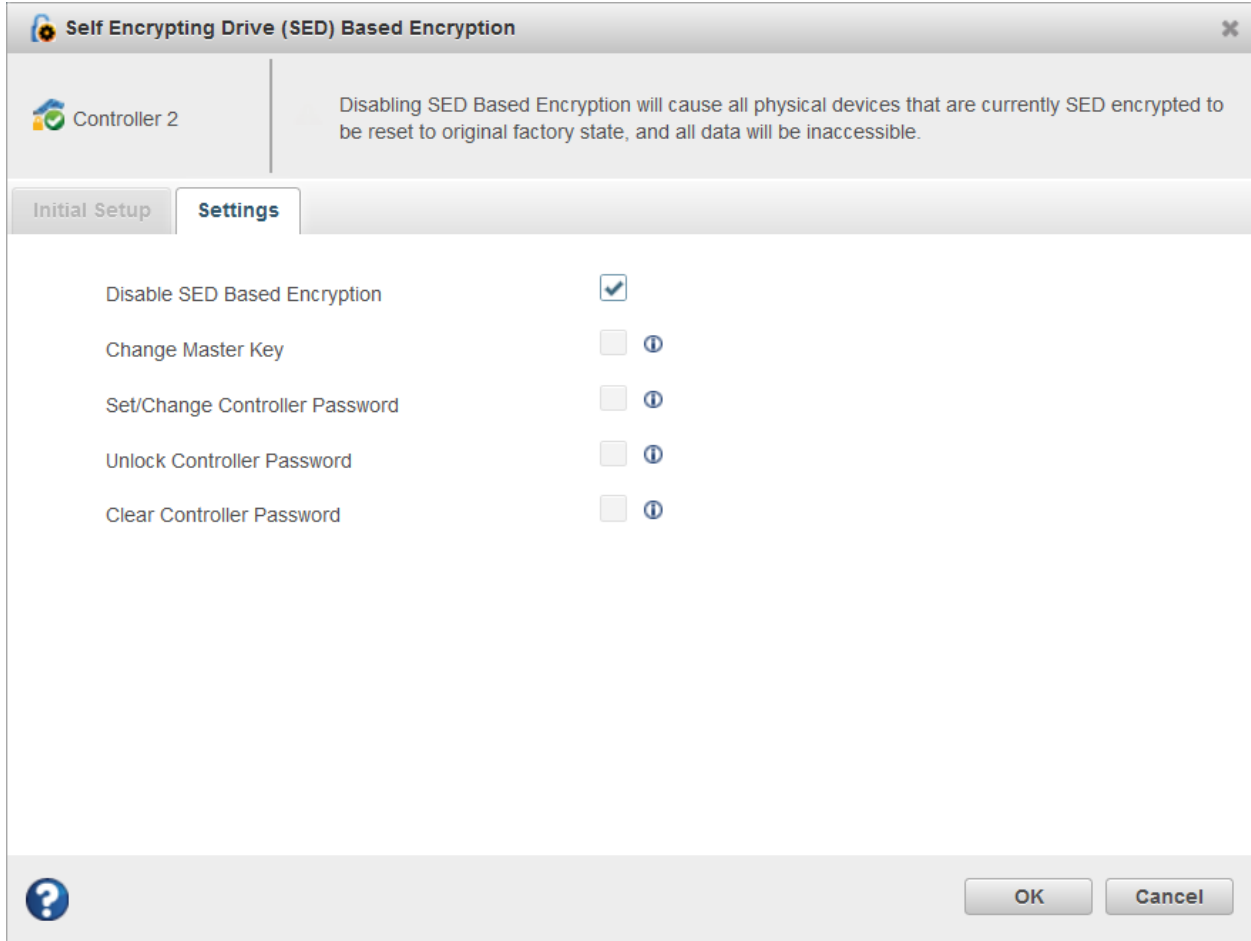
- **Disable SED Based Encryption:** This operation disables the Self Encrypting Drive (SED) based encryption configuration.
- **Change Master Key:** Update the existing master key with a new master key.
- **Change Master Key Identifier:** Change the hint to remember the master key.
- **Set/Change Controller Password:** This operation provides the option to set/change the controller password.
- **Unlock With Controller Password:** This operation provides the option to unlock the SED locked offline logical device, which may occur when the controller password was not entered or an invalid controller password was entered at boot time. This option is only applicable when a controller password is configured, and SED Encryption status is *"Waiting on Controller Password"*.
- **Clear Controller Password:** This operation removes the configured controller password.

**Note:** The **Change Master Key**, **Change Master Key Identifier**, **Set/Change Controller Password**, **Unlock With Controller Password**, and **Clear Controller Password** fields are applicable only for Local Mode and are disabled in Remote Mode.

### 10.2.1 Disabling SED Based Encryption

Perform the following steps to disable the SED based encryption:

1. Open the **Self Encrypting Drive (SED) Based Encryption** dialog box and then click the **Settings** tab.
2. Select the **Disable SED Based Encryption** check box and then click **OK**.  
This removes the SED based encryption configuration.



**Disable SED Based Encryption** check box is disabled if one or more SED is not in Original Factory State (OFS) or SED Encryption has *Waiting on Controller Password* status.

### 10.2.2 Changing Master Key

Perform the following steps to change the master key:

1. On the Settings tab, select the **Change Master Key** check box. Click **OK**.  
**Note:** A message is displayed in the header while changing the master key, "Please record the Master Key. There is no way for recovering or displaying the Master Key once the value is set. Failure to provide the Master Key may result in encrypted data being inaccessible".



**Self Encrypting Drive (SED) Based Encryption**

Controller 1

Please record the Master Key. There is no way for recovering or displaying the Master Key once the value is set. Failure to provide the Master Key may result in encrypted data being inaccessible.

Initial Setup | **Settings**

Disable SED Based Encryption  ⓘ

Change Master Key

New Master Key  ⓘ

Re-Enter Master Key  ⓘ

Master Key  ⓘ

Change Master Key Identifier  ⓘ

Set/Change Controller Password  ⓘ

Unlock With Controller Password  ⓘ

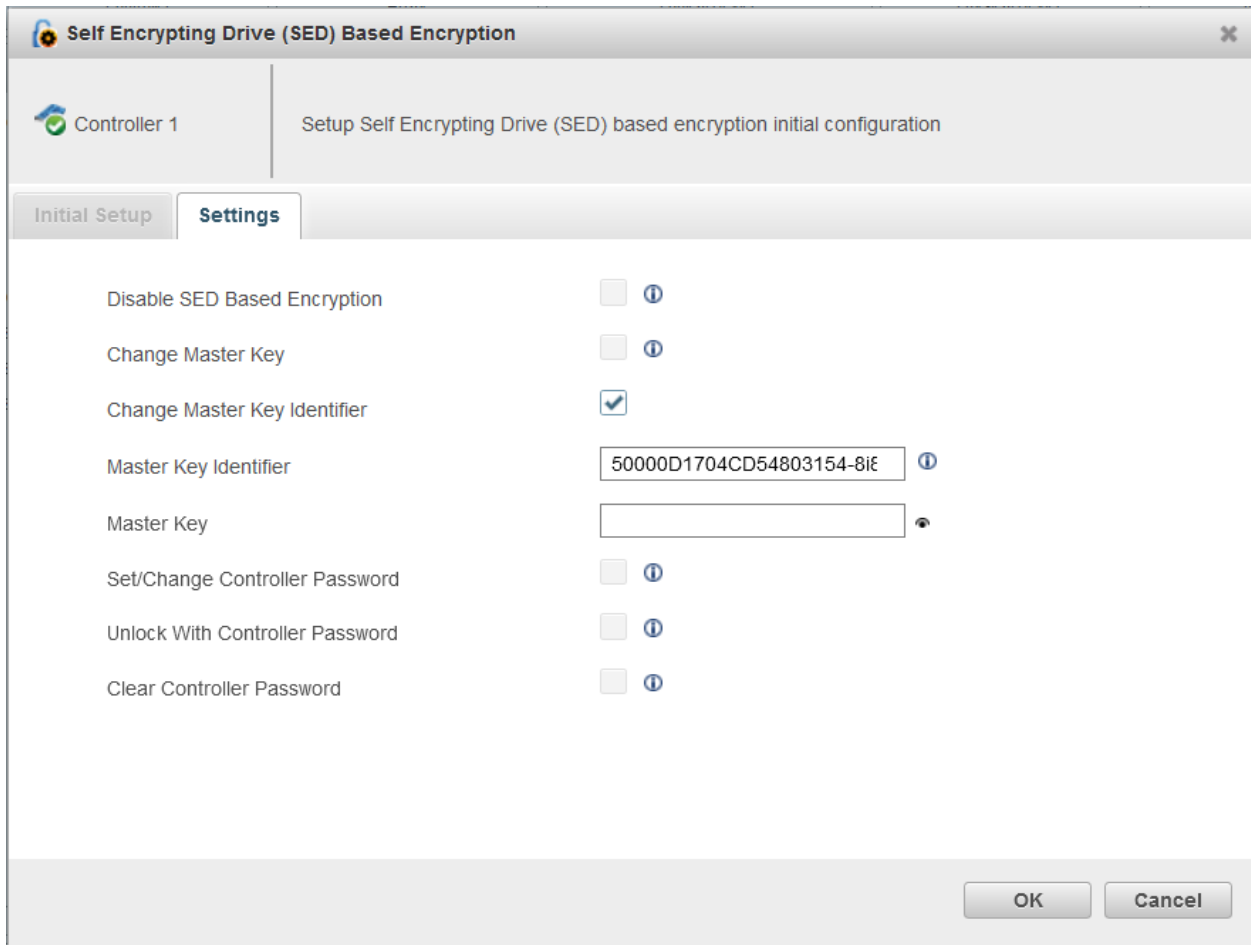
Clear Controller Password  ⓘ

OK Cancel

2. Enter the following details:
    - **New Master Key:** Enter the new master key
    - **Re-Enter Master Key:** Re-enter the new master key
    - **Master Key:** Enter the previous master key
  3. Click **OK**.
- Note:** When SED Encryption status is "Waiting on Controller Password", the **Change Master Key** check box is disabled until the controller password is supplied.

### 10.2.3 Changing Master Key Identifier

This operation is used to change the hint to remember the master key.



If the Master Key Identifier is not set during the initial configuration, it automatically takes the default value.

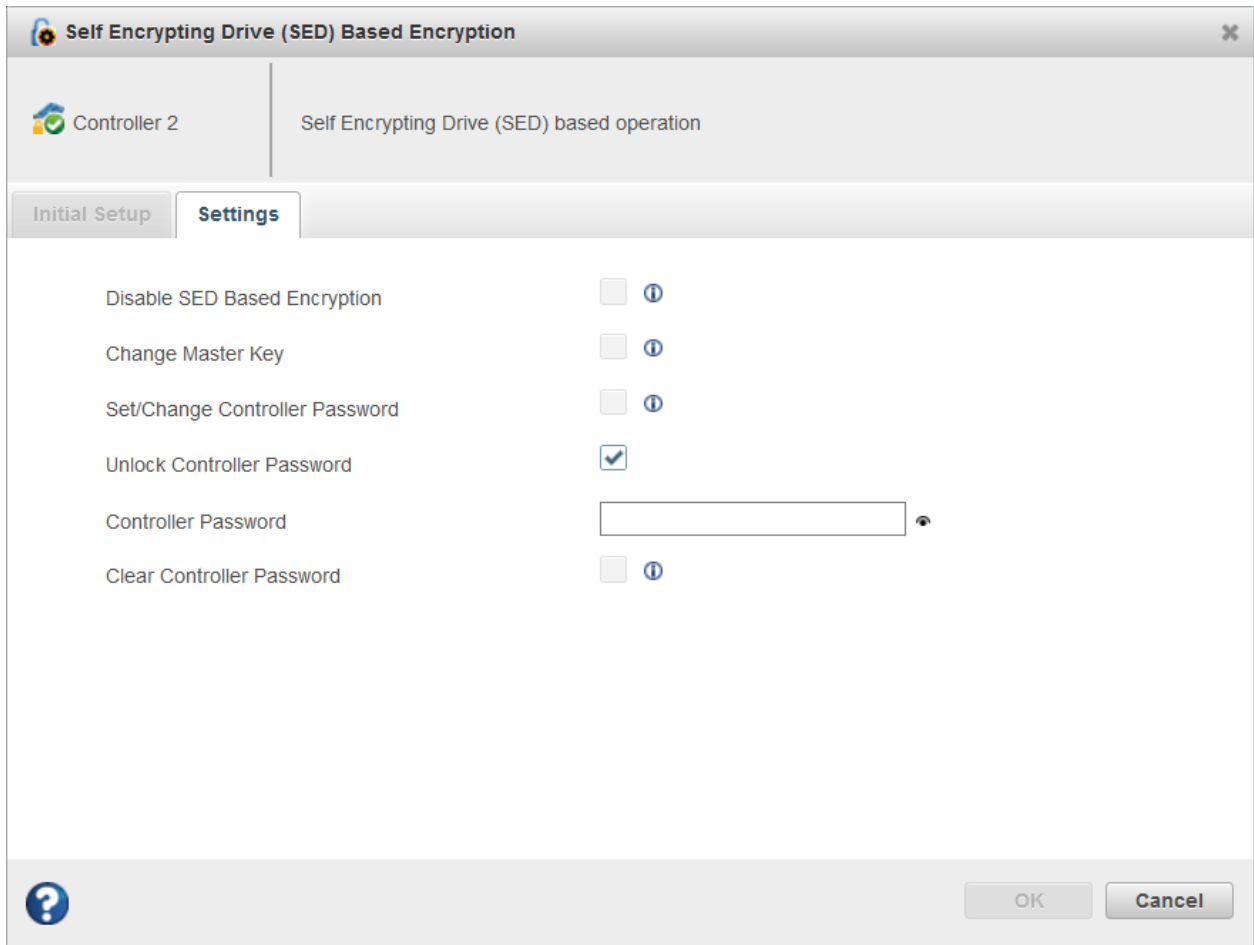
To change the Master Key Identifier, the Master key should be provided.

**Note:** When SED Encryption status is *"Waiting on Controller Password"*, the **Change Master Key Identifier** check box is disabled until the controller password is supplied.

### 10.2.4 Unlocking Controller Password

This operation provides the option to unlock the SED locked logical device, which may occur when the controller password was not entered or an invalid controller password was entered at boot time. This option is only applicable when the controller password is configured and SED Encryption status has *"Waiting for Controller Password"*.

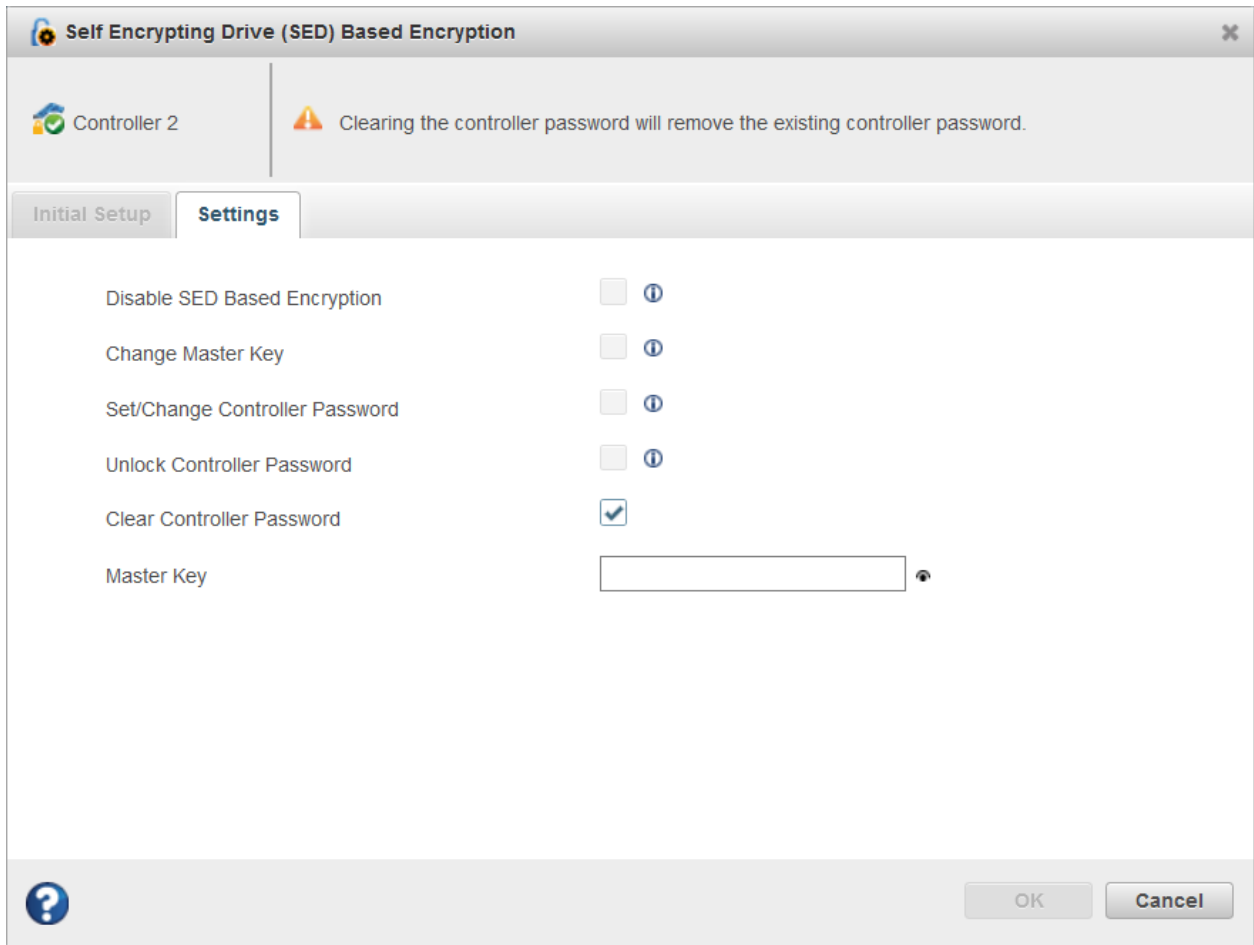
Once the **Unlock Controller Password** check box is checked, then provide the controller password.



### 10.2.5 Clear Controller Password

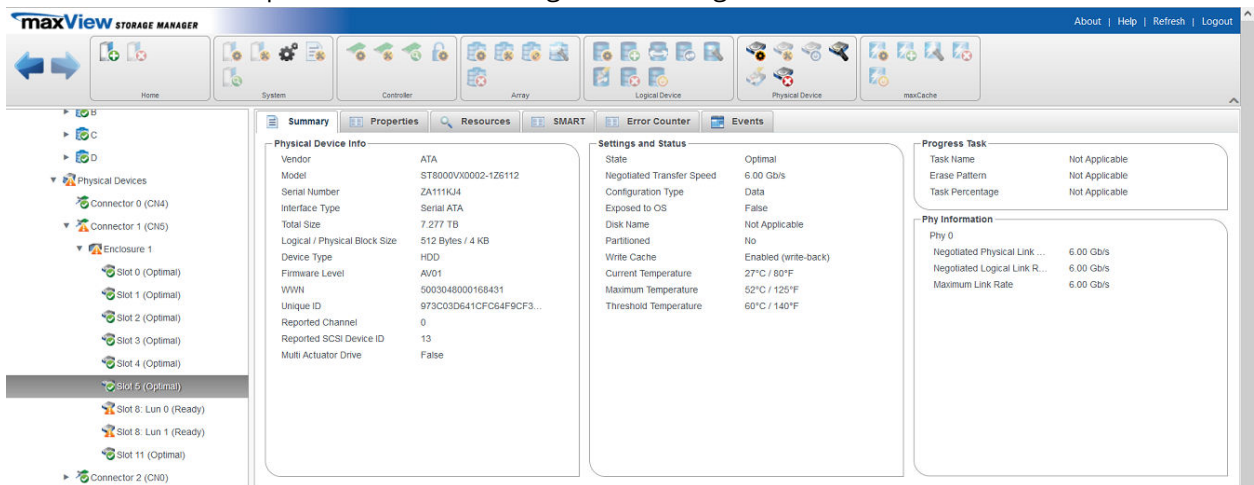
This operation removes the configured controller password.

Once the **"Clear Controller Password"** check box is checked, then provide the master key details.



### 10.3 Physical Device Self Encrypting Drives (SEDs) Properties

The controller level operation on SEDs changes the setting of all the selected SEDs.



Self Encrypting Drive (SED) related properties are added on the physical device summary page.

The following properties are available under the **Physical Device Info** panel:

- **Encryption Capability:** Displays whether the drive is SED or not.
- **SED Type:** Displays the type of SED (Opal or Enterprise).

The following properties are available under the **Settings and Status** panel:

- **SED Security Status:** Status of the SED.
- **SED Qualification Status:** Status of SED qualification.
- **Original Factory State (OFS):** Display whether the SED is **Original Factory State (OFS)** or not.
- **SED Ownership Status:** Describes the ownership status of the SED.
- **Foreign Key Identifier:** Foreign Key Identifier is the master key identifier of the previous controller.
- **Foreign Reset Key Identifier:** Foreign Reset Key Identifier is the old master key identifier of the controller before a master key change on which the SED drive was removed from the system when the drive was undergoing or was queued for a master key change.

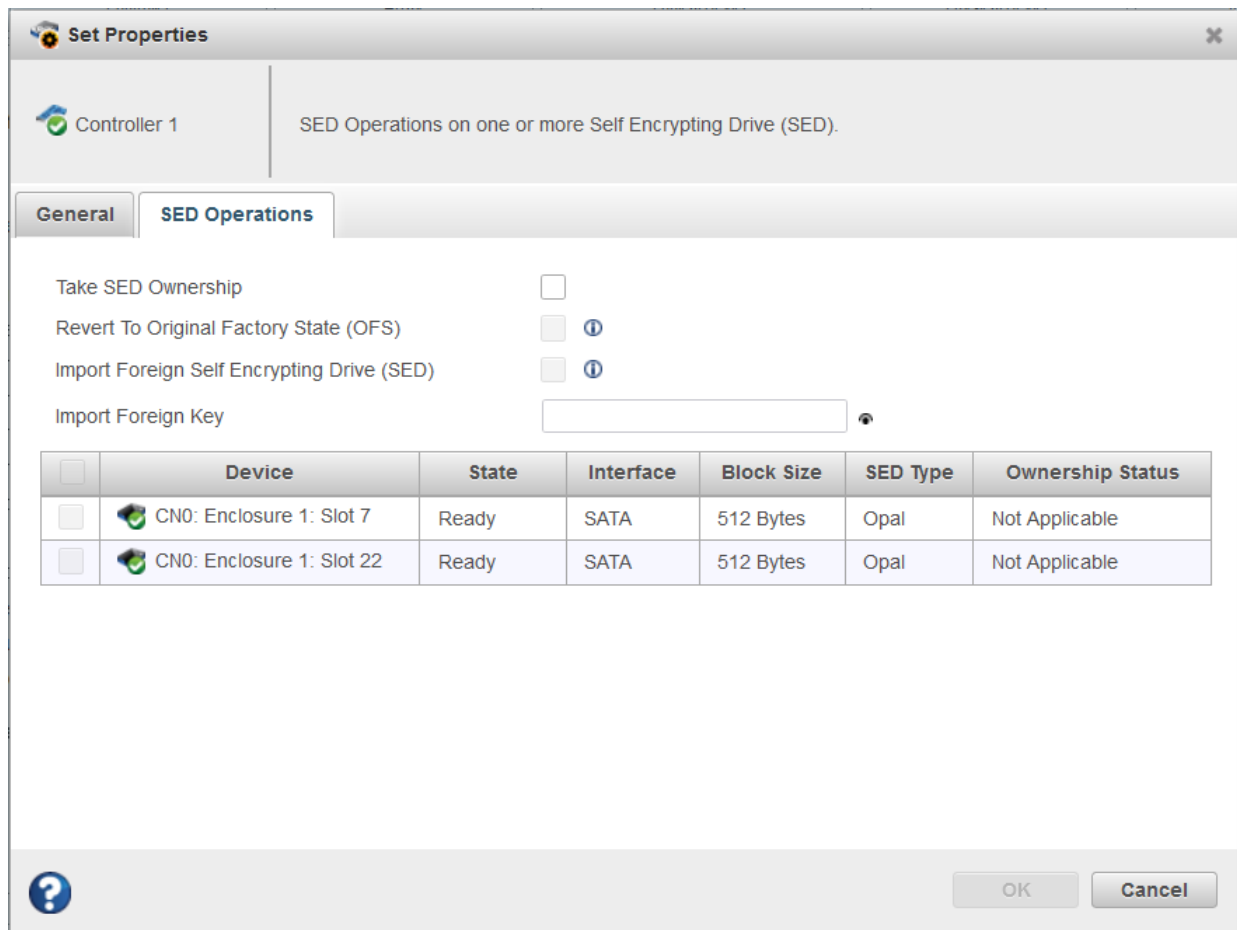
## 10.4 Controller Level Operation on Self Encrypting Drives (SEDs)

To display the SED operations:

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



The **Set Properties** window opens.



3. Click the **SED Operations** tab and perform the following actions:

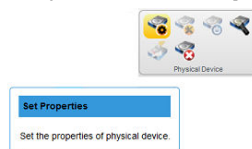
- a. **Take SED Ownership:** This option takes the ownership of all the SEDs. Once the check box is selected, the table gets updated with the list of valid SEDs, which are in OFS. Select the SEDs to take ownership. If all SEDs are not in OFS then, **Take SED Ownership** check box is disabled. After having the ownership, all the selected SEDs have a property called Ownership Status as **MCHP Owned** and **Original Factory State (OFS)** is set as False. When the controller's SED Encryption status is *"Waiting on Controller Password"*, the **Take SED Ownership** check box is disabled until controller password is provided.
- b. **Revert To Original Factory State (OFS):** This option deletes all the user's data stored in the drive and resets to its factory state. At the controller level, Revert to OFS operation is only performed on the MCHP owned SEDs and the Physical Security ID (PSID) is not required for MCHP owned SEDs. Sometimes ownership status is **"MCHP Owned, Foreign"**, in this case, Revert to Original Factory State (OFS) operation is not allowed on the respective SED. When the controller's SED Encryption status is *"Waiting on Controller Password"*, the **Revert To Original Factory State (OFS)** check box is disabled until controller password is provided. When controller's SED Encryption status is *"Waiting on Master Key"*, the **Revert To Original Factory State (OFS)** check box is disabled until system is rebooted.
- c. **Import Foreign Self Encrypting Drive (SED):** An SED is said to be Foreign, when the SED is owned by MCHP and have different master key compared to its connected controller. This happens under the following circumstances, when:
  - The SED has migrated from a different controller.
  - The SED has been previously owned by the connected controller but was removed for a period. At that time, the connected controller's master key has changed.

This operation converts the Foreign SED to MCHP Owned SED. Only Foreign SED whose Foreign Key matches with that SED will be properly imported. For others, this operation should be repeated with different Foreign Key until all the SEDs are imported. Import Foreign SED has one more text field as **"Import Foreign Reset Key"**. It is displayed only when this key is required based on the **"Foreign Reset Key Identifier"** property. If this property value is other than *"Not Applicable"*, this option gets displayed.

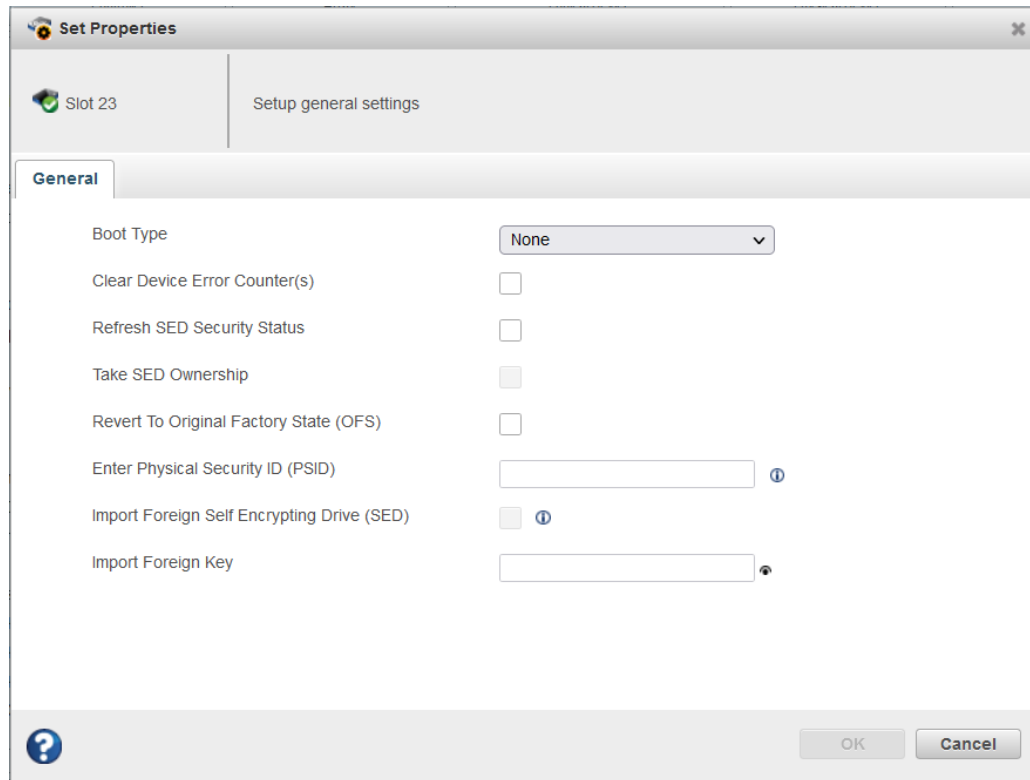
## 10.5 Physical Device Level Operation on Self Encrypting Drives (SEDs)

To perform the physical device level operations on Self Encrypting Drives (SEDs):

1. In the Enterprise view, select the Physical Device node.
2. On the ribbon, in the Physical Device group, click **Set Properties**.



The **Set Properties** window opens.



3. Perform one of the following options:

- **Take SED Ownership:** This option takes the ownership of the selected SEDs by selecting the **Take SED Ownership** check box. **Take SED Ownership** check box is disabled when the SED is not in **Original Factory State (OFS)**.  
After getting the ownership, the selected SED's Ownership status changes to "MCHP Owned" and OFS will be set as False. When the controller's SED Encryption status is "Waiting on Controller Password", the **Take SED Ownership** check box gets disabled until the controller password is provided.
- **Revert To Original Factory State (OFS):** This option deletes all the user's data stored in the drive and resets to its factory state. On physical device level, Revert to Original Factory State (OFS) operation can be performed on all SED with Physical Security ID (PSID). If the ownership status is MCHP Owned, then Physical Security ID (PSID) is not a mandatory field. Sometimes ownership status is "**MCHP Owned, Foreign**", in this case, Revert to Original Factory State (OFS) operation is not allowed on the respective SED using PSID. When the controller's SED Encryption status is "Waiting on Controller Password", the **Revert To Original Factory State (OFS)** check box gets disabled until controller password is provided. When controller's SED Encryption status is "Waiting on Mater Key", the **Revert To Original Factory State (OFS)** checkbox gets disabled until the system is rebooted.
- **Import Foreign Self Encrypting Drive (SED):** An SED is said to be Foreign, when the SED is owned by MCHP and have a different master key compared to its connected controller. This happens under the following circumstances, when:
  - The SED has migrated from a different controller.
  - The SED has been previously owned by the connected controller but was removed for a period. At that time, the connected controller's master key has changed.

This operation converts the Foreign SED to MCHP Owned SED. Only Foreign SED whose Foreign Key matches with that SED will be properly imported. Import Foreign SED has one more text field as "**Import Foreign Reset Key**". It gets displayed only when this key is

required based on the “**Foreign Reset Key Identifier**” property. If this property value is other than “Not Applicable”, this option gets displayed.

## 10.6 Creating Logical Device

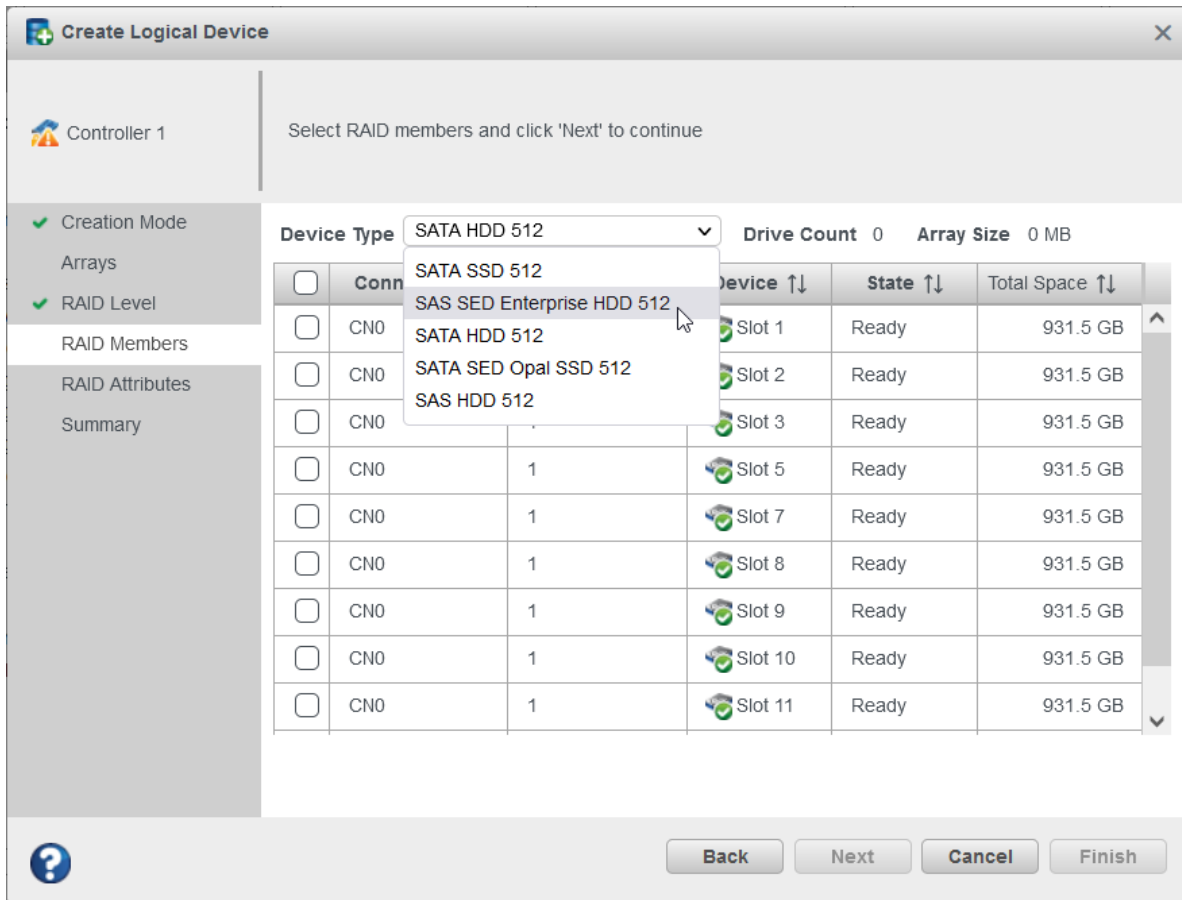
This section explains how to create a logical device using SED drives. Mixing of drives to create the logical device is not allowed, for example; mixing of block sizes (512 Bytes and 4K), interface types (SATA, SAS, NVMe), drive types (HDD and SSD), and SED types (Opal and Enterprise). To create a logical device, the SED drive must be either in OFS or the ownership status should be **MCHP Owned**.

Additional device types with the following combination are listed along with the other device type in the **Create Logical Device** window only when the SED based encryption is configured/enabled.

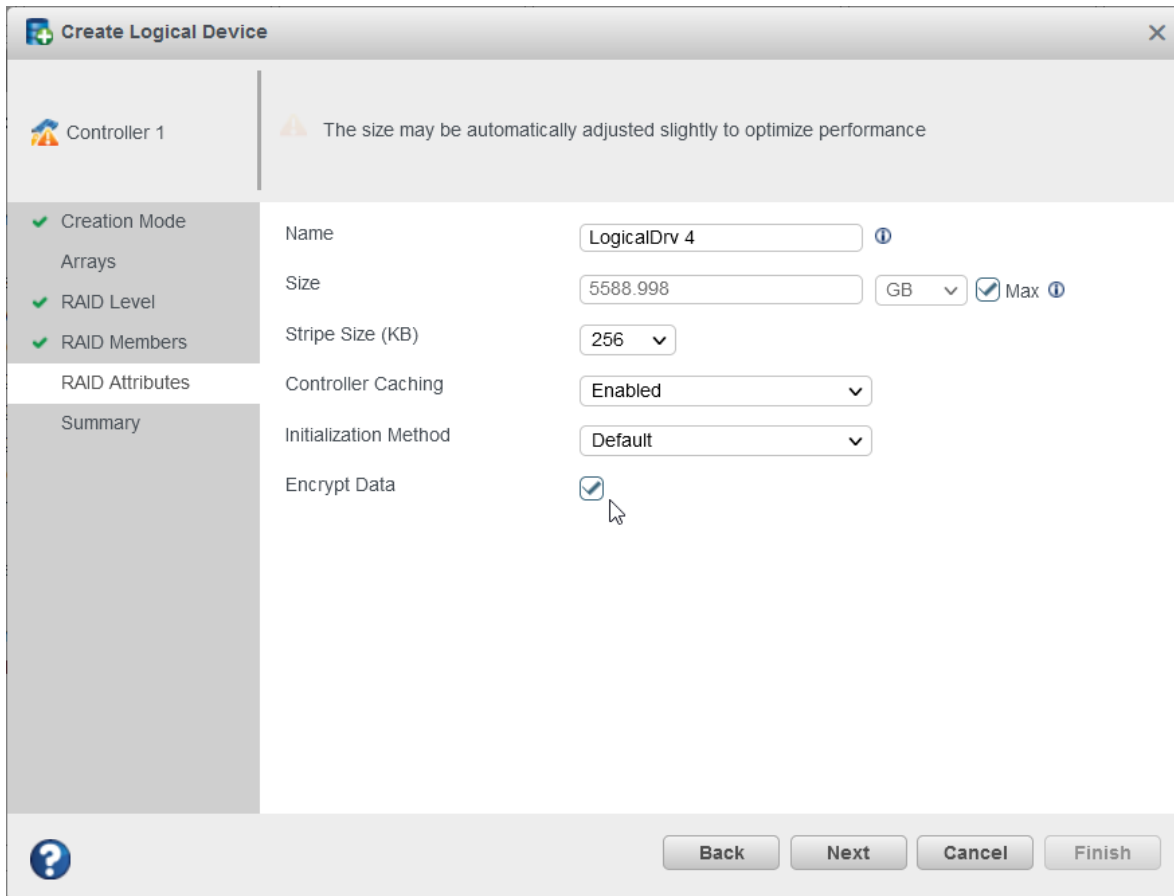
- SATA SED Opal HDD 512
- SATA SED Enterprise HDD 512
- SATA SED Opal SSD 512
- SATA SED Enterprise SSD 512
- SAS SED Opal HDD 512
- SAS SED Enterprise HDD 512
- SAS SED Opal SSD 512
- SAS SED Enterprise SSD 512
- SATA SED Opal HDD 4K
- SATA SED Enterprise HDD 4K
- SATA SED Opal SSD 4K
- SATA SED Enterprise SSD 4K
- SAS SED Opal HDD 4K
- SAS SED Enterprise HDD 4K
- SAS SED Opal SSD 4K
- SAS SED Enterprise SSD 4K

**Note:** The device types are listed only if the possible drive combination exists.





Once the SED based encryption is configured, on the **RAID Members** tab, the **Device Type** dropdown will have the extra device type(s). Select the SED drives and click **Next**.



On the RAID Attributes tab, select the **Encrypt Data** check box to encrypt the array and logical device; else it will create the plaintext logical device.

## 10.7 Assigning Spares at the Array Level

Dedicated and auto-replace spare for SED logical device can be assigned at the array level.

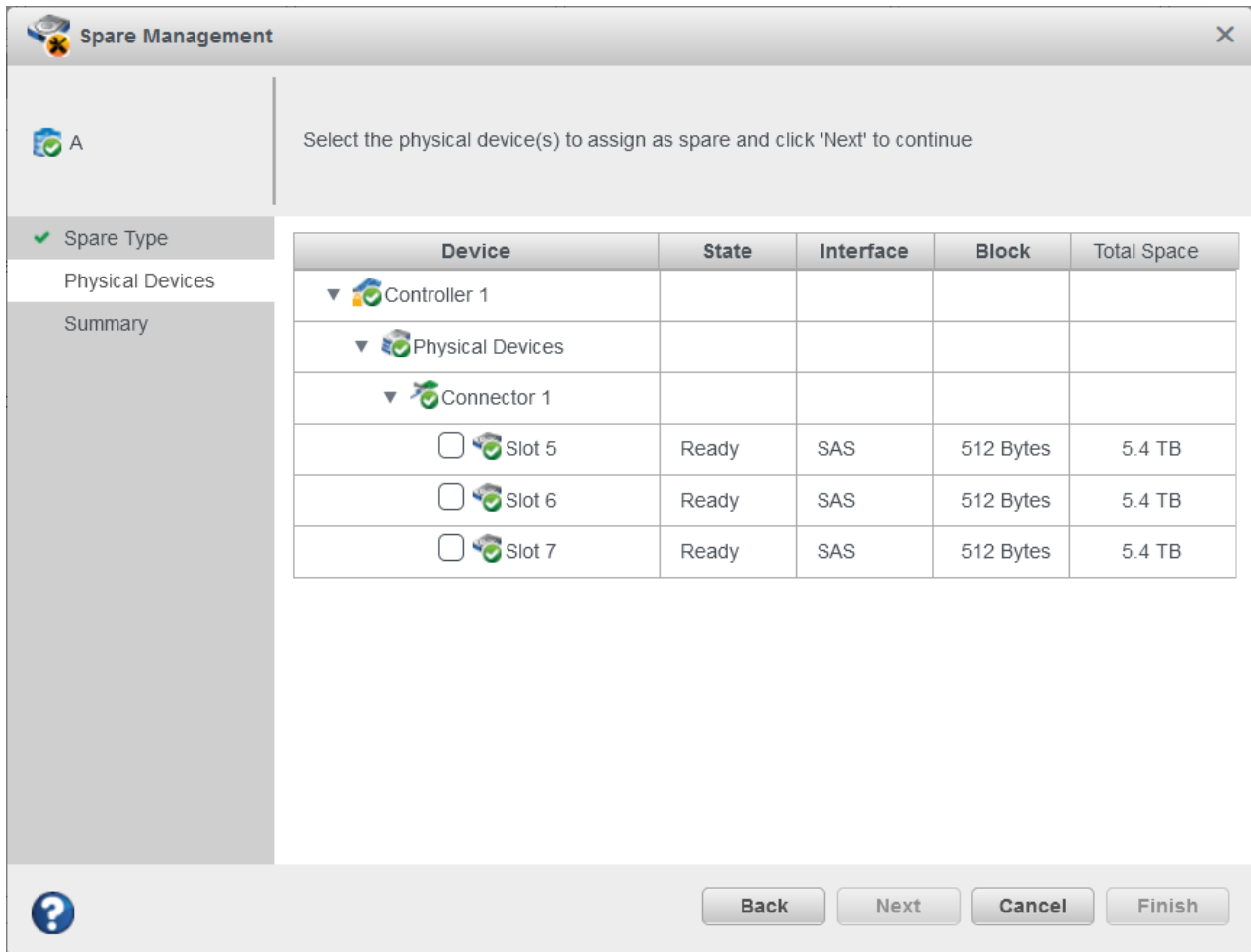
**Assigning a dedicated/auto-replace spare for an encrypted array:** Only the self-encrypting drive of the same SED type is allowed to assign a spare, for example; if an array is created with SED type enterprise, then only the enterprise drive is allowed to assign a spare.

Once the encrypted array is assigned with a dedicated spare, the dedicated spare drive can only protect encrypted arrays, which is created using same SED type drives. Similarly, once the plaintext/unsecured array is assigned with a dedicated spare, that dedicated spare drive can only protect plaintext/unsecured arrays which is created using same SED type drives.

**Assigning a dedicated spare for a plaintext/unsecured array (SED drives):** Only the self-encrypting drive of the same SED type is allowed to assign a spare. For example, if an array is created with SED type Enterprise, then only the enterprise drive is allowed to assign a spare. Later, the array cannot be converted to an encrypted data as a dedicated spare (Sharable Spare) is assigned.

**Assigning an auto-replace spare for a plaintext/unsecured array (SED drives):** Only the self-encrypting drive of same SED type is allowed to assign a spare. For example, if an array is created with SED type Enterprise, then only the enterprise drive is allowed to assign a spare. And once auto-replace spare is assigned, it can convert the plaintext/unsecured data to the encrypted data.

While selecting the array that is created using self-encrypting drive, the **Spare Management** window only lists the valid self-encrypting drive for the spare assignment.

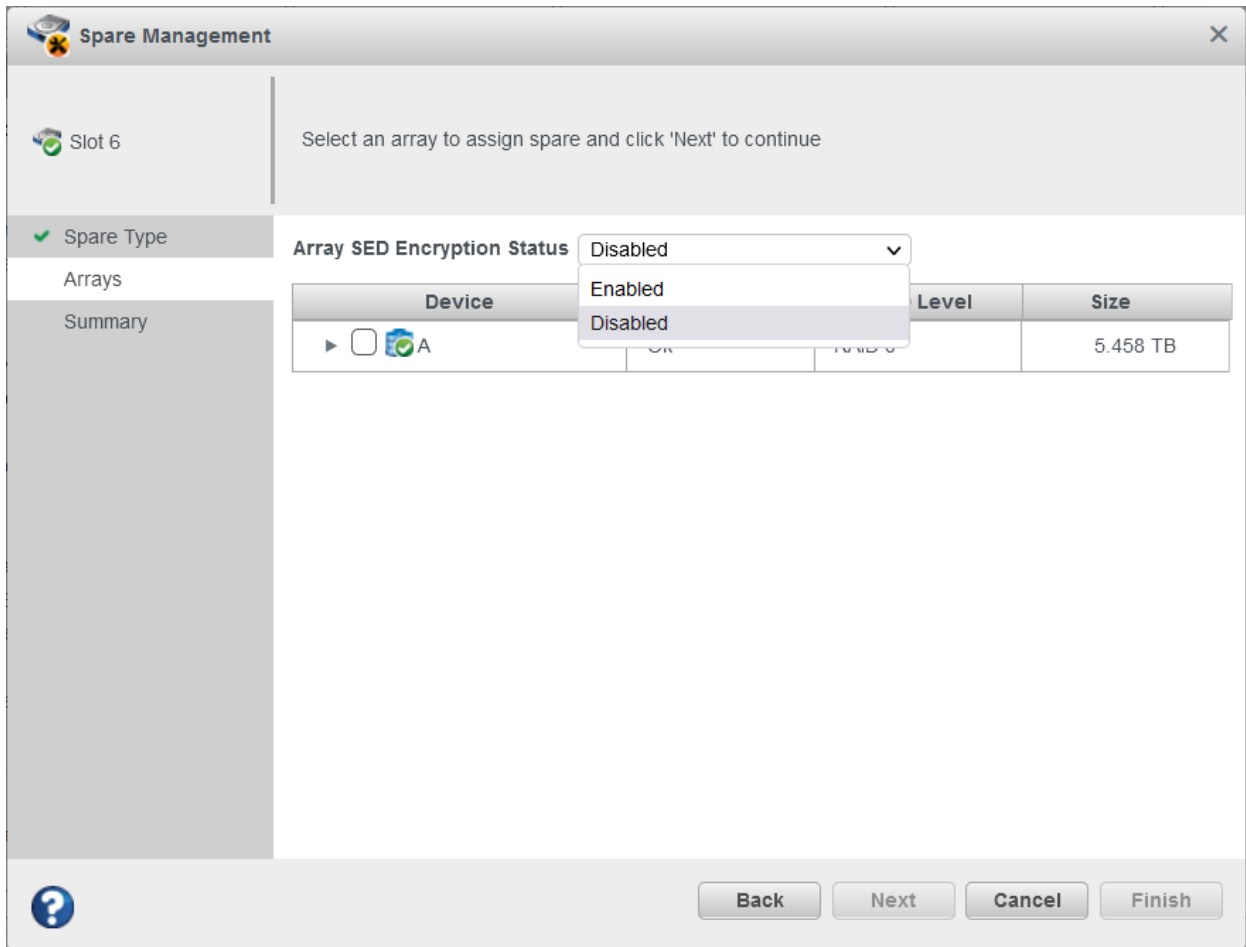


## 10.8 Assigning Spares at the Physical Device Level

A spare can be assigned from the physical device level. On selecting the SED drives, the Spare Management window lists the valid array that is created using self-encrypting drive of the same SED type.

If the controller has a combination of encrypted and plaintext/unsecured array, the **Spare Management > Arrays** tab displays the **Array SED Encryption Status** dropdown option. If enabled, only the encrypted array is listed in the table. If disabled, the plaintext/unsecured array is listed in the table.

If the controller has only encrypted array or plaintext/unsecured array then the **Array SED Encryption Status** option is not displayed.



## 10.9 Creating maxCache

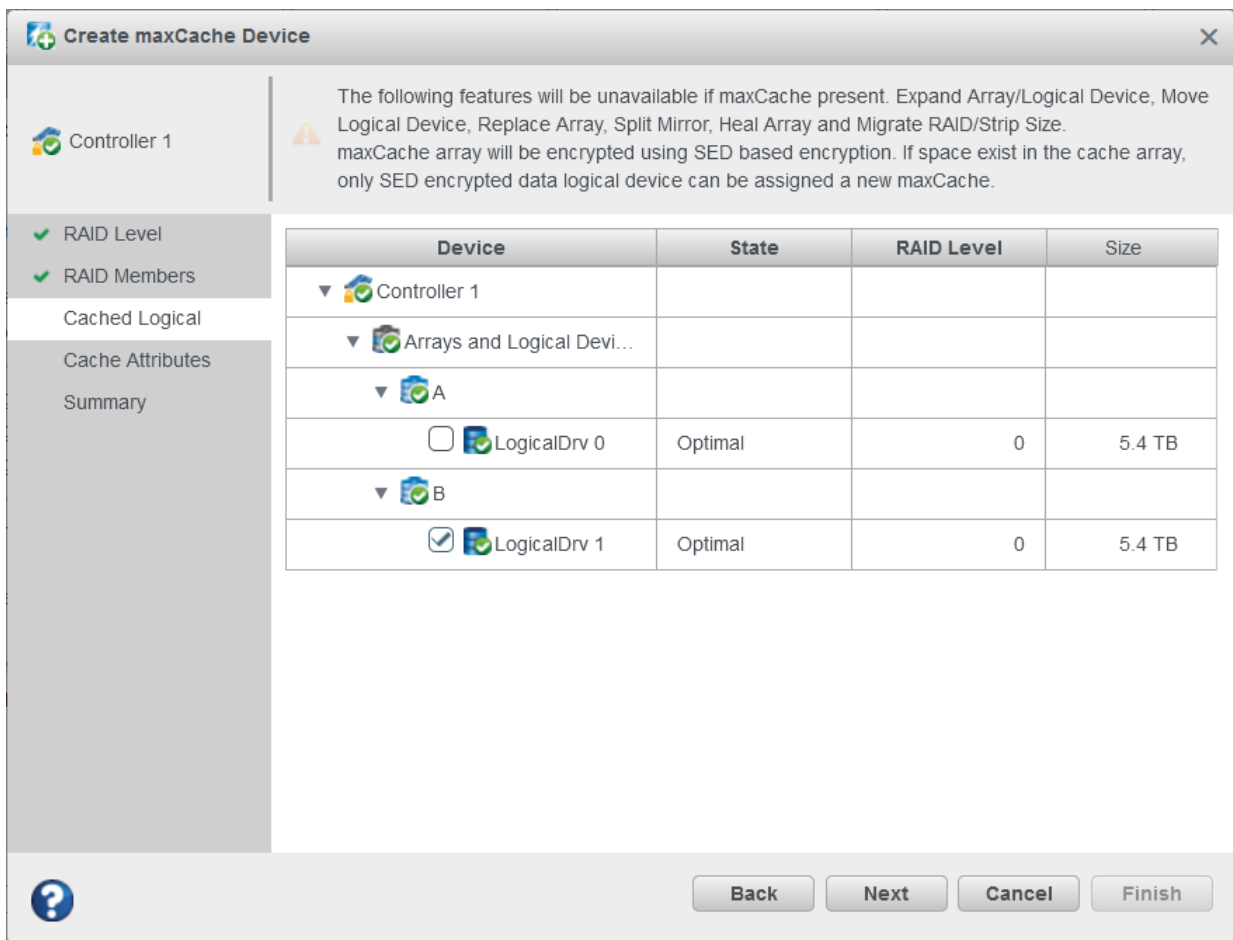
This section explains how to create a maxCache logical device using SED drives. Mixing of drives to create the maxCache logical device is not allowed; for example, mixing block size (512 Bytes and 4K), interface type (SATA, SAS, NVMe), and SED type (Opal and Enterprise). To create a maxCache logical device, the SED drive must be either in OFS or the ownership status must be **MCHP Owned**.

Additional device types with the following combination are listed along with the other device type in the **Create Logical Device** window only when the SED based encryption is configured/enabled.

- SATA SED Opal SSD 512
- SATA SED Enterprise SSD 512
- SAS SED Opal SSD 512
- SAS SED Enterprise SSD 512
- SATA SED Opal SSD 4K
- SATA SED Enterprise SSD 4K
- SAS SED Opal SSD 4K
- SAS SED Enterprise SSD 4K

When no maxCache logical device is created, the following combination of drives are listed.





1. When the self-encrypting drives (SEDs) are selected, the data logical device listed in the **Cached Logical** page is either an encrypted or plaintext/unsecured data logical device.
2. When the non-self-encrypting drives (SEDs) are selected, the data logical device listed in the **Cached Logical** page is either a non-SED data logical device or plaintext/unsecured data logical device.
3. If an encrypted data logical device is selected, then maxCache logical device is also encrypted. The new encrypted data logical device can be assigned a new maxCache (**Cached Logical** page lists only new encrypted data logical device).
4. If a plaintext/unsecured data logical device is selected, then maxCache logical device is also a plaintext/unsecured. The new plaintext/unsecured data logical device and non-SED logical device can be assigned with a new maxCache (**Cached Logical** page lists only new plaintext/unsecured data logical device and non-SED logical device).
5. If a non-SED data logical device is selected, then maxCache logical device is also a plaintext/unsecured using self-encrypting drive (SED) or non-SED drives. The new plaintext/unsecured data logical device and a non-SED logical device can be assigned with a new maxCache (**Cached Logical** page lists only new plaintext/unsecured data logical device and non-SED logical device).  
**Note:** If an encrypted maxCache logical device is created, then only a new encrypted data logical device can be assigned with a new maxCache logical device.
6. If a plaintext/unsecured maxCache logical is created, then only a new plaintext/unsecured data logical device and new non-SED logical device can be assigned with a new maxCache logical device.

7. Once the plaintext maxCache logical device is assigned to a plaintext data logical device, then at Array level the **Convert Plaintext Data to Encrypted Data** option gets disabled. It displays the following message:  
*"Cannot convert plaintext data to encrypt data as the array has one or more logical device(s) associated with maxCache."*

## 10.10 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, a minimum of three drives are required for RAID 5.

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

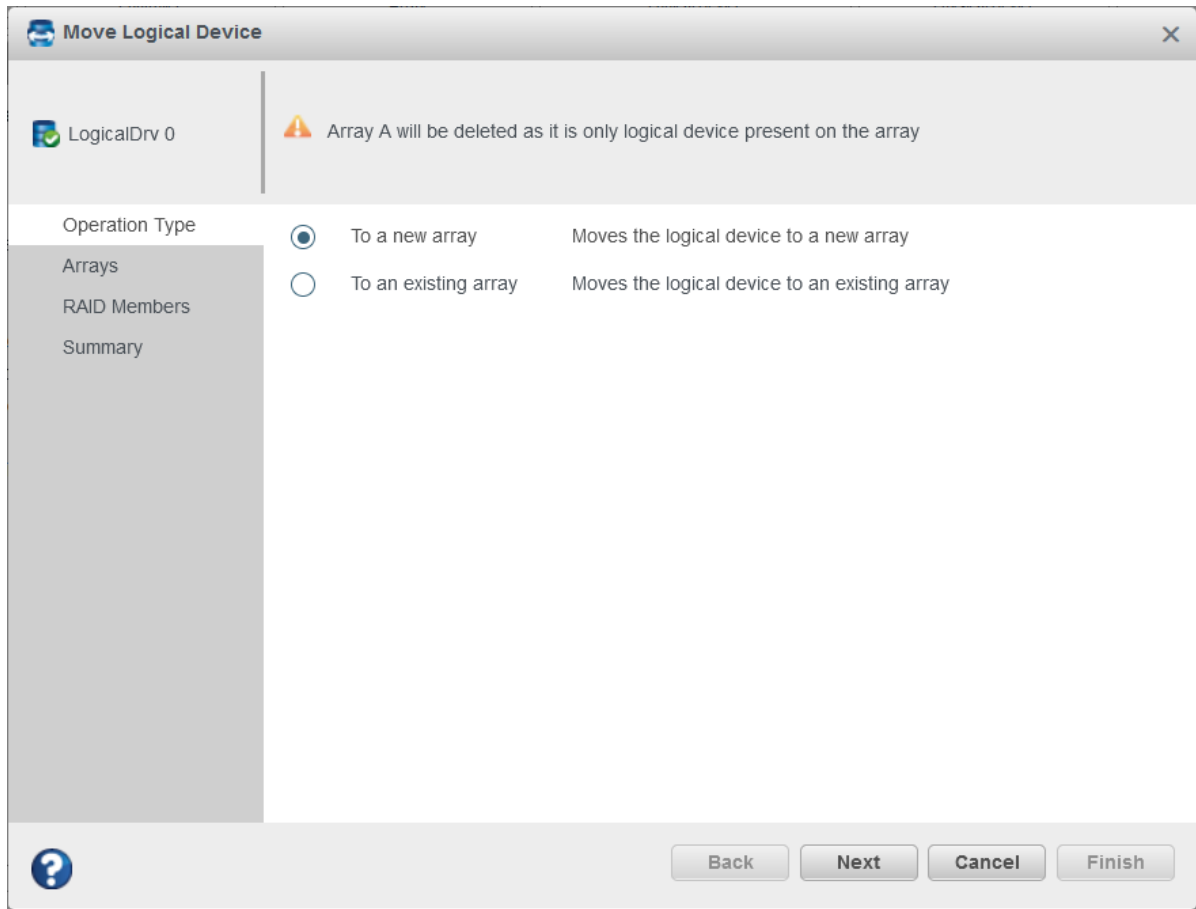
Perform the following steps to move a logical drive to a new array:

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



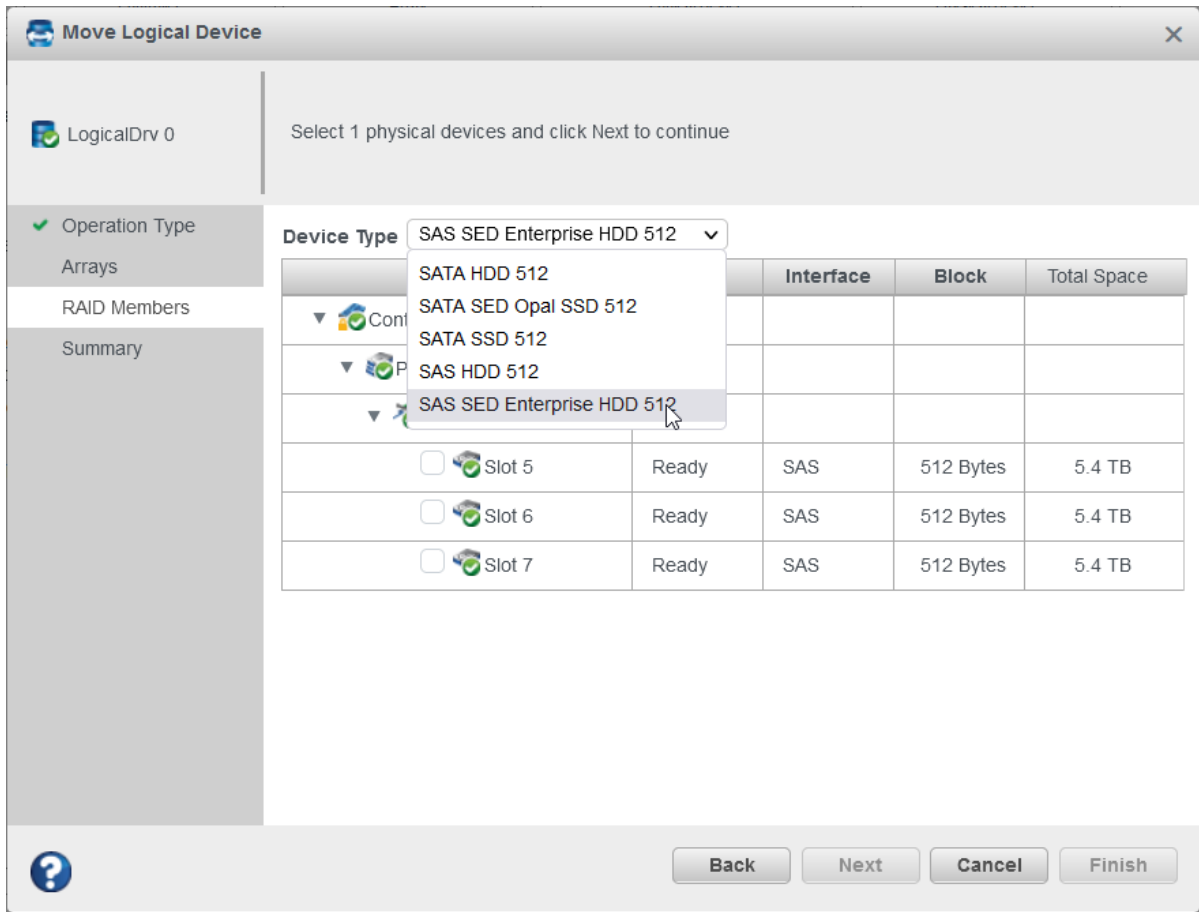
The **Move Logical Device** window opens.

3. Select Operation Type as **To a new array** and click **Next**.



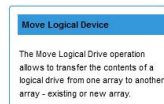
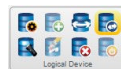
4. On the **RAID Members** tab, select the **Device Type** option. Based on the selection, the drives are listed. For details on Move Logical device and SED support operations on moving a logical device, see [7.5. Moving a Logical Drive](#) and [5.5.2. Moving a Logical Drive](#) respectively.





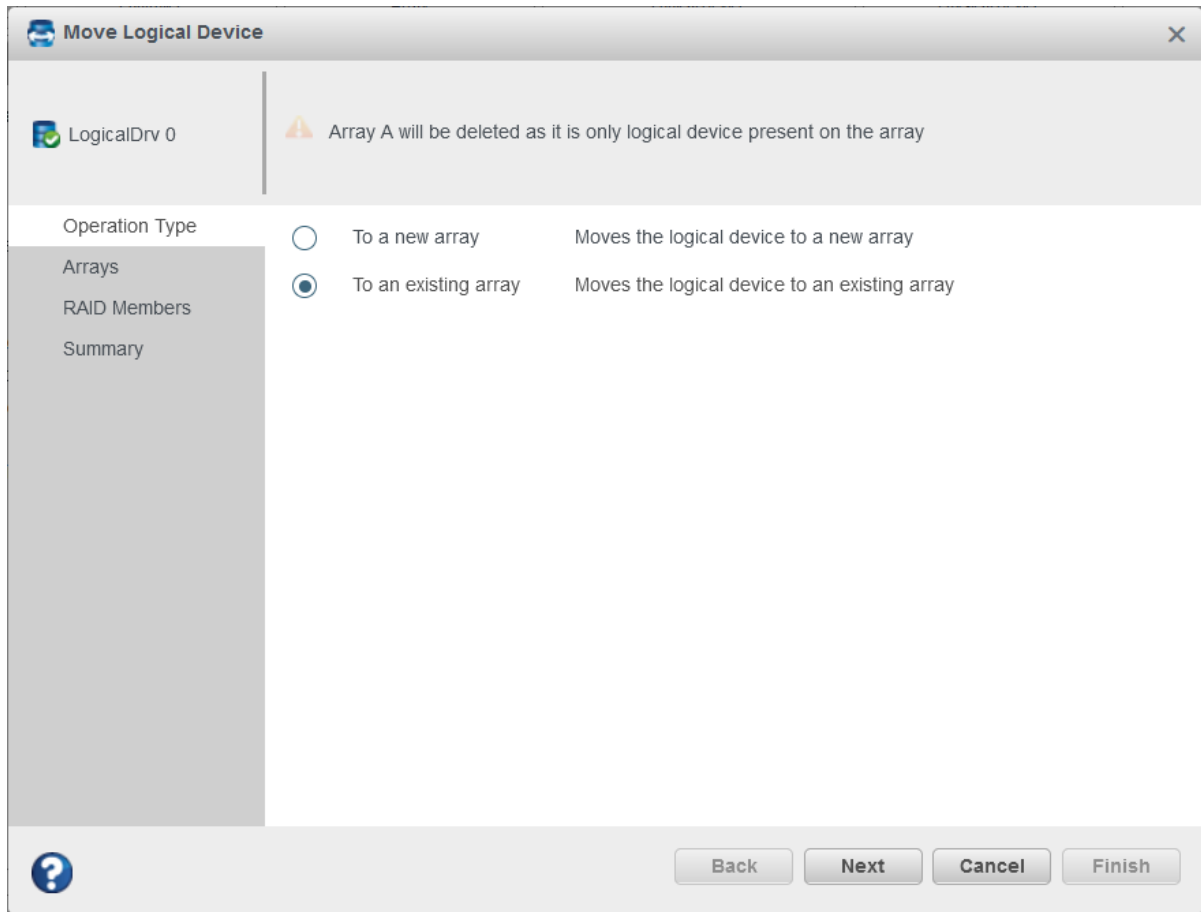
Perform the following steps to move a logical drive to an existing array:

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

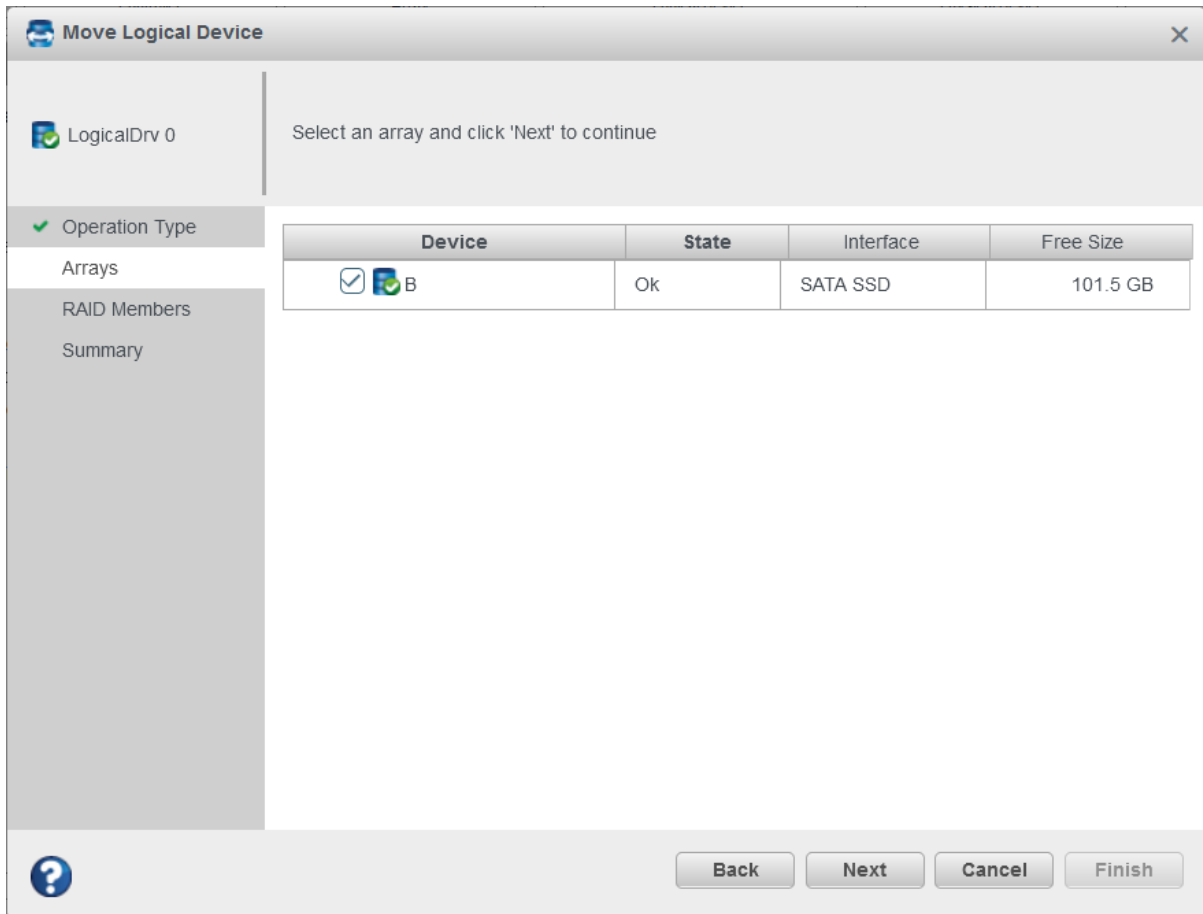


The **Move Logical Device** window opens.

3. Select Operation Type as **To an existing array** and click **Next**.



4. On the **Arrays** tab, select an array to move the logical drive. For details on Move Logical device and SED support operations on moving a logical device, see [7.5. Moving a Logical Drive](#) and [5.5.2. Moving a Logical Drive](#) respectively.



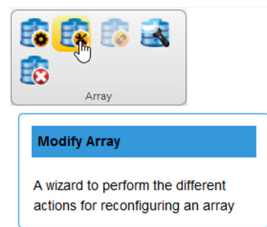
## 10.11 Moving an Array

You can move an array by replacing its physical drives with the same type of drives. For example, you can replace the SED Enterprise drives in the array with the other SAS SED Enterprise drives. You can also change the drive type by replacing its physical drives with the different type of drives. For example, replacing SAS SED Enterprise drives with SATA SED Enterprise drives.

The replacement drives must be in Ready state and the SED Ownership status should be either in Original Factory State (OFS) or MCHP Owned.

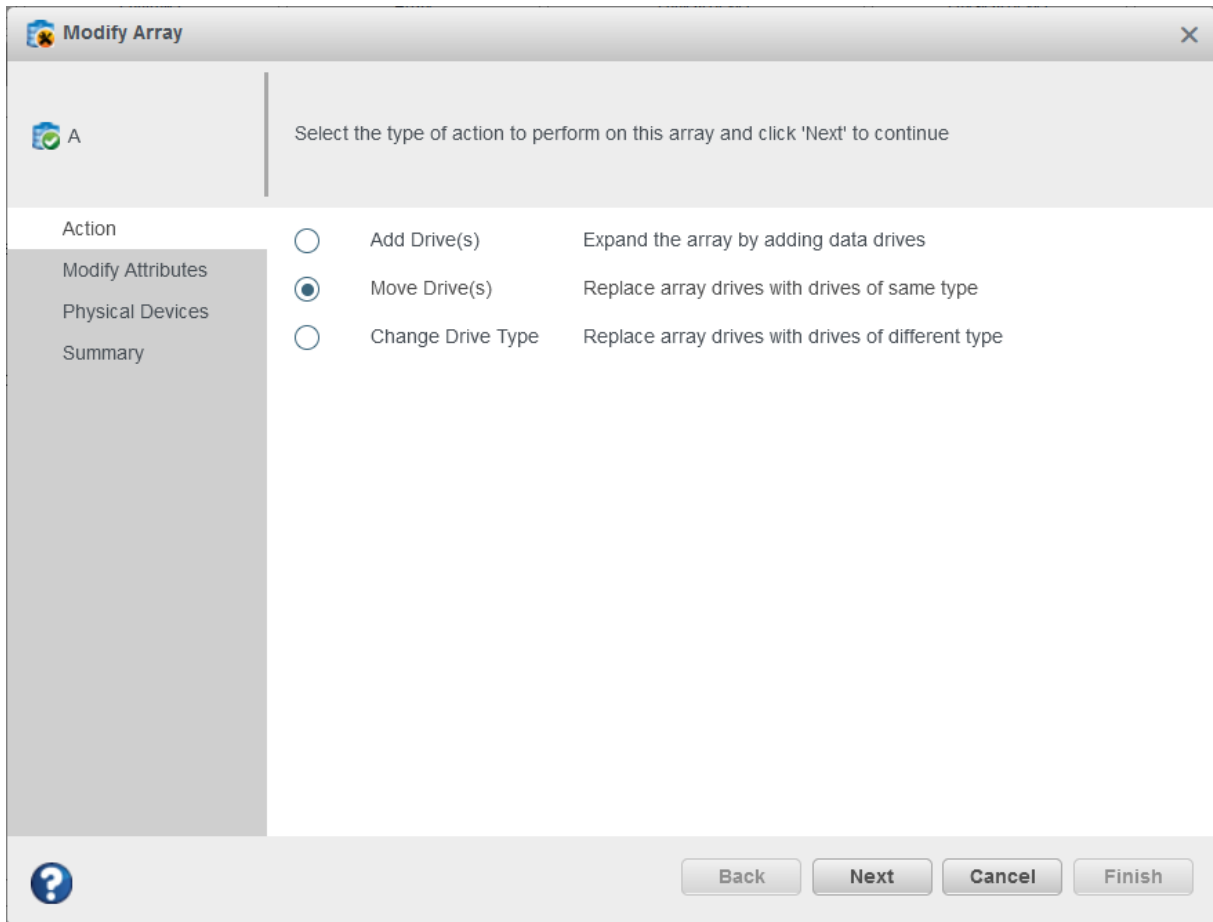
Perform the following steps to move an array:

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



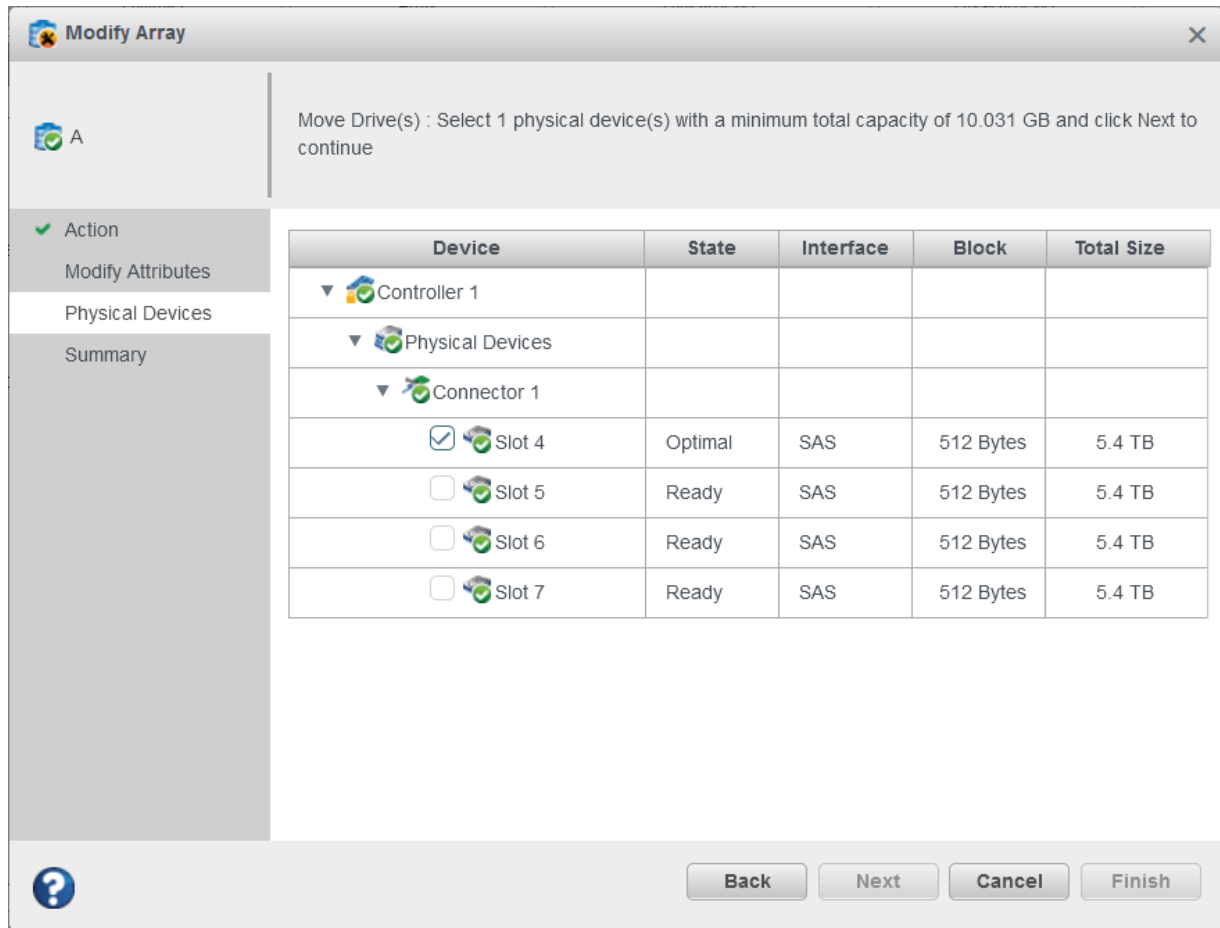
The **Modify Array** window opens.

3. Select **Move Drive(s)** and click **Next**.



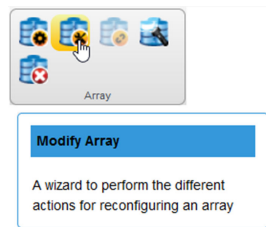
The Move Drive(s) option lists only the drives with same interface type, block size, and SED type; for example, if an Array is created using the **SATA SED Enterprise HDD 512**, then on the **Physical Devices** tab only **SATA SED Enterprise HDD 512** is available. All the valid drives are listed along with the array's member drives. You can either replace all the drives or you can replace the specific drive.

For details on Moving an Array and SED support, see [7.6. Moving an Array](#) and [5.6.2. Modify Array](#) respectively.



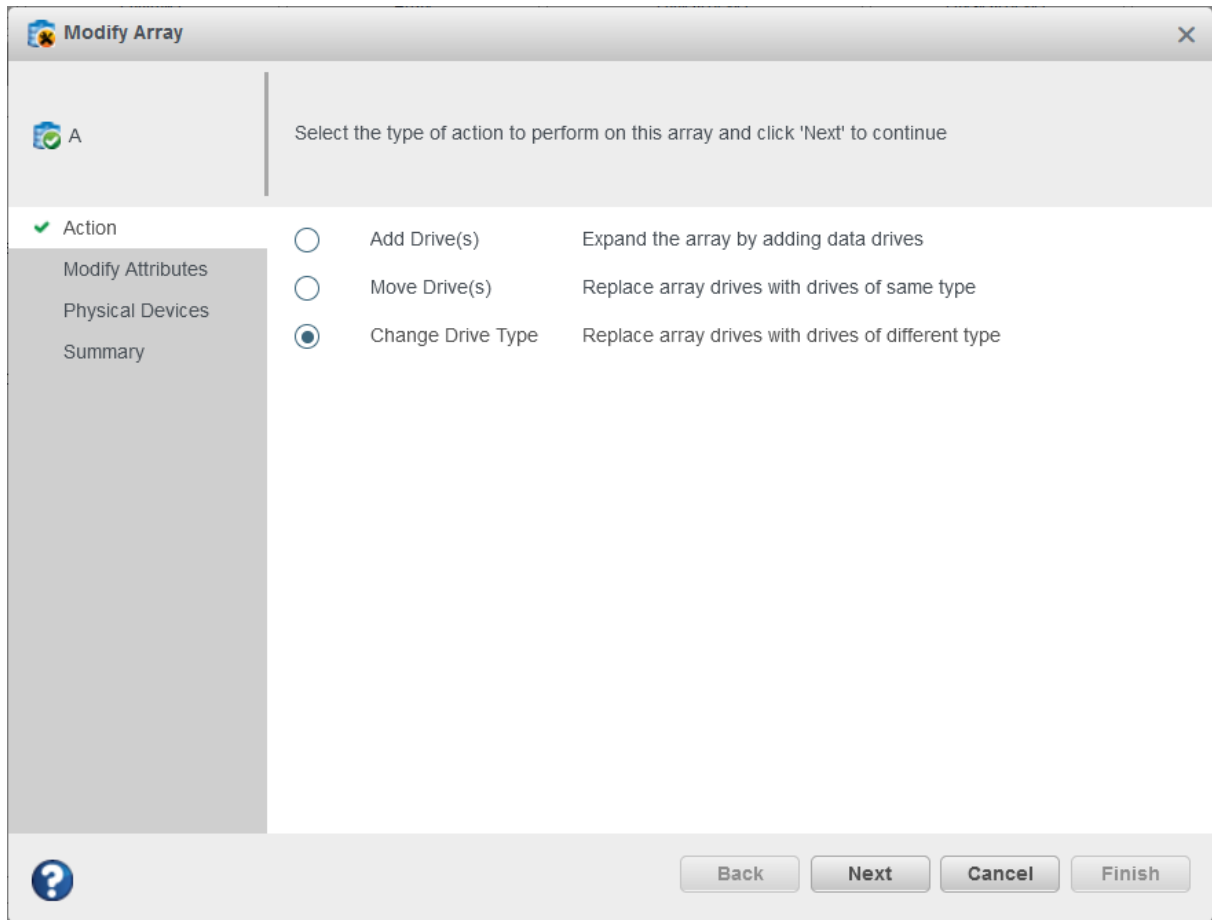
Perform the following steps to change the drive type of an array:

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



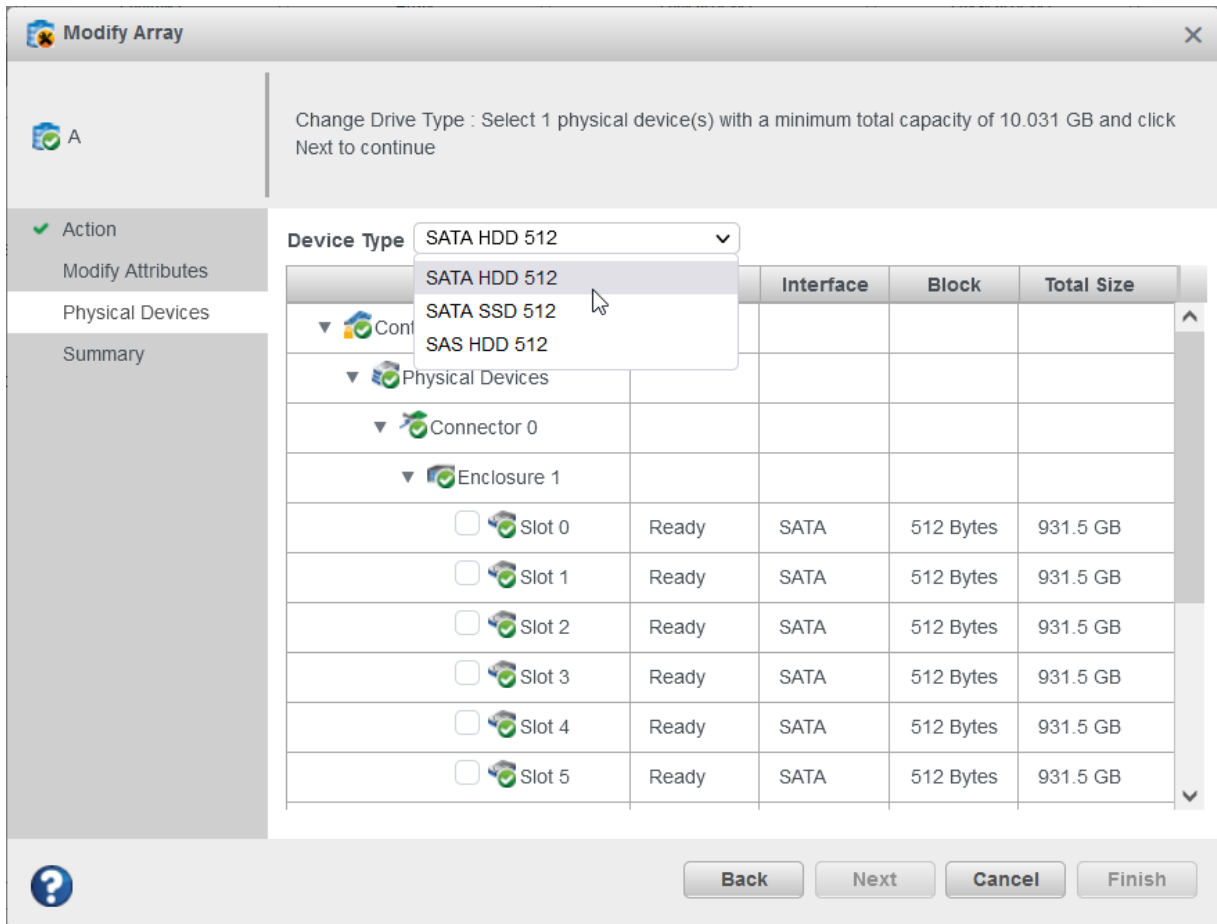
The **Modify Array** window appears.

3. Select **Change Drive Type** and click **Next**.



The Change Drive Type option lists only the drives with different interface type, block size, or SED type. For example, if an array is created using the **SATA SED Enterprise HDD 512**, then on the **Physical Devices** tab only **SATA SED Enterprise HDD 512** is available.

For details on Moving an Array and SED support, see [7.6. Moving an Array](#) and [5.6.2. Modify Array](#) respectively.



## 10.12 Modifying an Array

maxView Storage Manager allows you to modify an array by choosing any of the following options:

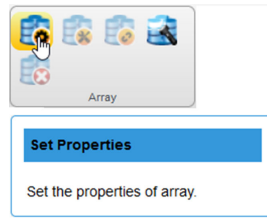
- **Add Drives to an Array:** You can expand the array by adding the data drives. This option lists only the valid drives for addition. For example, create an array using **SATA SED Enterprise HDD 512**, then only the valid and available **SATA SED Enterprise HDD 512** drives are listed. Otherwise, this option does not display.
- **Remove Drives from an Array:** You can shrink the array by removing the data drives. This only lists the array's member drives.  
For details on Modifying an Array and SED support, see [7.7. Modifying an Array](#) and [5.6.2. Modify Array](#) respectively.
- **Healing an Array:** You can use the Heal Array operation to replace the failed physical drives in an array with the healthy physical drives. For example, create an Array using **SATA SED Enterprise HDD 512**, then only the valid and available **SATA SED Enterprise HDD 512** drives are listed. Otherwise, this option does not display. For details on Healing an Array and SED support, see [15.3.6. Healing an Array](#) and [5.6.2. Modify Array](#) respectively.

## 10.13 Importing Foreign Array

When an SED encrypted logical drive is moved from one controller to another, the master key of the controller is required to make the logical device online. Use the **Foreign Key Identifier** option to import the master key, so that the logical drive data can be accessed and managed on the new controller.

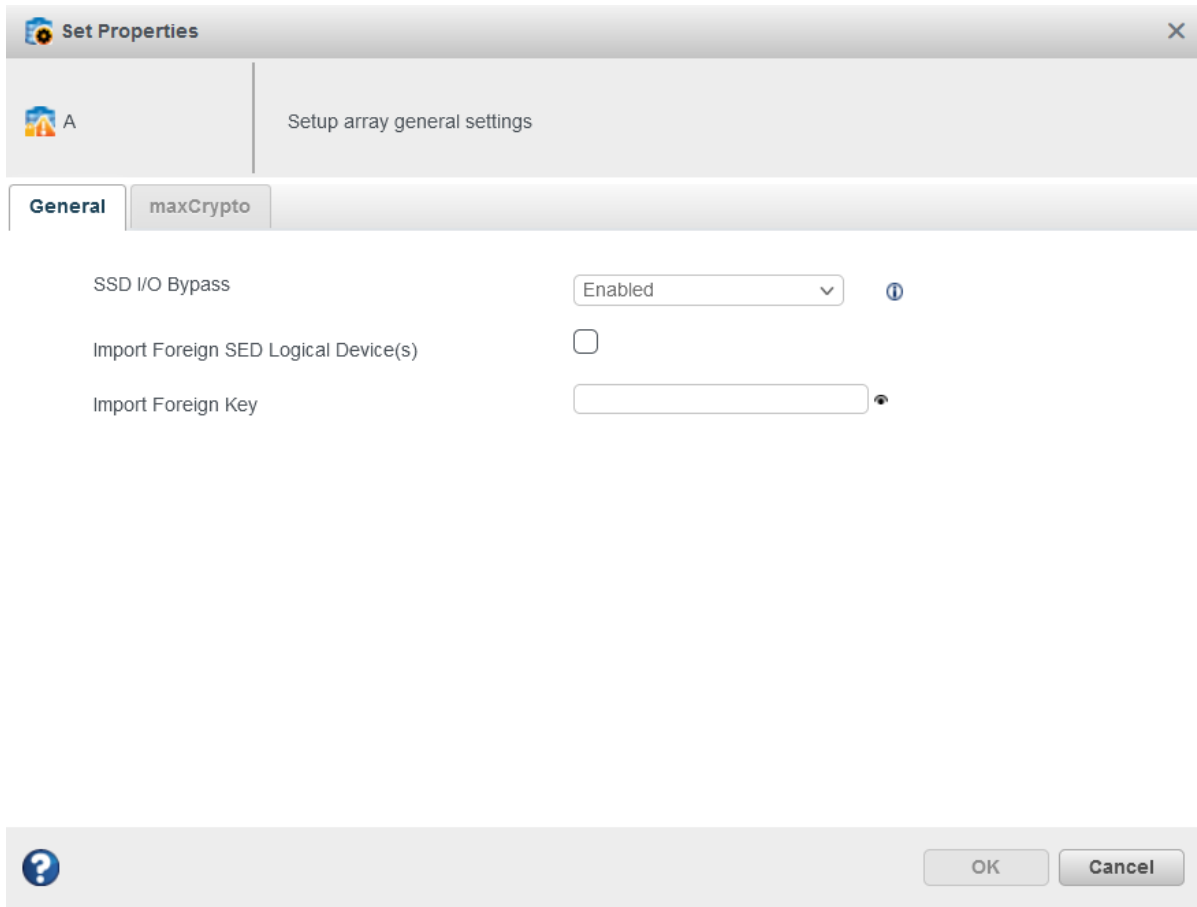
To import a foreign array:

1. In the Enterprise View, select an array with “**Has Logical Drive with Foreign SED**” status.
2. On the ribbon, in the Array group, click **Set Properties**.



The Set Properties window appears.

3. On the **General** tab, click **Import Foreign SED Logical Device(s)** check box. Specify the **Foreign Key Identifier** value. The **Foreign Key Identifier** is the master key of the controller from which the array/logical device is imported to the current controller.



4. Click **OK**.



## 11. Working with Security Protocol and Data Model (SPDM)

SPDM defines messages, data objects, and sequences for performing message exchanges between devices over a variety of transport and physical media. It coordinates the message exchanges between the Baseboard Management Controllers (BMC) and end-point devices over a Management Component Transport Protocol (MCTP).

SPDM Message exchanges enable the requester to:

- Discover and negotiate the security capabilities of a responder
- Authenticate the identity of a responder
- Retrieve the measurements of a responder
- Securely establish cryptographic session keys to construct a secure communication channel for the transmission or reception of application data

maxView provides the following operations:

- Get the certificate chain from the specified slot [0-7]
- Import the certificate chain to the specified slot [0-7]
- Invalidate the certificate chain on the specified slot [0-7]

### 11.1 Security Protocol and Data Model (SPDM) Properties

The following figure shows the properties of Security Protocol and Data Model (SPDM) information and settings.

Click on Controller node in the Enterprise tree view, then click on **Security** tab to view the properties of Security Protocol and Data Model (SPDM).

The screenshot shows the maxView Security tab with three panels:

- Security Info**:
  - maxCrypto Info**: maxCrypto/SSD I/O Bypass Mi... Supported, maxCrypto/maxCache Mixing Supported
  - SED Encryption Info**: Encryption Disabled, Key Mode None, Status Not Applicable, Operation in Progress Not Applicable, Master Key Identifier Not Applicable, Controller Password Not Configured, Controller Password Unlock A... Not Applicable, Controller Password Count D... Not Applicable
  - Security Protocol and Data Model (SPDM) Info**: Version 0x00, Endpoint ID 0x00, Authority Key ID 00:00:00:00:00:00:00:..., Crypto Timeout Exponent 20, Capabilities Available
- Settings and Status**:
  - maxCrypto Status Disabled
  - Allow New Plaintext Logical... Not Applicable
  - Key Management Mode Local
  - Master Key Configured
  - Firmware Locked for Update Unlocked
  - Local Key Cache Not Supported
  - Encrypted Logical Device ... 0
  - Encrypted Foreign Logical... 0
  - Encrypted Physical Device... 0
  - Security Protocol and Data Model (SPDM) Settings**: Slot 0 Valid and Sealed, Slot 1 Valid and Sealed, Slot 2 Valid and Sealed, Slot 3 Valid and Sealed, Slot 4 Valid and Sealed, Slot 5 Valid and Sealed, Slot 6 Available, Slot 7 Available
- Account Info**:
  - Login Status Not Logged In
  - Crypto Officer Password Configured
  - User Password Not Configured
  - Crypto Password Unlock Atte... 10
  - User Password Unlock Attemp... 10
  - Crypto Officer Password Rec... Not Configured

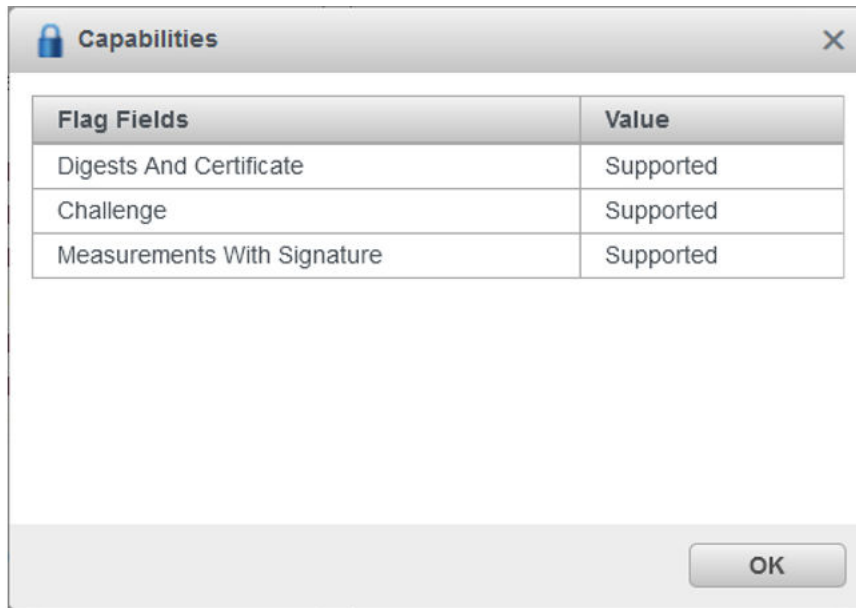
The **Security** tab contains the following three panels:

- Security Info
- Settings and Status
- Account Info

Security Protocol and Data Model (SPDM) properties are available in **Security Info** and **Settings and Status** panel.

The **Security Info** panel has **Security Protocol and Data Model (SPDM) Info** section that contains the following properties:

- **Version:** Current version of the SPDM.
- **Endpoint ID:** Endpoint ID of a peer device.
- **Authority Key ID:** It is a field in the Security Protocol and Data Model (SPDM) specification that identifies the public key of the authority that issued a certificate.
- **Cryptographic Timeout Exponent:** It is reported in microseconds in the capabilities message. The equation for cryptographic timeout (CT) is  $2^{CT}$  microseconds.
- **Capabilities:** Describes the capabilities of the Endpoint. Click on the info icon to see the capabilities supported. For more information, see SPDM specification.



Flag Fields	Value
Digests And Certificate	Supported
Challenge	Supported
Measurements With Signature	Supported

Following are the Flag Fields as per SPDM specification:

- **Cache Negotiated State:** Cache Negotiated State is a feature that allows the Responder to cache the state of a previously negotiated parameter during a previous SPDM session. This feature is used to optimize subsequent SPDM sessions by avoiding the need to renegotiate the same parameter.
- **Digests and Certificate:** Digests and Certificate are used to ensure the integrity and authenticity of communication between the Requester and Responder. Digests are used in SPDM to compute a fixed-length hash value of a message or data. Certificates are used in SPDM to provide authentication and to ensure the integrity of communication between the Requester and Responder.
- **Challenge:** A Challenge is a cryptographic mechanism used to authenticate the Requester and the Responder during the protocol initialization phase. The Challenge mechanism involves the exchange of challenge messages between the Requester and Responder, which are used to verify each other's identity and establish a shared secret for subsequent communication.
- **Measurements Fresh:** Measurements Fresh feature requires the Responder to provide fresh platform measurements during each SPDM session. This feature is used to ensure that the platform measurements are up-to-date and were not tampered earlier.
- **Measurements With Signature:** Measurements With Signature feature requires the Responder to sign the platform measurements before sending them to the Requester. This feature is used to ensure the integrity and authenticity of the measurements and to provide an additional layer of security to the SPDM protocol.

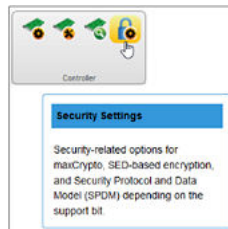
- **Measurements Without Signature:** Measurements Without Signature feature allows the Requester to send a Measurement message to the Responder without requiring the Responder to sign the measurement data.
- **Derived Pre-Shared Key:** Pre-Shared Key (PSK) is a type of cryptographic key that is shared in advance between two parties to secure their communication. A Derived Key in the context of SPDM is a cryptographic key that is derived from a shared secret using a key derivation function (KDF).
- **Single Pre-Shared Key (PSK):** Pre-Shared Key (PSK) is a type of cryptographic key that is shared in advance between two parties to secure their communication. A Single Key refers to a cryptographic key that is used for both message encryption and message authentication.

For more information, see the Security Protocol and Data Model (SPDM) specification at <https://www.dmtf.org/standards/spdm>.

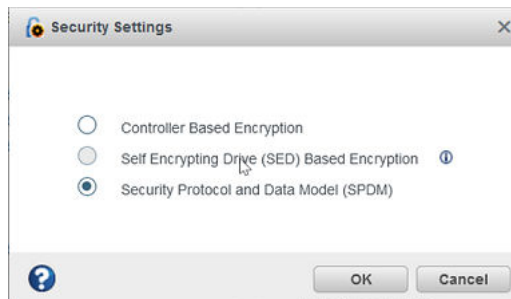
## 11.2 SPDM Security Settings

To perform the operation of Security Protocol and Data Model (SPDM):

1. In Enterprise View, select a **Controller**.
2. On the ribbon, in Controller group, select the **Security Settings**.



3. Click the **Security Settings** ribbon icon to open a dialog based on the following criteria.
  - If both or any one of **maxCrypto** and **Self Encrypting Drive (SED) Based Encryption** is supported along with **Security Protocol and Data Model (SPDM)**, the following dialog box gets displayed. Click the maxCrypto Settings ribbon icon to display the **Security Settings** dialog box.

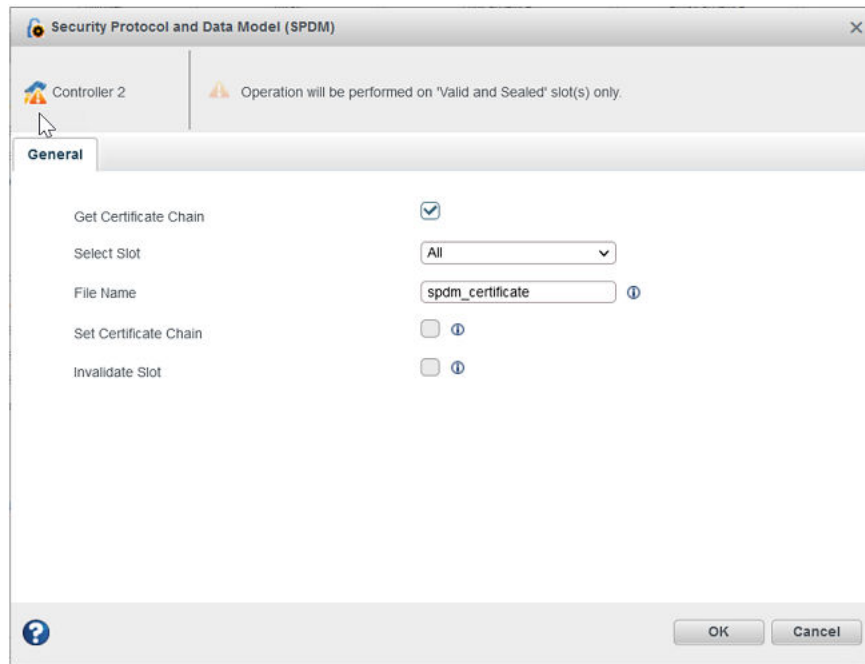


- Select the **Security Protocol and Data Model (SPDM)** option and then click OK. The **Security Protocol and Data Model (SPDM)** dialog appears, which is explained further in this section.

## 11.3 Get Certificate Chain

Get certificate chain operation retrieves the certificate chain from the specified slot number. This takes a slot number as an input.

The following figure shows the SPDM operations.

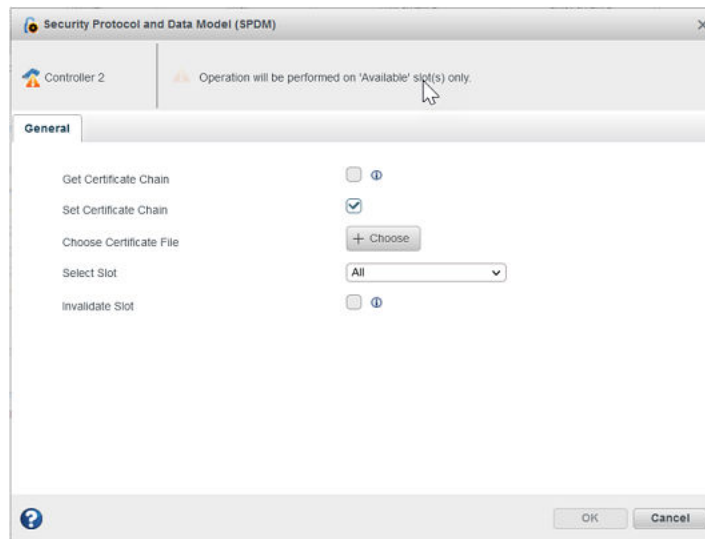


After checking the **Get Certificate Chain** check box, the **Select Slot** drop down option gets enabled to select the slot number. It displays only the valid slot number which has a certificate. You can select **All** option to retrieve the certificate chain from all the valid slot number.

If the slot status for the specific slot is **Valid and Sealed**, then it can retrieve the certificate.

## 11.4 Import Certificate Chain

Import certificate chain is used to set/write the certificate chain on the specified slot number.

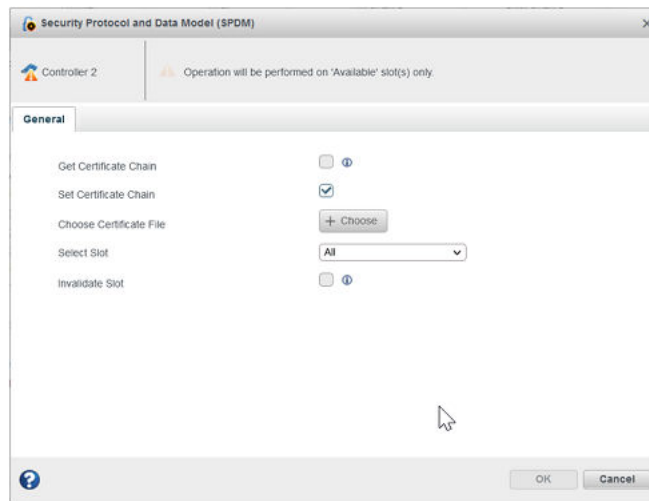


After checking the **Import Certificate Chain** checkbox, **Choose Certificate File** button and **Select Slot** drop down option gets enabled. Select the proper certificate file and upload it. Select the slot number to which the certificate chain should be written.

If the slot status for the specific slot is **Available**, then it can set/write the certificate into the slot.

## 11.5 Invalidate Slot

Invalidate Slot is used to invalidate the certificate chain on the specified slot.



After checking the **Invalidate Slot** check box, the **Select Slot** drop down option gets enabled to select the slot number. It displays only the valid slot number which has a certificate.

If the slot status for the specific slot is **Valid and Sealed**, then it can retrieve the certificate.

## 12. Maintaining Physical Devices

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

### 12.1 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 following figure shows the properties for a controller. For more information about using the Storage Dashboard to monitor the components in your storage space, see [13.2.3. Viewing Component Status in the Storage Dashboard](#).

The screenshot displays the 'Properties' tab for a controller in the Storage Dashboard. It is divided into three main sections: Controller Info, Settings, and Key Features.

Controller Info	
Physical Slot	8
Driver Version	Windows 1.52.0.0
Driver Name	smartsamd.sys
Negotiated PCIe Data Rate	PCIe 4.0 x8 (15752 M...
PCI Address (Domain Bus/Dev...	0:3:0:0
I2C Address	0x0
NCO	Supported
Number of Ports	2 Internal Only
NVMe Configuration	Supported
Manufacturing Model	Not Applicable
Manufacturing SKU Number	Not Applicable
Reboot Required Reasons	Not Available
EEPROM Version	0
CPLD Revision	22

Settings	
Post Prompt Timeout	0 sec
Rebuild Priority	Not Applicable
Expand Priority	Medium
Consistency Check Priority	Not Applicable
Consistency Check Delay	Not Applicable
Parallel Consistency Check ...	Not Applicable
Raid 6/60 Alternate Inconsist...	Not Applicable
Consistency Check Inconsist...	Not Applicable
Spare Activation Mode	Failure
Maximum Drive Request Que...	Not Applicable
Monitor and Performance De...	Not Applicable
Physical Drive Request Elev...	Not Applicable
Degraded Mode Performanc...	Not Applicable
HDD Flexible Latency Optimi...	Not Applicable
Primary Boot Volume	None
Secondary Boot Volume	None
Sanitize Lock	Freeze
Pending Sanitize Lock	Not Applicable
Expander Minimum Scan Dur...	132 sec
Persistent Event Log Policy	Newest
Active PCIe Maximum Read ...	2048 Bytes
Deadline PCIe Maximum Doo...	Not Applicable

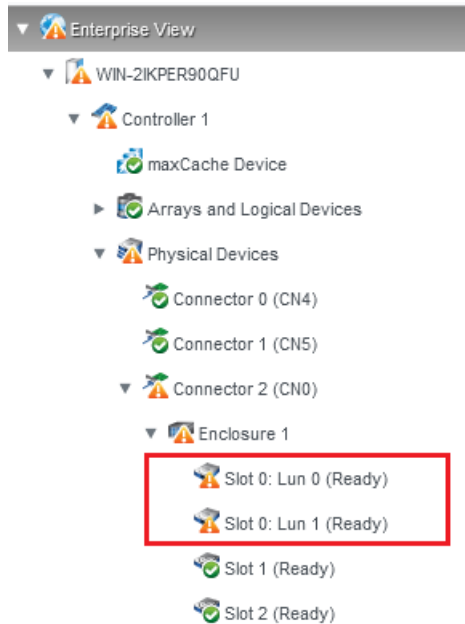
  

Key Features	
<b>Intelligent Power Management</b>	
Current Power Mode	Maximum Performance
Pending Power Mode	Not Applicable
Survival Mode	Enabled
<b>Controller Cache</b>	
Cache Status	Not Configured
Cache Ratio	Not Applicable
Write Cache Bypass Threshold...	1040
No-Battery Write Cache	Disabled
Wait for Cache Room	Disabled
<b>maxCache</b>	
Status	Disabled
Version	4
<b>Drive Cache</b>	
Write Cache Policy for Configu...	Enabled
Write Cache Policy for Unconf...	Enabled
Write Cache Policy for HBA Dr...	Enabled

### 12.2 Multi Actuator Drives

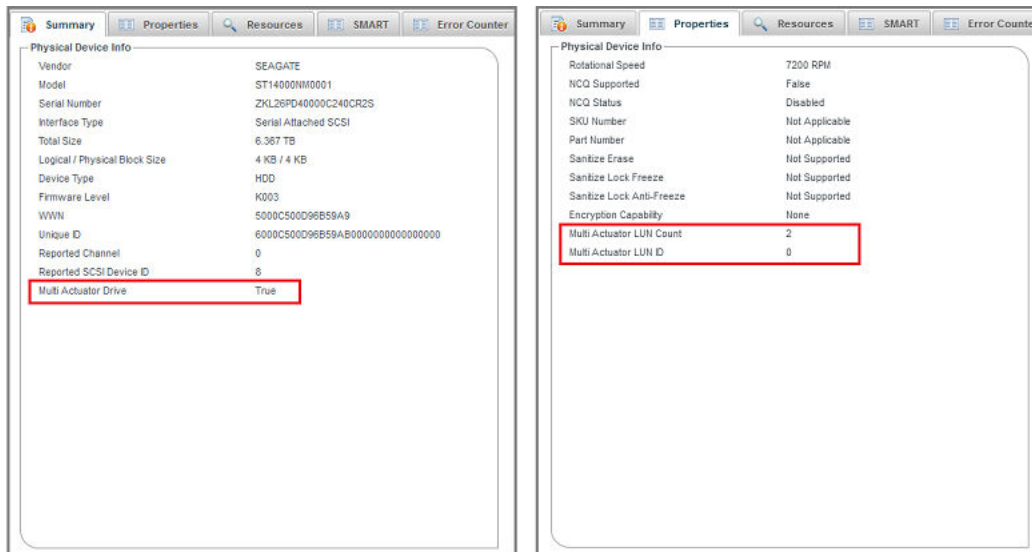
Multi Actuator drives are hard disk drives which contain two or more independent actuators that transfer data concurrently. It solves the need for increased performance by enabling parallelism of data flows in and out of a single hard drive. By allowing the data center host computer to request and receive data from two areas of the drive simultaneously, it increases the IOPS performance of each individual hard drive.

In enterprise tree view, multi actuator drive is listed along with its LUN number and every LUN is listed as a separate physical device.



Following are the properties of a multi actuator drive:

- **Multi Actuator Drive** - Specifies whether this physical device is multi actuator or not.
- **Multi Actuator LUN Count** - Specifies number of LUN's in the multi actuator drive.
- **Multi Actuator LUN ID** - ID of the current LUN in the multi actuator drive.








### 12.3 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. The following table describes how to locate specific devices.

**Note:**

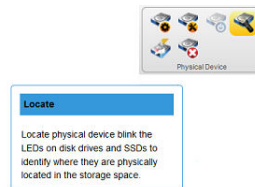
Once any of the device is located, the timeout value will be overwritten with the latest timeout value for all the located devices.

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: 
All SSDs in the maxCache Device	maxCache Device icon: 

### 12.3.1 Locating Disk Drives

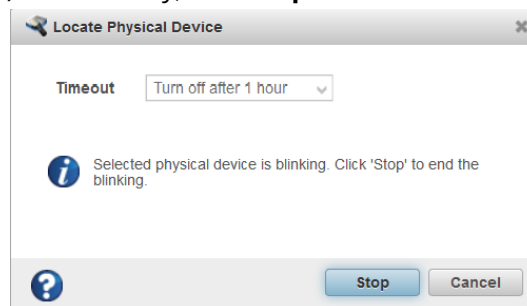
To locate an individual disk drive or all physical drives on the controller:

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**.



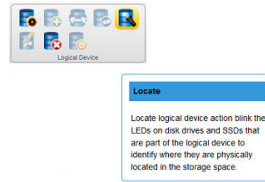
6. Click **Cancel** to close the Locate Physical Device window.  
The LED(s) continue to blink for the duration of the timeout period.

### 12.3.2 Locating Physical Disks in an Array or Logical Drive

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

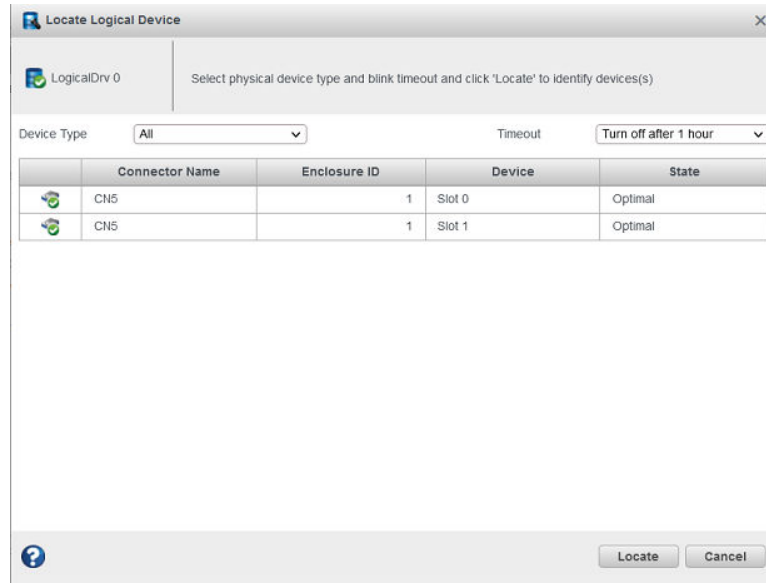
1. In the Enterprise View, open the Arrays and Logical Devices tree for a controller, then select an array or logical drive.
2. On the ribbon, in the Array group or Logical Device group (shown below), click **Locate**.





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**.



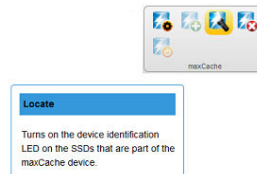
The LEDs on the disk drives begin to blink.

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.

### 12.3.3 Locating SSDs in the maxCache Device

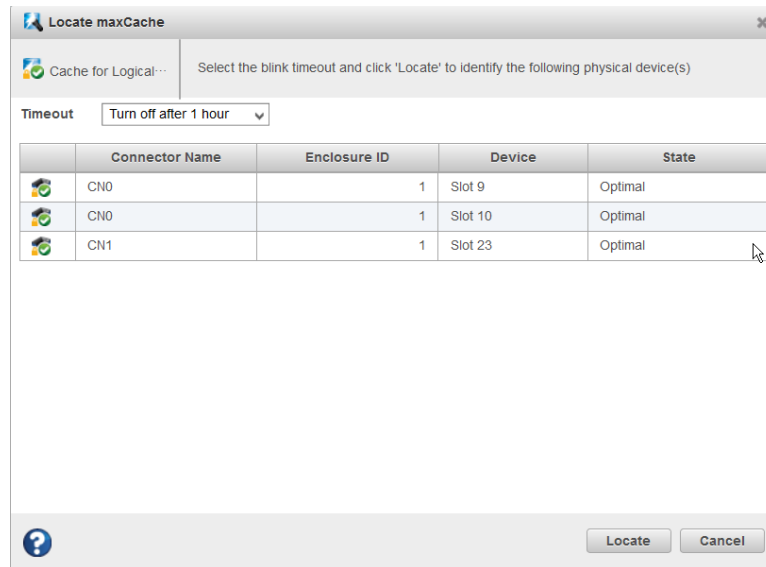
To locate the Solid State Drives (SSDs) in the maxCache Device:

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.



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.

## 12.4 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.

### 12.4.1 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
Aborted Command	0
Bad Target Error	0
ECC Recovered Read Error	0
Failed Read Recover	0
Failed Write Recover	0
Format Error	0
Hardware Error	0
Hard Read Error	0
Hard Write Error	0
Hot-Plug Count	0
Media Failure	0
Not Ready Error	0
Time-Out Error	0
Predictive Failure	0
Retry Recovered Read Error	0

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

.....continued

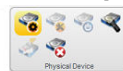
Error Counter	Description
Bad Target Error	Number of times that this drive did something that did not conform to the SCSI Bus Protocol. It will cause a reset of the SCSI bus that this drive is attached to.
ECC Recovered Read Errors	Number of ECC-corrected read errors.
Failed Read Recover	Number of times 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.

### 12.4.2 Clearing Error Counters from a Physical Device

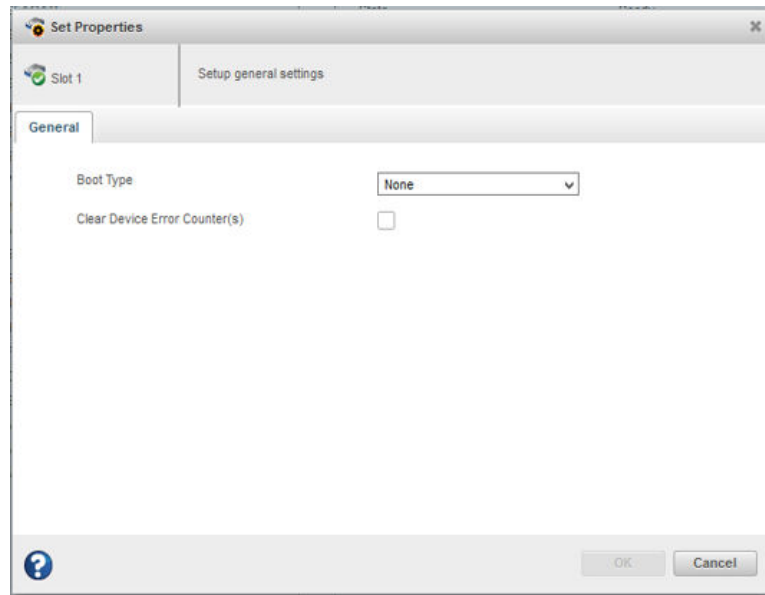
Use this option to clear the device error counters of a specific physical device.

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.



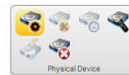
3. To clear the device errors, select the Clear Device Error Counter(s) check box.
4. Click **OK**.

### 12.4.3 Clearing Error Counters from a Controller

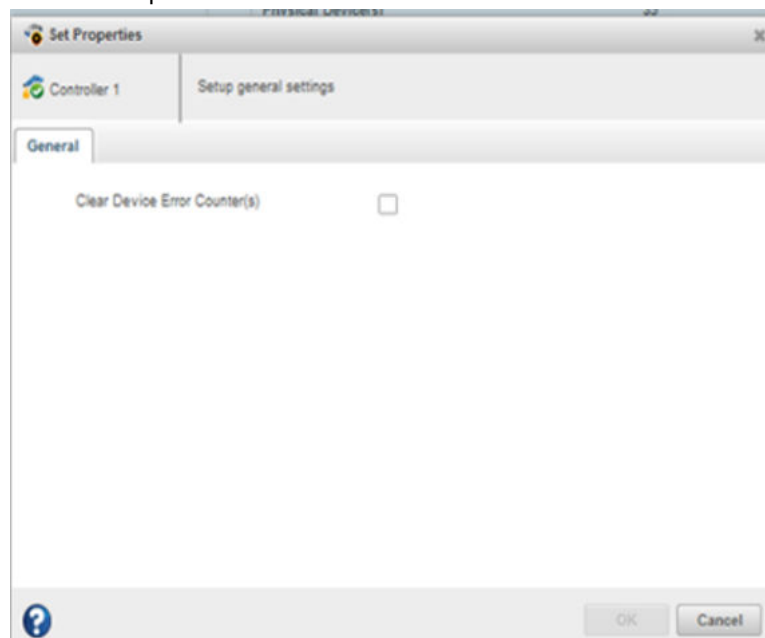
Use this option to clear the device error counters of all the physical devices from controller.

To clear the the device errors from a controller:

1. In the Enterprise View, select the controller 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**.

## 12.5 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:

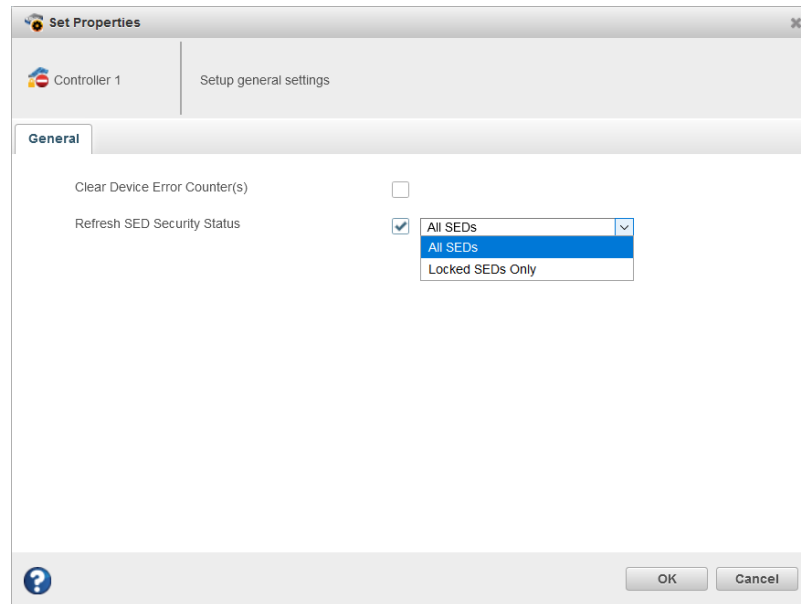
- On Controller
- On Physical Device

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**.



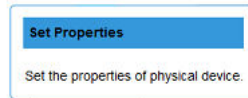
The **Set Properties** window opens.



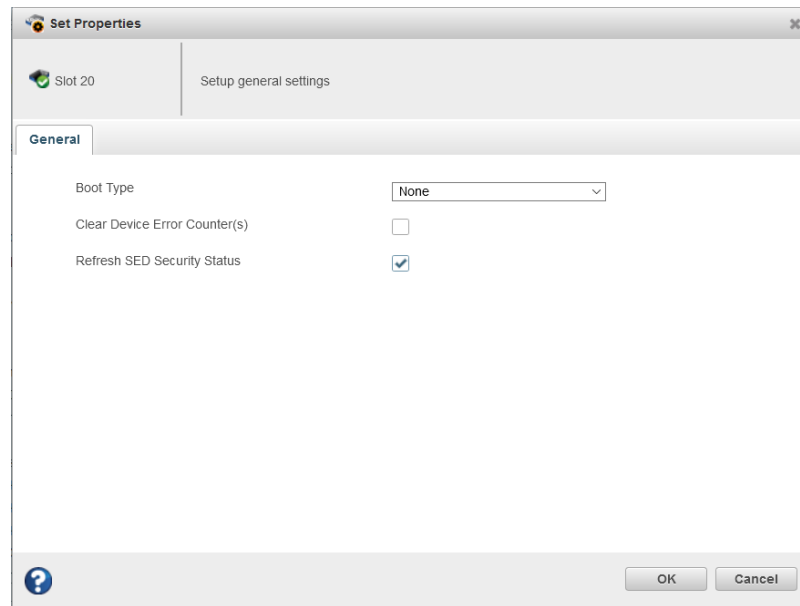
3. Select one of the following option from the **Refresh SED Security Status** drop-down menu:
    - All SEDs: This will refresh the SED security status for all the SED drive attached to the controller.
    - Locked SEDs Only: This will refresh the SED security status for all locked SED drive attached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

## 12.6 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.

### 12.6.1 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.



If another disk drive in the logical drive fails during rebuild (see [15.4. 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 [12.6.2. 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 [15.4. Rebuilding Logical Drives](#).)

- Repeat these steps for each disk drive you want to replace.

### 12.6.2 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.

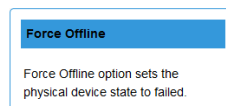
---

**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:

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



The Force Offline window opens.

- 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.

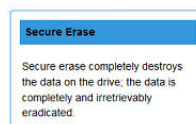
## 12.7 Erasing a Disk Drive

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:

- In the Enterprise View, select a controller then, in the Physical Devices tree, select the drive you want to erase.
- On the ribbon, in the Physical Device group, click **Secure Erase**.



The Secure Erase Physical Device window opens.

- 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 data. It provides a very fast, complete, and robust erasure of the solid state device.
  - **Sanitize Crypto Scramble**— Changes the internal encryption keys that are used for data, making the data irretrievable. This option is available for HDD and SSD devices when supported by the device.
4. Click **Erase** to erase the drive.

### 12.7.1 Restricted/Unrestricted Secure Erase

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

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

For more information about Sanitize erase patterns, see [12.7. Erasing a Disk Drive](#) .

## 12.8 Initializing and Uninitializing Disk Drives

This section describes how to initialize/uninitialize disk drives to enable the erased drive, erase data and meta-data (including logical drive 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.

### 12.8.1 Uninitializing a Disk Drive

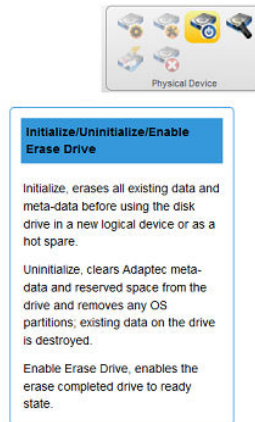
You can uninitialize any disk drive (or SSD) containing Smart Controller configuration metadata. Uninitializing a disk drive clears the meta-data and reserved space from the drive and removes any OS partitions; existing data on the drive is destroyed.

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

To uninitialize a disk drive:

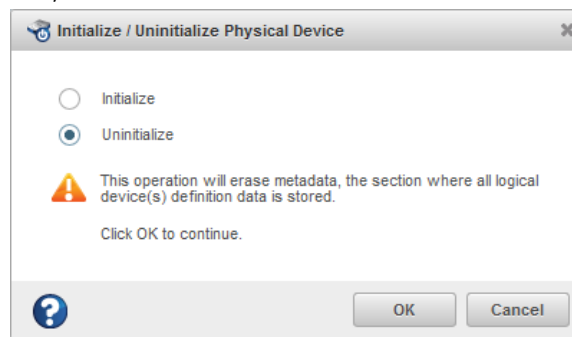
1. In the Enterprise View, select a controller; then, in Physical Devices tree, select the disk drive you want to uninitialize.
2. On the ribbon, in the Physical Device group, click **Initialize/Uninitialize/Enable Erase Drive**.





The Initialize/Uninitialize Physical Device window opens.

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



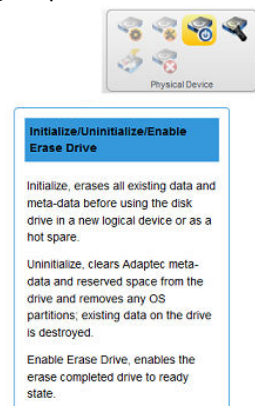
4. When prompted, click **OK** to close the Initialize/Uninitialize Device window.

## 12.8.2 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.

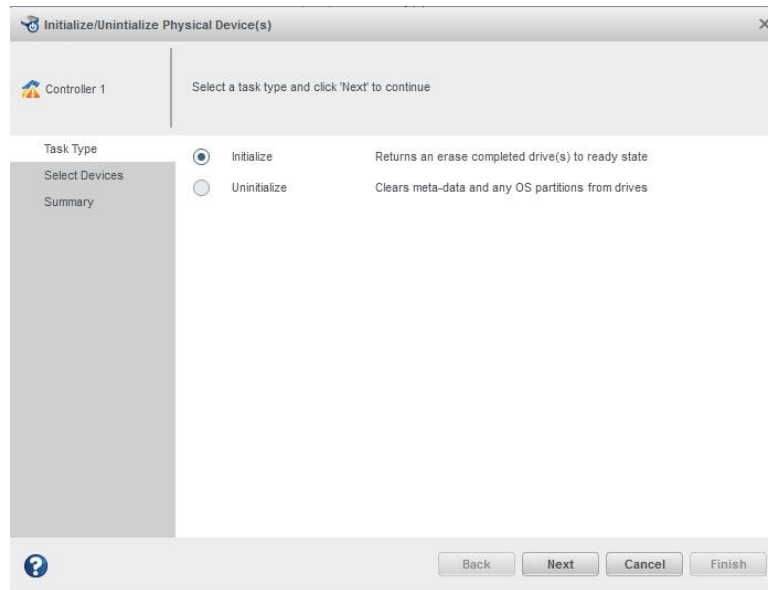
To initialize or uninitialize drives with the wizard:

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**.



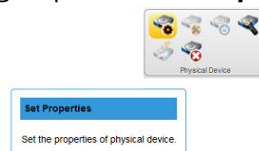
4. Select drives on the controller to initialize or uninitialize, then click **Next**.
5. Review the Summary, then click **Finish**.

## 12.9 Setting the Physical Drive Boot Priority

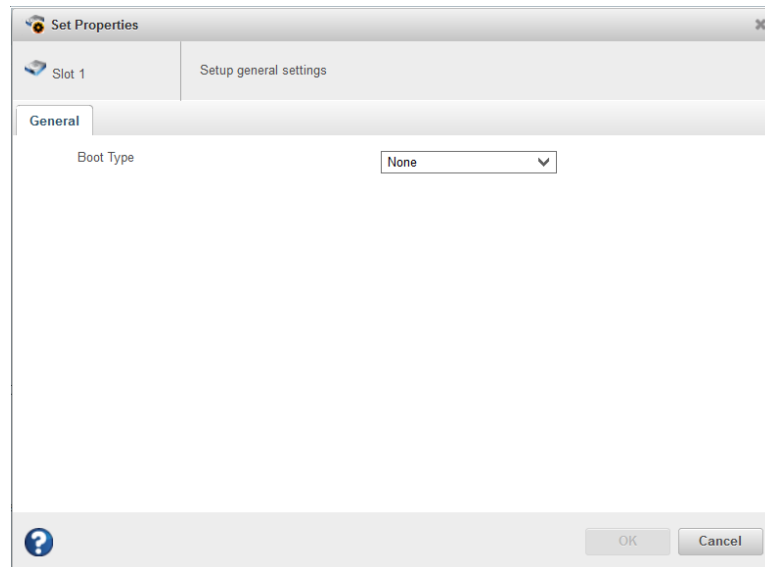
Use this option to set the boot priority of a physical device to Primary, Secondary, Primary and Secondary, or None (default). A controller can have only one physical (or logical) device as the primary or secondary boot device. When you select a new physical device as the primary/secondary boot drive,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

## 12.10 Working with Controllers

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

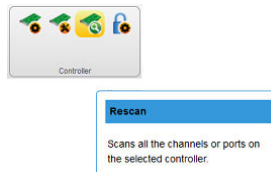
- To re-scan a controller, see [12.10.1. Rescanning a Controller](#).
- To optimize controller performance, see [12.10.2. Optimizing Controller Performance](#).
- To change the operating mode of connectors on the controller, see [12.10.3. Changing the Connector Operating Mode](#).

### 12.10.1 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, a success message is displayed. Click **OK** to close the Rescan window.

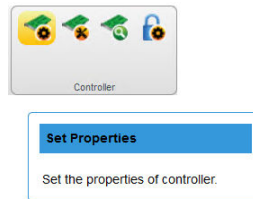
### 12.10.2 Optimizing Controller Performance

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.

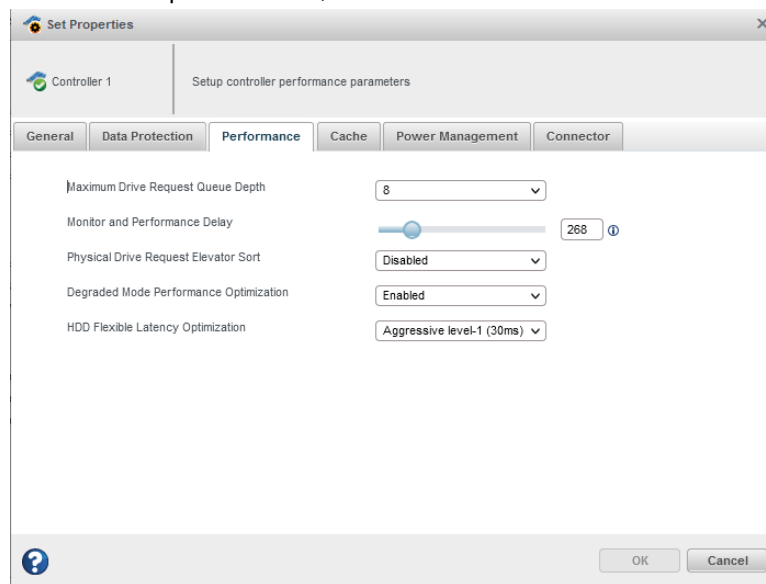
To enable/disable performance optimizations on a controller:

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**.

### 12.10.3 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

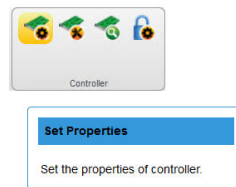
By default, products with RAID support are configured to operate in Mixed Mode. Mode options vary, depending on the configuration of logical and physical devices on the connector. For example, you cannot switch the connector to HBA mode if the connector is already configured with a RAID volume.

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.

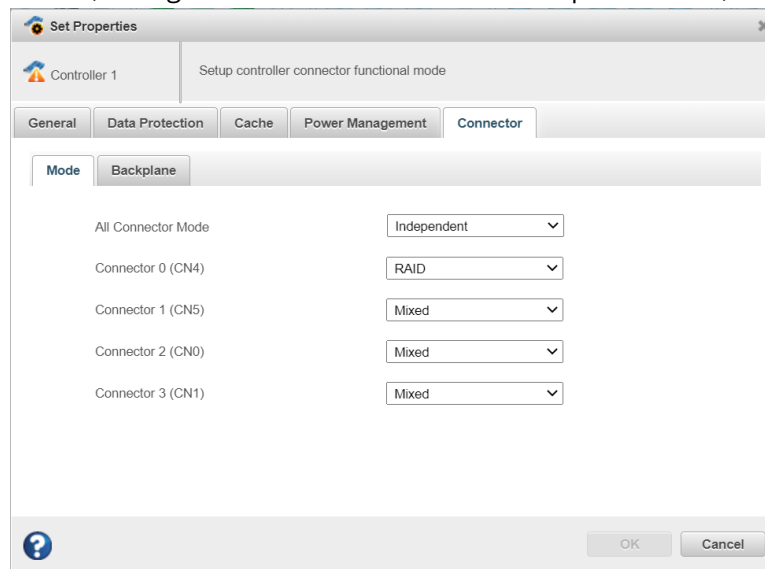
To change the connector mode on a controller:

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.

#### 12.10.4 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.
- **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. 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:**

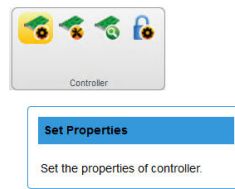
If the port discovery protocol is not configured correctly, some features of the backplane may not function as expected. A reboot is required for the new port discovery protocol to take effect.

**Note:**

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

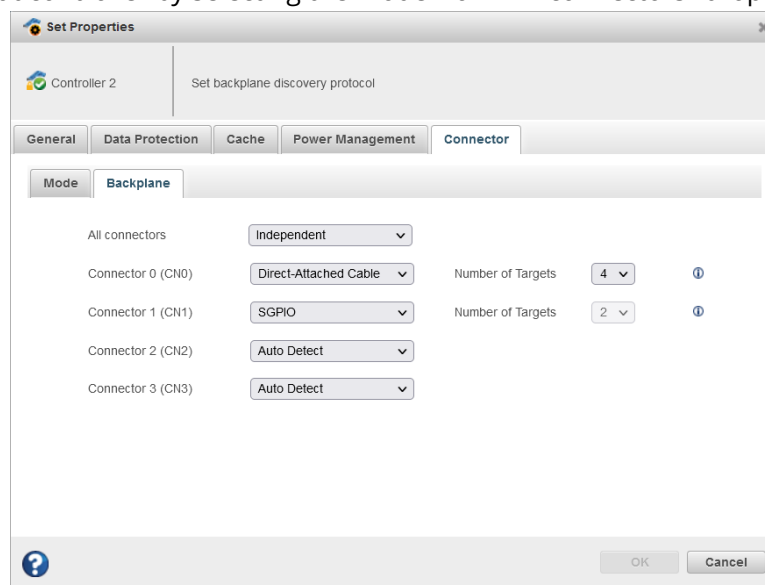
To change the backplane discovery mode protocol settings:

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.

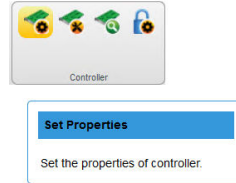
### 12.10.5 Changing the Expander Minimum Scan Duration Settings

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 effect on the next power cycle. The controller waits for the specified duration and then scans/discovers the drive attached to the expander.

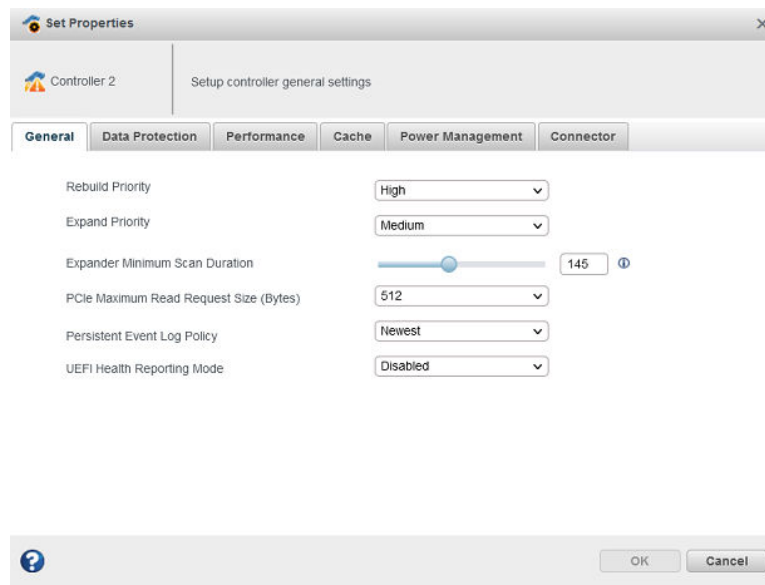
To change the expander minimum scan duration settings:

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.

### 12.10.6 Setting the PCIe Maximum Read Request Size

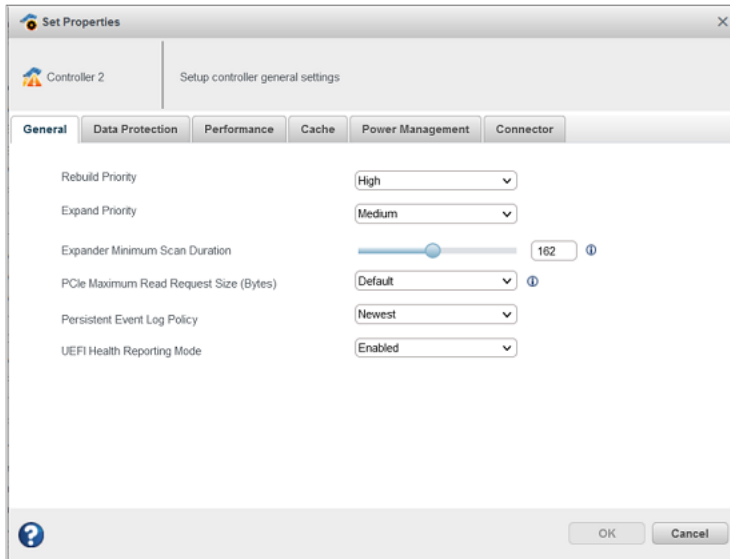
PCIe Maximum Read Request Size allows optimization of data flow to improve the controller performance. This option is used to change the PCIe Maximum Read Request Size value on your Adaptec Smart Storage Controller.

The PCIe Maximum Read Request Size takes one of the following values (default): 128, 256, 512, 1024, or 2048 Bytes. The default value setting refers to the server's Maximum Read Request Size.

The system must be restarted for the PCIe Maximum Read Request Size to take effect.

To change the PCIe Maximum Read Request Size on a controller:

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. Select the **PCIe Maximum Read Request Size** value from the drop-down list.



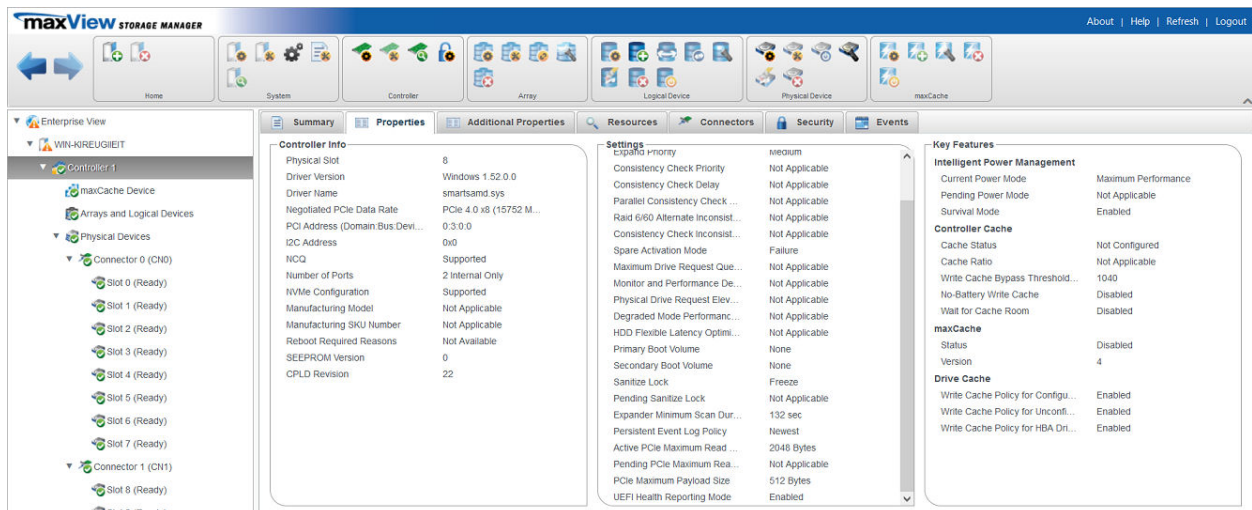
4. Click **OK**.
5. Reboot the server.

The value of the PCIe Active and Pending Maximum Read Request Size gets displayed under the **Properties** tab of the controller.

### PCIe Maximum Payload Size

The PCIe Maximum Payload Size is the maximum size of PCIe payload for one transfer. The PCIe Maximum Payload Size reports the values as 128, 256, or 512 bytes and gets displayed under **Properties** tab of controller.

**Note:** The value of PCIe Maximum Payload Size cannot be changed from the maxView GUI.





### 12.10.7 Changing the Persistent Event Log Policy Setting

The firmware generated events are read by consumers to know details of what occurred on the controller. These events are also persisted in the NVRAM to ensure that the consumers can get those events when it occurred during offline.

The existing behavior of providing events to consumers shall remain unchanged when fewer than 300 pending events. If there are more than 300 events pending for delivery, then the event delivery will be based persistent event log policy.

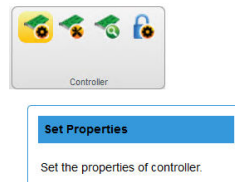
Persistent Event Log Policy can be either Oldest (Least Recently Consumed) or Newest (Most Recently Occurred). The maximum number of events that can be stored by firmware at any point is 300.

When the policy is “Least Recently Consumed”, the maximum unconsumed events in NVRAM can be 300. After that the controller stops adding new events to the persistent log in NVRAM.

When the policy is “Most Recently Occurred”, firmware shall continue to log a new event when it occurs in the NVRAM. The consumer will be provided with the most recent events (up to 300 events).

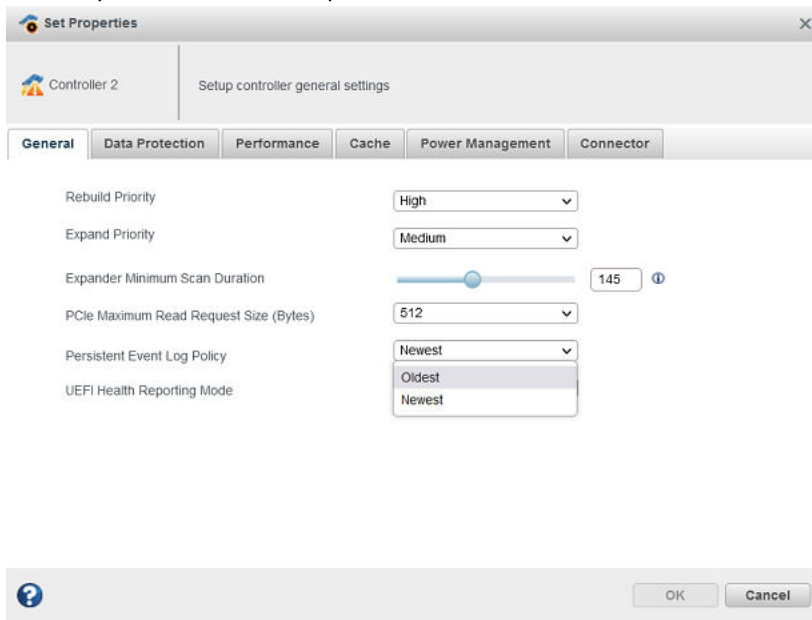
To change the persistent event log policy setting:

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 change the Persistent Event Log Policy setting, select **Oldest** or **Newest** from the dropdown in order to persist the oldest events and newest events respectively.



4. Click **OK**.  
The value of Persistent Event Log Policy gets displayed in the Properties tab of the controller.

### 12.10.8 Changing UEFI Health Reporting Mode Setting

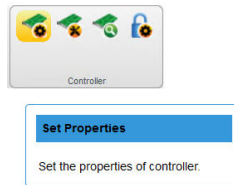
UEFI Health Reporting Mode allows the users to change whether to report UEFI driver health error messages on boot screen and halt the boot process or not. The UEFI Health Reporting Mode can be either “Enabled” or “Disabled”.

The default mode is **Enabled**, which reports all the UEFI driver health error messages on the boot screen and halts the boot process.

The **Disabled** mode does not report any UEFI driver health error messages on the boot screen and continues the booting regardless of the errors.

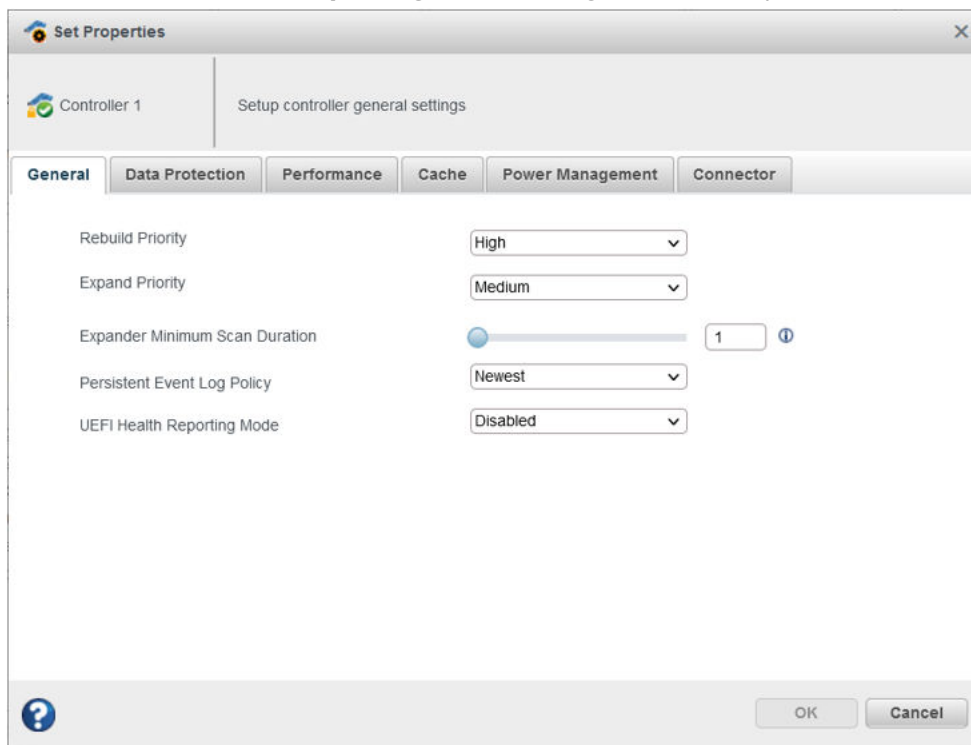
To change the UEFI Health Reporting Mode settings:

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. Select the **UEFI Health Reporting Mode** setting from the drop-down list, as needed.



- Enabled - Reports all the UEFI driver health error messages on the boot screen and halts the boot process.
- Disabled - UEFI driver health error messages will not be reported on the boot screen and the booting will be continued regardless of the errors.

4. Click **OK**.

The value of UEFI Health Reporting Mode gets displayed in the Properties tab of the controller.

## 12.11 Updating Controller, Enclosure, Backplane, 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, backplane, 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, backplane, or disk drives in your storage space, review the prerequisites in [12.11.1. Before You Begin](#), then follow one of these sets of instructions:

- [12.11.2. Updating the Controller Firmware](#)
- [12.11.3. Updating the Disk Drive Firmware](#)
- [12.11.4. Updating the Enclosure Firmware](#)
- [12.11.5. Updating the UBM Backplane Firmware](#)

**Note:** When the controller is configured with Self Encrypting Drive (SED) Based Encryption with Remote Mode, then downgrading the firmware to the older version fails, which does not support 255 character master key identifier. This information is available at both the System level and Controller level firmware upgrade process.

### 12.11.1 Before You Begin

Before you begin, download the latest firmware images from [start.adaptec.com](http://start.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, backplane, and enclosure image file names vary by manufacturer.

### 12.11.2 Updating the Controller Firmware

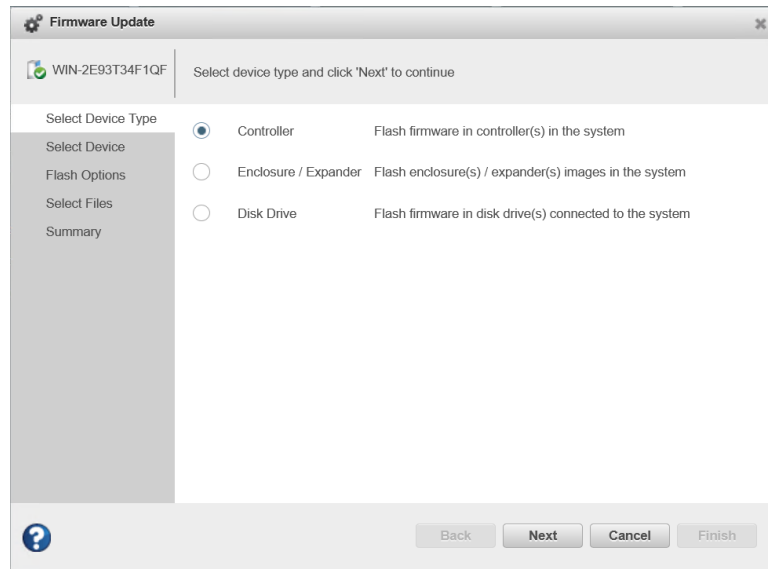
Use the Firmware Update wizard to update the firmware for one or more controllers of the same type on the local or a remote system.

To update the controller firmware:

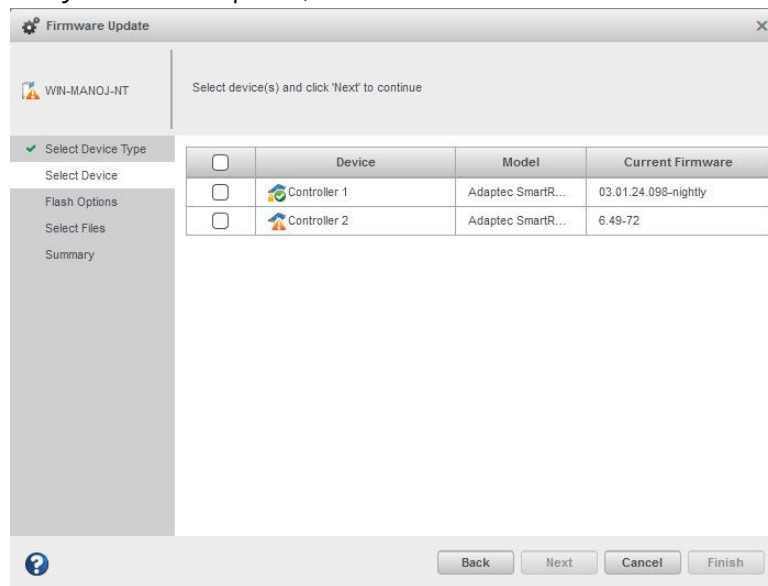
1. In the Enterprise View, select a system.
2. On the ribbon, in the System group, click **Firmware Update**.



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

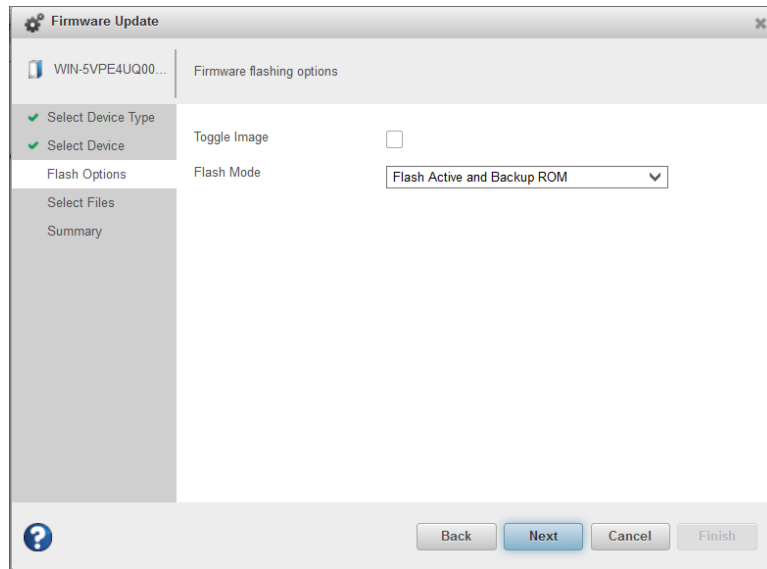


4. Select the controllers you want to update, then click **Next**.

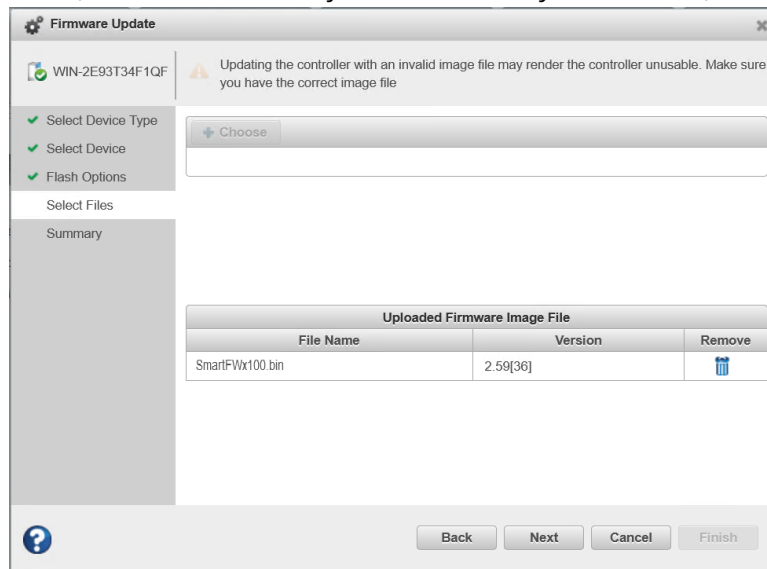


5. Select flash options for the update, then click **Next**. Choose Toggle Image to replace the active image with the backup image.

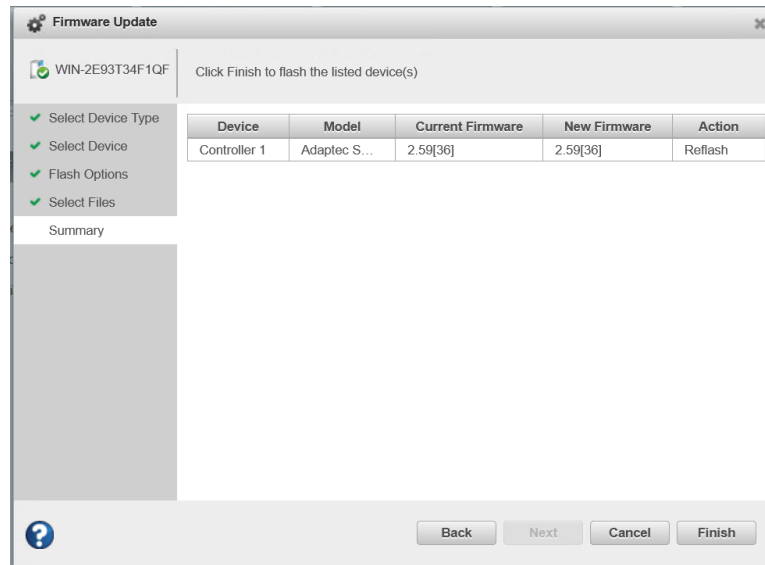
**Note:** If you choose Toggle Image, Step , Select Files 6, is skipped.



- 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).



- When the file name appears in the Uploaded Firmware File(s) list, click **Next**.
- Review the update summary, then click **Finish**.



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

- When the update is complete, click **OK**. Restart the server to activate the new firmware image

**Note:** If the controller write cache is enabled and the controller firmware update includes a hardware security update, the controller firmware update operation fails with the following warning message:

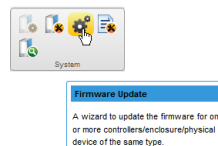
*The given controller firmware update contains a hardware security update and the controller write cache is enabled. Disable the controller write cache to update the controller firmware.*

### 12.11.3 Updating the Disk Drive Firmware

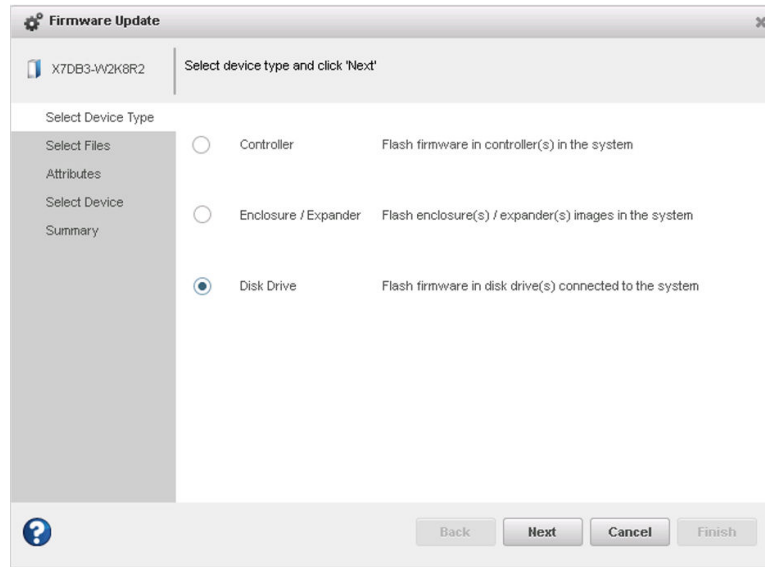
Use the Firmware Update wizard to update the firmware for one or more disk drives of the same type on the local or a remote system. The procedure is similar to updating the controller firmware (see [12.11.2. Updating the Controller Firmware](#)).

To update the disk drive firmware:

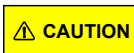
- In the Enterprise View, select a system.
- On the ribbon, in the System group, click **Firmware Update**.



- 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**.



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.

#### 12.11.4 Updating the Enclosure Firmware

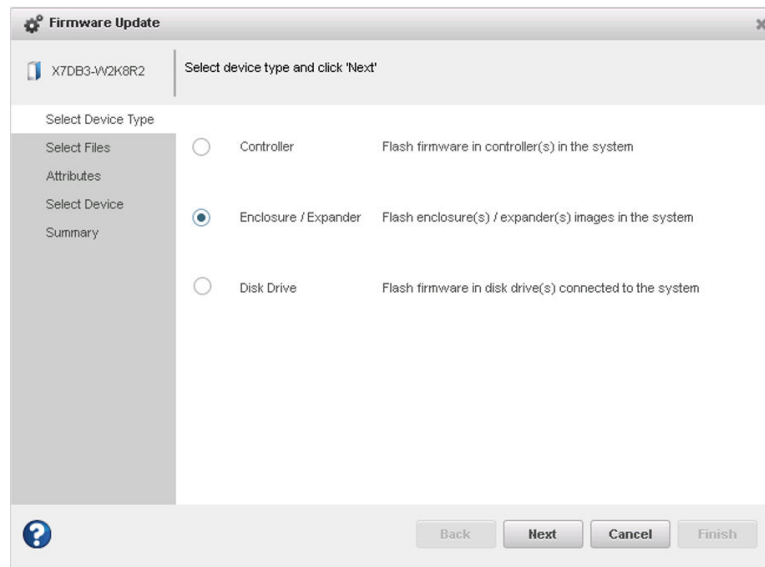
Use the Firmware Update wizard to update the firmware for one or more enclosures or expanders of the same type on the local or a remote system.

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**.



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.



### 12.11.5 Updating the UBM Backplane Firmware

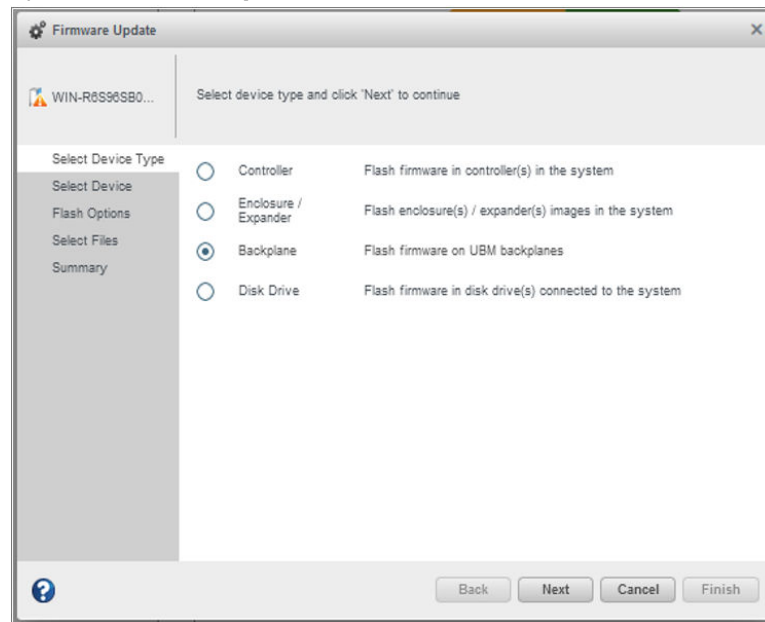
UBM is a standard from SNIA SFF for the management of SAS, SATA, and NVMe backplanes by storage controllers, chipsets, and switches. UBM provides a single industry standard design mechanism for backplanes to interoperate with the storage ecosystem in a single self-describing standard way reducing costs and development time within storage partner ecosystems. Use the Firmware Update wizard to update the firmware for one or more backplanes of the same type on the local or a remote system.

To update the UBM backplane firmware:

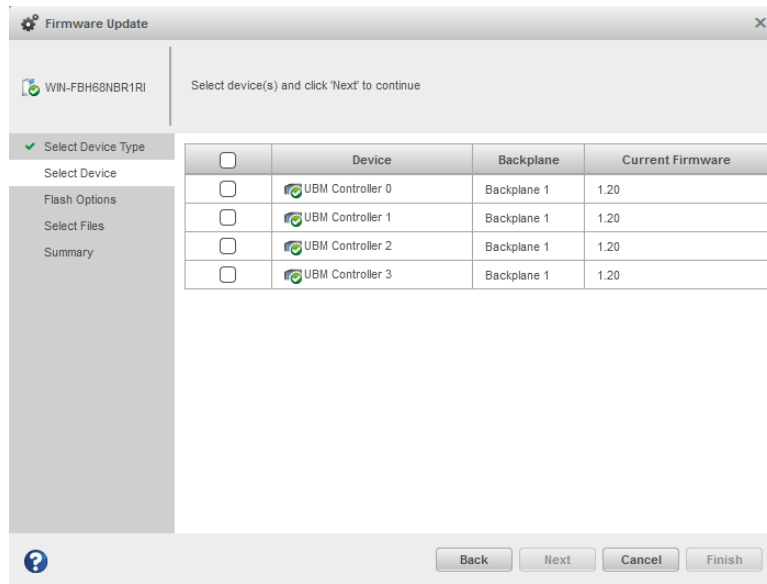
1. In the Enterprise View, select a system.
2. On the ribbon, in the System group, click **Firmware Update**.



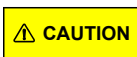
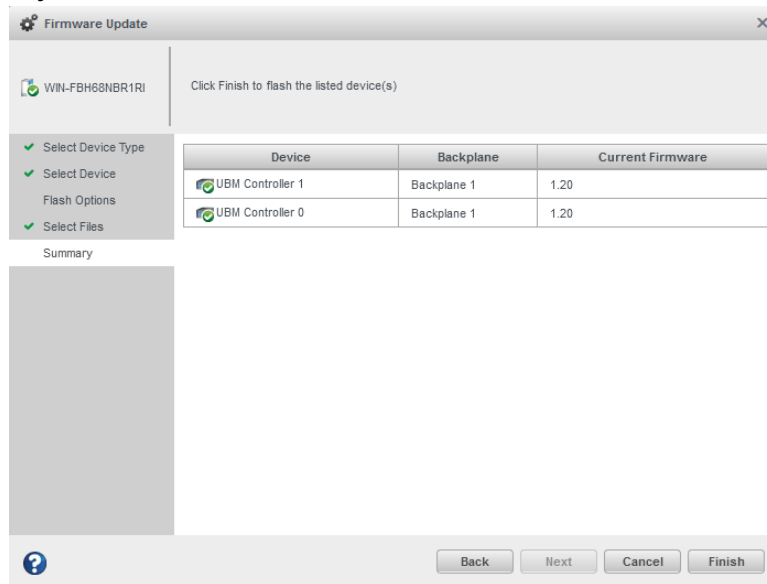
3. When the wizard opens, select **Backplane**, then click **Next**.



4. In the Select Device Type panel, select the **Backplane** to perform firmware update operation, then click **Next**.



- 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).
- When the file name appears in the Uploaded Firmware File(s) list, click **Next**.
- Review the summary information, then click **Finish**.



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

- When the update is complete, click **OK**. Restart the server to activate the new firmware image, as needed.

## 13. Monitoring Status and Activity

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

### 13.1 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 [13.2.1. Viewing Activity Status in the Event Log](#) and [13.4. 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 [13.2.2. 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 [13.2.3. 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 [13.2.4. 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 [13.3. Notifying Users by Email About Status and Activity](#) .
- **Audible Alarm**—A series of beeps sounds whenever a serious event occurs on your storage space.

### 13.2 Checking Status from the Main Window

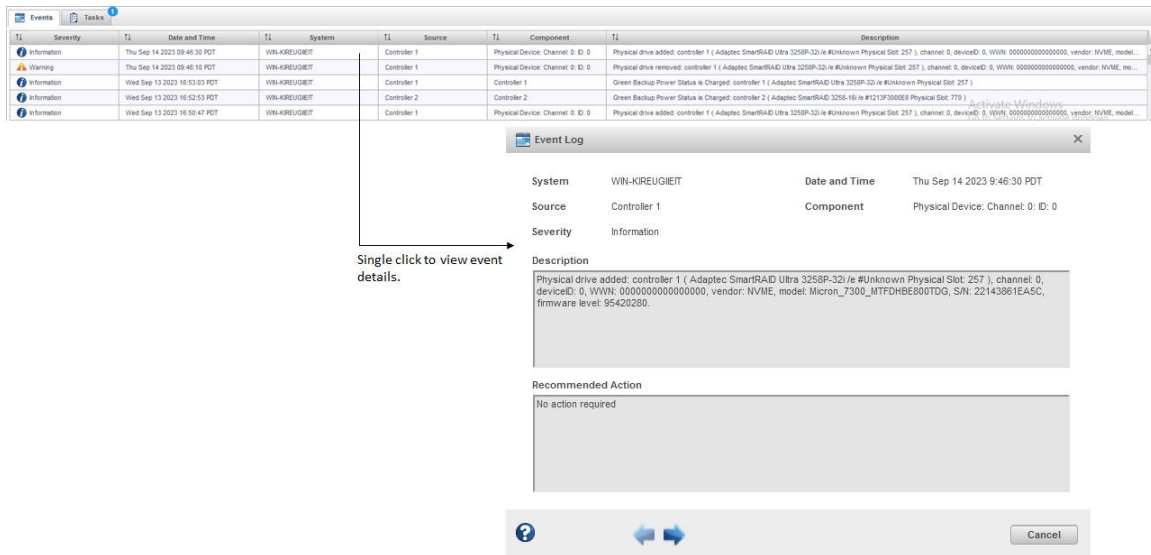
You can view status information and messages about the activity occurring in your storage space by looking at the *event log*, status icons, and *task log* in the main window of maxView Storage Manager. (You can also view all events for a system in its operating system event log; see [13.4. Changing 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.

#### 13.2.1 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 [13.2.1.1. 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 [13.2.3. Viewing Component Status in the Storage Dashboard](#)).

Single-click any event to open the Event Log Detail window to see more information in an easier-to-read format. Use the up and down arrows to view previous or following events.



To make it easier to find a specific event, click on the column heads to sort the events. For example, sorting the events by Severity can help you find specific Error- or Warning-level events quickly.

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

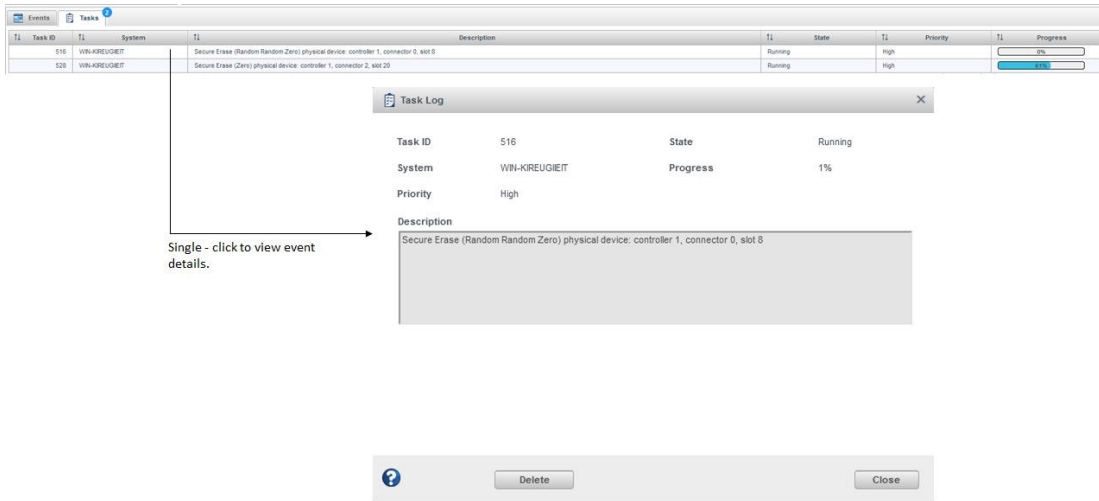
maxView Storage Manager indicates event status with icons. This table lists the three categories, or types, of events based on severity.

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.

### 13.2.2 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.

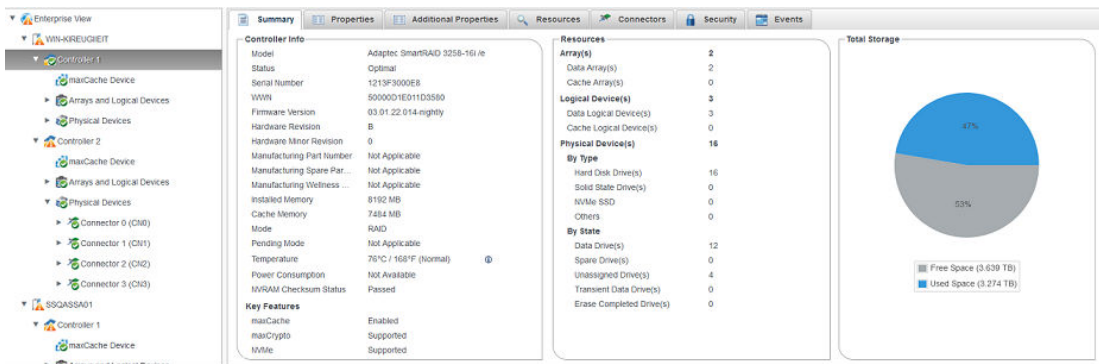


### 13.2.3 Viewing Component Status in the Storage Dashboard

The Storage Dashboard provides detailed information about the components of the storage space, including local and remote systems, controllers, arrays, logical drives, enclosures, backplanes, 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 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 13.2.1. Viewing Activity Status in the Event Log).

**Note:** For information about Chart View, on the right side of the Storage Dashboard, see 13.2.4. Viewing Storage Space Usage in Chart View.



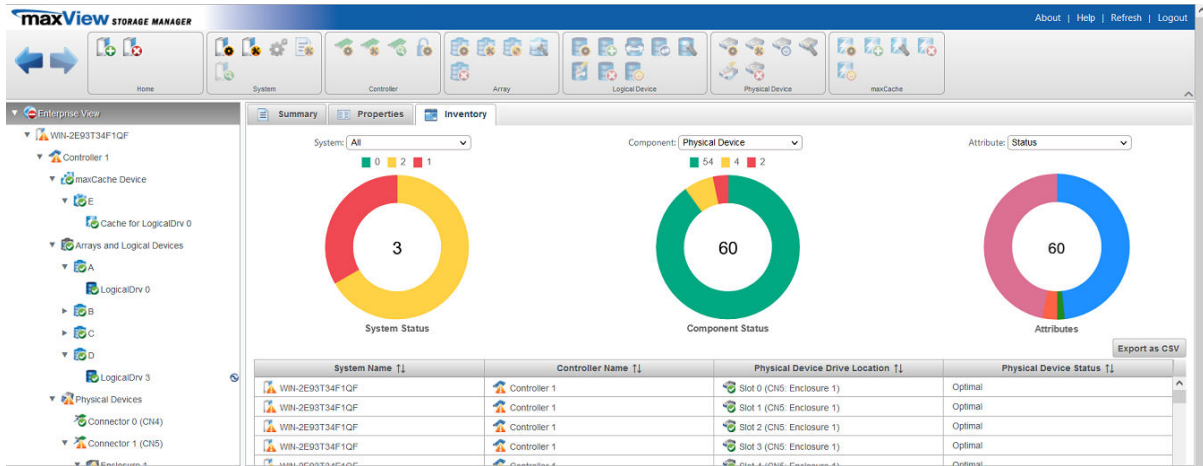
The following table lists the categories and types of information provided on the Storage Dashboard for each component in the storage space. All top-level nodes in the Enterprise View (System, Controller, Arrays, Logical Drives, Enclosures, Backplane, Physical Devices, and so on) include a Summary tab 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 <a href="#">9.1.3. Checking maxCrypto Status</a> ) 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 <a href="#">4.5. Revealing More Device Information</a> )
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 <a href="#">13.2.3.2. Monitoring Enclosure Status</a> ) Speaker status Slot allocation and usage
Backplane	Summary	Backplane ID, type, UBM Controller ID, firmware version, part number, model, device code PCI Vendor ID
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 <a href="#">13.2.3.3. Viewing SMART Statistics</a> )

### 13.2.3.1 Storage Inventory

Perform the following steps to view storage inventory. It provides the complete view of the data and its statuses.

1. In Enterprise tree view, select **Enterprise View** node.
2. Click on the **Inventory** tab to display the storage inventory.



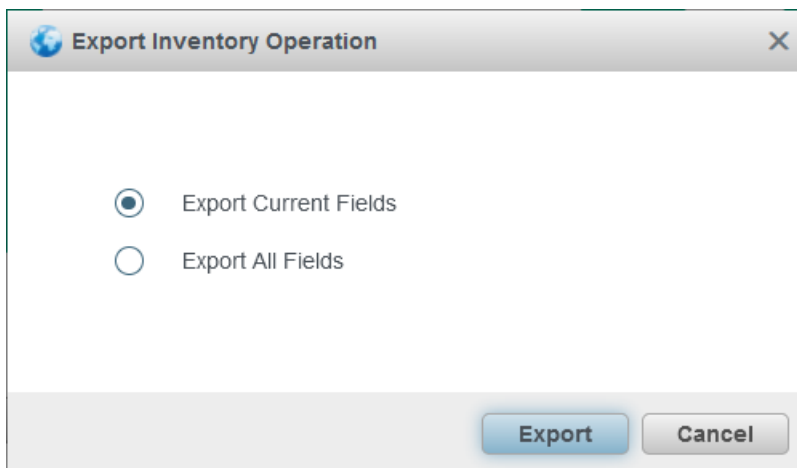
The storage inventory shows the following three charts:

- System chart that displays the tree node status of the system(s). The drop-down menu of the system chart provides the option to view system or all the system currently being managed using maxView.
- Component chart that displays the tree node status of each selected component. The component chart drop-down menu provides option as Controller, Logical Device, Enclosure, Backplane, and Physical Device. You can select the specific component to know the details of it along with Attributes chart.
- Attribute chart displays the attributes related to the selected component.

The table preceding the charts display the details based on the drop-down values.

To export the details in a .csv format, perform the following steps:

1. On the Inventory page, click **Export as CSV**.  
The **Export Inventory Operation** dialog box appears.



2. Select **Export Current Fields** option to export the data currently available in the table as .csv format. Or, select **Export All Fields** to export all the data in .csv format depending on the drop-down options selected on system, component, and attributes.

### 13.2.3.2 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.

Resources	
<b>Fan(s)</b>	<b>6</b>
Optimal	6
Malfunctioning	0
Not Installed	0
<b>Power Supplies</b>	<b>2</b>
Optimal	2
Malfunctioning	0
Not Installed	0
<b>Temperature Sensor(s)</b>	<b>2</b>
Normal	2
Abnormal	0
Not Installed	0
<b>Speaker(s)</b>	<b>1</b>
On	1
Off	0
Not Installed	0

### 13.2.3.3 Viewing SMART Statistics

You can use the Storage Dashboard to view various indicators of reliability for the SAS, SATA, and NVMe drives 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.



Summary Resources SMART Events

Please refer to drive vendors data sheet for description

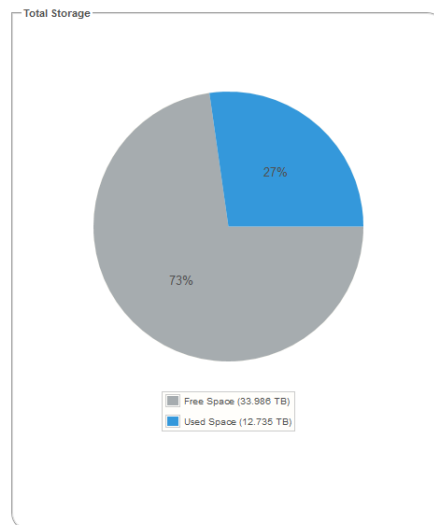
ID	Name	Normal
0xBB	Temperature	100
0xC2	Reported I/O Error Detection Code Errors	30
0xC3	Unknown Attribute	120
0xC4	Unknown Attribute	100
0xC9	Unknown Attribute	120
0xCC	Unknown Attribute	120
0xE6	Life Curve Status	100
0xE7	SSD Life Left	100
0xE9	Unknown Attribute	0
0xEA	Unknown Attribute	0

SSD wear-level and longevity indicators

### 13.2.4 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.



## 13.3 Notifying Users by Email About Status and Activity

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

Only the users you specify receive email notifications. You can specify which types of events generate email messages (Error, Informational, Warning). You can also specify if you want to be notified instantly when an event occurs to ensure that urgent issues receive immediate attention

from the right people. Alternatively, you can specify that you want events “coalesced” and receive only one email message for each event type.

Follow the instructions in this section to:

- Set up email notifications (see [13.3.1. Setting Up Email Notifications](#)).
- Send a test email (see [13.3.2. Sending a Test Message](#)).
- Modify or remove an email recipient (see [13.3.3. Modifying or Removing an Email Recipient](#)).
- Modify email server settings (see [13.3.4. Modifying Email Server Settings](#)).
- Disable email notifications (see [13.3.5. Disabling Email Notifications](#))

### 13.3.1 Setting Up Email Notifications

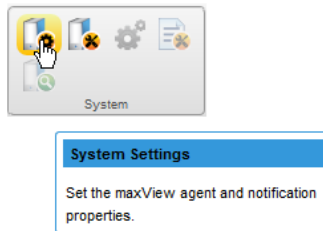
This section describes how to set up email notifications for one system. If you want to monitor multiple systems by email, you must complete the tasks in this section for each one separately.

Before you begin, note this information:

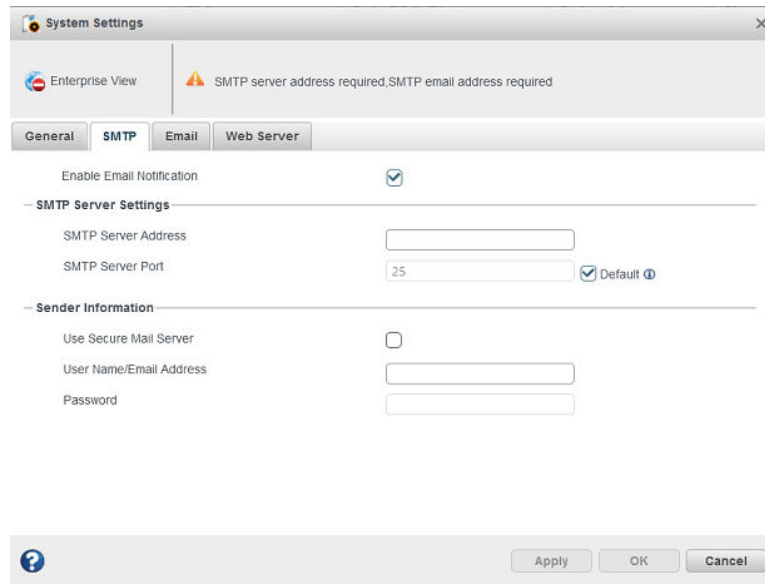
- The address of your Simple Mail Transfer Protocol (SMTP) server (host name and domain, or TCP/IP address)
- The email address of each person who will receive email notifications

To set up email notifications:

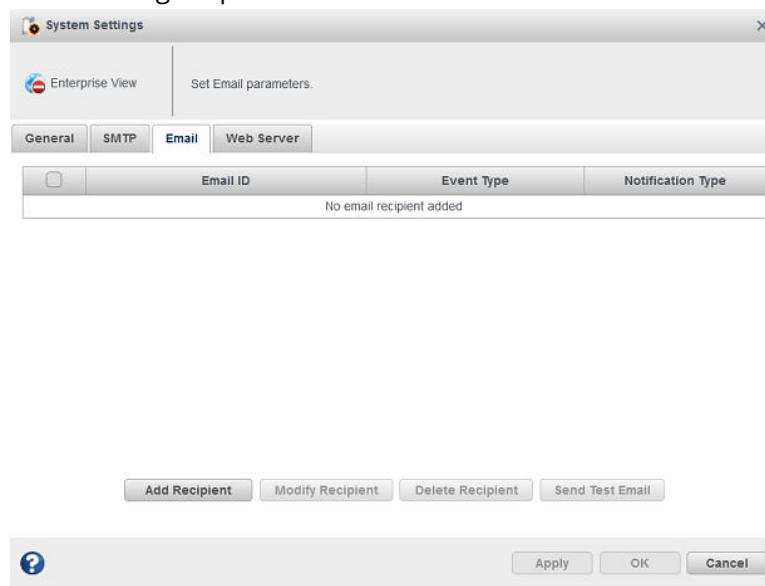
1. Select the Enterprise View node.
2. On the ribbon, in the System group, click **System Settings**.



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 Recipient**. When the Add Recipient 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 [13.2.1.1. What Do the Event Status Icons Mean?](#); for more information about the support archive file, see [15.5. Creating a Support Archive File](#).)

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

	Email ID	Event Type	Notification Type
<input type="checkbox"/>	richard_stanton@lantec.com	Error	Instant
<input type="checkbox"/>	ann_thomas@lantec.com	Error	Instant

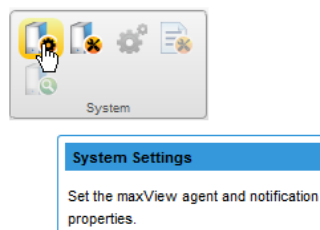
9. When you're done adding email recipients, click **OK**.  
The email recipients and your SMTP server settings are saved.
10. Repeat the steps in this section *for each system* you want to monitor with email notifications, then continue by sending test messages to all recipients (see [13.3.2. Sending a Test Message](#)).

### 13.3.2 Sending a Test Message

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

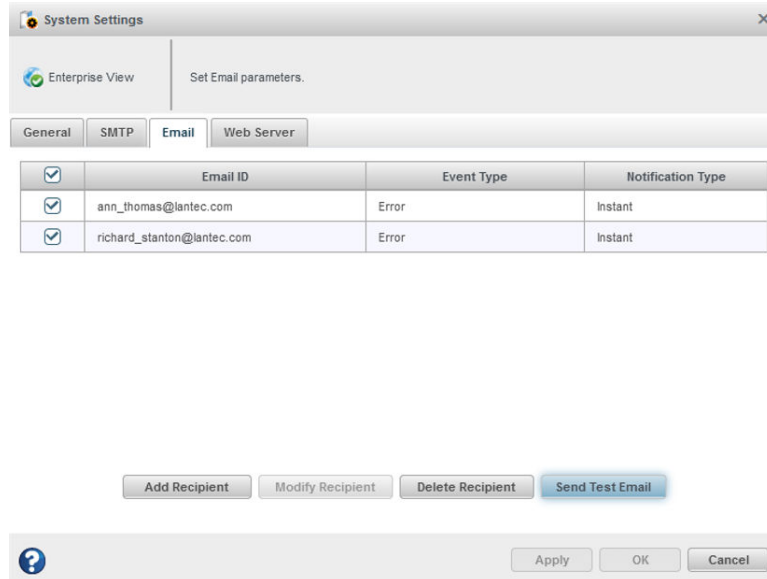
To send a test message:

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.

- 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.



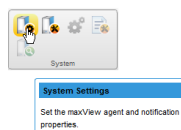
- Click **Send Test Email**.  
If the test is successful, the email recipient(s) receive the test message. If the test fails:
  - Ensure that the recipient's email address is correct. (See [13.3.3. Modifying or Removing an Email Recipient](#).)
  - Ensure that your SMTP server address is correct. (See [13.3.4. Modifying Email Server Settings](#).)
  - Try sending the test message again.

### 13.3.3 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:

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



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

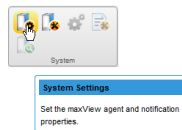
### 13.3.4 Modifying Email Server Settings

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.

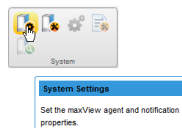
### 13.3.5 Disabling Email Notifications

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.

- Click **OK** to save your changes.

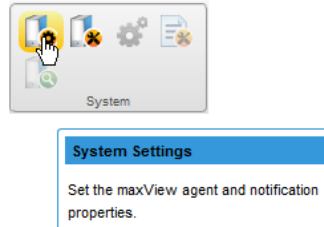
### 13.4 Changing an Operating System's Event Log Setting

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.

**Note:** This setting is not applicable for ESXi operating system.

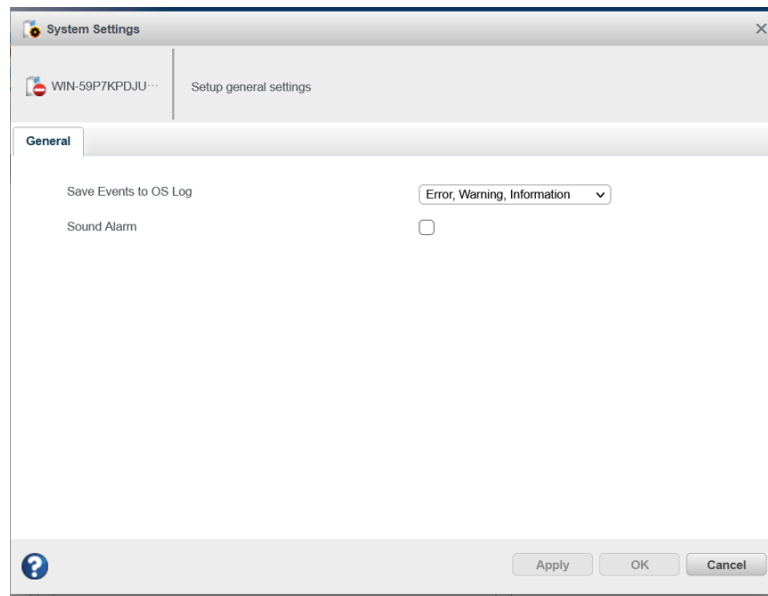
To change or disable operating system event logging on a system:

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



The System Settings window opens.

- In the Save Events to OS Log drop-down list, select the type of events that you want to log, then click **OK**.



- Restart maxView Storage Manager to apply the new setting.

## 14. 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

### 14.1 Deploying Servers

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

The basic procedure works like this:

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

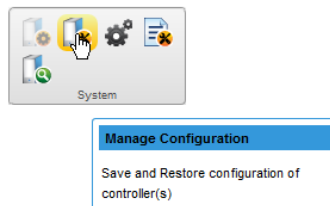
The following sections provide details on each of these steps.

#### 14.1.1 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:

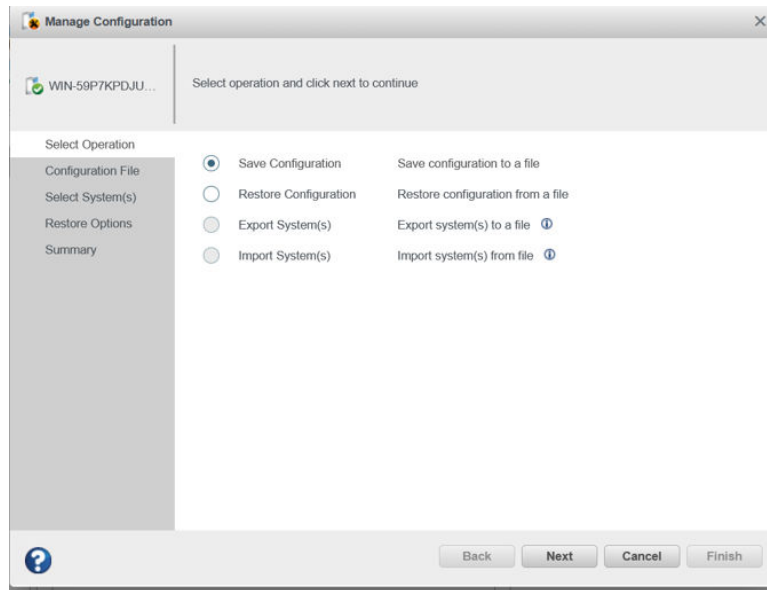
1. In the Enterprise View, select a system.
2. On the ribbon, in the System group, click **Manage Configuration**.



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 [14.1.2. Duplicating the Server Template](#) to deploy the same configuration on multiple systems in your storage space.

### 14.1.2 Duplicating the Server Template

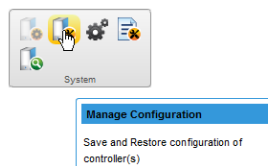
When you are ready to duplicate the server template on other systems in your storage space, you can restore the configuration from the server template file.

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%.

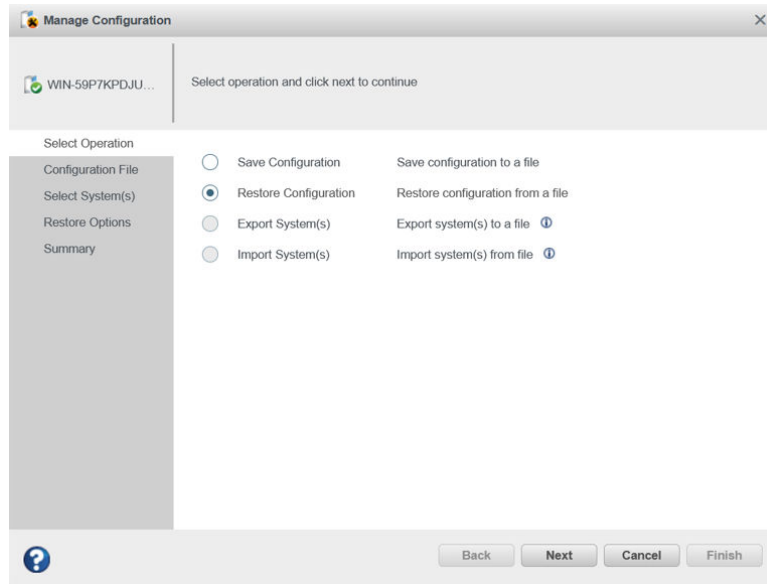
To duplicate the server template on another system:

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

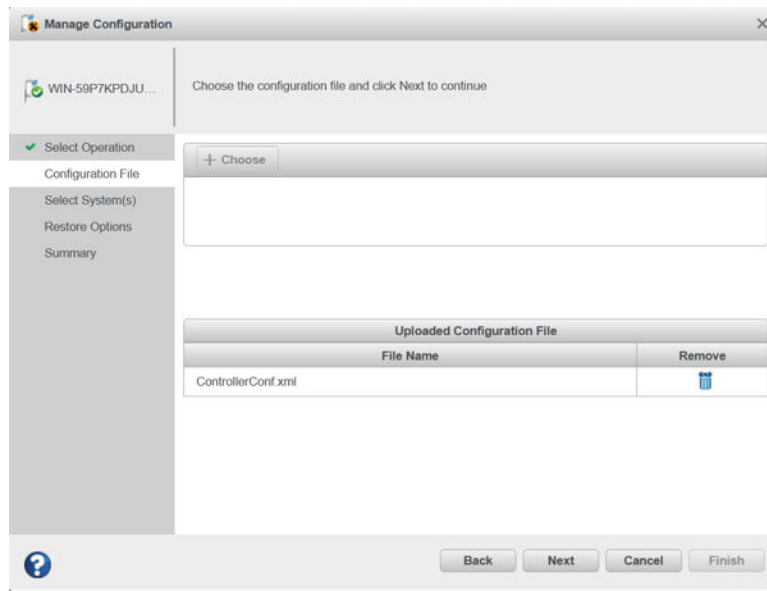


The Manage Configuration wizard opens.

3. Select **Restore Configuration**, then click **Next**.

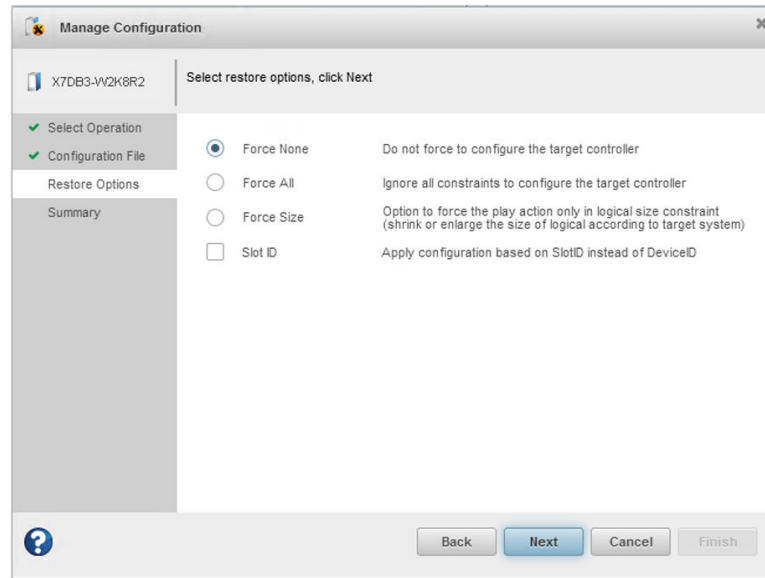


- In the Configuration File panel, click **Choose**, navigate the file system to your server template file, then click **Open**. When the file name appears in the "selected file" area, click **Upload**, wait for the upload to complete, then click **Next**.



- 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

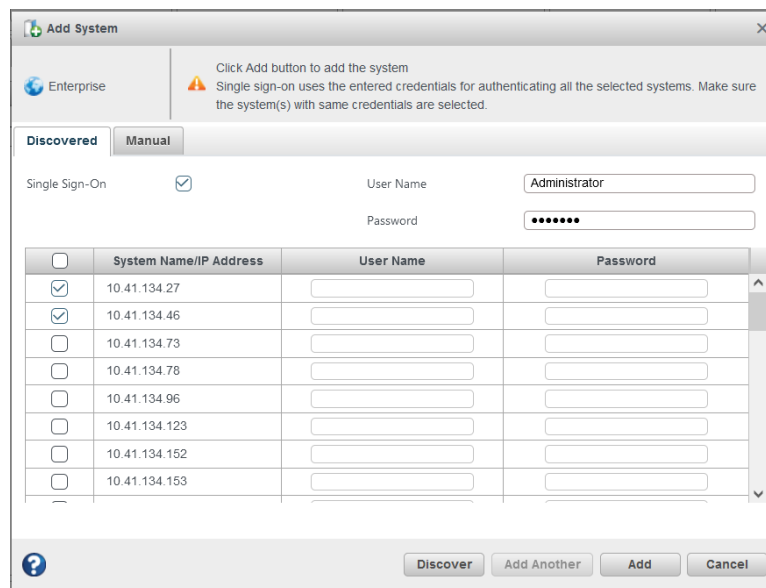


6. To apply the configuration based on SlotID rather than DeviceID, click the **Slot ID** check box.
7. Click **Next**, review the summary information, then click **Finish**.  
maxView Storage Manager duplicates the system configuration on the new controller.

## 14.2 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.



**Note:** Discover button gets enabled when "Enable auto discovery" check box is checked in System Settings dialog.

### 14.2.1 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.

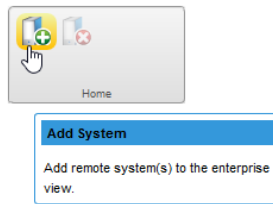
**Note:** The wizard adds all selected systems to the Enterprise view even if login fails on some systems. For those systems, try running the wizard again with different login credentials.

### 14.2.2 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 **Manual**.
3. Enter the system name and login credentials in the space provided. Select the Operating System from the drop down list and specify the Port number when applicable.

**Note:** **Discover** button gets enabled when "**Enable auto discovery**" check box is checked in **System Settings** dialog.

4. Click **Add**.  
maxView Storage Manager connects to the remote system and adds it to the Enterprise View.

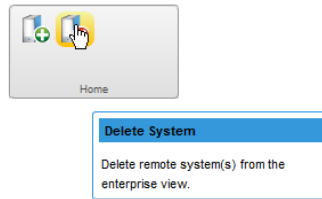
### 14.2.3 Removing a Remote System

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.

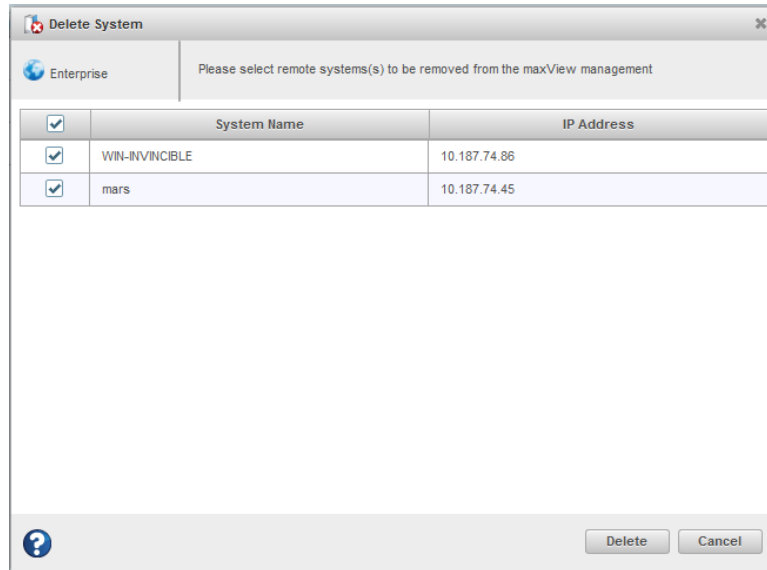
To remove a remote system:

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.



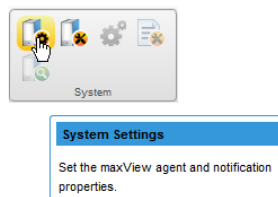
3. Click **Delete**.  
maxView Storage Manager removes the remote system(s) from the Enterprise View.

#### 14.2.4 Changing the Auto-Discovery Settings

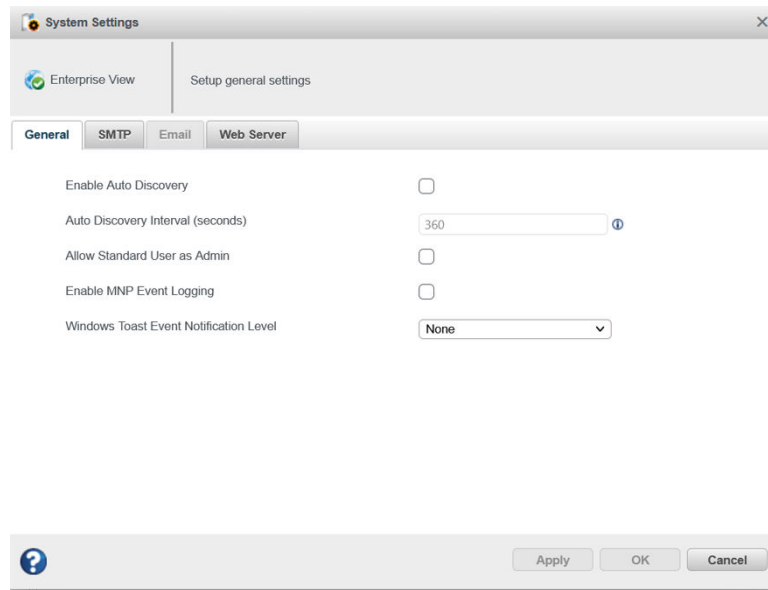
Auto-discovery, in maxView Storage Manager, is disabled by default. If enabled, the auto-discovery task runs in the background each time maxView Storage Manager is started. You can enable the auto-discovery if desired, and configure the auto-discovery settings as described in this section.

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 appears under **General** tab..



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.

### 14.2.5 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**.

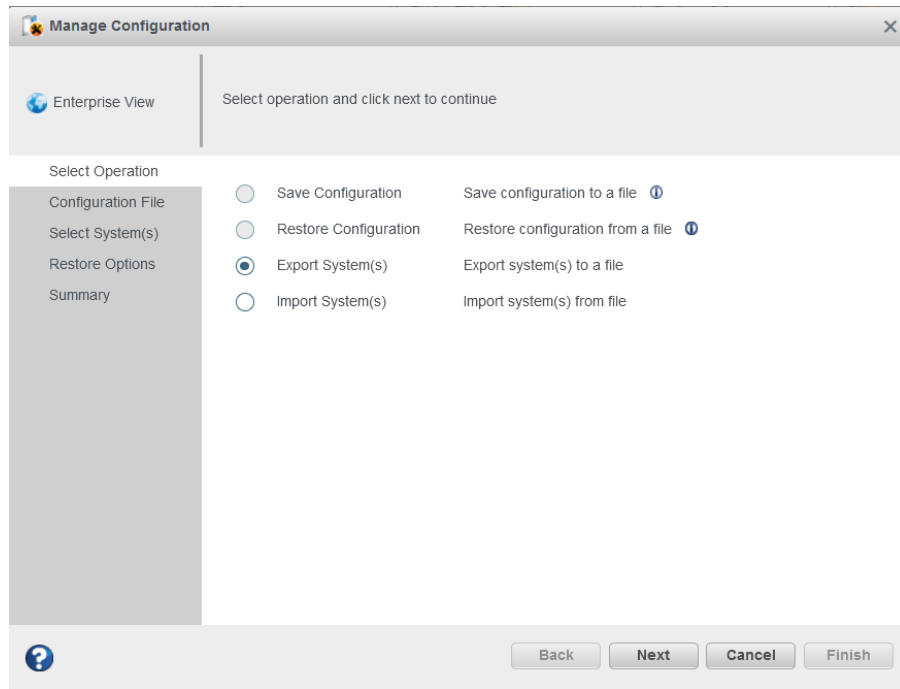


#### Manage Configuration

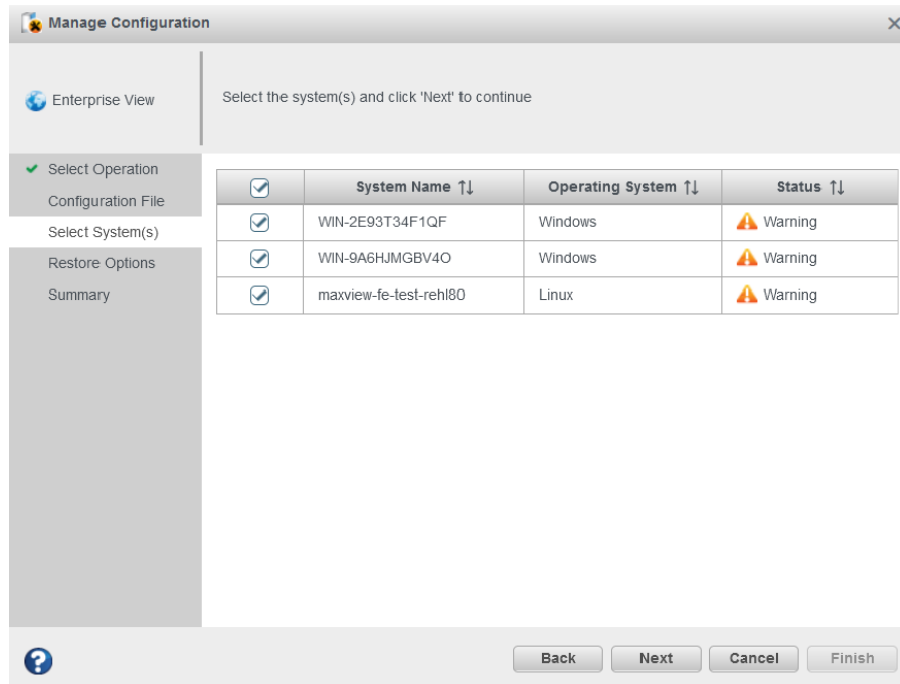
Save and Restore configuration of controller(s) on system node. Import and Export system(s) on the enterprise view node.

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.

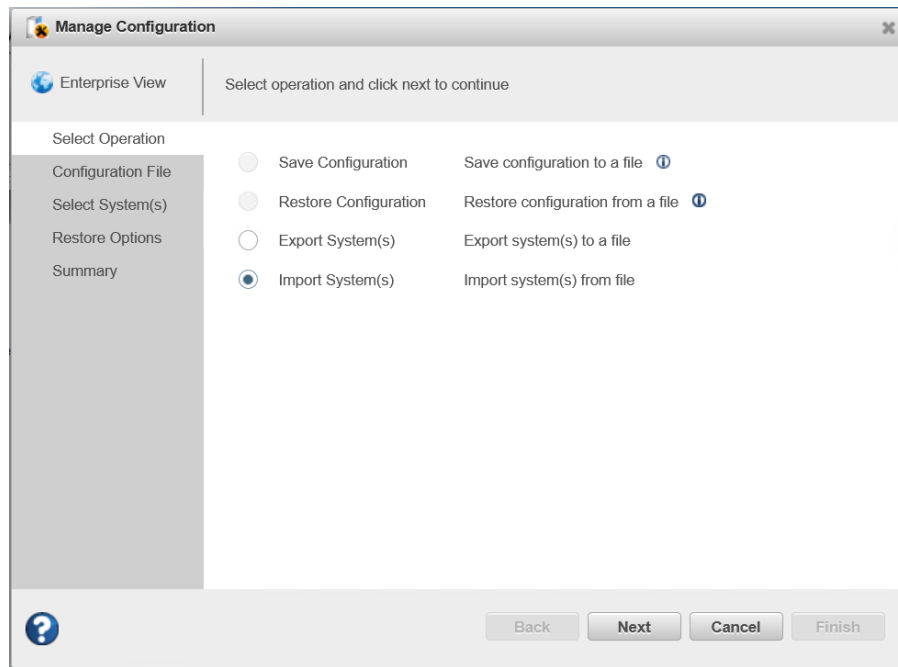
The **Manage Configuration Summary** page appears.

5. Click **Finish**.

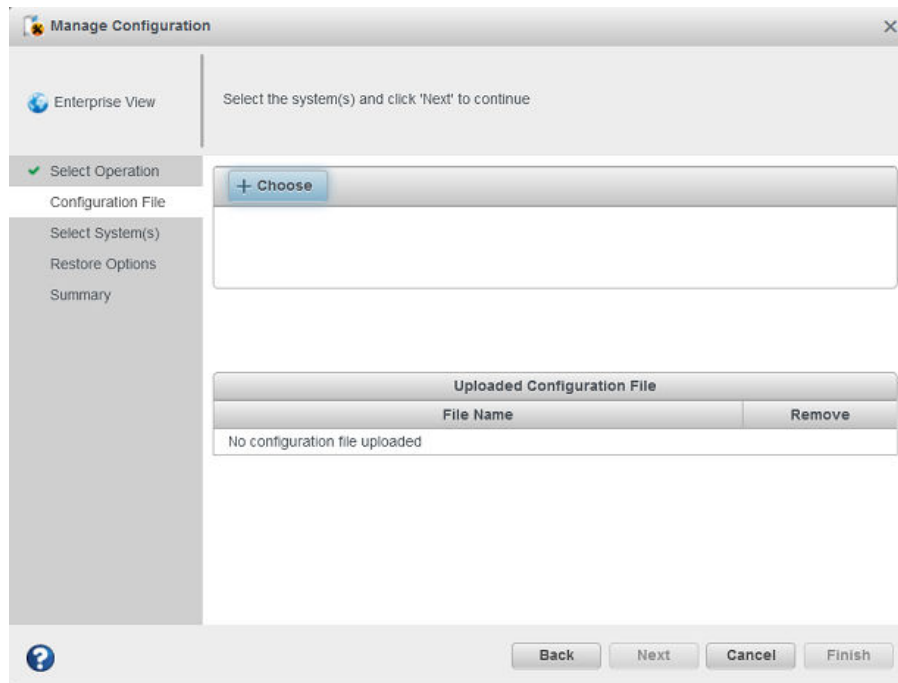
The exported systems are downloaded in a "SystemConf.json" file.

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.

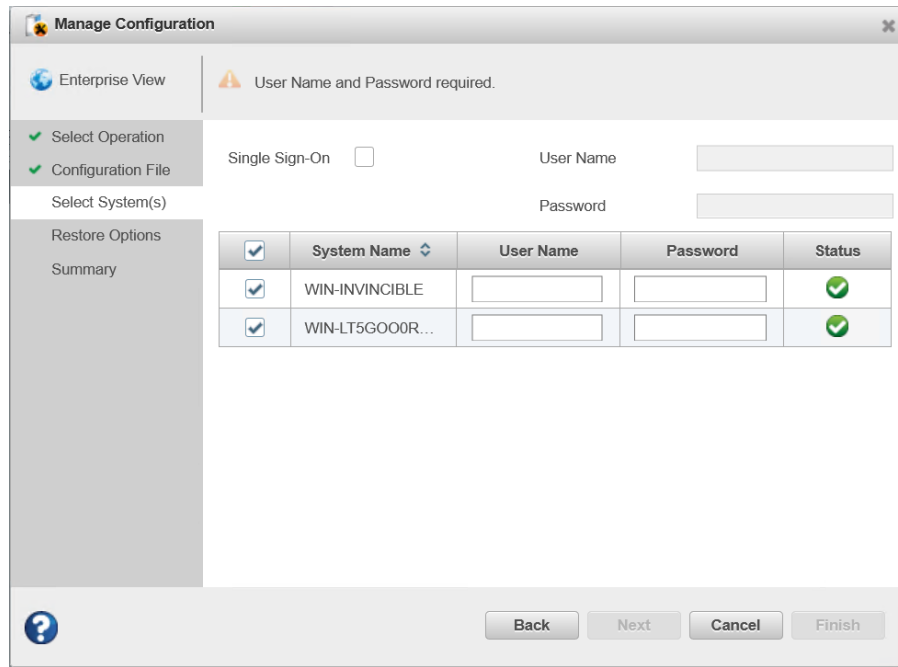
5. Click **Next**. The **Select Systems** screen appears.



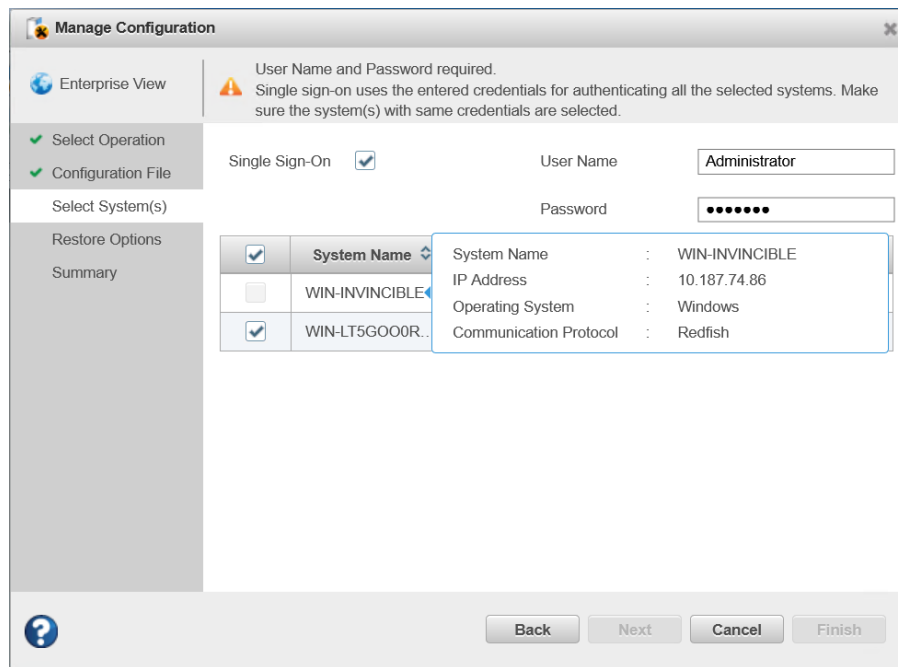
- Select the system name(s) and specify the login credentials. Select **Single Sign-On** option to specify the **User Name** and **Password** for all the selected systems that have same credentials. Otherwise, specify each system's credentials manually.

**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.



- Click **Next**.  
The **Manage Configuration Summary** page appears that shows the list of imported systems.
- Click **Finish**.

The imported systems will appear in the Enterprise View.

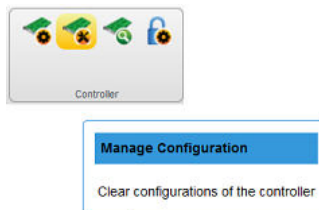
### 14.3 Clearing the Controller Configuration

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, 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.

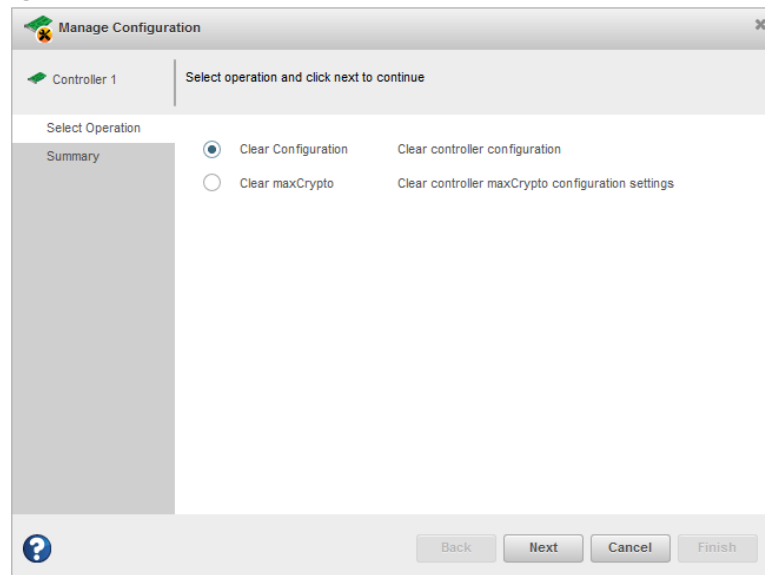
To clear the controller configuration:

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**.

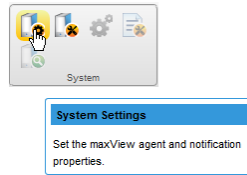
### 14.4 Changing the Web Server Port

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.

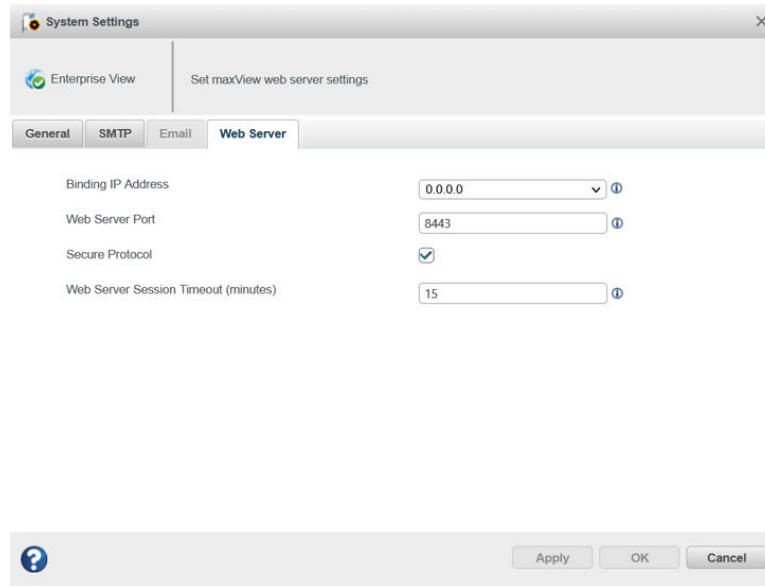
To change the Web Server port:

1. Select the Enterprise View node.

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



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



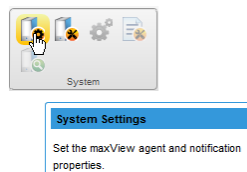
- Enter the new Web Server port. Optionally, click **Secured Protocol** to enable/disable secure communication over https.
- Click **Apply**.
- Restart maxView Storage Manager.

## 14.5 Granting Standard Users Admin Privilege

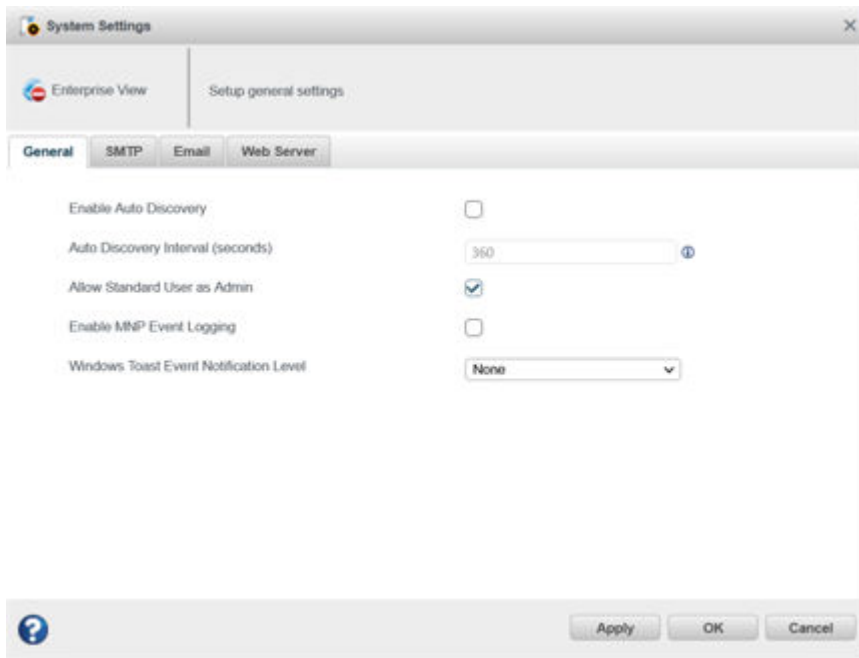
The standard users have restricted access to the storage space with limited ability to perform non-destructive operations in maxView Storage Manager (see [4.2. Working in maxView Storage Manager](#)). You can grant admin privileges to the standard users to accommodate changes in your system policies or IT requirements.

To grant admin privilege to standard users:

- Select the Enterprise View node.
- 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.

## 15. Solving Problems

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

### 15.1 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 [5.3. 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.

### 15.2 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.

The screenshot shows the Enterprise View hierarchy. Under 'WIN-V07FSIQGHQE', 'Controller 2' is expanded to show 'Arrays and Logical Devices'. 'Array3' is expanded to show 'LogicalDrive3' and 'LogicalDrive2', which are highlighted with a callout: "...affecting two Logical Drives". 'Physical Devices' is expanded to show 'Enclosure 0', which is further expanded to show 'Slot 1' and 'Slot 2'. 'Slot 2' is highlighted with a callout: "...and a physical device in Slot 2 in Enclosure 0. Click **Slot 2** to check the device status on the Storage Dashboard and continue tracing the fault to its source...".

The detailed view of 'Slot 2' shows a 'Disk drive' with the following properties:

Device		Status	
Type :	Disk drive	State :	Failed
Vendor :	Unknown	Negotiated transfer speed :	Failed
Model :	ST3250620NS	Write-cache mode :	Write back
Serial No :	5QE4MAS1	S.M.A.R.T warnings :	0
Firmware level :	3.AEK	SSD(non-spinning) :	false
Reported channel :	0	MaxCache capable :	Not supported

...a disk drive failure.

## 15.3 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 [15.3.1. 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 [15.3.3. Failure in Multiple Logical Drives Simultaneously](#).
- If it is a RAID 0 logical drive, see [15.3.4. Disk Drive Failure in a RAID 0 Logical Drive](#).
- If multiple disk drives fail within the same logical drive, see [15.3.5. Forcing a Logical Drive with Multiple Drive Failures Back Online](#).

### 15.3.1 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 failed drive is replaced, the dedicated hot spare drive will be back to hot spare state and can protect another drive failure.

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 [6. Protecting Your Data](#) for more information about managing spares.

### 15.3.2 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](#).

### 15.3.3 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](#).

### 15.3.4 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". For more details, see [6.6. Setting the Spare Activation Mode](#)

### 15.3.5 Forcing a Logical Drive with Multiple Drive Failures Back Online

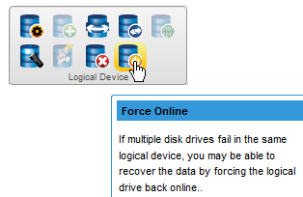
If multiple disk drives fail in the same logical drive, you may be able to recover the data by forcing the logical drive back online. For instance, if two drives fail in a RAID 5, forcing it online may allow you to access the data, depending on which disk drives failed.



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 [15.2. Identifying a Failed or Failing Component](#)).
2. On the ribbon, in the Logical Device group, click **Force Online**.



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

### 15.3.6 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 [7.6. Moving an Array](#)). It is available in the wizard only if:

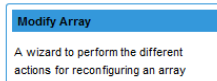
- The array has at least one failed drive.
- The array is not rebuilding to a spare.
- A sufficient number of Ready physical drives of the same type and correct size are available to replace each failed physical drive in the array.

**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.

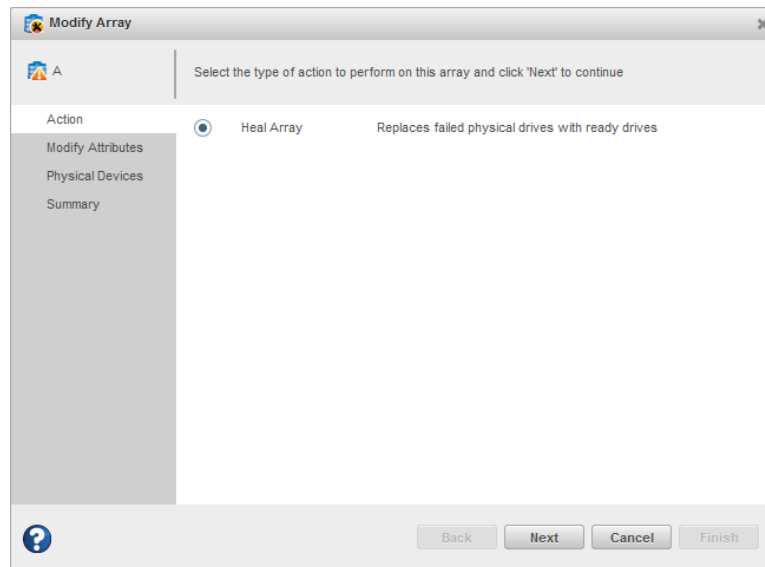
For a RAID 0 volume, the heal operation recreates the volume. For other RAID volume types, the heal operation rebuilds the volume.

To heal an array:

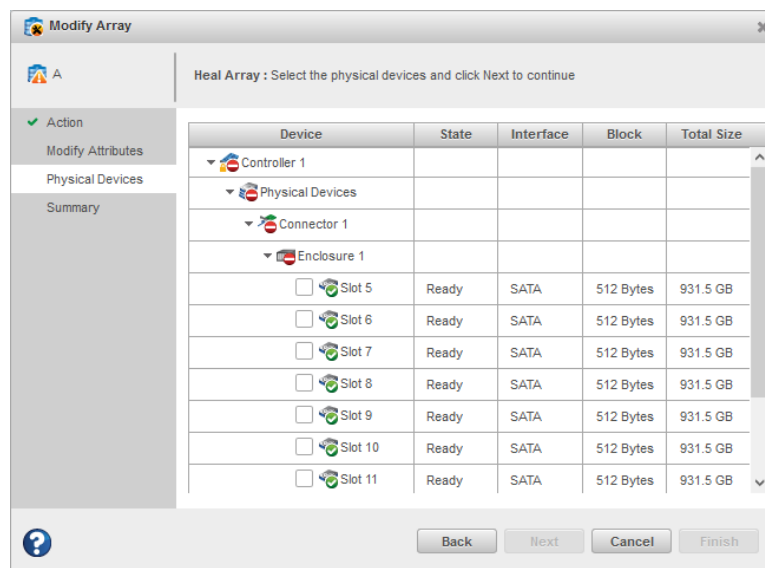
1. In the Enterprise View, select an array.
2. On the ribbon, in the Array group, click **Modify Array**.



- When the wizard opens, select **Heal Array**, then click **Next**.



- 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 [5.6.2. Modify Array](#).

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

## 15.4 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 [15.3.6. Healing an Array](#).

To start a hot-swap rebuild:

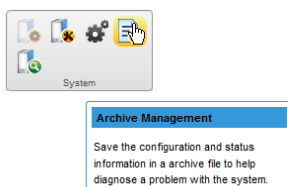
1. Following manufacturer's instructions, gently pull the failed disk drive from the server without fully removing it, then wait for it to spin down fully before continuing.
2. If there is nothing wrong with the disk drive, reinstall it, following manufacturer's instructions. If necessary, replace the 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.

## 15.5 Creating a Support Archive File

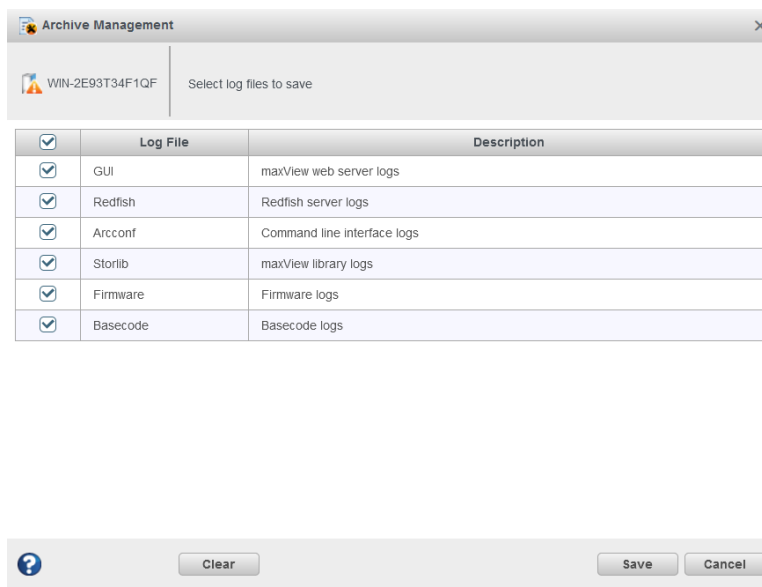
Your support representative might ask you to create a support archive file to help diagnose a problem with your system. Saved information includes device logs, drive logs, event logs, error logs, controller logs, history logs, and SMART statistics.

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.

## 16. 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.

### 16.1 Completing a Silent Installation

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

#### 16.1.1 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 [3.1.2. 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 [16.1.1.1. 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.

#### 16.1.1.1 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:\pvc.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\ <b>Note:</b> The default installation path is "C:\Program Files\Adaptec\maxView Storage Manager".
ADDLOCAL (optional)	<ul style="list-style-type: none"> <li>• ALL (default)—Installs the maxView Storage Manager GUI, Redfish server, and ARCCONF (CLI). If you specify ALL, do not specify any of the following values.</li> <li>• ARCCONF—Installs the Command Line Interface tool (ARCCONF)</li> <li>• RedfishServer—Installs the maxView Storage Manager Redfish Server</li> <li>• Console—Installs the maxView Storage Manager GUI</li> </ul> <b>Note:</b> Use commas to separate multiple values.
LOCALHOSTMODE	TRUE - Installs the maxView Storage Manager in the standalone mode. Standalone Mode is a highly secure option. No ports gets opened though firewall. User need to login to the system's local desktop to operate maxView. Standalone maxView cannot be managed remotely from another maxView.

.....continued	
Switch or Property	Description
DESKTOPWEBAPPLICATION	<p>TRUE - Installs the maxView Storage Manager in the desktop web application mode. Desktop web application mode does not install Tomcat/Redfish service. Desktop web application mode is a highly secure option.</p> <p>No ports get opened through the firewall. Users need to login to the system's local desktop to operate maxView. Desktop web application maxView cannot be managed remotely from another maxView installation.</p>

### 16.1.2 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 LOCALHOSTMODE=TRUE or DESKTOPWEBAPPLICATION=TRUE

**Note:** Linux systems also support silent upgrade and silent removal. See [16.2. Example Command Line Installations](#).

## 16.2 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):

```
rpm -e StorMan
```

## 17. 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.

### 17.1 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"
```

### 17.2 Setting Up SNMP Notifications on Linux

1. Install the Net-SNMP RPM packages:
  - net-snmp

- libsnmp15
  - snmp-mibs
2. In `/etc/snmp/snmpd.conf` configuration file:
    - 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
```

## 18. Using the maxView Plugin for VMware vSphere 7 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.

### 18.1 Installing the maxView Plugin for vSphere 7 HTML5 Client

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

VMware ESXi 7 and vCenter Server Appliance (VCSA) 7 versions are required to be 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 copying 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](https://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 certificate.  
**Note:** Check the JDK version. vCenter Server Appliance (VCSA) requires JDK 8 to run the plugin.

- The maxView plugin is placed either at [download.adaptec.com/raid/storage\\_manager/maxView-plugin.zip](https://download.adaptec.com/raid/storage_manager/maxView-plugin.zip) or, you can use the IP address of the machine where the 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 preceding step.

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

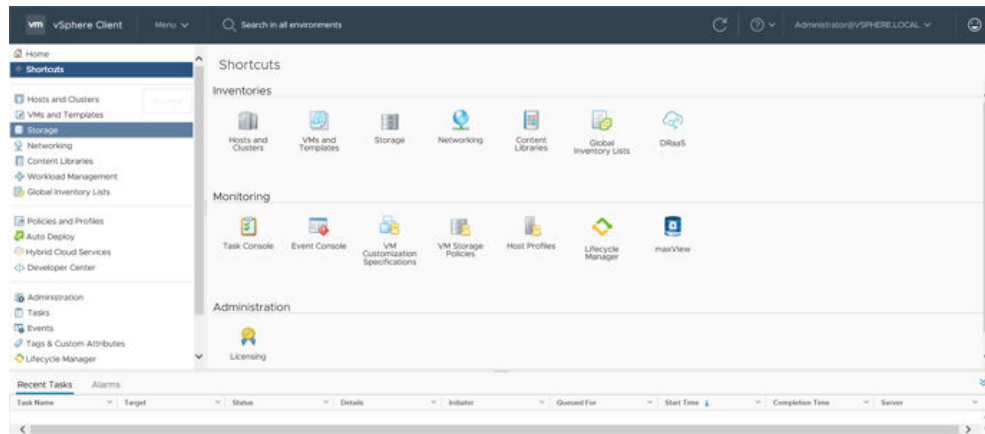
Once the maxView vSphere plugin is registered, the maxView icon is displayed in shortcut of vCenter Server Appliance ([https://VCSA\\_IP/ui/app/shortcuts](https://VCSA_IP/ui/app/shortcuts)).

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](https://VCSA_IP:5480). Click on the firewall and add the entry.  
**Note:** Replace VCSA\_IP with the user installed vCenter Server Appliance IP address.

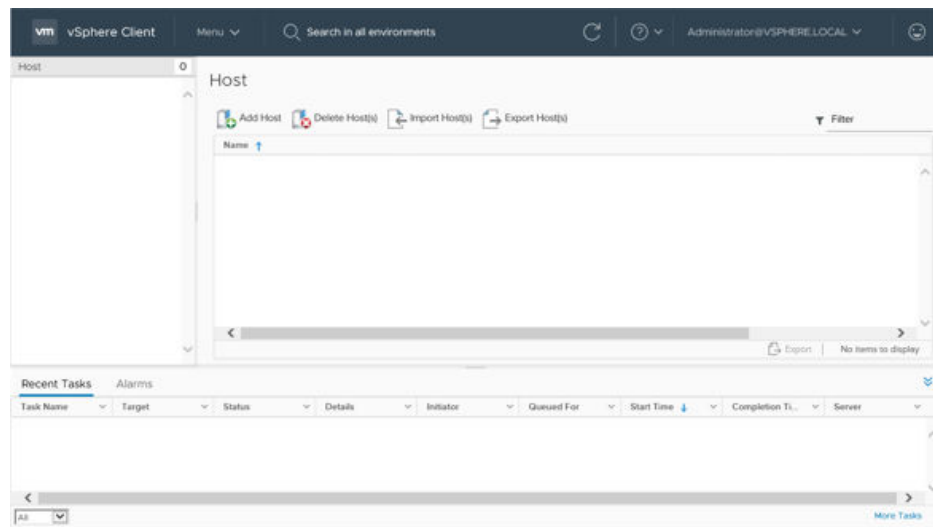
**Note:** The configuration or events are not delivered, if the firewall is not added.

## 18.2 Starting the maxView Plugin for vSphere 7 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.

Add Host
×

Hostname or IP Address	<input type="text" value="Hostname/IP Address"/>
Host Username	<input type="text" value="Username"/>
Host Password	<input type="password" value="Password"/> <span>👁</span>

CANCEL
ADD

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

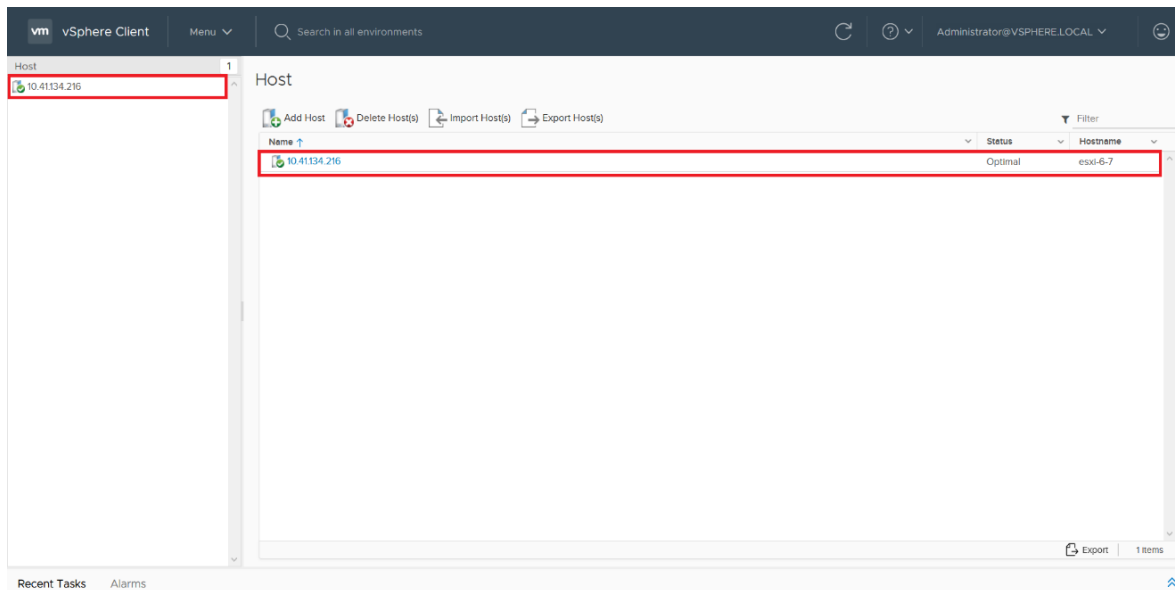
**Note:** Before adding the system, make sure to install the `arconf`, and `AdaptecRedfish_x.xx.xxxxx-MIS.x.x.x.xxxxxxxx_xxxxxxxx.zip` on the ESXi server.



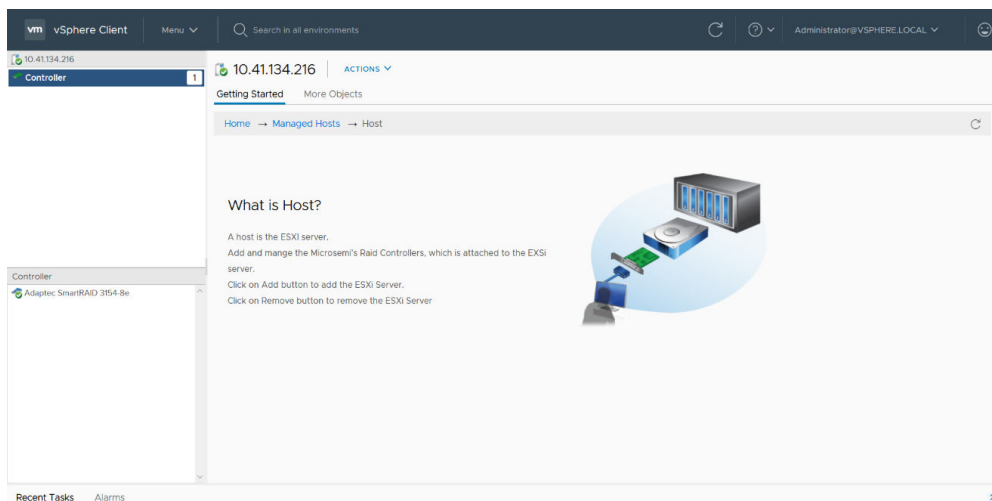
### 18.3 Monitoring maxView Resources in vSphere 7 HTML Client

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 18-1.** Host Tab Details

Tab	Details
Getting Started	Provide details on the ESXi server

.....continued

Tab	Details
More Objects	List the controller details

### 18.3.1 maxView vSphere Plugin Resources

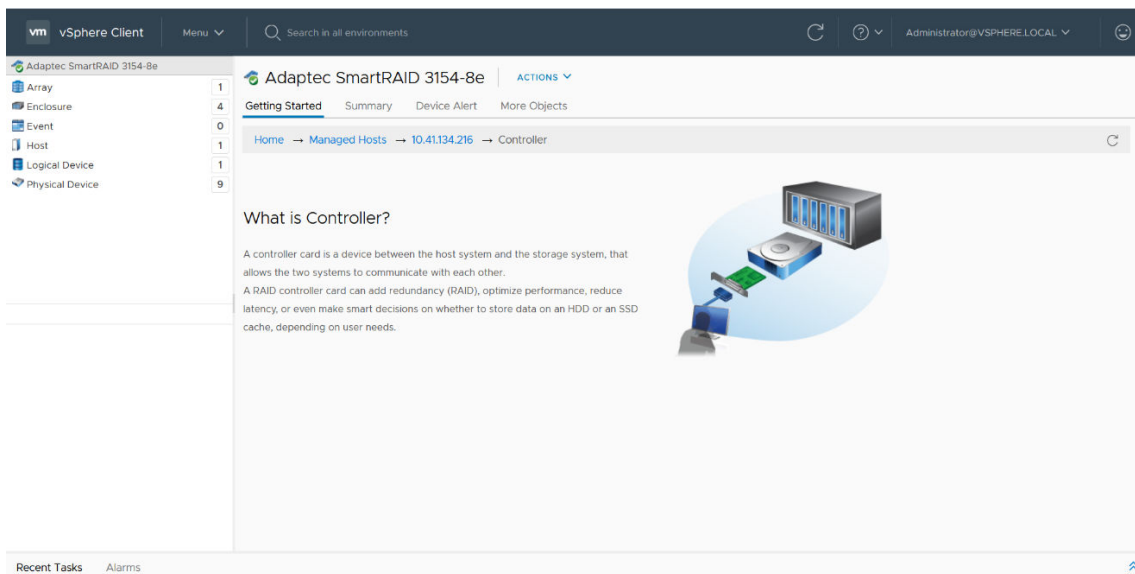
The following section describes the controller details of the maxView vSphere plugin.

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.

The screenshot displays the vSphere Client interface for an Adaptec SmartRAID 3154-8e controller. The main content area is divided into several sections:

- Summary Card:** Shows the controller's status as 'Optimal', WWN as '50000D1E00188AD0', Serial Number as '7A45F30008B', and Mode as 'Mixed'.
- Pie Chart:** Displays storage usage: Free Size (%) at 77.78 and Used Size (%) at 22.22.
- Controller Information Table:**

Controller Number	1
Firmware Version	2.89[106]
Driver Version	VMware 10.1.553-12vmw
Driver Name	smartpqi
Hardware Revision	B
- Settings Table:**

Post Prompt Timeout	15 sec
Rebuild Priority	High
Expand Priority	Medium
Consistency Check Mode	Idle
Consistency Check Delay	3 sec
Parallel Consistency Check	1
- Resources Table:**

Number of Arrays	1
Number of Logical Device	1
Number of Physical Device Count	9

## Device Alert Tab

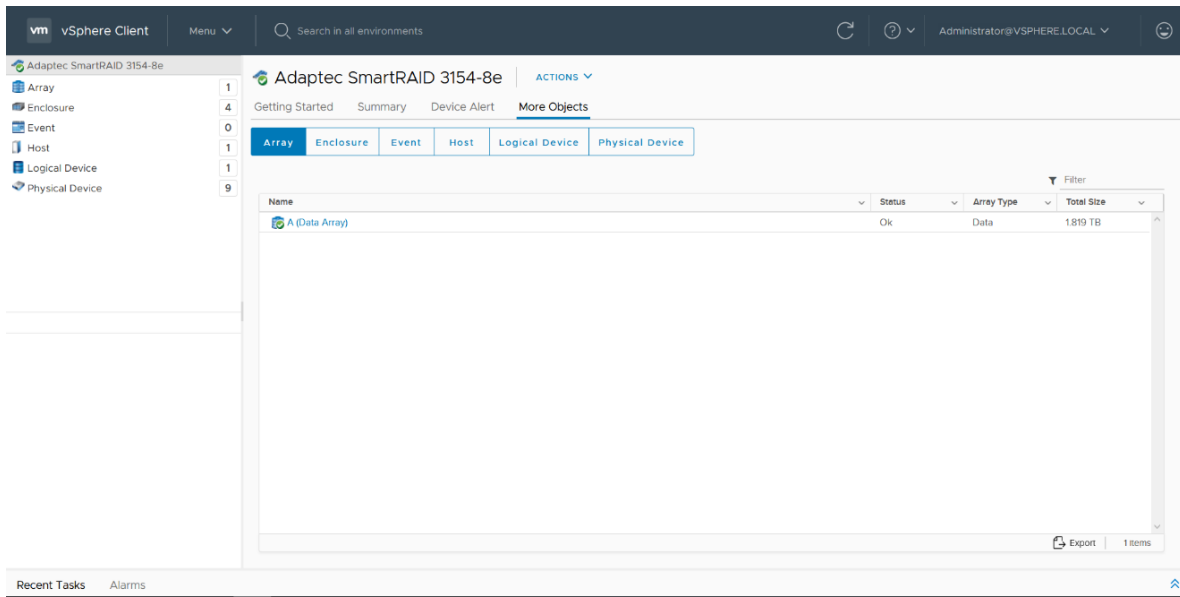
The **Device Alert** tab displays the information(s), warning(s), and errors(s) of the controller.

The screenshot displays the vSphere Client interface for the same Adaptec SmartRAID 3154-8e controller, but with the 'Device Alert' tab selected. The main content area shows a table of alerts:

Status	Message
	Device configuration has changed while using configuration based power settings. Controller ID : 0 ( Adaptec SmartRAID 3154-8e #7A45F30008B Physical Slot : 6 )
	A reboot will enable additional power savings. Controller ID : 0 ( Adaptec SmartRAID 3154-8e #7A45F30008B Physical Slot : 6 )
	HBA mode cannot be enabled on ports with logical devices. To enable HBA mode, please delete any logical devices on the port. Controller ID : 0 ( Adaptec SmartRAID 3154-8e #7A45F30008B Physical Slot : 6 )

## 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.

## 18.4 Import and Export Remote ESXi Systems using maxView Plugin in vSphere 7 HTML Client

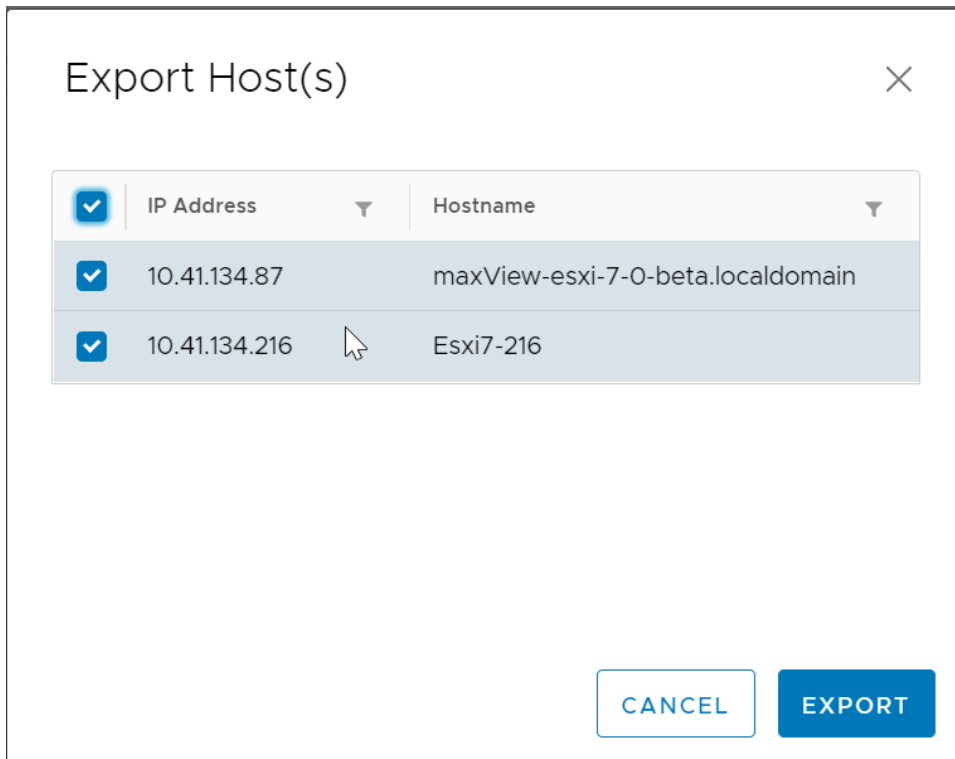
maxView plugin provides the Import and Export systems feature to add multiple systems and export the added systems in "SystemConf.json" file, which can be used later to import the added systems in maxView plugin running on another machine.

**Note:**

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

Perform the following steps to export the ESXi systems:

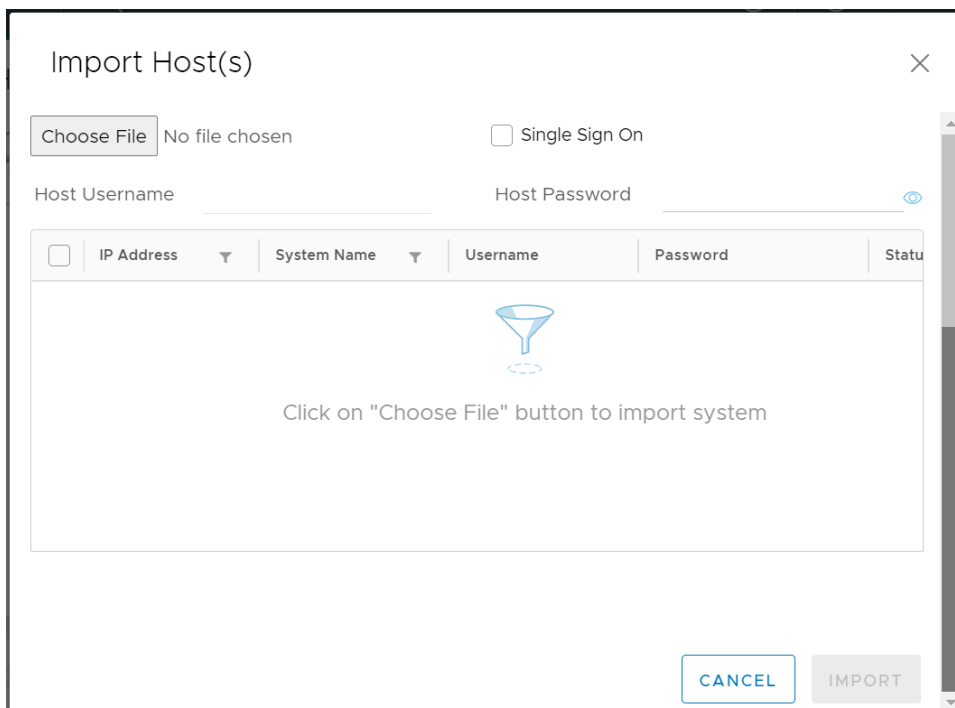
1. In the Monitoring section on the vSphere client's Shortcut page screen, click the **maxView** icon; the Host information screen appears.
2. Click on the **Export Host(s)** button.
3. Select the IP address of the system that need to be exported. Click **Export**.



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.

Import Host(s)

Choose File SystemConf.json  Single Sign On

Host Username \_\_\_\_\_ Host Password \_\_\_\_\_

<input type="checkbox"/>	IP Address	System Name	Username	Password	Status
<input type="checkbox"/>	10.41.134.87	maxView-esxi-7-...	_____	_____	<input type="checkbox"/> ✓
<input type="checkbox"/>	10.41.134.216	Esxi7-216	_____	_____	<input type="checkbox"/> ✓

CANCEL IMPORT

- 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.

Import Host(s)

Choose File SystemConf.json  Single Sign On

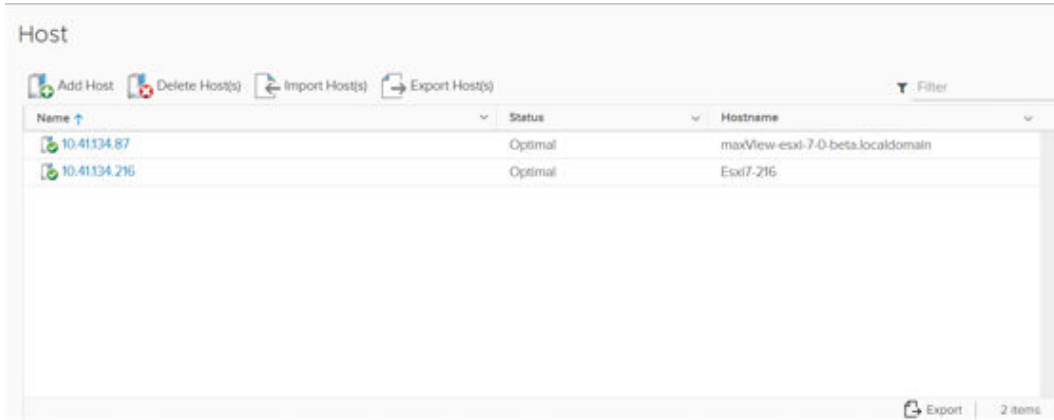
Host Username \_\_\_\_\_ Host Password \_\_\_\_\_

<input checked="" type="checkbox"/>	IP Address	System Name	Username	Password	Status
<input checked="" type="checkbox"/>	10.41.134.87	maxView-esxi-7-...	root	.....	<input checked="" type="checkbox"/> ✓
<input checked="" type="checkbox"/>	10.41.134.216	Esxi7-216	root	.....	<input checked="" type="checkbox"/> ✓

CANCEL IMPORT

- Click **Import**.  
A **Status** message box appears stating that the "System added successfully".
- Click **Close** and refresh the screen.

The imported systems will appear under the Host screen.



## 19. Using the maxView Plugin for VMware vSphere 8 HTML5

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

### 19.1 Installing the maxView Plugin for vSphere 8 HTML5 Client

Follow the instructions in this section to install the maxView vSphere 8 Plugin HTML5 on a vCenter Server Appliance.

VMware ESXi 7, VMware ESXi 8, and vCenter Server Appliance (VCSA) 8 versions are required to be 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 the following steps to install the maxView vSphere plugin:
  - Copy `maxview-plugin-1.0.0.jar` and `maxview_plugin_Installation.sh` to vCenter Server
  - Run the `maxview.sh` from the same location and provide the following information:
    - vCenter Server GUID: To retrieve vCenter Server GUID, perform the following steps:
      1. Login to vCenter Server appliance.
      2. Navigate to the inventory and copy the GUID from the URL. See the following figure to retrieve vCenter Server GUID from the URL:
    - vCenter Server FQDN: IP address of the vCenter Server Appliance
    - vCenter Server Thumbprint: The vCenter Server Appliance SHA1 Thumbprint. See [Retrieve SHA1 Thumbprint](#) to retrieve SHA1 Thumbprint.
5. Execute the following steps to install the maxView vSphere plugin.
  - a. Navigate to `\html-client-sdk\tools\vCenter plugin registration\prebuilt\` location that contains the plugin registration script.
  - b. Run the following command to register the plugin from the Windows machine

```
extension-registration.bat -action registerPlugin -remote -url https://
IP_Address /sdk -username Username -password Password --vcenterServerThumbprint
vcenterServerThumbprint -key com.mchp.maxview.maxviewvsphere -version 1.0.0
-pluginUrl https:// IP_Address:8443/maxView-ui/plugin.json -serverThumbprint
ServerThumbprint -c "2023 Microchip Technology Inc." -n "maxView Remote Plugin" -s
"This is maxView Remote Plugin"
```

**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
  - `Password` is the password of the vCenter Server Appliance
  - `vcenterServerThumbprint` is the vCenter Server Appliance SHA1 Thumbprint
- Note:** `ServerThumbprint` is the SHA256 Thumbprint of `https:// IP_Address:8443/maxView-ui/plugin.json`.



- c. 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
- `Password` is the password of the vCenter Server Appliance
- `vcenterServerThumbprint` is the vCenter Server Appliance SHA1 Thumbprint

Once the maxView vSphere plugin is registered, the maxView icon is displayed in shortcut of vCenter Server Appliance ([https://VCSA\\_IP/ui/app/shortcuts](https://VCSA_IP/ui/app/shortcuts)).

- Click on the maxView icon to list the ESXi systems added.
 

**Note:** Initially, none of the system are added.
- Click on **Add system** to add the ESXi systems.
- Add the firewall entry by using URL: [https://VCSA\\_IP: 5480](https://VCSA_IP:5480). Click on the firewall and add the entry.
 

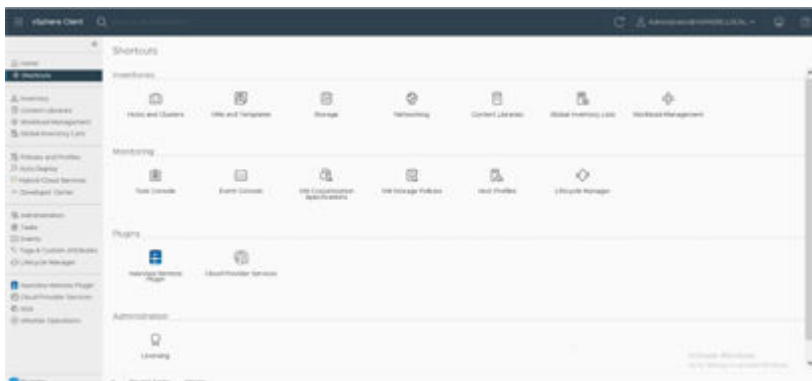
**Note:** Replace VCSA\_IP with the user installed vCenter Server Appliance IP address.

**Note:** The configuration or events are not delivered, if the firewall is not added.

## 19.2 Starting the maxView Plugin for vSphere 8 HTML Client

Perform the following steps to start the maxView Plugin:

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



The maxView plugin loads and displays add system dialog.

- Click on the **Add System** icon to add and manage the ESXi host.

The **Add System** dialog box opens.

5. Enter the following credentials:
  - Hostname or IP address of the ESXi Server
  - Username and password of the ESXi Server
  - Operating System of the ESXi Server
6. Click the **Add** button.  
The status dialog is displayed with success or failure status.
7. Click **OK**.
8. Click on **Global Refresh** icon to display the new added system in the list.

**Note:** Before adding the system, make sure to install the `arconf` and `AdaptecRedfish_x.xx.xxxxx-MIS.x.x.x.xxxxxxxxxxxxx_xxxxxxxxx.zip` on the ESXi server.

## 19.3 Monitoring maxView Resources in vSphere 8 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").

### 19.3.1 maxView vSphere Plugin Resources

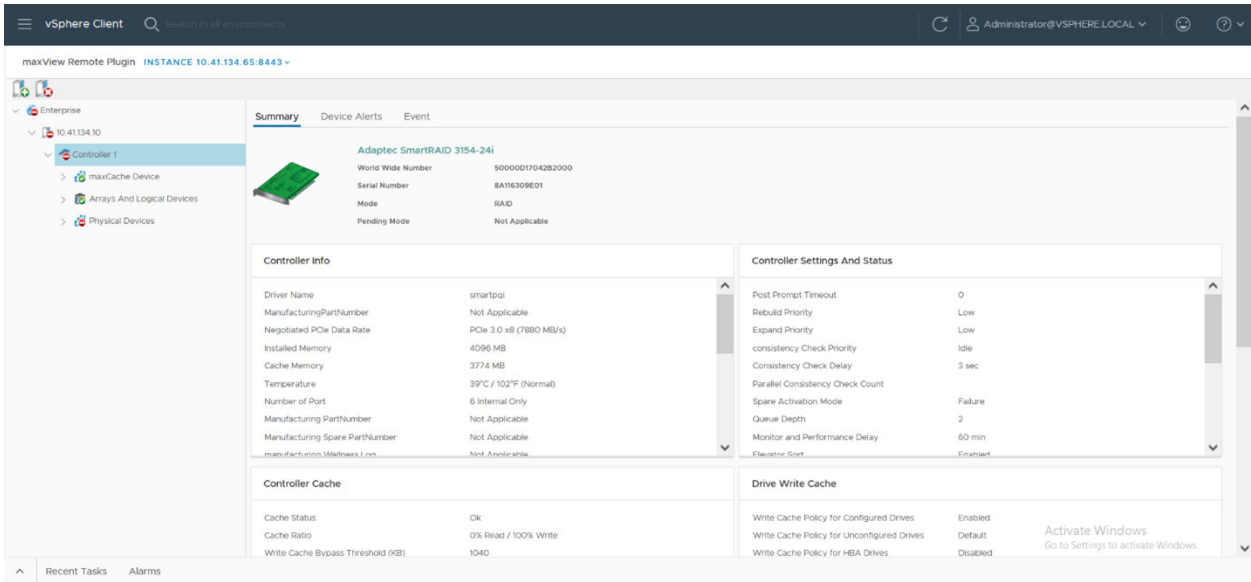
The following section describes the controller details of the maxView vSphere plugin.

The controller has the following four tabs:

- Summary
- Device Alert
- Event

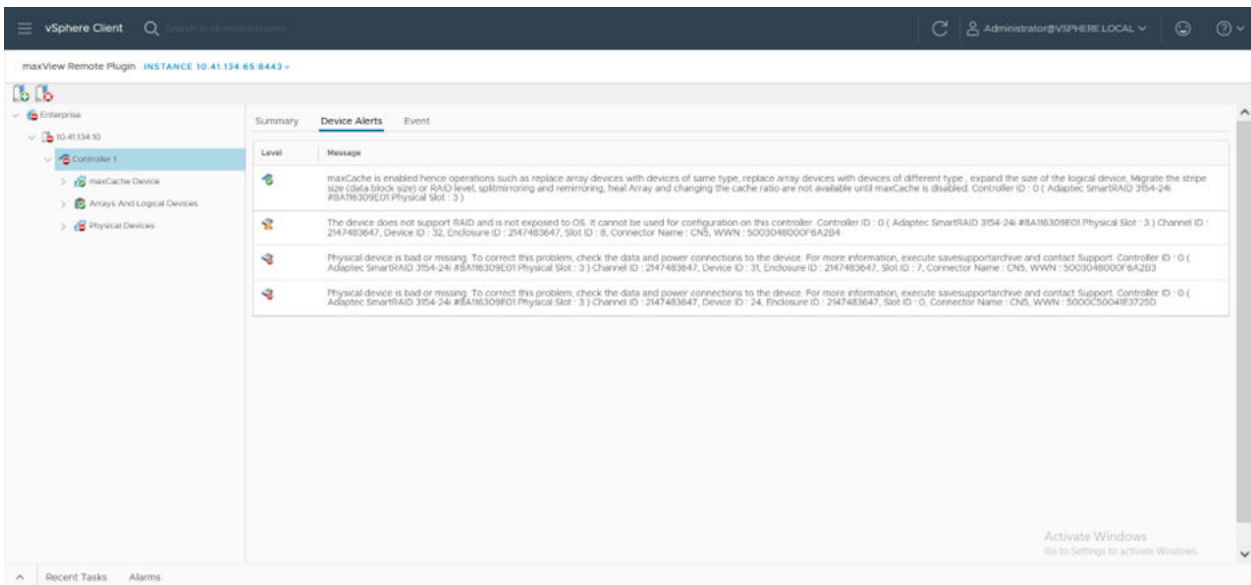
#### Summary Tab

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



### Device Alert Tab

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



### Event Tab

**Event tab** provides at-a-glance status information about activity (or *events*) occurring in the node. All Information, Error, and Warning level events are recorded.

Severity	Date And Time	System	Source	Component	Description
Information	09/22/2022 09:12:32	maxView-frontend-test- esxi8.microchip.com	Controller 1	Controller 1	Controller expander minimum scan duration changed from 10 seconds to 5 seconds: controller 1 ( Adaptec SmartRAID 3154-24i #8A116309E01 Physical Slot: 3 )
Information	09/22/2022 09:12:22	maxView-frontend-test- esxi8.microchip.com	Controller 1	Controller 1	Controller expander minimum scan duration changed from 74 seconds to 10 seconds: controller 1 ( Adaptec SmartRAID 3154-24i #8A116309E01 Physical Slot: 3 )
Information	09/22/2022 09:11:57	maxView-frontend-test- esxi8.microchip.com	Controller 1	Controller 1	HDD Flexible Latency Optimization changed from Disabled to Aggressive level-2 (10ms): controller 1 ( Adaptec SmartRAID 3154-24i #8A116309E01 Physical Slot: 3 ).
Information	09/22/2022 09:11:21	maxView-frontend-test- esxi8.microchip.com	Controller 1	Controller 1	Controller Queue Depth changed from 2 to 16: controller 1 ( Adaptec SmartRAID 3154-24i #8A116309E01 Physical Slot: 3 ).
Information	09/22/2022 09:07:35	maxView-frontend-test- esxi8.microchip.com	Controller 1	Controller 1	Controller expander minimum scan duration changed from 0 seconds to 74 seconds: controller 1 ( Adaptec SmartRAID 3154-24i #8A116309E01 Physical Slot: 3 )
Information	09/22/2022 09:07:35	maxView-frontend-test- esxi8.microchip.com	Controller 1	Controller 1	Controller Rebuild Priority changed from High to Low: controller 1 ( Adaptec SmartRAID 3154-24i #8A116309E01 Physical Slot: 3 ).
Information	09/22/2022 09:07:35	maxView-frontend-test- esxi8.microchip.com	Controller 1	Controller 1	Controller Expand Priority changed from High to Low: controller 1 ( Adaptec SmartRAID 3154-24i #8A116309E01 Physical Slot: 3 ).

**Note:**

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

## 19.4 Import and Export Remote ESXi Systems using maxView Plugin in vSphere 8 HTML Client

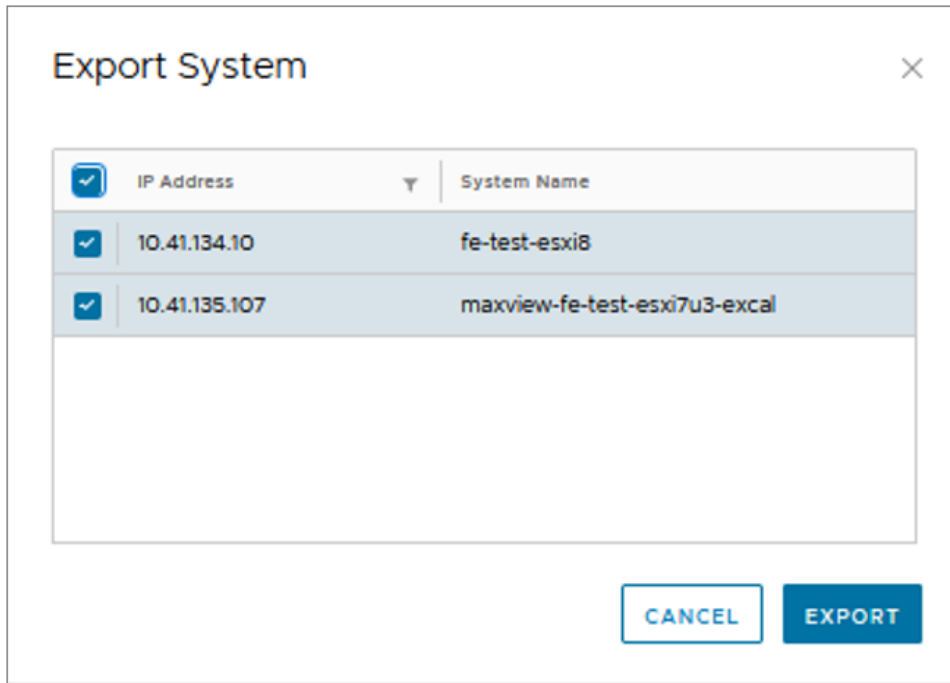
maxView plugin provides the Import and Export systems feature to add multiple systems and export the added systems in "SystemConf.json" file, which can be used later to import the added systems in maxView plugin running on another machine.

**Note:**

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

Perform the following steps to export the ESXi systems:

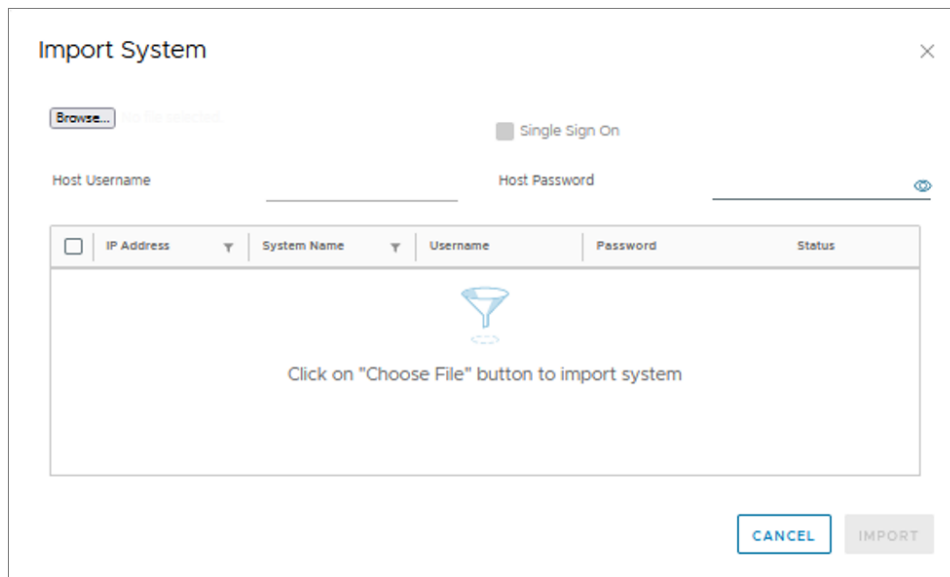
1. In the Monitoring section on the vSphere client's Shortcut page screen, click the **maxView** icon; the Host information screen appears.
2. Click on the **Export System** button.
3. Select the IP address of the system that need to be exported. Click **Export**.



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 System** screen appears.



2. Click **Browse** to specify the path of the “SystemConf.json” file.

Import System ×

System Name (Optional)

Single Sign On

Host Username  Host Password

<input type="checkbox"/>	IP Address	System Name	Username	Password	Status
<input type="checkbox"/>	10.41.135.107	maxview-fe-test-...	<input type="text"/>	<input type="password"/>	✓
<input type="checkbox"/>	10.41.134.10	fe-test-esxi8	<input type="text"/>	<input type="password"/>	✓

- 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.

Import System ×

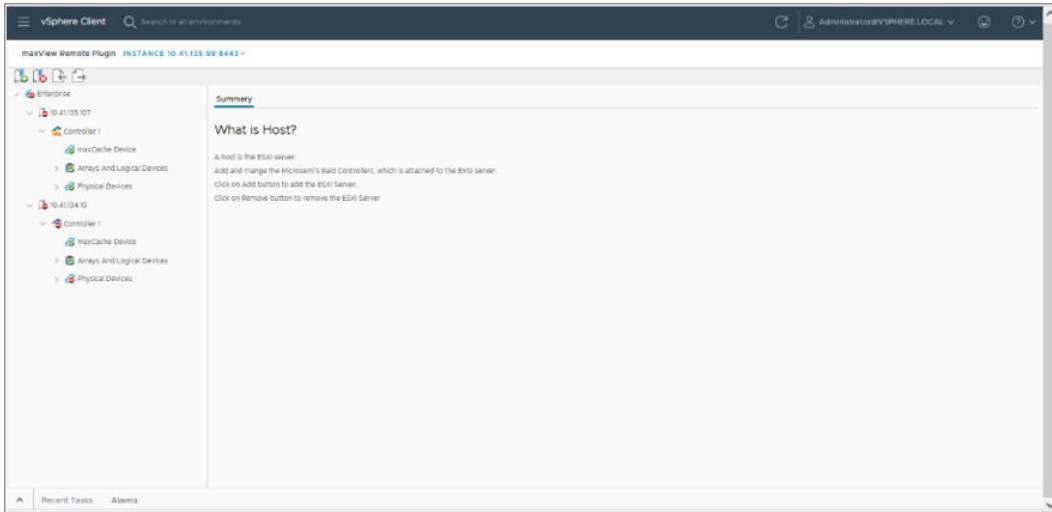
System Name (Optional)

Single Sign On

Host Username  Host Password

<input checked="" type="checkbox"/>	IP Address	System Name	Username	Password	Status
<input checked="" type="checkbox"/>	10.41.135.107	maxview-fe-test-...	root	*****	✓
<input checked="" type="checkbox"/>	10.41.134.10	fe-test-esxi8	root	*****	✓

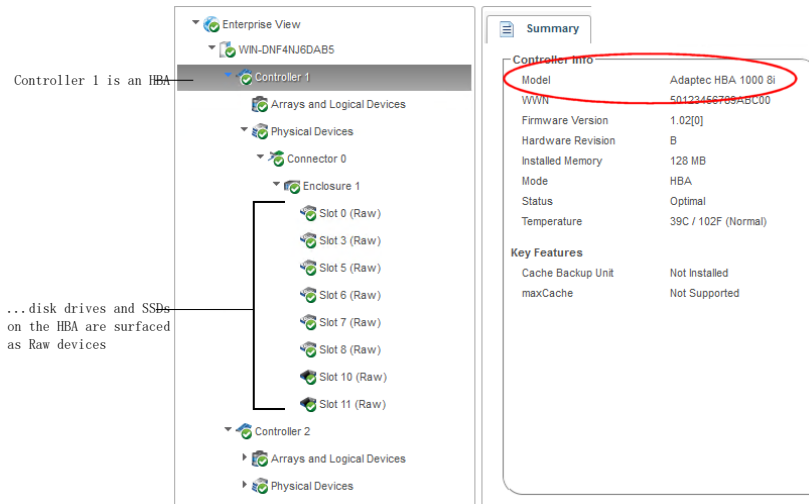
- Click **Import**.  
A **Status** message box appears stating that the "System added successfully".
- Click **Close** and refresh the screen.  
The imported systems will appear under the Host screen.



## 20. 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 [12.10.3. 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 [13.2.3. 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 [13.2.1. 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 <a href="#">13.2.3.2. Monitoring Enclosure Status</a> ) 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 <a href="#">13.2.3.3. Viewing SMART Statistics</a> )

## 21. 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.

### 21.1 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

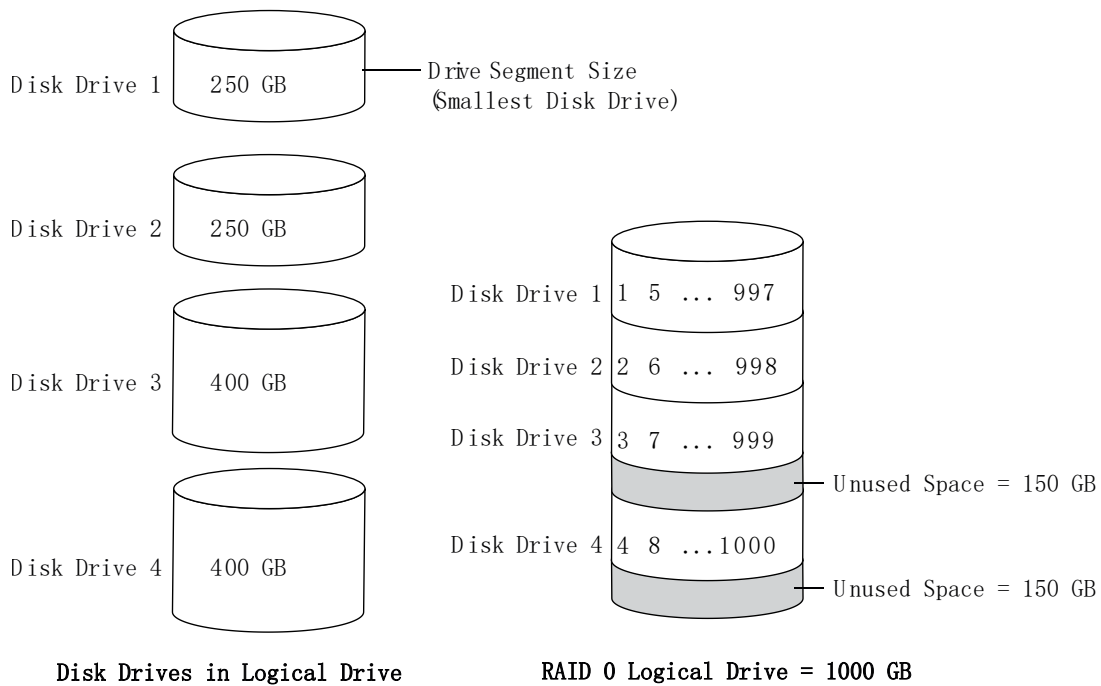
Disk drive usage, read performance, and write performance depend on the number of drives in the logical drive. In general, the more drives, the better the performance.

### 21.2 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.

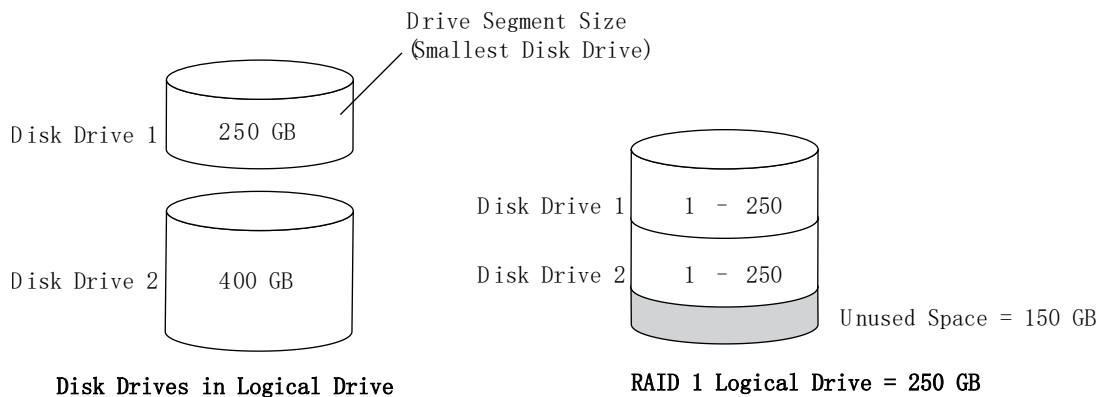
Drive segment size is limited to the size of the smallest disk drive in the logical drive. For instance, an array with two 250 GB disk drives and two 400 GB disk drives can create a RAID 0 drive segment of 250 GB, for a total of 1000 GB for the volume, as shown in this figure.



### 21.3 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.

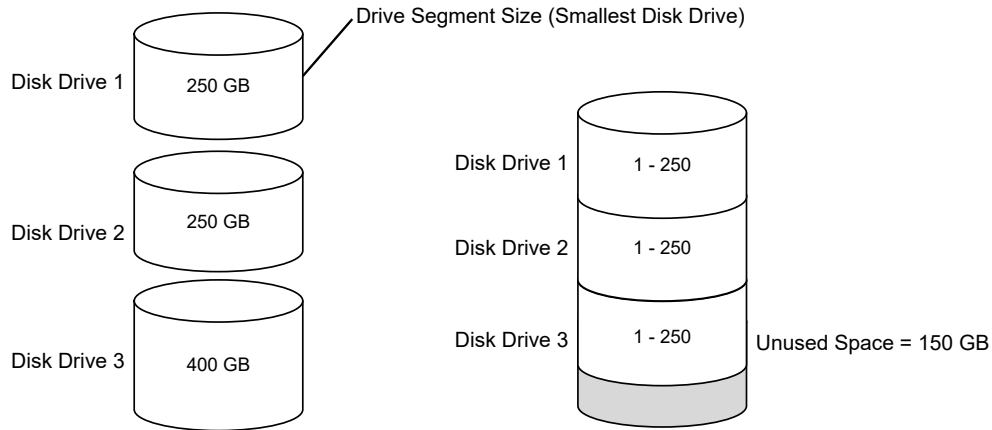
If the RAID 1 logical drive is built from different-sized disk drives, the free space, drive segment size is the size of the smaller disk drive, as shown in this figure.



### 21.4 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 data.

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



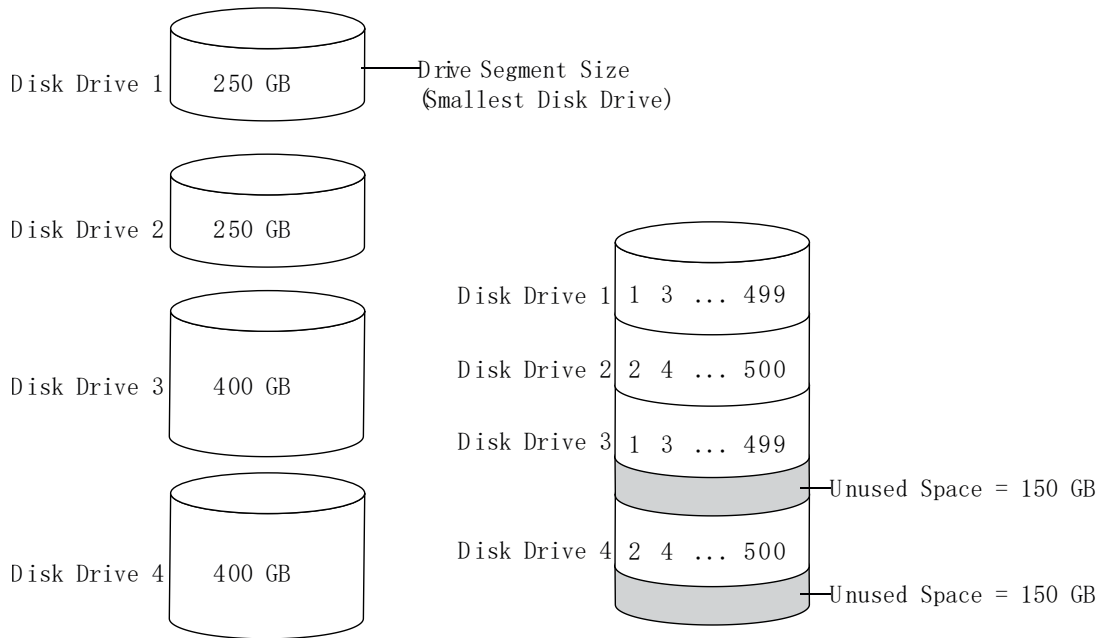
Disk Drives in Logical Drive

RAID 1 Triple Logical Drive = 250 GB

### 21.5 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.



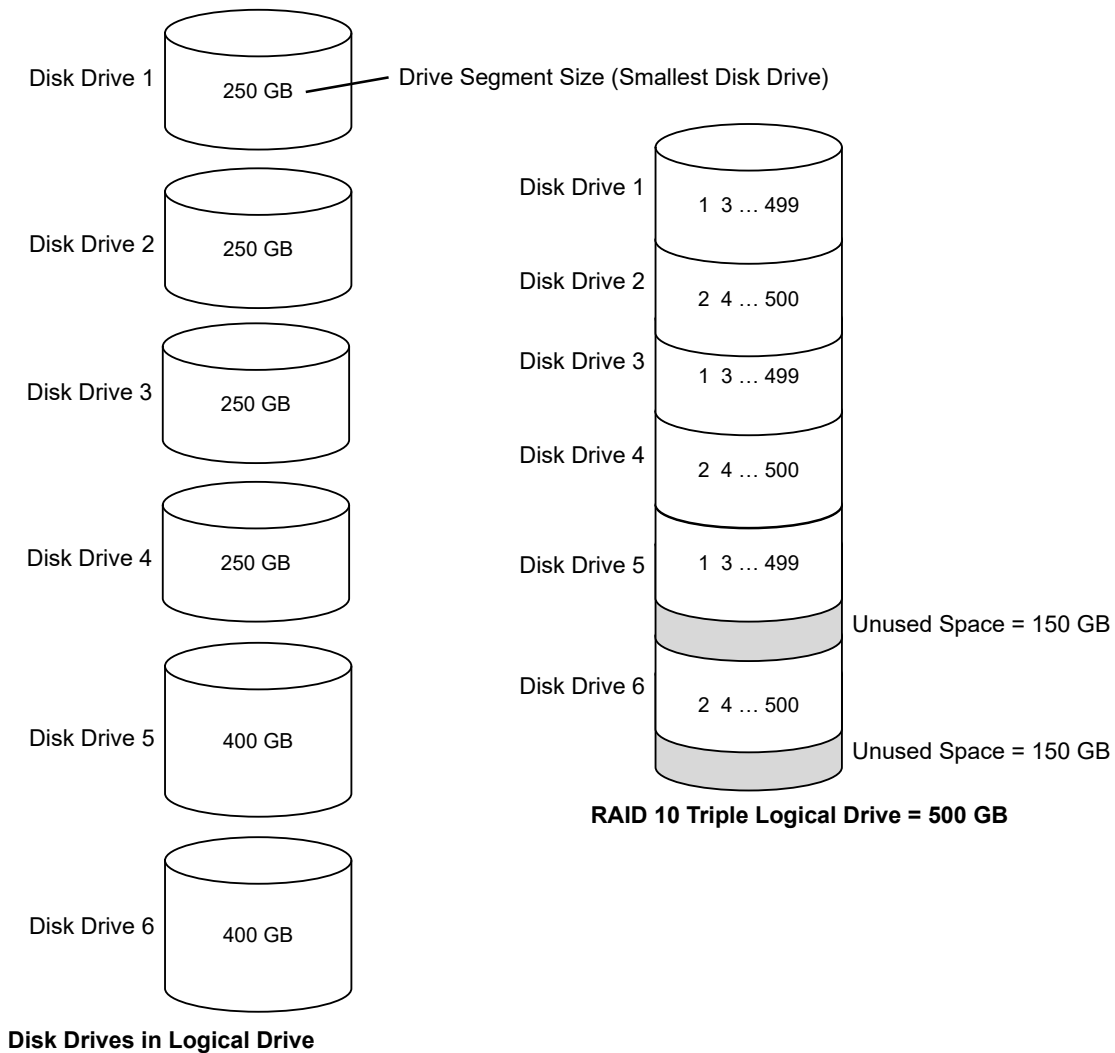
Disk Drives in Logical Drive

RAID 10 Logical Drive = 500 GB

### 21.6 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.

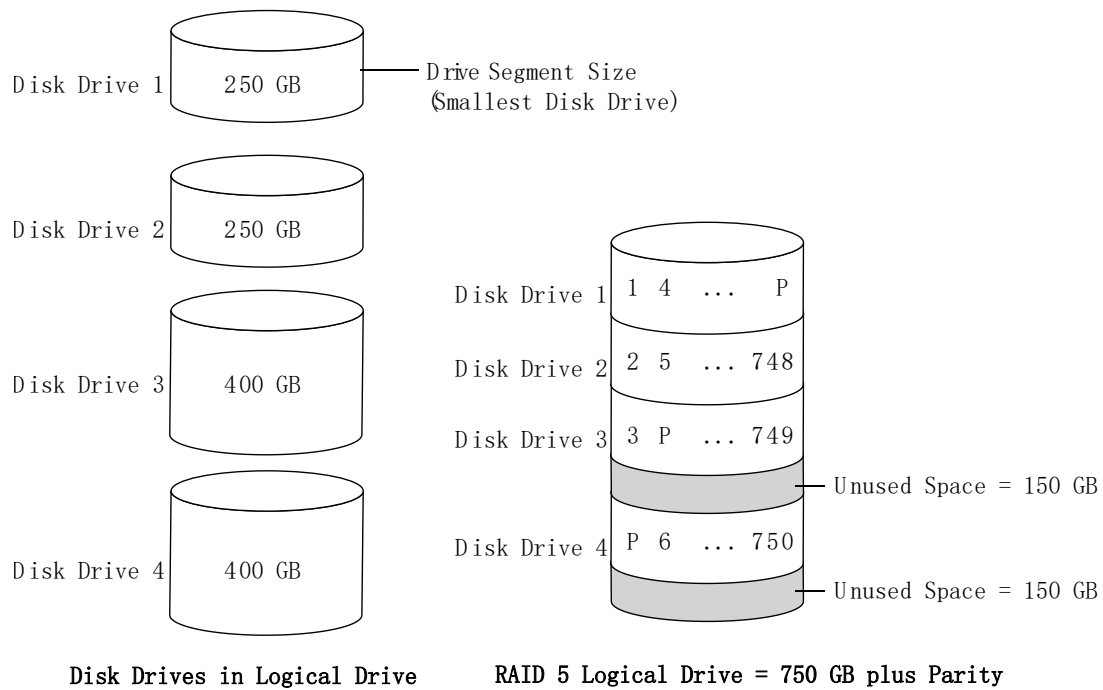


## 21.7 RAID 5 Logical Drives

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.



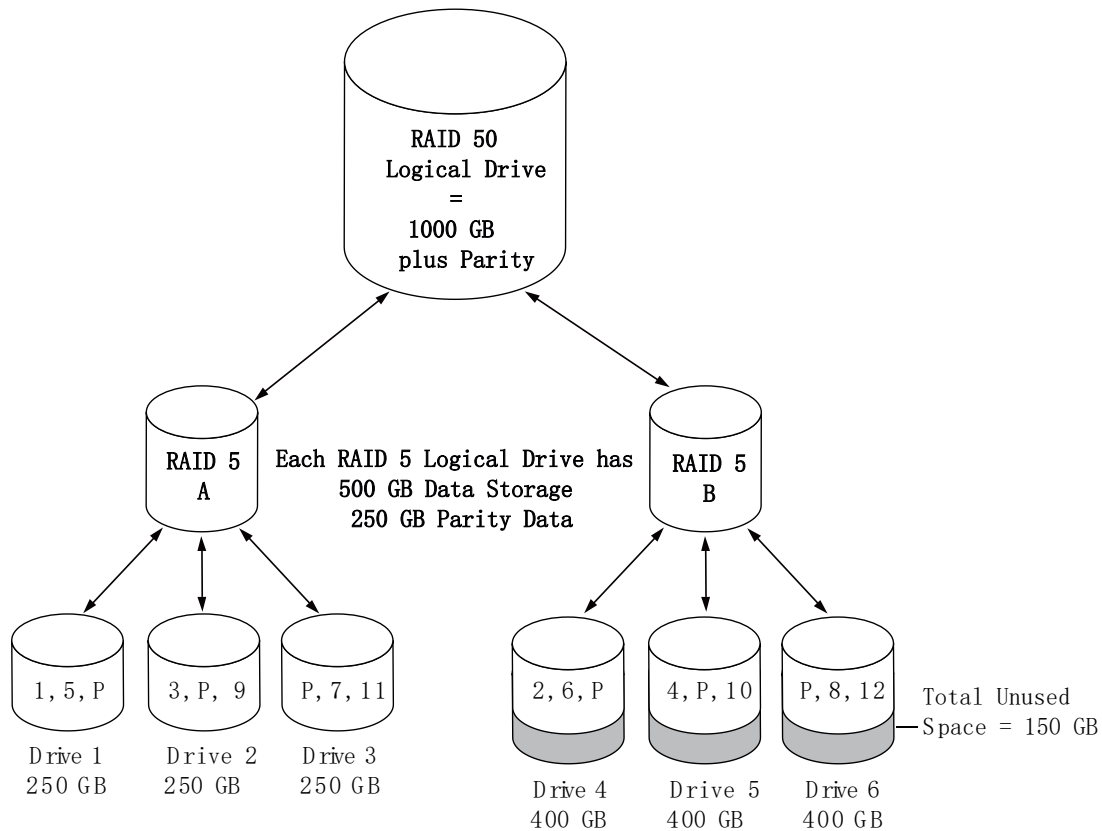
## 21.8 RAID 50 Logical Drive

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.

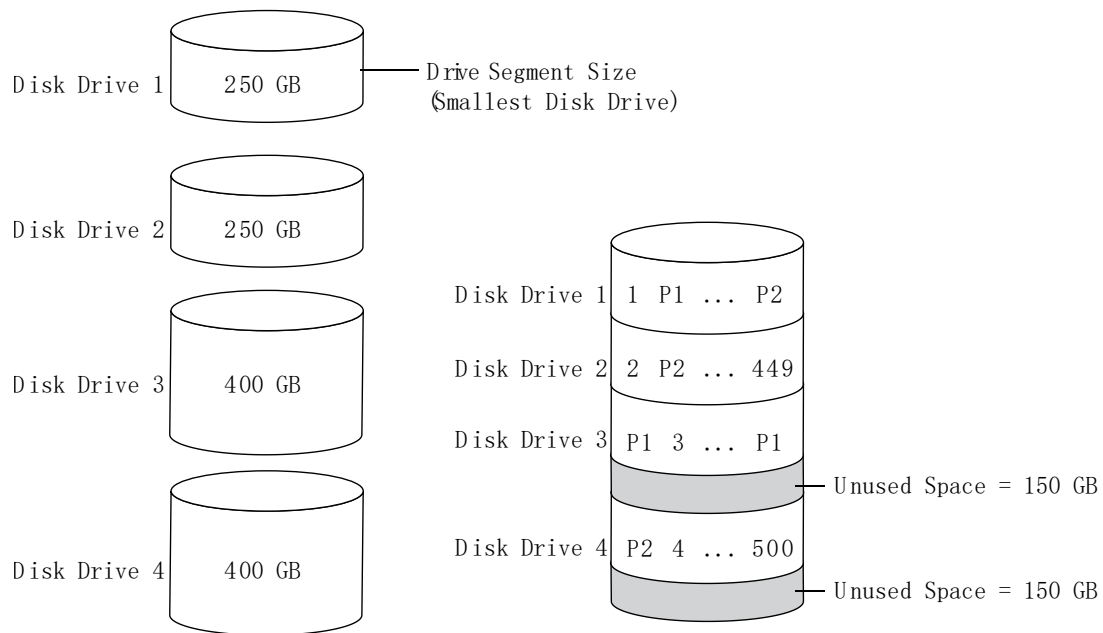


## 21.9 RAID 6 Logical Drives

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.



Disk Drives in Logical Drive

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

### 21.10 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.



## 22. 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 [4.3. 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
	System refresh

### Ribbon Controller Icons

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






.....continued

Icon	Description
	Logical drive expand/migrate
	Logical drive locate
	Logical drive erase
	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
	Initialize/Uninitialize/Enable Erase drive






### Ribbon maxCache Icons

Icon	Description
	maxCache Device create
	maxCache Device set properties
	maxCache Device locate
	maxCache Device delete
	maxCache Device Force online





### Enterprise View Icons

Icon	Description
	Enterprise View
	Local or remote system
	Controller
	Enclosure
	Logical disk
	Logical disks
	Physical disk
	Hard disk drive






.....continued

Icon	Description
	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







### 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

## 23. 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".
Has Logical Drive with Foreign SED	Indicates the presence of foreign logical device, which was imported from different controller.
Has Offline Logical Drive	Array has offline or data locked logical device(s).

### Status Details of a Logical Device

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

.....continued	
Status	Description
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 deleted/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.
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.

.....continued

Status	Description
SED Qualification Failed	This state indicates that the SED qualification is failed.
SED Locked	Indicates the presence of foreign logical device, which was imported from different controller.
Data Locked	Indicates that the controller is waiting on controller password. Data is locked out on the physical device.

### 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 device 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
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.
Data Locked	Indicates that the controller is waiting on controller password. Data is locked out on the physical device.

## 24. 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 24-1.** 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 a unique identifier of the controller.
Firmware Version	Active firmware version of the controller
Hardware Revision	Describes the hardware revision information about the controller.
Hardware Minor Revision	Describes the hardware minor 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.
NVMe	Determines whether the Controller supports NVMe drive.
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.
Negotiated PCIe Data Rate	Negotiated PCIe Data Rate describes the PCIe version, lane width and throughput details.
PCI Address (Domain: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.



.....continued

Property	Tooltip Details
NVMe Configuration	Determines whether the Controller supports creation of logical drives using NVMe drives.
Manufacturing Model	Manufacturing model of the controller.
Manufacturing SKU Number	SKU Number of the controller.
Reboot Required Reasons	Indicates the reason, why a controller cold reboot is required.
SEEPROM Version	Describes the SEEPROM version of the controller.
CPLD Revision	Describes the CPLD revision information about the controller.
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.
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. When set to high, the check will run in parallel to host I/O and may have an impact on performance. When set to idle, the check will only run during periods of host inactivity and will not impact performance.
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. The default value is 3 seconds.
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.

.....continued

Property	Tooltip Details
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.
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't support FLS), the controller will sort incoming requests in order to minimize the amount of travel for the HDD's 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. <ol style="list-style-type: none"> <li>None : No freeze lock or anti-freeze lock commands are sent to any physical device.</li> <li>Freeze : Supported physical devices are freeze locked and sanitize is not allowed.</li> <li>Anti-Freeze : Supported physical devices are anti-freeze locked and freezing the physical devices is not allowed.</li> </ol>
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.

.....continued

Property	Tooltip Details
PCIe Maximum Read Request Size	<p>PCIe Maximum Read Request Size allows optimization of data flow for the purpose of improving the controller performance. This option is used to change the PCIe Maximum Read Request Size value on the Adaptec Smart Storage Controller.</p> <p>The PCIe Maximum Read Request Size takes one of the following values: 128, 256, 512, 1024, 2048 Bytes.</p> <p>By default, the value of Maximum Read Request Size is set to Default value which depends on the controller (128   256   512   1024   2048 bytes).</p> <p>The system must be restarted for the PCIe maximum read request size to take effect.</p>
PCIe Maximum Payload Size	<p>The PCIe Maximum Payload Size is the maximum size of PCIe payload for one transfer. The PCIe Maximum Payload Size takes the values as 128   256   512 Bytes and is displayed under Properties tab of controller.</p> <p><b>Note:</b> The value of PCIe Maximum Payload Size cannot be changed from the maxView GUI.</p>
Persistent Event Log Policy	<p>Persistent Event Log Policy can be either Oldest (Least Recently Consumed) or Newest (Most Recently Occurred). The maximum number of events that can be stored by firmware at any point is 300.</p> <ul style="list-style-type: none"> <li>When the policy is “<b>Least Recently Consumed</b>”, the maximum unconsumed events in NVRAM are 300. After that, the controller stops adding new events to the persistent log in NVRAM.</li> <li>When the policy is “<b>Most Recently Occurred</b>”, firmware continues to log a new event when it occurs in the NVRAM. The consumer is provided with the most recent events up to 300 events.</li> </ul>
UEFI Health Reporting Mode	<p>UEFI Health Reporting Mode allow the users to change whether to report UEFI driver health error messages on boot screen and halt the boot process or not. The UEFI Health Reporting Mode can be either “Enabled” or “Disabled”.</p> <p>The default mode is “Enabled”, which reports all the UEFI driver health error messages on the boot screen and halts the boot process.</p> <p>The “Disabled” mode does not report any UEFI driver health error messages on the boot screen and continues the booting regardless of the errors.</p>
Intelligent Power Management	
Current Power Mode	<p>Power mode setting determines controller static settings based on work load.</p> <p>MAXIMUM PERFORMANCE : Set static settings to highest possible. Do not reduce dynamically.</p>
Pending Power Mode	<p>Power mode setting determines controller static settings based on work load before system reboot.</p> <p>MAXIMUM PERFORMANCE : Set static settings to highest possible. Do not reduce dynamically.</p>
Survival Mode	<p>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.</p>
Spindown Spares Policy	<p>Inactive spares can be spun down to achieve power efficiency gain. Enabling the Spindown Spares Policy will spin down the inactive spares. Disabling the Spindown Spares Policy will not spin down the inactive spares.</p> <p><b>Note:</b> Spindown Spares Policy is supported only in RAID and Mixed Mode</p>
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.

.....continued

Property	Tooltip Details
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. The valid threshold size is between 16 KB and 1040 KB and the value must be a multiple of 16 KB.
No-Battery Write Cache	No-Battery Write Cache setting allows the controller to enable write cache when no battery is present or when the battery fails. Values are Enable or Disable. Enabling No-Battery Write Cache can result in data loss if the server loses power and there is no battery present or the battery has failed.
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.
Green Backup Unit	
Backup Power Status	Status of backup power unit.
Battery/Capacitor Pack Count	Number of backup power units connected to controller.
Hardware Error	Hardware error type occurred on backup power unit.
Power Type	Type of the green backup unit.
Current Temperature	Current temperature in degrees Celsius of the backup power pack.
Maximum Temperature	Maximum temperature in degrees Celsius recorded during the product life.
Threshold Temperature	Maximum allowable temperature in degrees Celsius for the backup power pack. At this temperature, the green backup subsystem will shut down.
Voltage	Current voltage in millivolts of the backup power pack.
Maximum Voltage	Maximum backup power voltage in millivolts recorded during the lifetime of the product.
Current	Active current draw in milliamps of the backup power charging circuit.
Health Status	Predicted health of the backup power pack expressed as a percentage of Capacitance/Initial Capacitance. Initial Capacitance is estimated until a learning cycle occurs.
Relative Charge	Percentage of available energy expressed as a percentage of Capacitance * (Voltage-Vmin)/(Vcharging-Vmin)

**Table 24-2.** Array Display Properties

Property	Tooltip Details
ID	ID describes unique array identifier within the controller.
Name	Name describes unique name of array
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).
Status	Status of array is based on health of member disk drives.
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.
SED Encryption	Indicate whether the array is encrypted or not using SED based encryption.
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 24-3.** 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.
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).

.....continued

Property	Tooltip Details
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.
Consistency Check Status	Indicates whether the consistency check is currently running on the logical device or not.
Last Consistency Check Completion Time	Indicates when the last consistency check was completed on the logical device.
Last Consistency Check Duration	Indicates how long it took to complete the last consistency check on the logical device.
maxCrypto	
Encrypted	Indicate whether the logical device is encrypted or not.
Volatile Key	When volatile key is enabled for encrypted logical device, data keys are stored in volatile memory instead of disk. This provides stronger data protection, but it can also cause the data to be inaccessible during power loss.
Volatile Key With Backup	For remote key management mode, the data key will be backed up to remote key manager when enabling volatile key. You have an option to restore the key from the remote key manager.
SED Encryption	Indicate whether the logical device is encrypted or not using SED based encryption.
maxCache	
State	State of the associated maxCache logical device.

.....continued

Property	Tooltip Details
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 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 24-4.** 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 physical 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.
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.

.....continued

Property	Tooltip Details
Original Factory State (OFS)	Indicates whether the drive is in Original Factory State (OFS) or not.
SED Ownership Status	Describes the ownership status of Self-Encrypting drive (SED).
Foreign Key Identifier	Foreign Key Identifier is the master key identifier of the previous controller.
Foreign Reset Key Identifier	Foreign Reset Key Identifier is the old master key identifier of the controller before rekey on which the SED drive was removed from the system when the drive was undergoing a rekey or rekey was queued.
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
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.
Multi Actuator Drive	Specifies whether this physical device is multi actuator or not.
Multi Actuator LUN Count	Specifies number of LUN's in the multi actuator drive.
Multi Actuator LUN ID	ID of the current LUN in the multi actuator drive.



## 25. maxView Video Tutorials

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

**Table 25-1.** 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.	<a href="https://youtu.be/Wzcnz9KuL0U">https://youtu.be/Wzcnz9KuL0U</a>
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.	<a href="https://www.youtube.com/watch?v=9xPTgZASiSc">https://www.youtube.com/watch?v=9xPTgZASiSc</a>
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	<a href="https://www.youtube.com/watch?v=Nu-1l4eidlM&amp;feature=youtu.be&amp;ab_channel=MicrochipTechnology">https://www.youtube.com/watch?v=Nu-1l4eidlM&amp;feature=youtu.be&amp;ab_channel=MicrochipTechnology</a>
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.	<a href="https://www.youtube.com/watch?v=2ffi3Lm5LEE">https://www.youtube.com/watch?v=2ffi3Lm5LEE</a>
5	How to Force a Logical Drive with Multiple Drive Failures Back Online	In our previous video on <a href="#">How to Diagnose Errors using Adaptec® maxView Storage Manager</a> , 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.	<a href="https://youtu.be/pRNbd39UXdw">https://youtu.be/pRNbd39UXdw</a>

## 26. Revision History

The revision history describes the changes that were implemented in the document. The changes are listed by revision, starting with the most current publication.

Revision	Date	Description
G	10/2023	<p>The following is a summary of changes in revision G of this document:</p> <ul style="list-style-type: none"> <li>Added Spindown Spares Policy details in <a href="#">7.14. Maintaining an Energy-Efficient Storage Space</a> and <a href="#">24. Display Properties of a Controller, Array, Logical Device, and a Physical Device</a></li> <li>Added a warning for Software handling around 'FW rollback prevention' feature set in <a href="#">12.11.2. Updating the Controller Firmware</a></li> <li>Added SMART data details for NVMe drives in <a href="#">13.2.3.3. Viewing SMART Statistics</a></li> <li>Added UBM Controller ID, firmware version properties of Summary tab of Backplane in <a href="#">13.2.3. Viewing Component Status in the Storage Dashboard</a></li> <li>Updated screenshots for UBM Backplane Firmware in <a href="#">12.11.5. Updating the UBM Backplane Firmware</a></li> </ul>
F	06/2023	<p>The following is a summary of changes in revision F of this document:</p> <ul style="list-style-type: none"> <li>Added <a href="#">11. Working with Security Protocol and Data Model (SPDM)</a></li> <li>Added <a href="#">19.1. Installing the maxView Plugin for vSphere 8 HTML5 Client</a></li> <li>Added <a href="#">12.11.5. Updating the UBM Backplane Firmware</a></li> <li>Added support for Remote key management mode in <a href="#">10. Working with Self Encrypting Drive (SED) Based Encryption</a></li> <li>Added CPLD revision and Platform image revision in <a href="#">Display Properties of a Controller, Array, Logical Device, and a Physical Device</a> chapter</li> <li>Added Supercap temperature and voltage information in <a href="#">Display Properties of a Controller, Array, Logical Device, and a Physical Device</a> chapter</li> </ul>
E	01/2023	<p>The following is a summary of changes in revision E of this document:</p> <ul style="list-style-type: none"> <li>Added Desktop maxView Web Application support</li> <li>Added MPS and MRRS configuration support</li> <li>Added Multi Actuator drive support</li> <li>Added option to prevent halting boot process on UEFI driver health</li> <li>Deprecated Minimum Power mode support</li> </ul>

.....continued

Revision	Date	Description
D	10/2022	<p>The following is a summary of changes in revision D of this document:</p> <ul style="list-style-type: none"> <li>• Updated <b>Installing on VMware 7.x and ESXi 8.x</b> section with VMware (ESXi 8) support</li> <li>• Updated <b>The Ribbon</b> section with Classic and Simplified Ribbon View support</li> <li>• Added <b>Remote Key Management Mode</b> support</li> <li>• Added <b>Changing the Persistent Event Log Policy Setting</b> topic</li> <li>• Added <b>Storage Inventory</b> support</li> <li>• Removed <b>Using the maxView Plugin for VMware vSphere Web Client</b> chapter</li> <li>• Added <b>Using the maxView Plugin for VMware vSphere 8 HTML5</b> chapter</li> <li>• Updated <b>Display Properties of a Controller, Array, Logical Device, and a Physical Device</b> chapter with the following changes: <ul style="list-style-type: none"> <li>– Added <b>Persistent Event Log Policy</b></li> <li>– Added <b>Volatile Key</b> and <b>Volatile Key with Backup</b></li> <li>– Added <b>Consistency Check Status, Last Consistency Check Completion Time</b> and <b>Last Consistency Check Duration</b></li> </ul> </li> </ul>
C	06/2022	<p>The following is a summary of changes in revision C of this document:</p> <ul style="list-style-type: none"> <li>• Added <a href="#">10. Working with Self Encrypting Drive (SED) Based Encryption</a></li> <li>• Updated <a href="#">5.6. Controller Support for SED</a></li> </ul>
B	02/2022	<p>The following is a summary of changes in revision B of this document:</p> <ul style="list-style-type: none"> <li>• Added Event Log and Task Log details in <a href="#">4.4. Checking System Status from the Main Window</a></li> <li>• Added "Recover Cache Module" option in <a href="#">7.4.1. Enabling Cache Optimizations</a></li> </ul>
A	10/2021	<p>The following is a summary of changes in revision A of this document:</p> <ul style="list-style-type: none"> <li>• The document was updated to latest Microchip template.</li> <li>• The document number was changed from PMC-2153109 to DS00004219A.</li> <li>• Added section <a href="#">Installing on VMware 7.x and Uninstalling from VMware 7.x</a>.</li> </ul>

## Microchip Information

### The Microchip Website

Microchip provides online support via our website at [www.microchip.com/](http://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](http://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](http://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](http://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, 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, ClockWorks, The Embedded Control Solutions Company, EtherSynch, Flashtec, Hyper Speed Control, HyperLight Load, Libero, motorBench, mTouch, Powermite 3, Precision Edge, ProASIC, ProASIC Plus, ProASIC Plus logo, Quiet-Wire, SmartFusion, SyncWorld, TimeCesium, TimeHub, TimePictra, TimeProvider, 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, Clockstudio, CodeGuard, CryptoAuthentication, CryptoAutomotive, CryptoCompanion, CryptoController, dsPICDEM, dsPICDEM.net, Dynamic Average Matching, DAM, ECAN, Espresso T1S, EtherGREEN, EyeOpen, GridTime, IdealBridge, IGaT, In-Circuit Serial Programming, ICSP, INICnet, Intelligent Paralleling, IntelliMOS, Inter-Chip Connectivity, JitterBlocker, Knob-on-Display, MarginLink, maxCrypto, maxView, memBrain, Mindi, MiWi, MPASM, MPF, MPLAB Certified logo, MPLIB, MPLINK, mSiC, MultiTRAK, NetDetach, Omniscient Code Generation, PICDEM, PICDEM.net, PICkit, PICtail, Power MOS IV, Power MOS 7, 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, Trusted Time, TSHARC, Turing, 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, and Symmcom 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.

© 2023, Microchip Technology Incorporated and its subsidiaries. All Rights Reserved.

ISBN: 978-1-6683-3243-6

## **Quality Management System**

For information regarding Microchip's Quality Management Systems, please visit [www.microchip.com/quality](http://www.microchip.com/quality).

# Worldwide Sales and Service

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