

**maxView™ Storage Manager User Guide for Adaptec®
SmartRAID 4300 Series NVMe RAID Accelerator
Controller**



Table of Contents

1.	About this Guide.....	5
1.1.	What You Need to Know Before You Begin.....	5
1.2.	Terminology Used in this Guide.....	5
1.3.	How to Find More Information.....	5
2.	Introduction to maxView Storage Manager.....	7
2.1.	Getting Started.....	7
2.2.	About maxView Storage Manager.....	7
2.3.	System Requirements.....	7
2.4.	Browser Support.....	8
2.5.	Typical Storage Space Configurations.....	8
3.	Installing maxView Storage Manager.....	9
3.1.	Before You Begin the Installation.....	9
3.2.	Installing on Windows.....	9
3.3.	Installing on Red Hat or SuSE Linux.....	11
3.4.	Uninstalling maxView Storage Manager.....	11
4.	Exploring maxView Storage Manager.....	13
4.1.	Starting maxView Storage Manager and Logging In.....	13
4.2.	Working in maxView Storage Manager.....	13
4.3.	Overview of the Main Window.....	14
4.4.	Checking System Status from the Main Window.....	17
4.5.	Revealing More Device Information	18
4.6.	Getting Help.....	19
4.7.	Logging Out of maxView Storage Manager.....	19
5.	Building Your Storage Space.....	20
5.1.	Overview.....	20
5.2.	Choosing a Management System.....	20
5.3.	Logging into Remote Systems from the Local System.....	21
5.4.	Manage NVMe Drives.....	22
5.5.	Creating Arrays and Logical Drives.....	27
6.	Protecting Your Data.....	35
6.1.	Dedicated Spare or Auto-Replace Spare?.....	35
6.2.	Hot Spare Limitations.....	35
6.3.	Assigning a Dedicated Hot Spare.....	35
6.4.	Assigning an Auto-Replace Hot Spare.....	37
6.5.	Removing a Hot Spare.....	39
6.6.	Setting the Spare Activation Mode	41
7.	Modifying Your Storage Space.....	43
7.1.	Understanding Arrays and Logical Drives.....	43
7.2.	Creating and Modifying Logical Drives.....	43
7.3.	Enabling Background Consistency Check.....	45
7.4.	Modifying an Array.....	46

7.5.	Working with Mirrored Arrays.....	47
7.6.	Increasing the Capacity of a Logical Drive.....	49
7.7.	Changing the Logical Drive Rebuild Priority.....	50
7.8.	Renaming a Logical Drive.....	50
7.9.	Deleting an Array or Logical Drive	51
8.	Working with Security Protocol and Data Model (SPDM).....	52
8.1.	Security Protocol and Data Model (SPDM) Properties.....	52
8.2.	SPDM Security Settings.....	54
9.	Maintaining Physical Devices.....	57
9.1.	Viewing Device Properties.....	57
9.2.	Locating Drives in Your Storage Space.....	57
9.3.	Working with Physical Device Error Counters.....	59
9.4.	Working with Failed or Failing Physical Drives.....	62
9.5.	Erasing a Physical Drive.....	63
9.6.	Initializing and Uninitializing Physical Drives.....	64
9.7.	Working with Controllers.....	66
9.8.	Updating Accelerator and Physical Drive Firmware.....	68
10.	Monitoring Status and Activity.....	76
10.1.	Monitoring Options.....	76
10.2.	Checking Status from the Main Window	76
10.3.	Notifying Users by Email About Status and Activity	81
10.4.	Changing an Operating System's Event Log Setting.....	87
11.	Managing Your Storage Space.....	88
11.1.	Deploying Servers	88
11.2.	Managing Remote Systems.....	91
11.3.	Clearing the Controller Configuration.....	98
11.4.	Changing the Web Server Port.....	99
11.5.	Granting Standard Users Admin Privilege.....	99
12.	Solving Problems.....	101
12.1.	General Troubleshooting Tips.....	101
12.2.	Identifying a Failed or Failing Component.....	101
12.3.	Recovering from a Physical Drive Failure.....	101
12.4.	Rebuilding Logical Drives.....	104
12.5.	Creating a Support Archive File.....	105
13.	Silent Installation on Linux.....	106
13.1.	Completing a Silent Installation.....	106
13.2.	Example Command Line Installations.....	106
14.	Configuring SNMP Notifications on Linux.....	107
14.1.	Setting Up SNMP Notifications on Linux.....	107
15.	Selecting the Best RAID Level.....	108
15.1.	Comparing RAID Levels.....	108
15.2.	Non-redundant Logical Drives (RAID 0).....	108
15.3.	RAID 1 Logical Drives	109

15.4. RAID 10 Logical Drives.....	109
15.5. RAID 5 Logical Drives.....	110
15.6. RAID 50 Logical Drive.....	111
16. Icons At-a-Glance.....	112
17. Smart Controller Device Status.....	116
18. Display Properties of a Controller, Array, Logical Device, and a Physical Device.....	119
19. Revision History.....	124
Microchip Information.....	125
Trademarks.....	125
Legal Notice.....	125
Microchip Devices Code Protection Feature.....	125

1. About this Guide

maxView™ Storage Manager is a browser-based software application that helps you build a storage space using Microchip Smart NVMe RAID Accelerator Controller and disk drives, and then manage your stored data in a single server or multiple remote servers.

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.

Note: This guide focuses on using maxView Storage Manager with Microchip Smart NVMe RAID Accelerator Controller. For information about using maxView Storage Manager with Adaptec Series 8 (legacy) RAID controllers, see [How to Find More Information](#).

Note: Some features like SPDM support, SED support, maxCrypto and heal array will be available in the future releases.

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 and Microchip Smart NVMe RAID Accelerator Controller, 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.

1.2 Terminology Used in this Guide

Because this guide provides information that can be used to manage Microchip Smart NVMe RAID Accelerator Controller in a variety of configurations, the generic term “storage space” is used to refer to the controller(s), physical 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, physical 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)
- Non-Volatile Memory Express drives (also known as NVMe SSD)
- 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)

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 and the Microchip customer portal at www.microchip.com/wwwregister/default.aspx:

- *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.
- *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.

- *Adaptec® SmartRAID 4300 Installation and User Guide*—Describes how to install drivers and configure the SmartRAID 4300 NVMe RAID Accelerator Adapter.

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 [Installing maxView Storage Manager](#)).

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

Step 4: Build your storage space (see [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 and NVMe Solid State Drives (SSDs).

With maxView Storage Manager, you can group physical 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 and physical drives in your storage space from a single location.

The maxView Storage Manager GUI, or *graphical user interface*, runs on most contemporary Web browsers (for a list of supported browsers, see [Browser Support](#)). 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 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 physical drive space
- One of these operating systems:
 - Microsoft® Windows® Server
 - Red Hat® Enterprise Linux
 - SUSE Linux Enterprise Server

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 Server
- Google® Chrome™ 32 or newer
- Mozilla Firefox® 31 or newer

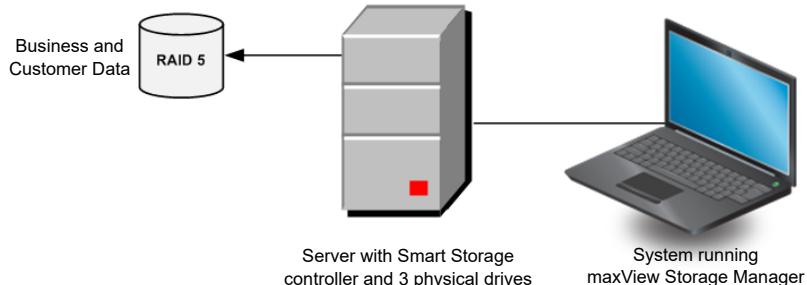
Note: The ideal resolution for the best view of the maxView Storage Manager is 1920 x 1080 ppi. The recommended display scaling setting and browser zoom setting is 100%.

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, physical devices, 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 physical drives installed in a server. For data protection, the physical drives have been used to build a RAID 5 logical drive.



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 [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 [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 [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/ 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 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.

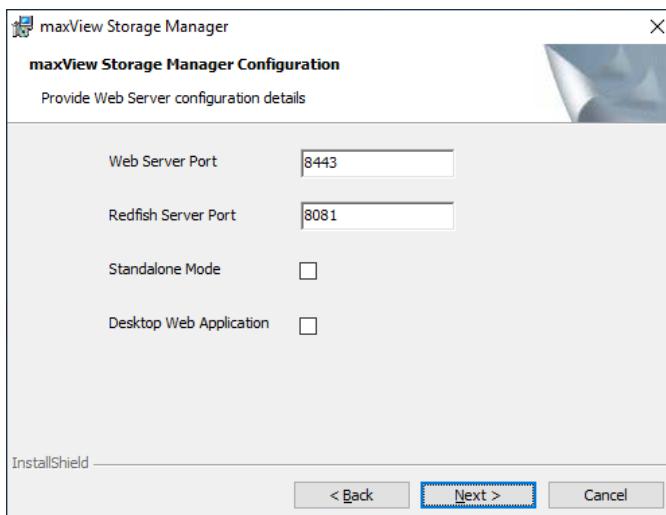
Note: You need administrator privileges to install maxView Storage Manager. For details on verifying privileges, see your operating system documentation.

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

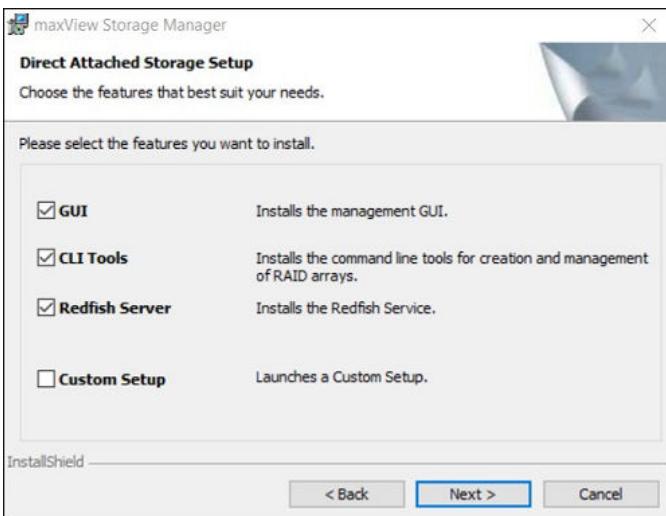
Option	Description
Windows 64-bit	setup_asm_x64.exe

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 or SuSE Linux

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

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

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

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

Uninstalling maxView Storage Manager

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

3.4.1

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.

3.4.2 Uninstalling from Red Hat or SuSE Linux

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

4. Exploring maxView Storage Manager

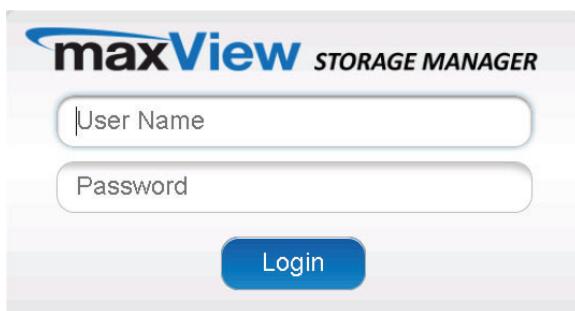
This section familiarizes you with the main features of the maxView Storage Manager graphical user interface. It describes how to start and login to maxView Storage Manager. It also explains how to get help and log out of maxView Storage Manager when you are finished working with the application.

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 [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, physical devices, logical drives, and so on)
- Clicking icons on the *ribbon*, at the top of the maxView Storage Manager main window
- Working with information in the *Storage Dashboard* and *Chart View*
- Checking status in the Event Log and Task Log

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

Note: maxView Storage Manager allows you to give Standard users Administrator privileges. For details, see [Granting Standard Users Admin Privilege](#).

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

Working in maxView Storage Manager (continued)

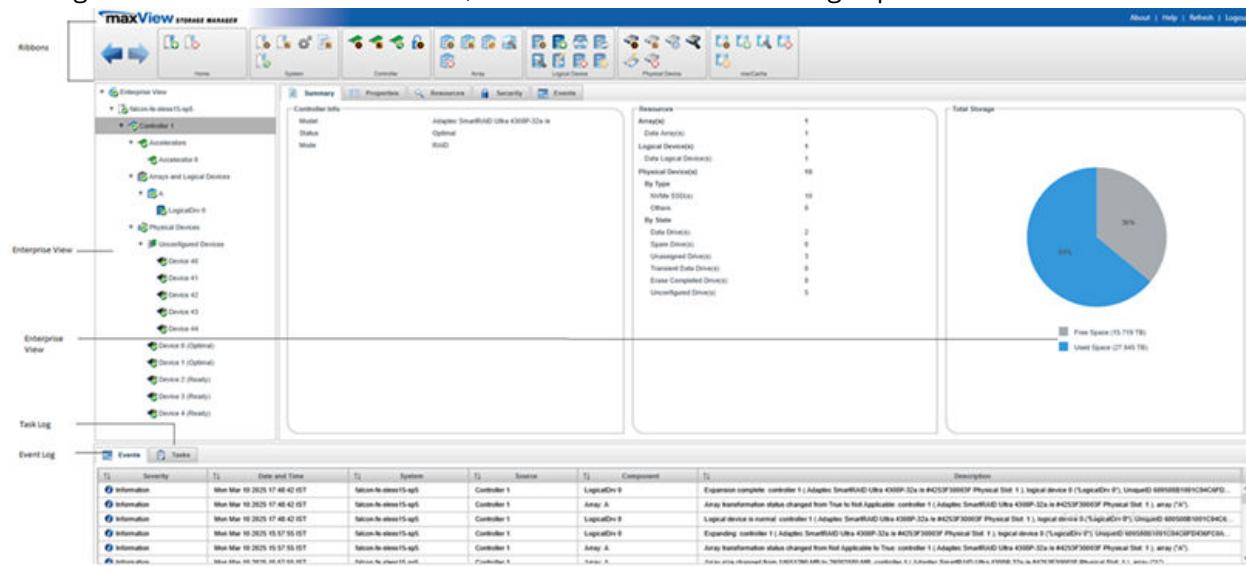
Standard users can:	Standard users can't:
Identify physical devices and logical devices	Delete arrays and logical drives
Silence alarms	Perform data migrations
View component properties on the Storage Dashboard	Clear the controller configuration

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.

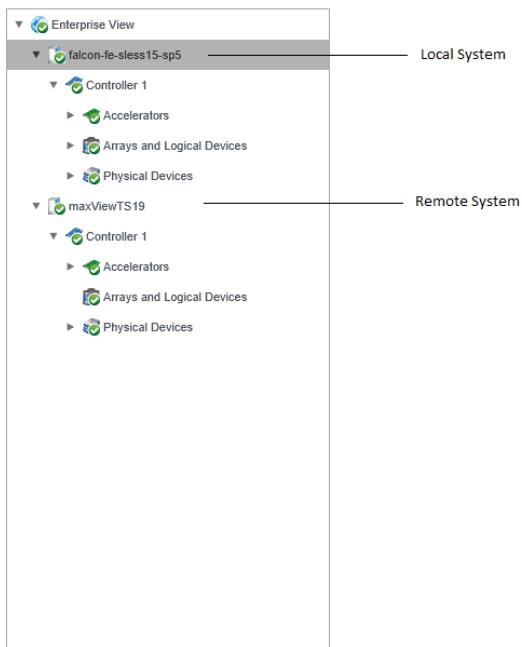
In example below, a controller is selected in the Enterprise View, and the right panel displays the Storage Dashboard for the controller, with a chart view of its storage space.



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

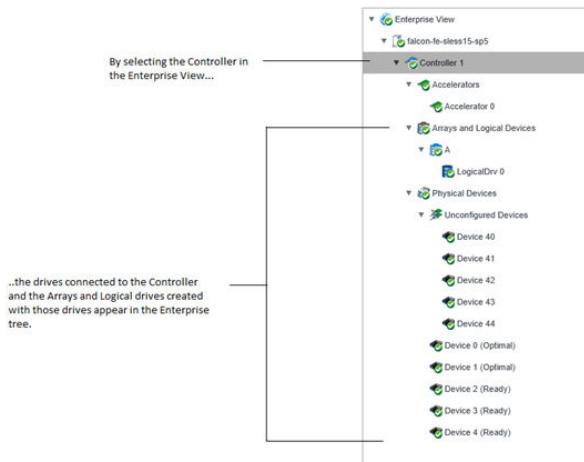
4.3.1 The Enterprise View

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 ‘[Local](#)’ or ‘[Remote?](#)’ for more information.)



Expand a system in the Enterprise View to see its controllers, arrays, logical drives (devices) and physical 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 physical drive, then using the related commands on the ribbon, as described in the following section.

4.3.1.1 What do the Enterprise View Icons Mean?

Icon	Description
	System with controller and directly attached physical drives
	Controller
	Accelerator
	Array (healthy)

What do the Enterprise View Icons Mean? (continued)

Icon	Description
	Logical drive
	NVMe Solid State Drive (SSD)

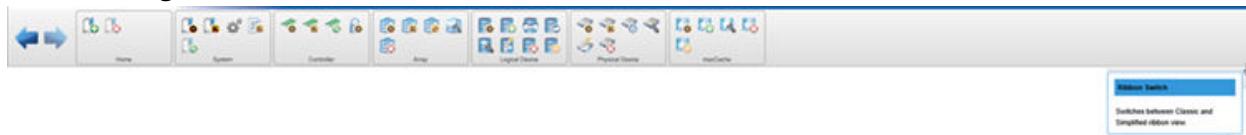
4.3.2 The Ribbon

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**:



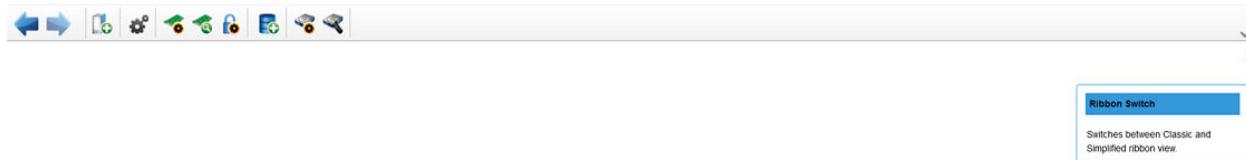
The classic ribbon is organized into groups of related tasks for Systems, Controllers, Arrays, Logical Devices and Physical Devices. The Home group (on the left) provides commands for working with remote systems (see [Managing Remote Systems](#)). Active options on the ribbon vary, depending on which 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
- All options in the Controller group

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

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



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

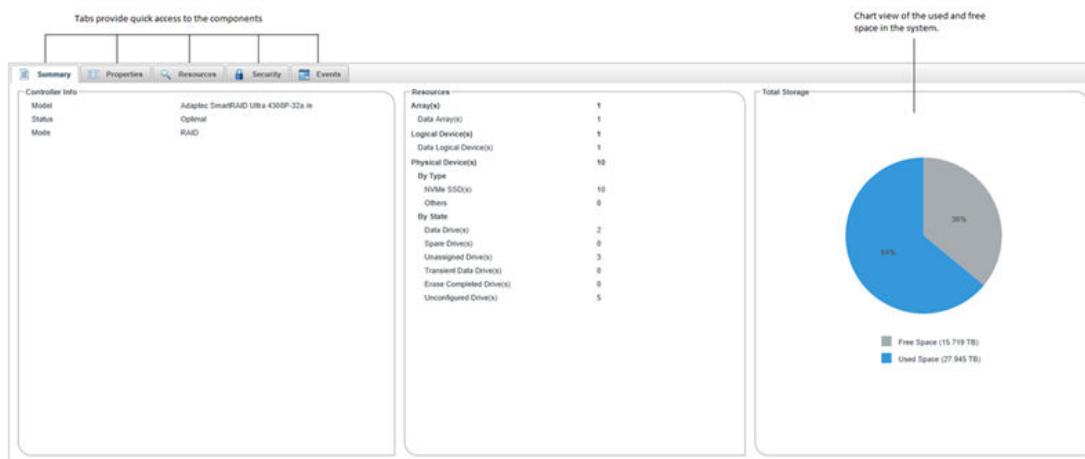
For instance, if a controller is selected in the Enterprise view, only the applicable ribbon icon is visible and activated.

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

For a description of the icons on the ribbon, see [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 NVMe SSDs. It also provides a chart view of free and used space in your system.



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

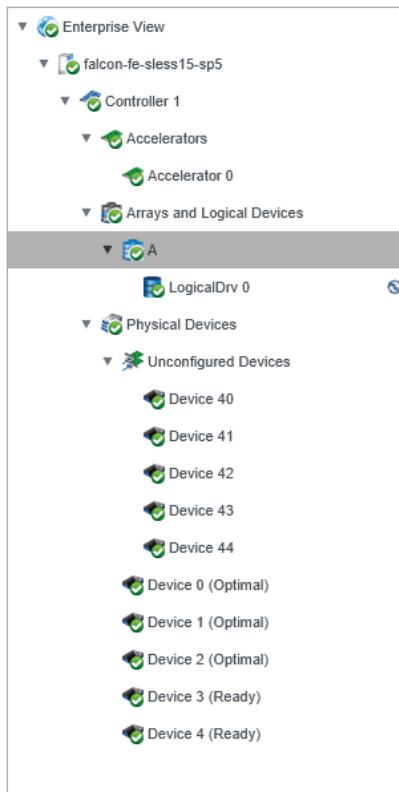
4.4

Checking System Status from the Main Window

maxView Storage Manager includes an Event Log and Task Log for at-a-glance status and activity information for all managed systems. The Event Log provides status information and messages about activity (or *events*) occurring in your storage space. The Task Log provides information about current 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 [Identifying a Failed or Failing Component](#) for more information.



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 physical drive, array, and logical drive usage in the storage space with the Resources view on the Storage Dashboard.

To reveal physical drives 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 physical drives and spares; similarly, clicking on a physical drive displays which array (if any) it belongs to. In the following figure, the Device 2 and Device 3 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.

Physical Device(s)					Array(s) and Logical Device(s)					maxCache Device(s)				
Device	Tl State	Tl Interface	Tl Block Size	Tl Total Size	Tl Array	Tl Logical Device	Tl State	Tl RAID Level	Tl Total Size	Tl Array	Tl Logical Device	Tl State	Tl RAID Level	Tl Total Size
Device 2	Optimal	NVMe SSD	512 Bytes	1.7 TB	A	LogicalDrv 0	Optimal	RAID 1	1.7 TB					
Device 3	Optimal	NVMe SSD	512 Bytes	1.7 TB	B	LogicalDrv 1	Optimal	RAID 0	3.4 TB					
Device 4	Ready	NVMe SSD	512 Bytes	1.7 TB										
Device 5	Ready	NVMe SSD	512 Bytes	1.7 TB										
Device 6	Ready	NVMe SSD	512 Bytes	1.7 TB										
Device 7	Optimal	NVMe SSD	512 Bytes	1.7 TB										
Device 8	Optimal	NVMe SSD	512 Bytes	1.7 TB										
Device 9	Ready	NVMe SSD	512 Bytes	1.7 TB										
Device 10	Ready	NVMe SSD	512 Bytes	1.7 TB										
Device 11	Ready	NVMe SSD	512 Bytes	1.7 TB										
Device 12	Ready	NVMe SSD	512 Bytes	1.7 TB										
Device 13	Auto Replace...	NVMe SSD	512 Bytes	1.7 TB										

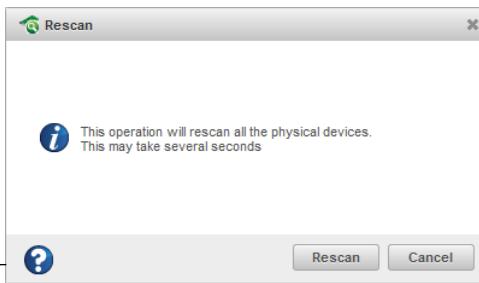
4.6 Getting Help

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

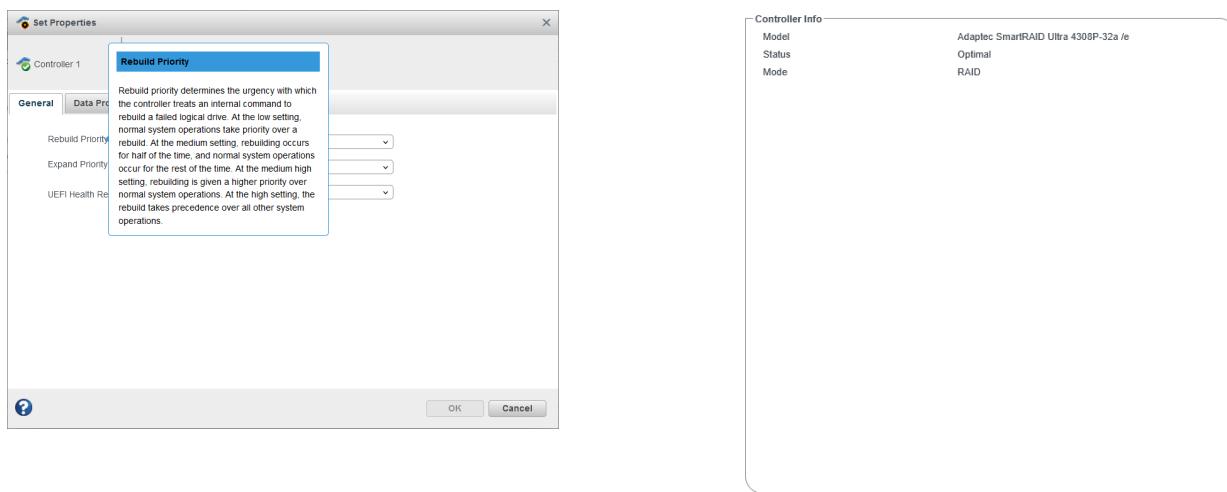
To open the online help, click the **Help** button at the upper-right corner of the main window.



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



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



4.7 Logging Out of maxView Storage Manager

To log out of maxView Storage Manager:

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



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

5. Building Your Storage Space

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

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

5.1 Overview

To build your storage space, complete these steps:

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

As your storage requirements change, you can add systems, controllers, and physical drives, then modify the arrays and logical drives in your storage space by following the instructions in [Modifying Your Storage Space](#).

5.2 Choosing a Management System

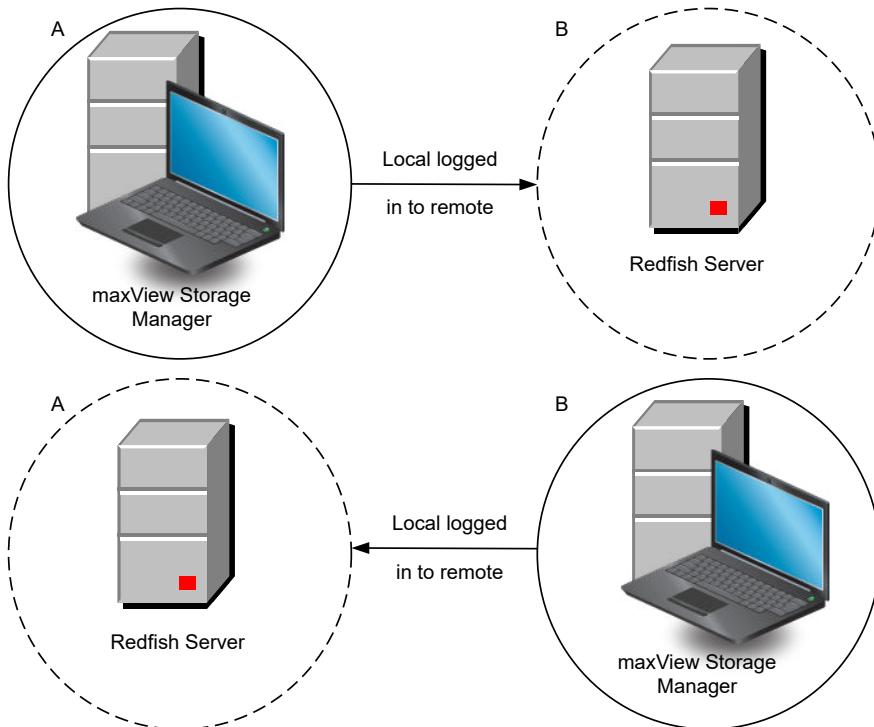
Designate at least one system as a *management system* from which you will manage the storage on all systems in your storage space.

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 [Starting maxView Storage Manager and Logging In](#).

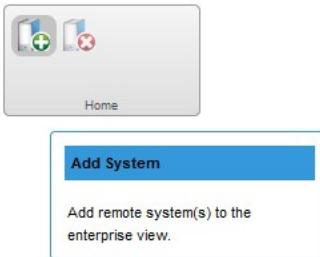
5.3 Logging into Remote Systems from the Local System

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, physical drives, and logical drives as if they were part of your local system.

To log in to a remote system:

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



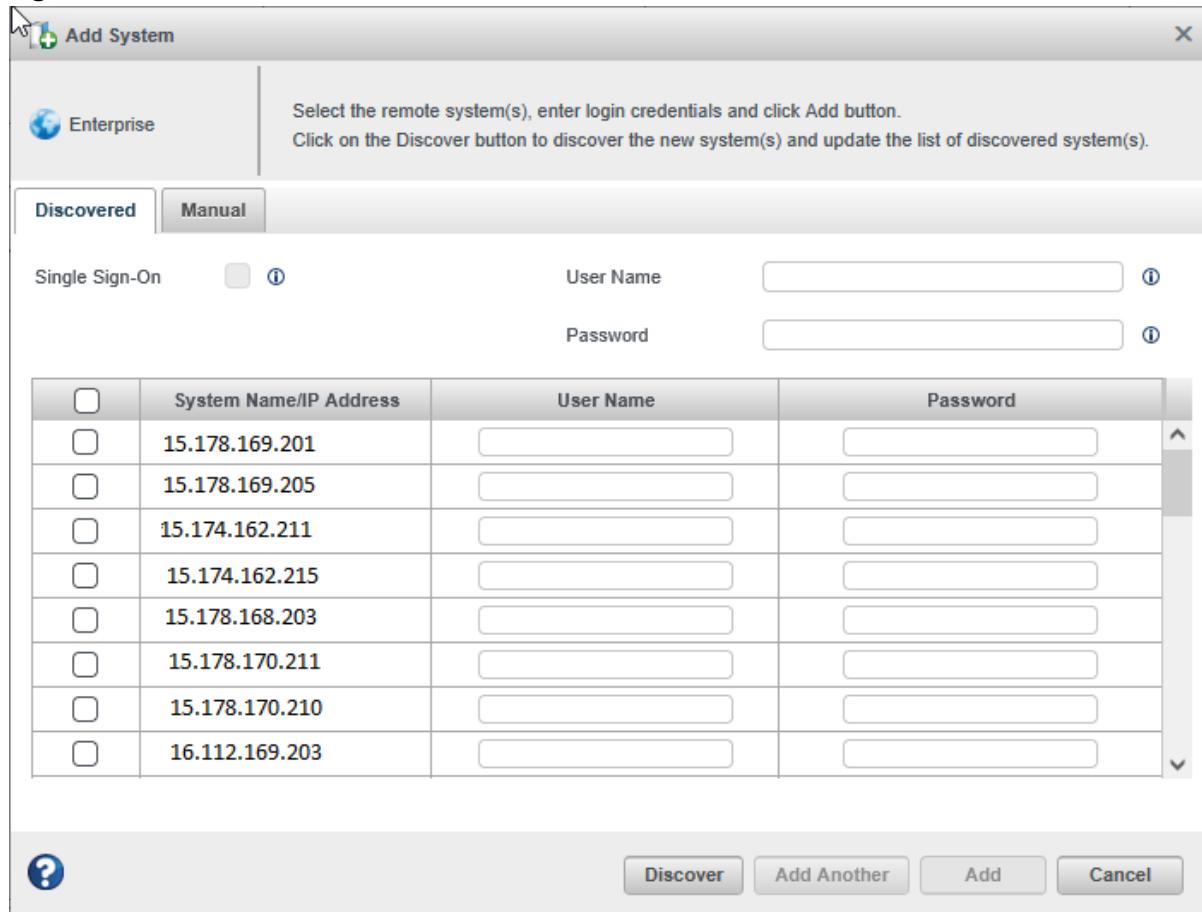
The Add System window opens, showing a list of "discovered" systems; that is, systems on your network that are running the Redfish.

Note:

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

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 Manage NVMe Drives

For the Microchip Smart NVMe RAID Accelerator controllers, NVMe drives can be managed by adding or removing them using the controller. Once the NVMe drives are configured for XLR management, they will no longer be accessible to the Operating System.

Note: Once you Configure/Unconfigure the NVMe drives, a reboot is necessary for any effect to take place. Until the reboot, no configuration change operations can be performed on the controller.

5.4.1 Manage NVMe Drives from Controller Level

You can add one or more devices by configuring the drive with the proper label and remove them by unconfiguring the drive.

Note: Only the configured drives that are not part of an array can be unconfigured.

To configure NVMe drives at the controller level:

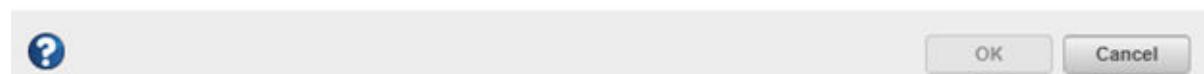
1. In Enterprise View, select a controller.
2. On the ribbon, in the Physical Device group, click **Set Properties** ribbon icon.



The Set Properties window opens. The **Manage NVMe Drives** tab is selected, by default.

3. Select **Configure** option from **Operation Type** drop-down list.
4. Select the checkboxes to configure and add the drives. Provide a label in ASCII format that does not include spaces and has a maximum of eight characters. This label is further used to identify each NVMe drive.

<input type="checkbox"/>	Device	PCI Address	Parent PCI Address	Label
<input type="checkbox"/>	Device 40	0000:09:00.0	0000:00:05.1	
<input type="checkbox"/>	Device 41	0000:07:00.0	0000:00:01.4	
<input type="checkbox"/>	Device 42	0000:43:00.0	0000:40:01.2	
<input type="checkbox"/>	Device 43	0000:61:00.0	0000:60:01.1	
<input type="checkbox"/>	Device 44	0000:89:00.0	0000:80:05.1	



5. Click OK.

The checked drives will get added.

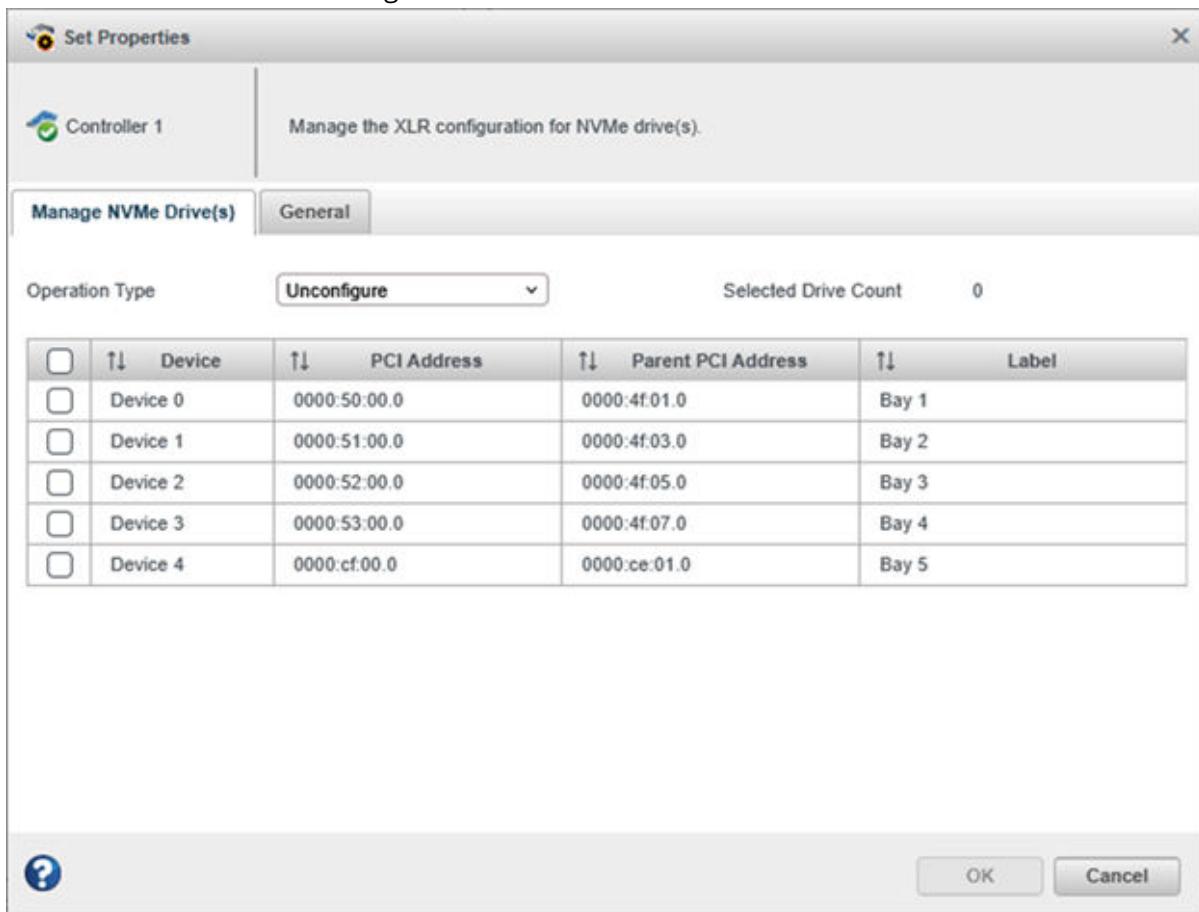
To unconfigure NVMe drives at the controller level:

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



The Set Properties window opens. The **Manage NVMe Drives** tab is selected, by default.

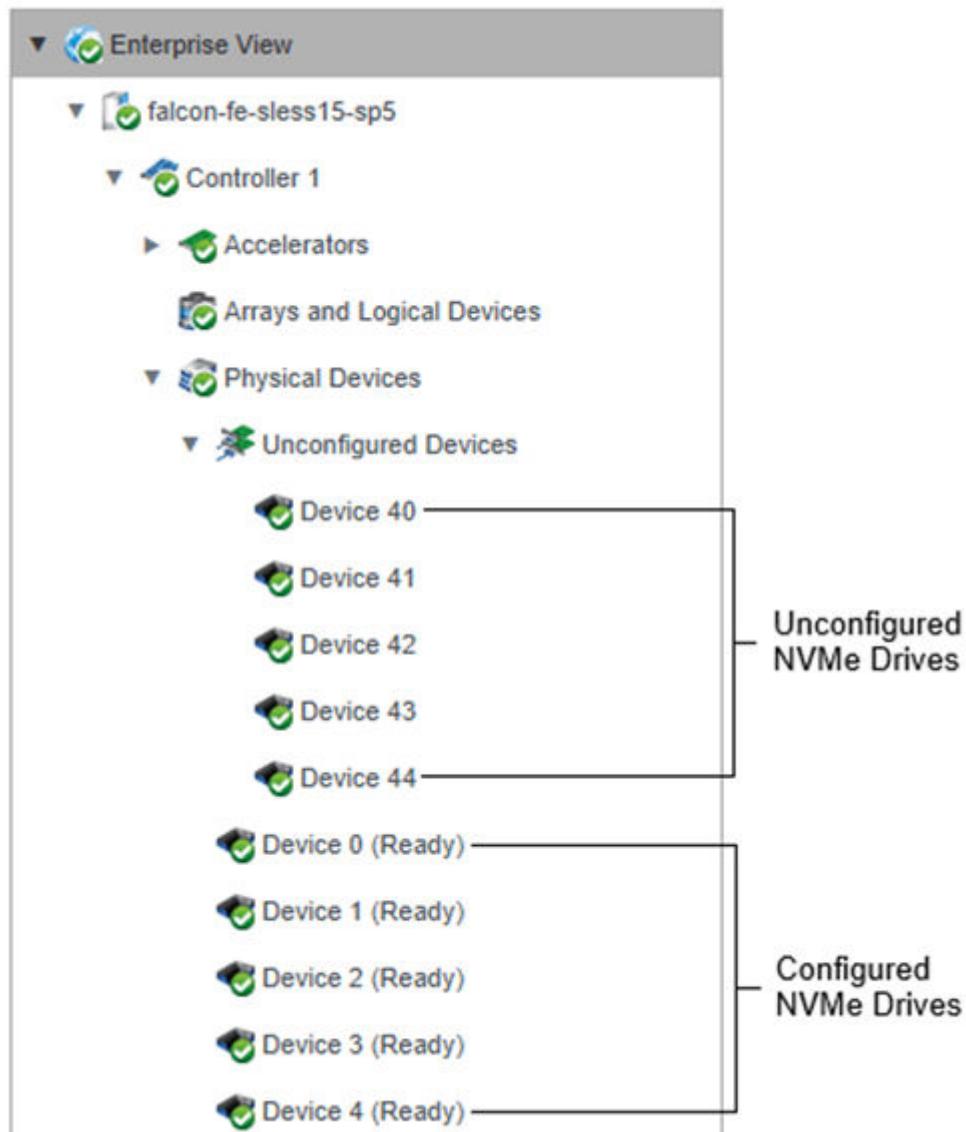
3. Select **Unconfigure** option from **Operation Type** drop-down list.
4. Select the checkbox to unconfigure the drive that has to be removed.



5. Click OK.
The checked drives will get removed.

5.4.2 Manage NVMe Drives from Physical Device Level

All the configured NVMe drives are listed as normal physical drives under the Physical Device group node, whereas unconfigured drives are listed under the Unconfigured Devices group node in the enterprise tree.



5.4.2.1 Configure a NVMe Drive from Physical Device Level

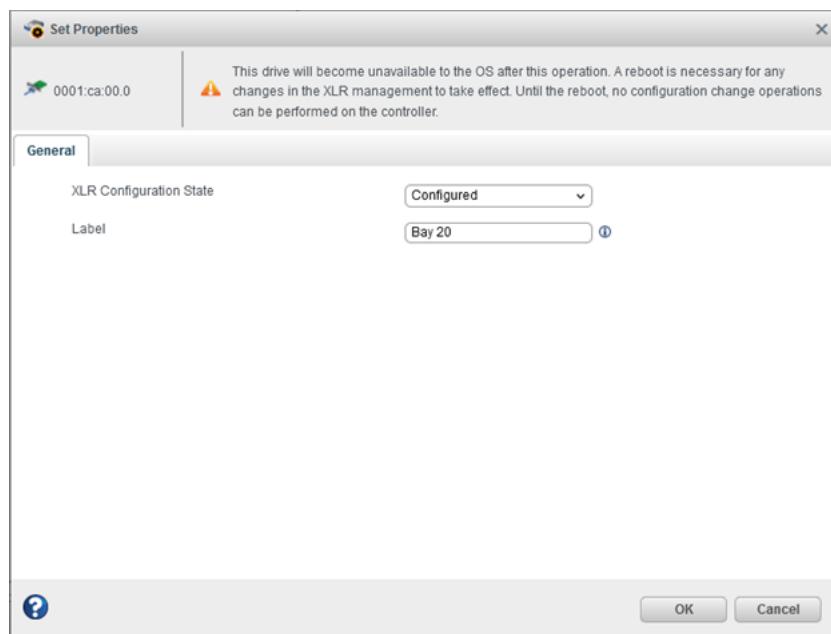
To configure the unconfigured NVMe drive:

1. Select the unconfigured device based on the PCIe address under the Unconfigured Devices group node.
2. On the ribbon, in the Physical Device group, click **Set Properties**.



The **Set Properties** window opens.

3. Select **Configured** option from the **XLR Configuration State** drop-down list.



4. Specify a label in ASCII format that does not include spaces and has a maximum of eight characters. This label is further used to identify each NVMe drive.
 5. Click Ok.
- Note:** Once you Configure/Unconfigure the NVMe drives, a reboot is necessary for any effect to take place. Until the reboot, no configuration change operations can be performed on the accelerator.

5.4.2.2 Unconfigure a NVMe Drive from Physical Device Level

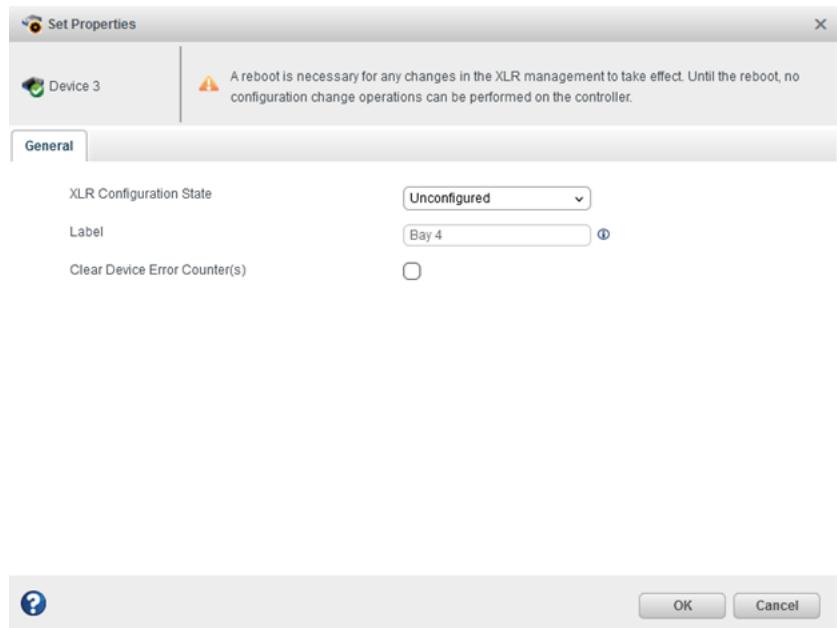
To unconfigure a configured NVMe drive which is not part of an array:

- 1.
2. Select a desired configured devices based on label.
3. On the ribbon, in the Physical Device group, click **Set Properties**.



The Set Properties window opens.

4. Select **Unconfigured** option from the **XLR Configuration State** drop-down list.



5. Click Ok.

Note: Once you Configure/Unconfigure the NVMe drives, a reboot is necessary for any effect to take place. Until the reboot, no configuration change operations can be performed on the accelerator.

5.5 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 NVMe SSDs, determine logical drive size and other advanced settings.
For instructions, see [Creating a Logical Drive on a New Array](#).
- Create logical drive on existing array—Helps you select an array on which to create the logical drive, set the RAID level, group NVMe SSDs, determine logical drive size and configure advanced settings.
For instructions, see [Creating a Logical Drive on an Existing Array](#).

5.5.1 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 [Creating a Logical Drive on an Existing Array](#).

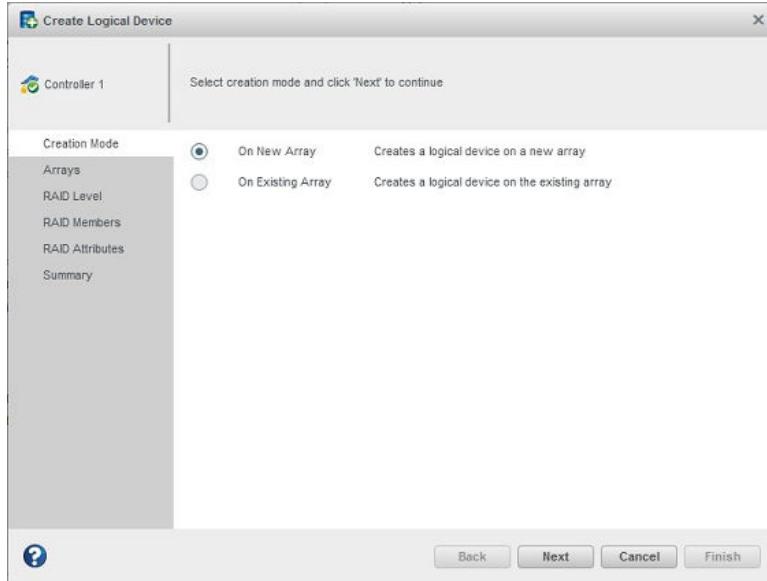
By default, maxView Storage Manager uses all available physical drive space to maximize the capacity of a new logical drive.

To create a logical drive on a new array:

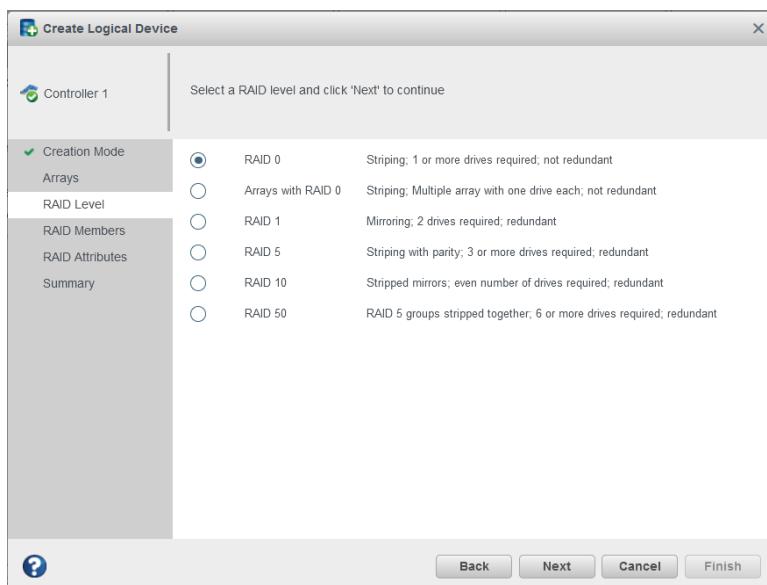
1. In the Enterprise View, select a system, then select a controller on that system.
2. On the ribbon, in the Logical Device group, click **Create Logical Device**.



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

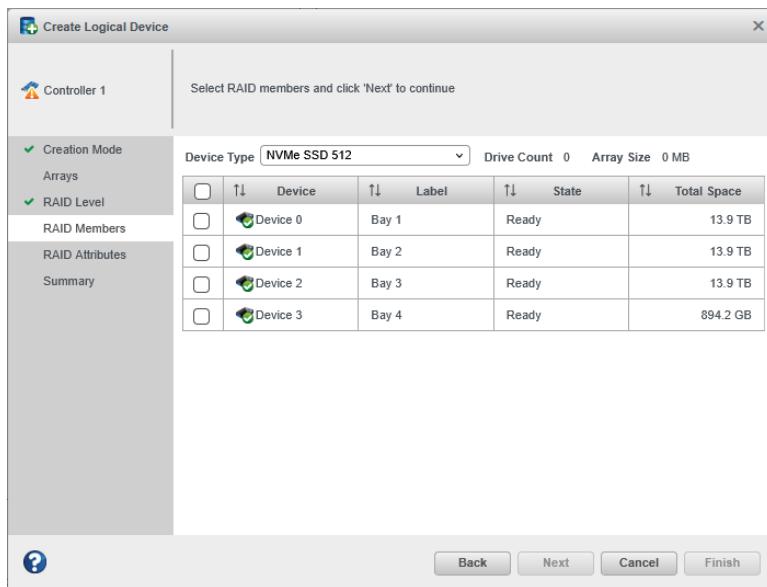


- Select a RAID level for the logical drive, then click **Next**.

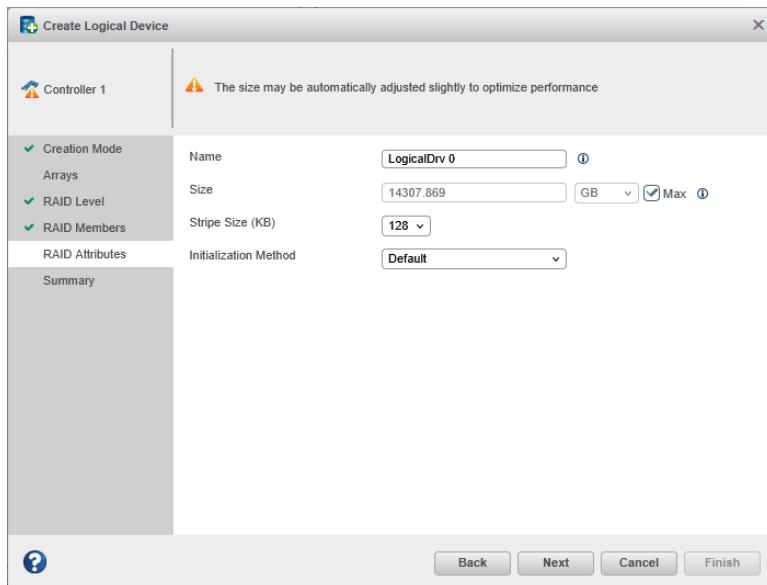


Note: Not all RAID levels are supported by all controllers. (See the Release Notes for more information.) See [Selecting the Best RAID Level](#) for more information about RAID levels.

- Select the physical drives you want to include in the logical drive, then click **Next**. Be sure that you select the right number of drives for the RAID level you selected.



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



You can:

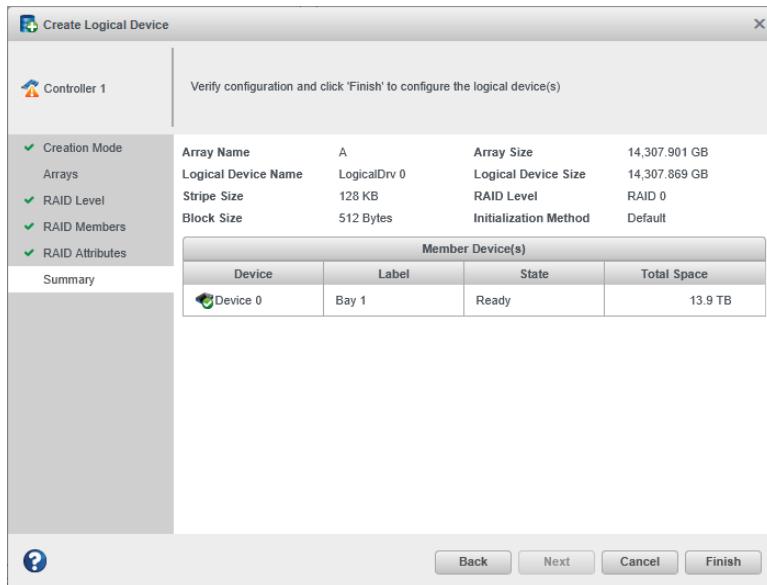
- Enter a name for the logical drive. Names can include any combination of letters, numbers, and spaces.
- Note:** Duplicate logical device names are not allowed.
- Set the size and unit of measure for the logical drive. (By default, a new logical drive uses all available physical drive space.)
- Change the stripe size—the amount of data, in bytes, written per physical drive in the logical drive. (The default stripe size usually provides the best performance.)
- 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.

- 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.



- Click **Finish**.

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

- If you have other physical drives or available physical drive space and want to create additional arrays on the controller, repeat Steps 2–8 .
- Repeat Steps 1–9 for each controller in your storage space.
- Partition and format your logical drives. See [Partitioning and Formatting Your Logical Drives](#).

5.5.2 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 [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:

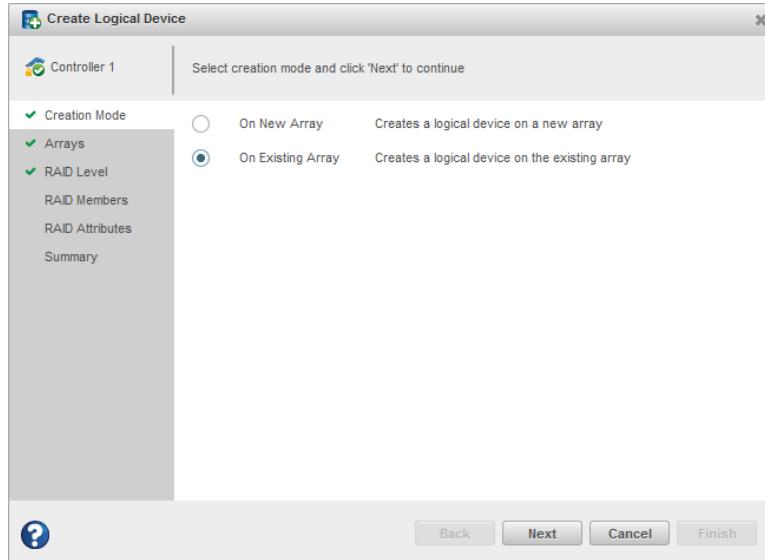
Logical drives can be added/created by selecting the existing array from the Enterprise view.

To create a logical drive on an existing array:

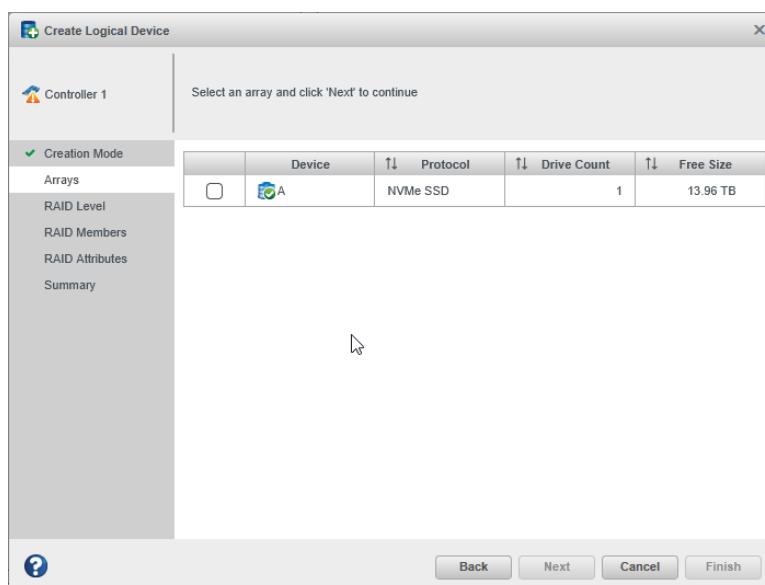
- In the Enterprise View, select a system, then select a controller on that system.
- On the ribbon, in the Logical Device group, click **Create Logical Device**.



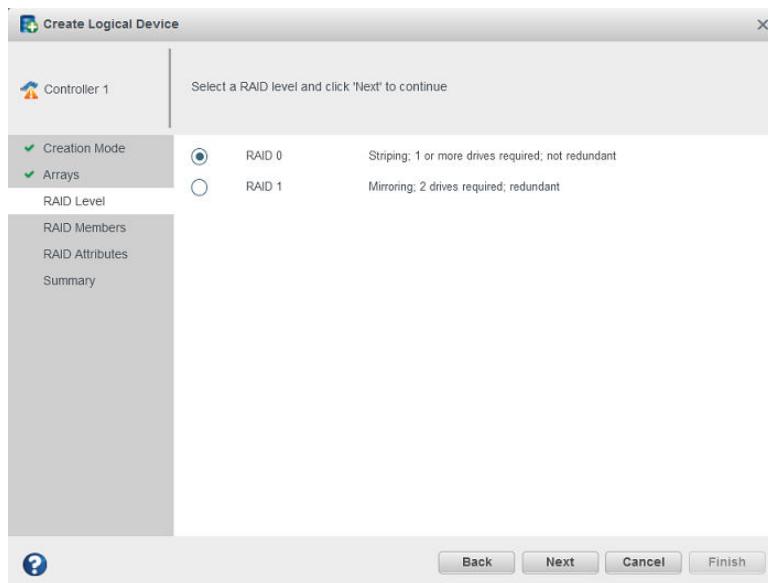
3. When the wizard opens, select **On Existing Array**, then click **Next**.



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

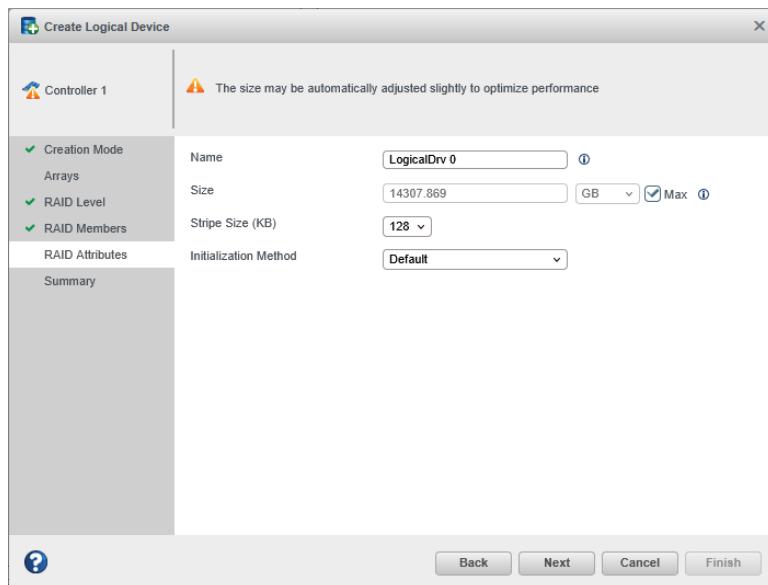


5. Select a RAID level for the logical drive, then click **Next**.



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:

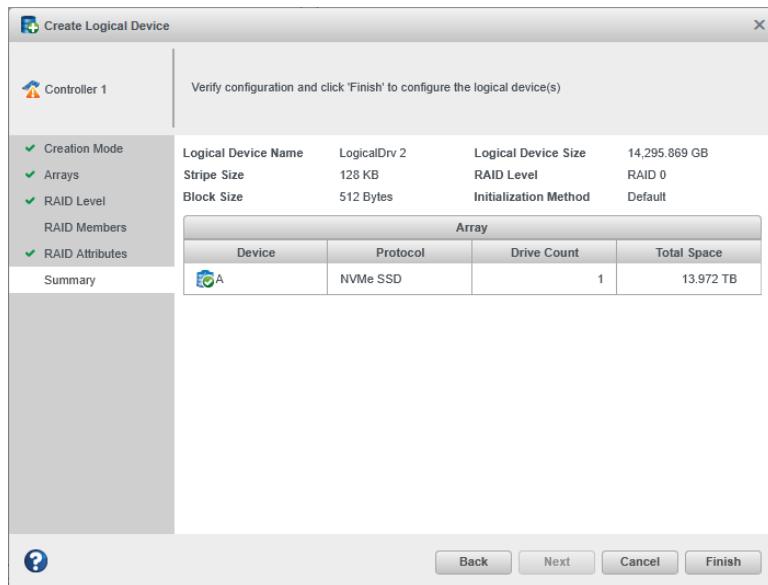
- Enter a name for the logical drive. Names can include any combination of letters, numbers, and spaces.
Note: Duplicate logical device names are not allowed.
- Set the size and unit of measure for the logical drive. (By default, a new logical drive uses all available disk space.)
- Change the stripe size—the amount of data, in bytes, written per disk in the logical drive. (The default stripe size usually provides the best performance.)
- 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.

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 physical drives or available physical drive space and want to create more logical drives on an existing array, repeat Steps 2-8.

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

11. Partition and format your logical drives. See [Partitioning and Formatting Your Logical Drives](#).

5.5.3 Partitioning and Formatting Your Logical Drives

The logical drives you create appear as physical 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.

See your operating system documentation for more information.

5.5.4 Creating Logical Drives on Other Systems in Your Storage Space

If maxView Storage Manager and Microchip Smart NVMe RAID Accelerator 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](#)).

6. Protecting Your Data

In addition to standard RAID (RAID 0, Arrays with RAID 0, RAID 1, RAID 5, RAID 10, RAID 50), Microchip controllers provide additional methods of protecting your data, including dedicated and auto-replace hot spare drives.

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

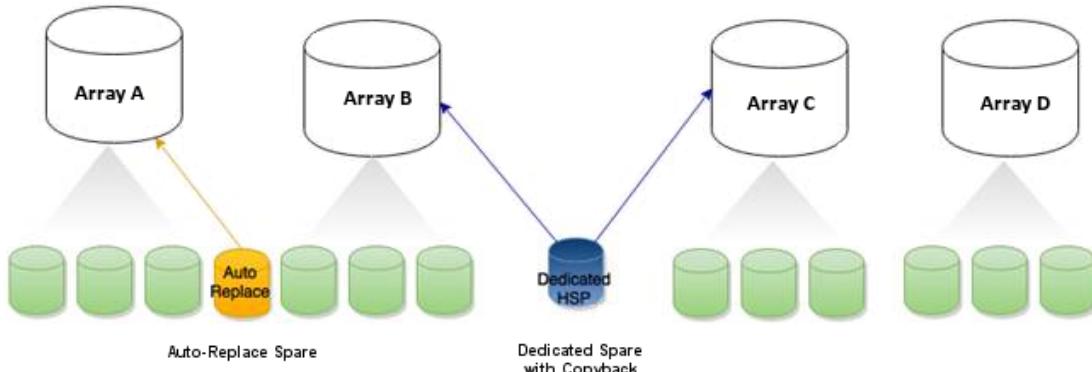
6.1

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 [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 [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 an NVMe SSD that is already part of an array.
- You should select an NVMe SSD that is at least as big as the smallest NVMe SSD in the array that it might replace.
- You must designate a NVMe SSD hot spare drive for an array comprised of NVMe SSD drives.
- Changing spare type for Shared Dedicated Spare Drive from physical device is not possible. The Array level Spare Management option must be used to change the Spare Type from Dedicated to Auto-Replace when the Dedicated Spare is protecting multiple arrays. By changing the spare type from Dedicated to Auto-Replace, the shared Dedicated Spare gets unassigned, and it does not protect the selected array anymore. The user must assign the ready drives as an Auto-Replace spare to protect the selected array.

6.3

Assigning a Dedicated Hot Spare

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

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

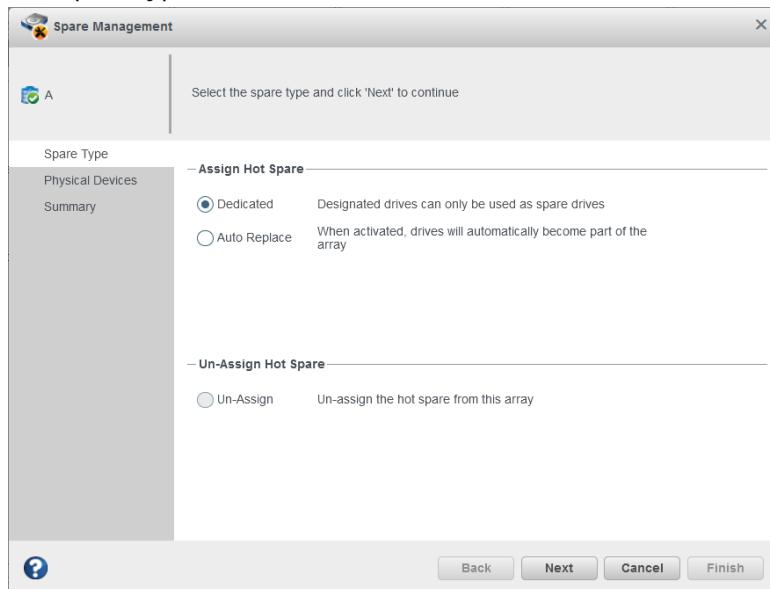
To assign a dedicated spare:

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

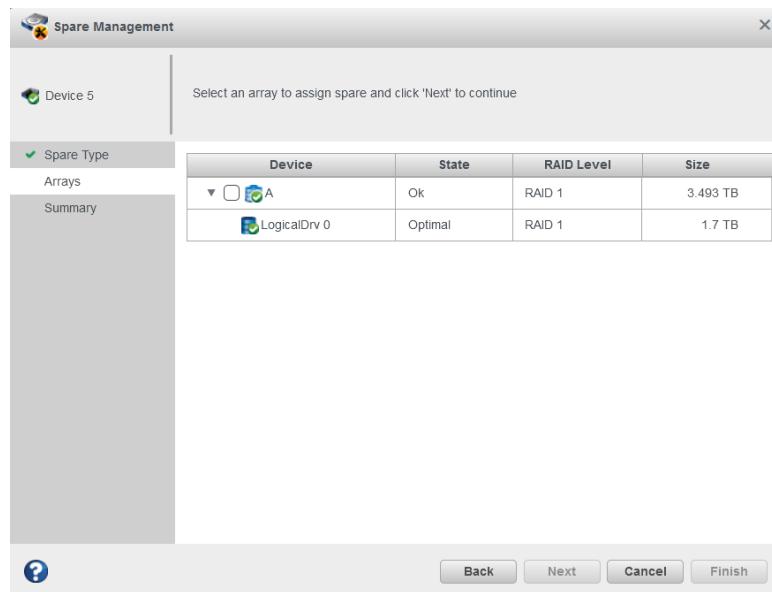


The Spare Management wizard opens.

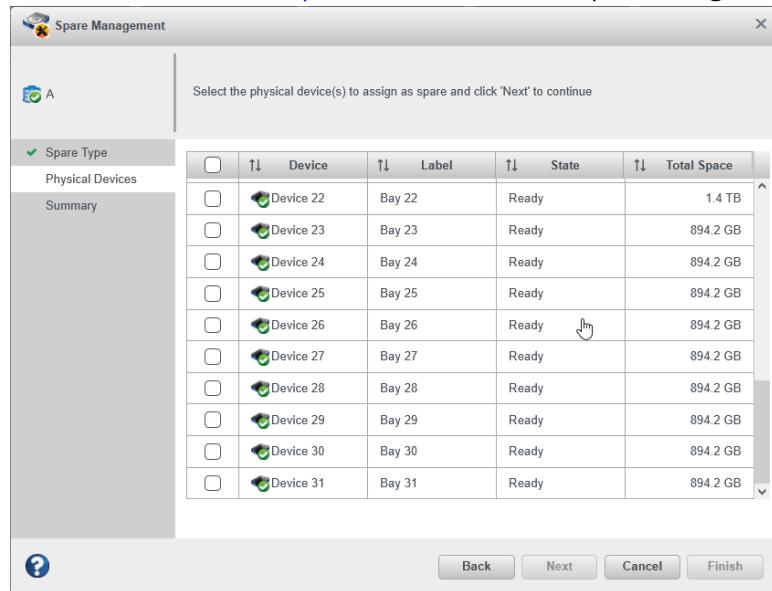
3. Select the **Dedicated** spare type, then click **Next**.



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



5. If you selected an array in the Enterprise view, select the physical drive(s) you want to dedicate as hot spares, then click **Next**. (See [Hot Spare Limitations](#) for help selecting drives.)



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

6.4

Assigning an Auto-Replace Hot Spare

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

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

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

Note: The auto-replace option is not available, if you select an array with a non-redundant logical device when the controller's "spare activation mode" is set to "failure activation".

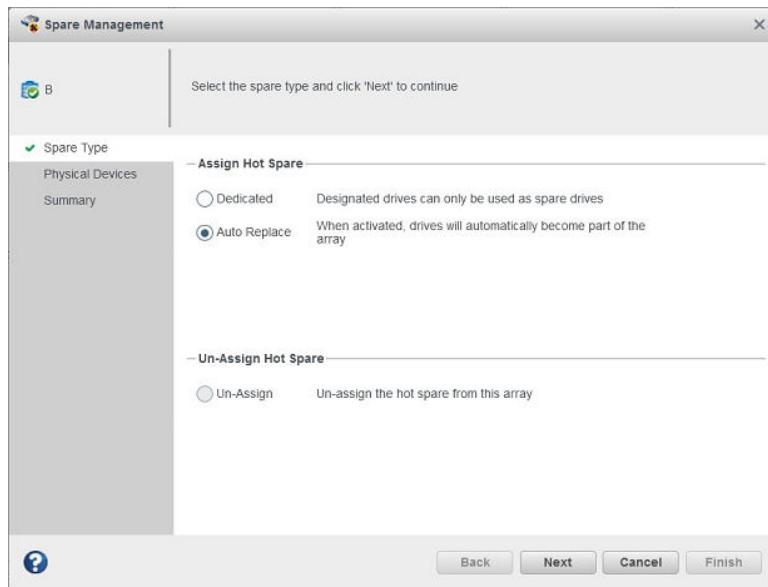
However, when you select a physical device itself, the option is available only if one or more auto-replace spares already exist. Otherwise, you can just assign Dedicated spares in the wizard.

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

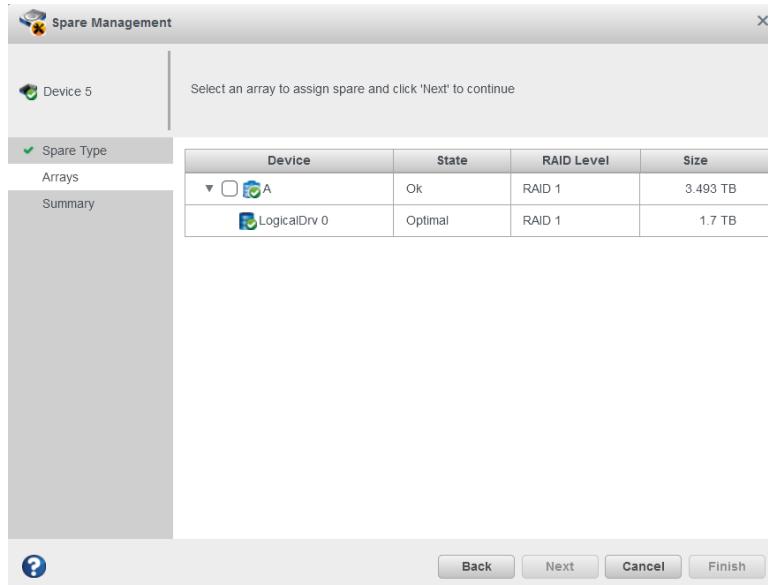


The Spare Management wizard opens.

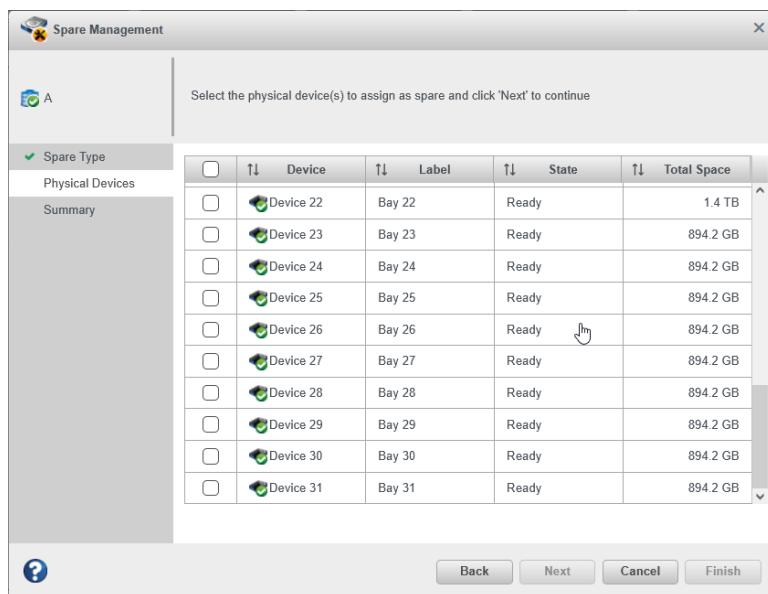
3. Select the **Auto-Replace** spare type, then click **Next**.



4. If you selected a controller in the Enterprise view, select the array you want to protect with an auto-replace spare, then click **Next**.



5. Select the physical drive(s) you want to assign as auto-replace hot spares, then click **Next**. (See [Hot Spare Limitations](#) for help selecting drives.)



- 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 physical 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.

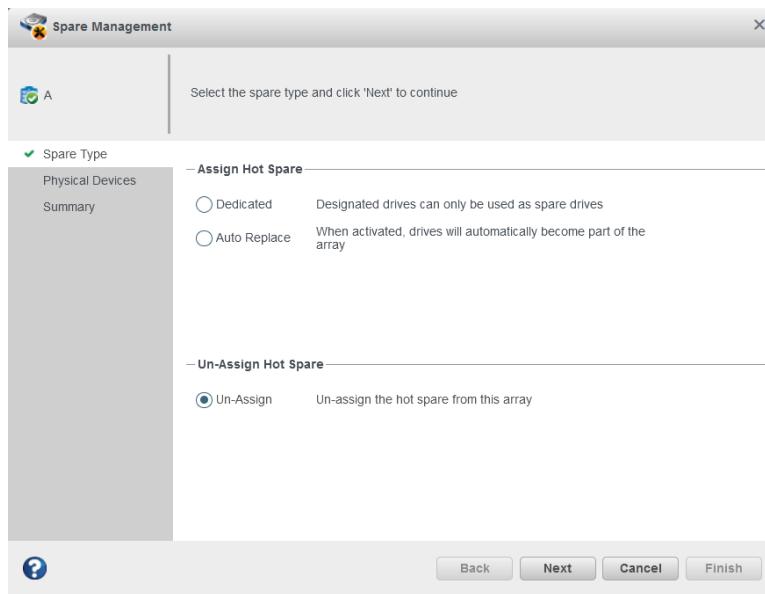
To remove a hot spare:

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

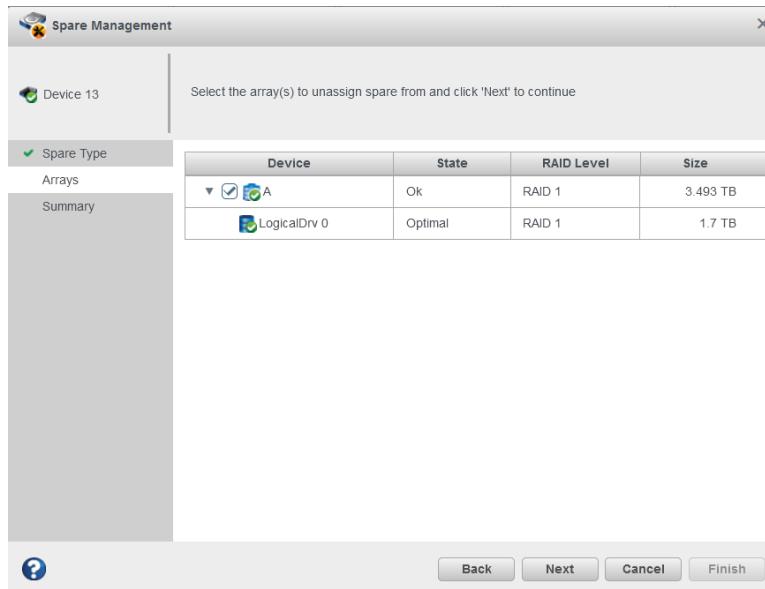


The Spare Management wizard opens.

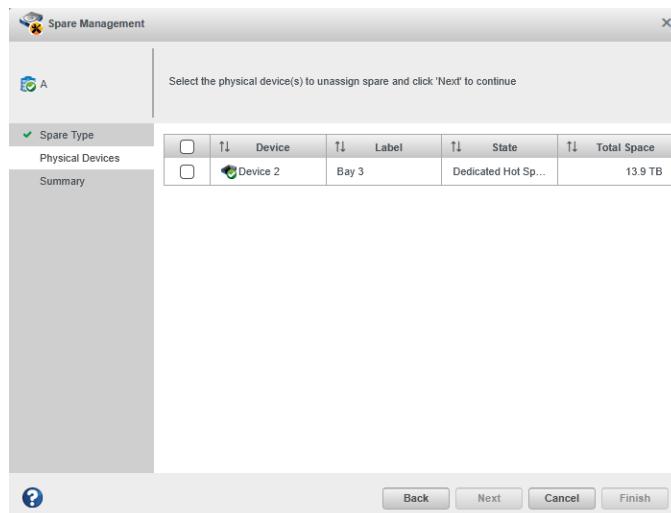
- Select **Un-Assign**, then click **Next**. (Un-Assign is preselected for an existing hot spare.)



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



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



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

6.6 Setting the Spare Activation Mode

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

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

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

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

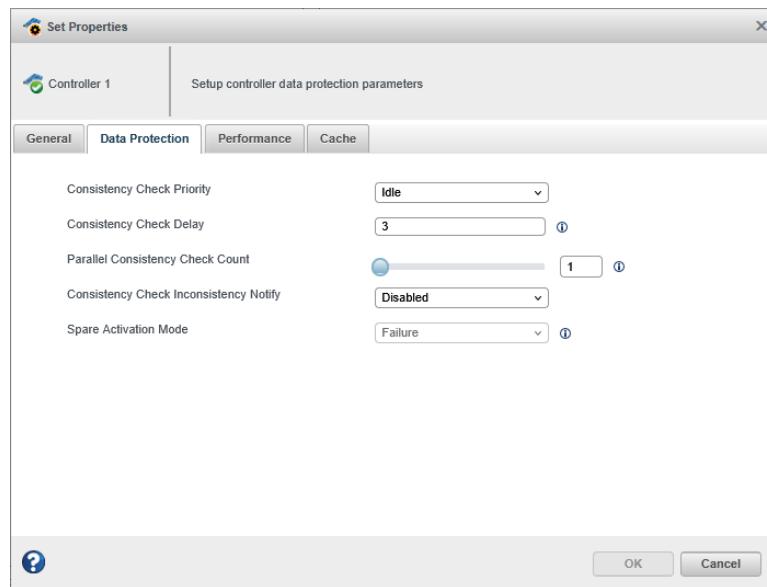
To set the spare activation mode:

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



The Set Properties window opens.

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



7. Modifying Your Storage Space

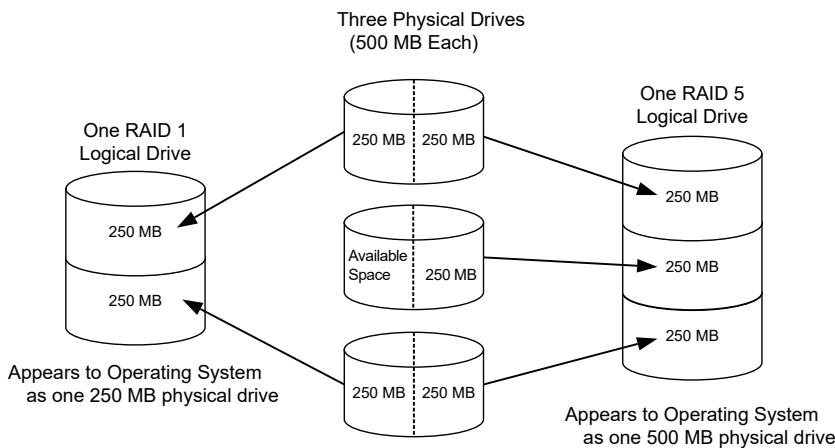
This section provides additional scenarios for creating and modifying arrays and logical drives. It explains how to check your logical drives for bad or inconsistent data; optimize controller and logical drive performance; move arrays and logical drives; and perform advanced operations, such as creating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

7.1 Understanding Arrays and Logical Drives

A *logical drive* is a group of physical 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 physical drive in two different logical drives by using just a portion of the space on the physical drive in each, as shown in the following figure.



Physical 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 physical drive's space. A physical drive with one segment is part of one logical drive, a physical 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 [Protecting Your Data](#) for more information.)

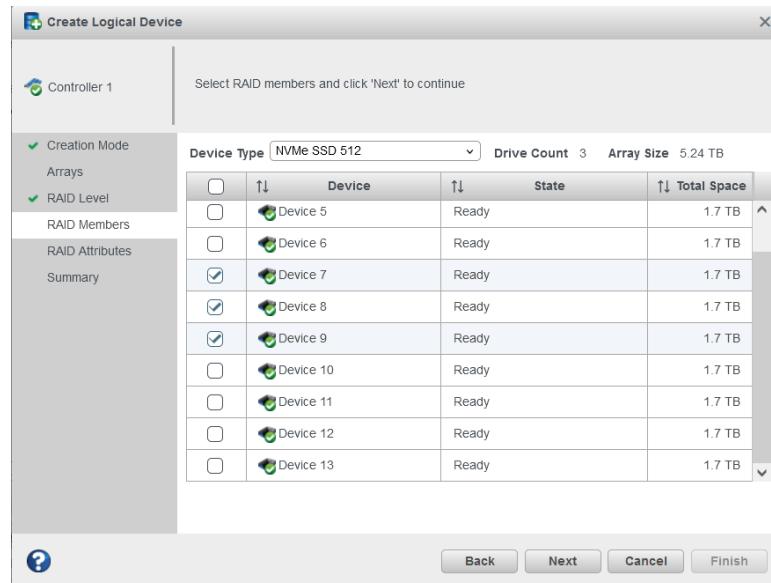
7.2 Creating and Modifying Logical Drives

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

7.2.1 Including Different-sized Physical Drives in a Logical Drive

You can combine physical 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 physical drive. (See [Selecting the Best RAID Level](#) for more information about redundancy.)

To create a logical drive with disk drives of different sizes, follow the instructions in [Creating a Logical Drive on a New Array](#). When the wizard displays the RAID Members panel, select different size drives, as shown in the following figure, 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.

Physical Device(s)						
	Device	State	Interface	Block Size	Total Size	
	Device 2	Ready	NVMe SSD	512 Bytes	1.7 TB	
	Device 3	Ready	NVMe SSD	512 Bytes	1.7 TB	
	Device 4	Ready	NVMe SSD	512 Bytes	1.7 TB	
	Device 5	Ready	NVMe SSD	512 Bytes	1.7 TB	
	Device 6	Ready	NVMe SSD	512 Bytes	1.7 TB	
	Device 7	Optimal	NVMe SSD	512 Bytes	1.7 TB	
	Device 8	Optimal	NVMe SSD	512 Bytes	1.7 TB	
	Device 9	Optimal	NVMe SSD	512 Bytes	1.7 TB	
	Device 10	Ready	NVMe SSD	512 Bytes	1.7 TB	
	Device 11	Ready	NVMe SSD	512 Bytes	1.7 TB	
	Device 12	Ready	NVMe SSD	512 Bytes	1.7 TB	
	Device 13	Ready	NVMe SSD	512 Bytes	1.7 TB	

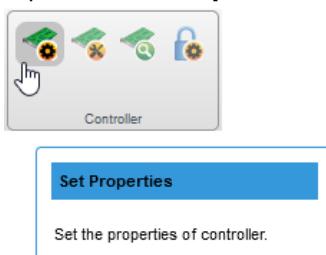
7.3 Enabling Background Consistency Check

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

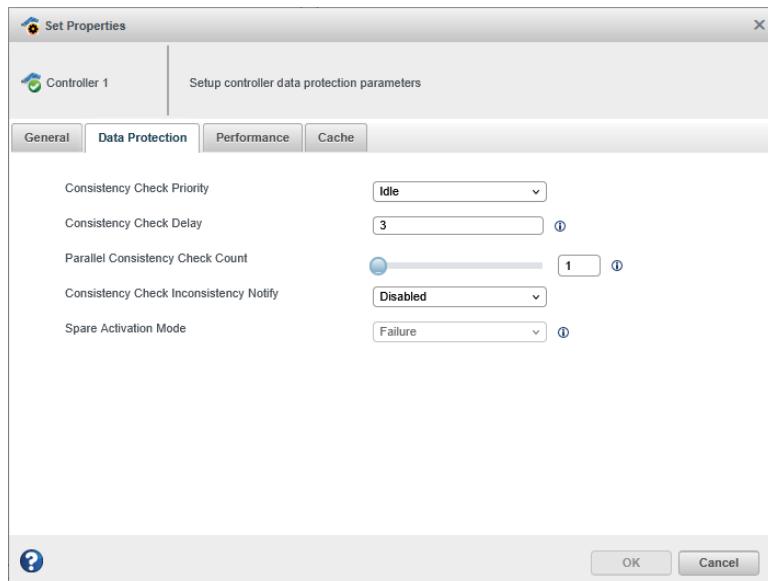
To enable or disable background consistency check:

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.

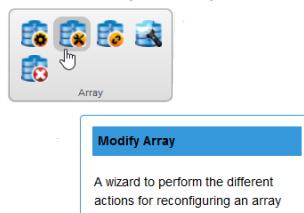
6. Click **OK**.

7.4 Modifying an Array

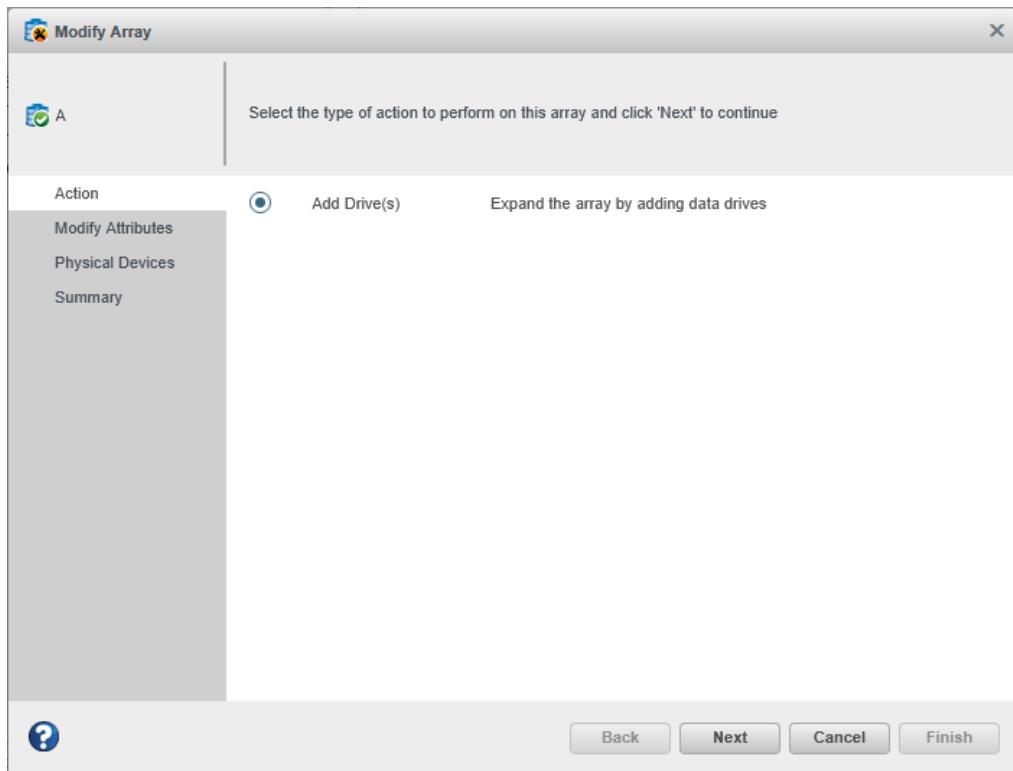
maxView Storage Manager allows you add Drives to an Array. If you add the logical drives, you are expanding the array by adding the data drives.

To add drives in an array:

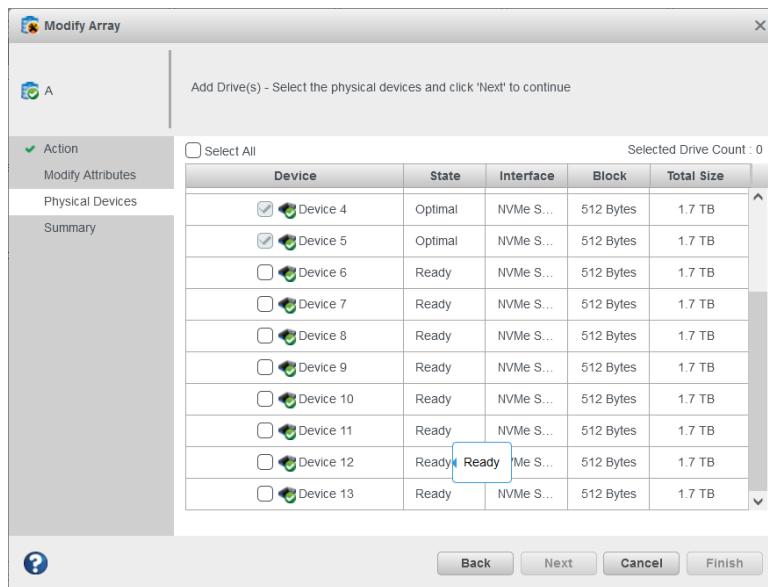
1. In the Enterprise View, select an array.
2. On the ribbon, in the Array group, click **Modify Array**.



3. When the wizard opens, select **Add Drive(s)**, 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.



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

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

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

7.5.1 Creating a Split Mirror Backup

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

- The primary array and backup array will contain identical RAID 0 logical drives.
 - The primary array continues to be fully accessible to the operating system.
 - The backup array is hidden from the operating system and data on the drive is frozen.
- Note:** You can use the backup array to restore the primary array with its original contents. See [Re-mirroring, Rolling Back, or Reactivating a Split Mirror Backup](#).
- 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**.



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

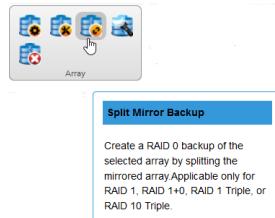
When you re-mirror a split mirrored array, you recombine the primary array and backup array into a single array. You can:

- 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.

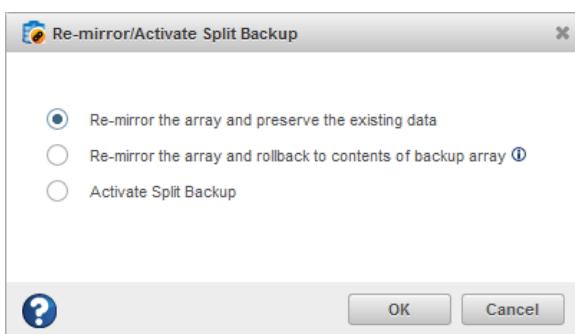
To re-mirror, roll back, or reactivate a split mirror backup:

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**.

7.6 Increasing the Capacity of a Logical Drive

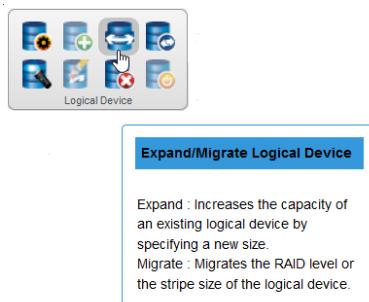
You can add more disk drive space, or *expand*, a logical drive, to increase its capacity.

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

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

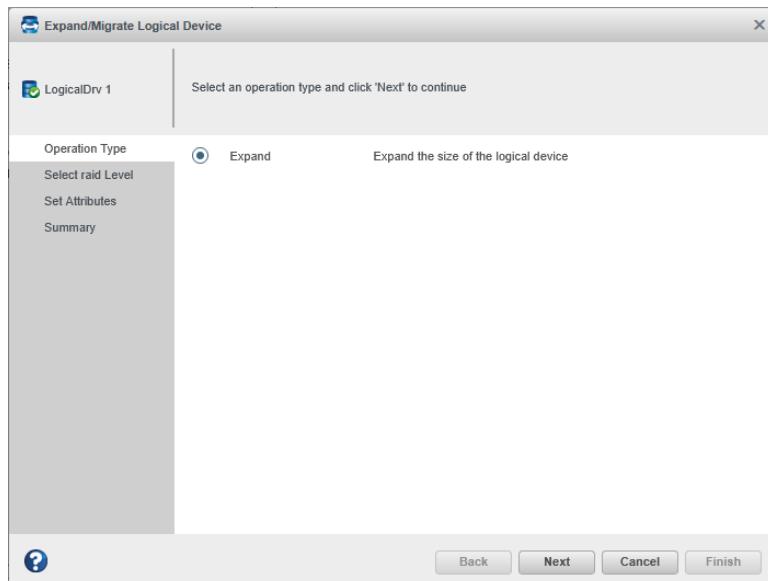
To increase the capacity of a logical drive:

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.

7.7 Changing the Logical Drive Rebuild Priority

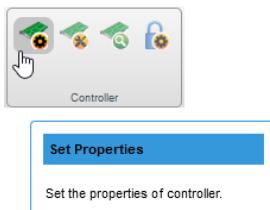
The Rebuild Priority setting determines the urgency with which the controller treats an internal command to rebuild a failed logical drive:

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

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

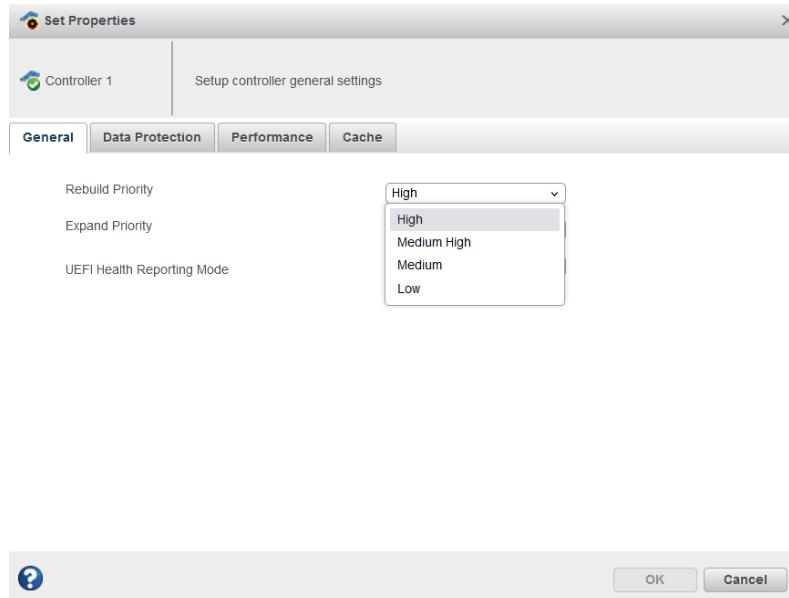
To change the rebuild priority:

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**.

7.8 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.

Note: Duplicate logical device names are not allowed.

7.9 Deleting an Array or Logical Drive

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



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

To delete an array or logical drive:

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



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

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

8. 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]

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

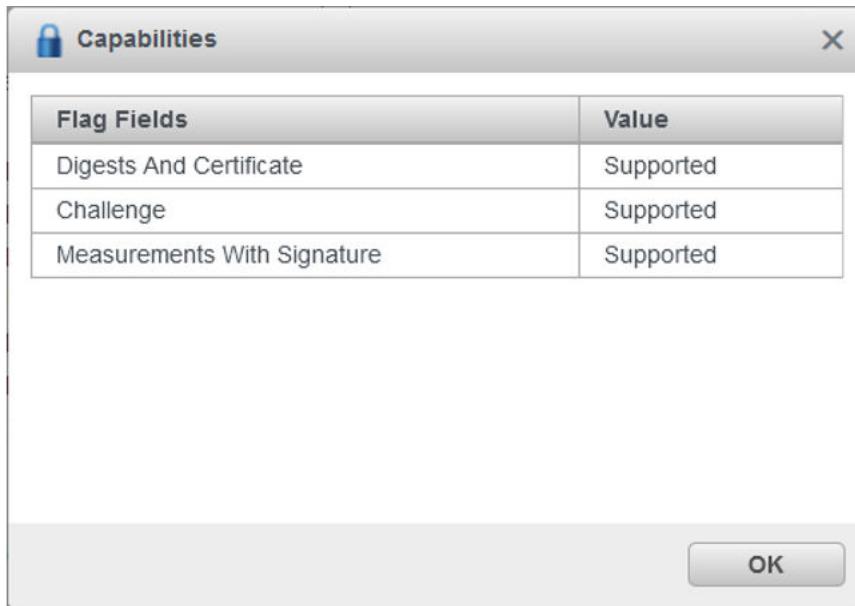
- SED Encryption Info
- maxCrypto Info
- Security Protocol and Data Model (SPDM) Info

Security Protocol and Data Model (SPDM) properties are available in **Security Protocol and Data Model (SPDM) Infopanel**.

The **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.



The screenshot shows a modal dialog box titled "Capabilities". At the top left is a lock icon, and at the top right is a close button (X). The main area contains a table with two columns: "Flag Fields" and "Value". The table has four rows, each with a "Supported" value. At the bottom right of the dialog is an "OK" button.

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).

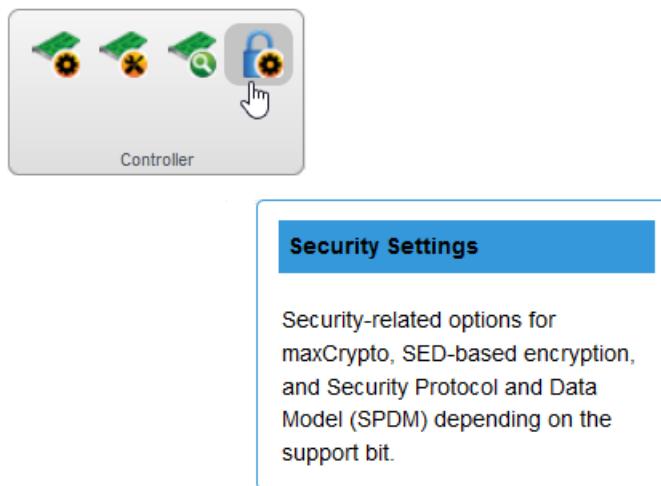
- **Single Pre-Shared Key (PSK):** Pre-Shared Key (PSK) is a type of cryptographic key that is shared in advance between two parties to secure their communication. A Single Key refers to a cryptographic key that is used for both message encryption and message authentication.

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

8.2 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 Security Settings ribbon icon to display the **Security Settings** dialog box.

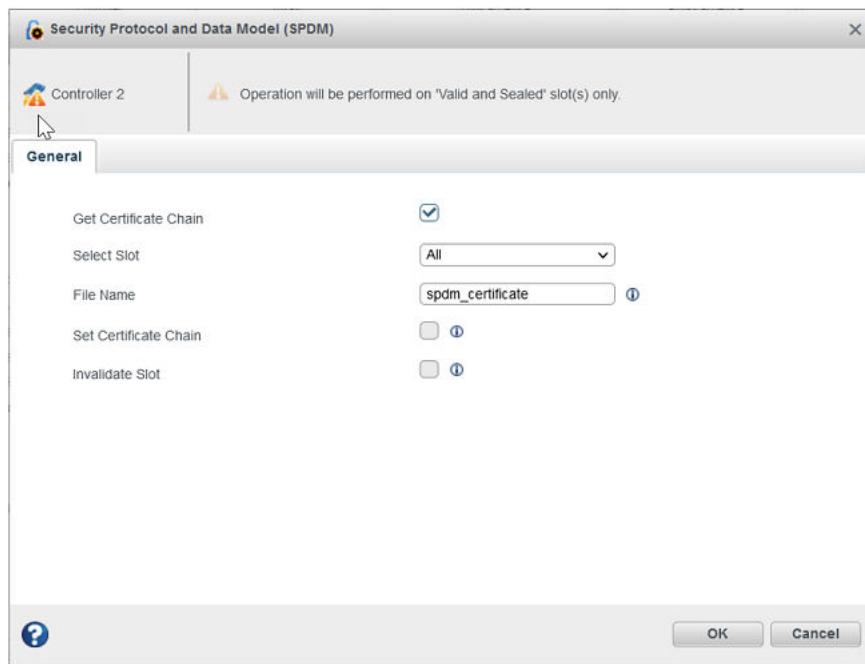


- Select the **Security Protocol and Data Model (SPDM)** option and then click OK. The **Security Protocol and Data Model (SPDM)** dialog appears, which is explained further in this section.

8.2.1 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.

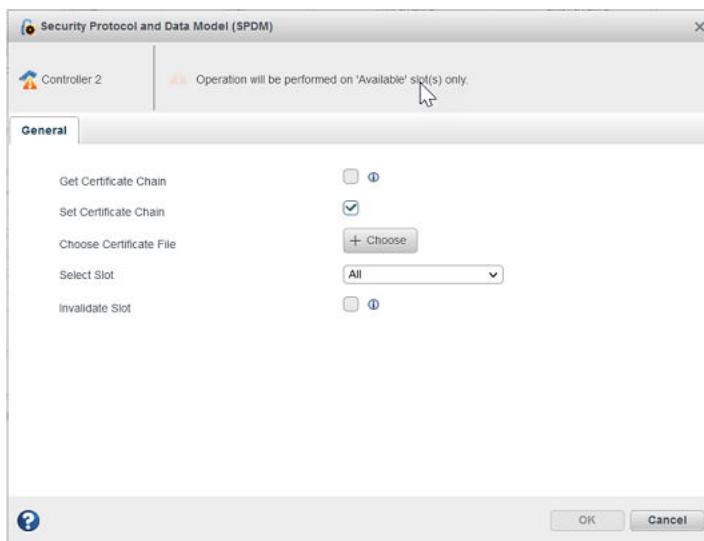


After checking the **Get Certificate Chain** check box, the **Select Slot** drop down option gets enabled to select the slot number. It displays only the valid slot number which has a certificate. You can select **All** option to retrieve the certificate chain from all the valid slot number.

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

8.2.2 Import Certificate Chain

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

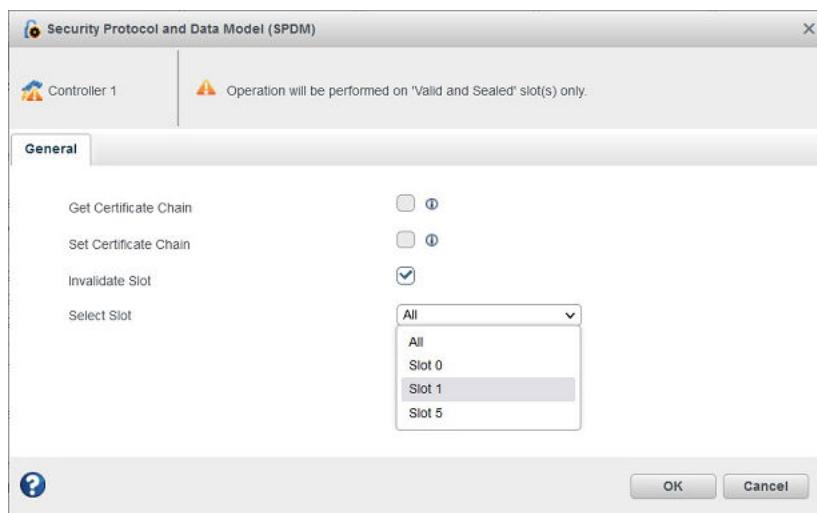


After checking the **Import Certificate Chain** checkbox, **Choose Certificate File** button and **Select Slot** drop down option gets enabled. Select the proper certificate file and upload it. Select the slot number to which the certificate chain should be written.

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

8.2.3 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.

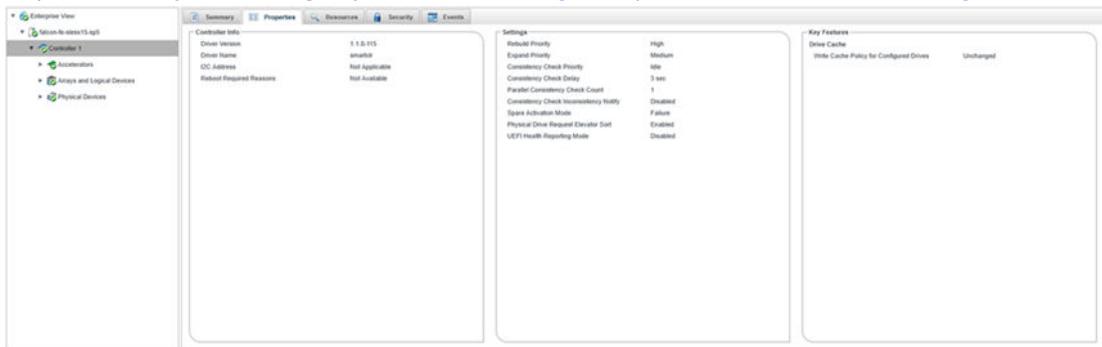
9. Maintaining Physical Devices

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

9.1 Viewing Device Properties

Click on any physical device in the Enterprise View then, on the Storage Dashboard, click the **Properties** tab to view version numbers, status, model numbers, features, and other information about the device.

The properties listed vary, depending on which type of device you select. The 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 [Viewing Component Status in the Storage Dashboard](#).



9.2 Locating Drives in Your Storage Space

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

Note:

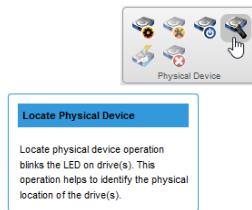
Once any of the device is located, the timeout value will be overwritten with the latest timeout value for all the located devices.

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

9.2.1 Locating Physical Drives

To locate an individual physical 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 Physical Device**.



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 physical drive(s) begin to blink.
5. To stop blinking the drive(s) immediately, click **Stop**.

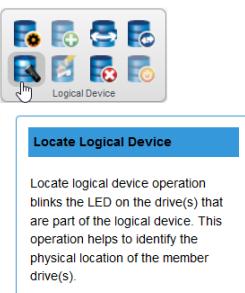


6. Click **Cancel** to close the Locate Physical Device window.
The LED(s) continue to blink for the duration of the timeout period.

9.2.2 Locating Physical Drives in an Array or Logical Drive

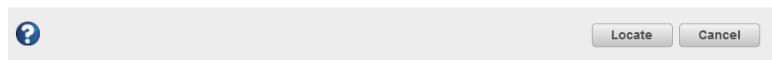
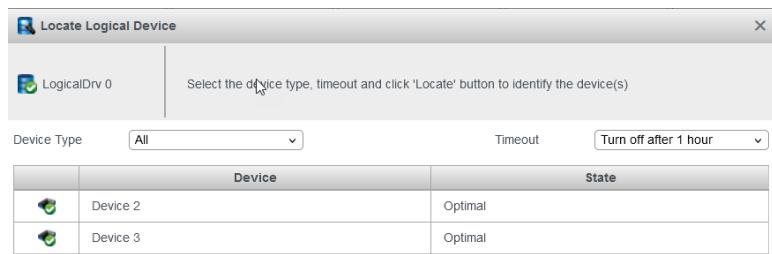
To locate all physical drives in an array or logical drive:

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 drives 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 physical drives begin to blink.

4. Click **Cancel** to close the Locate window.
The LEDs continue to blink for the duration of the timeout period.
5. Click **Stop** to stop blinking the drives immediately.

9.3 Working with Physical Device Error Counters

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

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

9.3.1 Viewing Physical Device Error Counters

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

Error Counter		Description
Aborted Command	0	Number of times a drive was failed due to aborted commands that could not be retried successfully.

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

Viewing Physical Device Error Counters (continued)

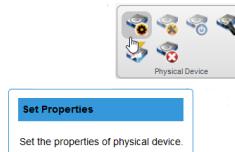
Error Counter	Description
Bad Target Error	Number of times that this drive did something that did not conform to the SCSI Bus Protocol. It will cause a reset of the SCSI bus that this drive is attached to.
ECC Recovered Read Errors	Number of ECC-corrected read errors.
Failed Read Recover	Number of times a recover of another physical drive in the logical volume failed due to a hard read error from this drive.
Failed Write Recover	Number of times a recover of this physical drive failed due to an error occurring on this drive during a write operation.
Format Error	Number of times a Format command (used when remapping defects) failed. A failed remap operation may cause the controller to fail a drive.
Hardware Error	Number of times a drive returned a bad hardware status. The drive may be failed if retries do not work.
Hard Read Error	Number of unrecoverable read errors.
Hard Write Error	Number of unrecoverable write errors.
Hot-Plug Count	Number of times this drive was hot-plugged (removed) from a box.
Media Failure	Number of times a drive was failed due to unrecoverable media errors.
Not Ready Error	Number of times the drive was failed because it never became ready after the "spin up" command was issued. If retries or drive spin-ups fail, the drive will be failed.
Other Timeouts	Timeouts other than Data ReQuest Timeouts (DRQ).
Predictive Failure	Number of times that the drive returned a predictive failure error.
Retry Recovered Read Error	Number of retry-recovered read errors.
Retry Recovered Write Error	Number of retry-recovered write errors.
SCSI Bus Fault	Number of "bus faults", which we define as SCSI bus parity errors, overrun/underrun conditions, etc.
Service Hours	Number of service hours since the last power cycle.
Sectors Written	Number of sectors written to media.
Sectors Read	Number of sectors read from the media. This value will include sectors read into the on-drive cache buffer only if the drive keeps track of this value. Otherwise, only sectors requested through the drive interface are counted.

9.3.2 Clearing Error Counters from a Physical Device

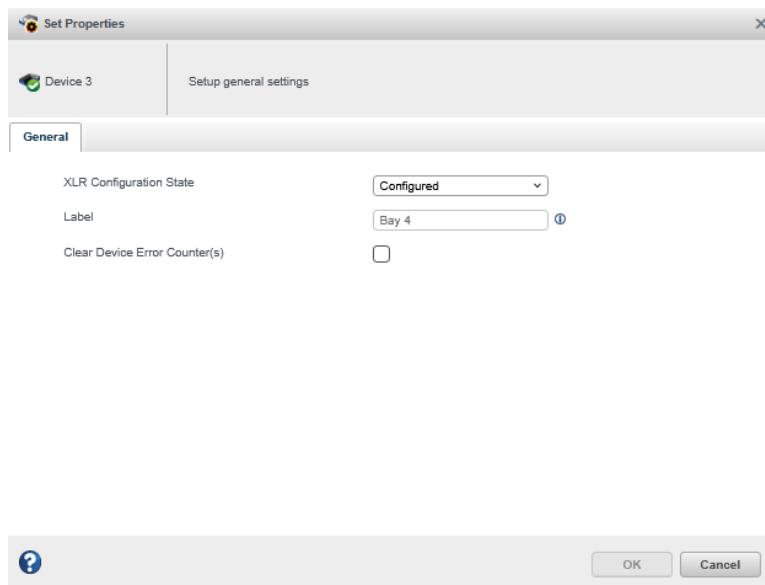
Use this option to clear the device error counters of a specific physical device.

To clear the error counters from a physical device:

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



The Set Properties window opens.



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

9.3.3 Clearing Error Counters from a Controller

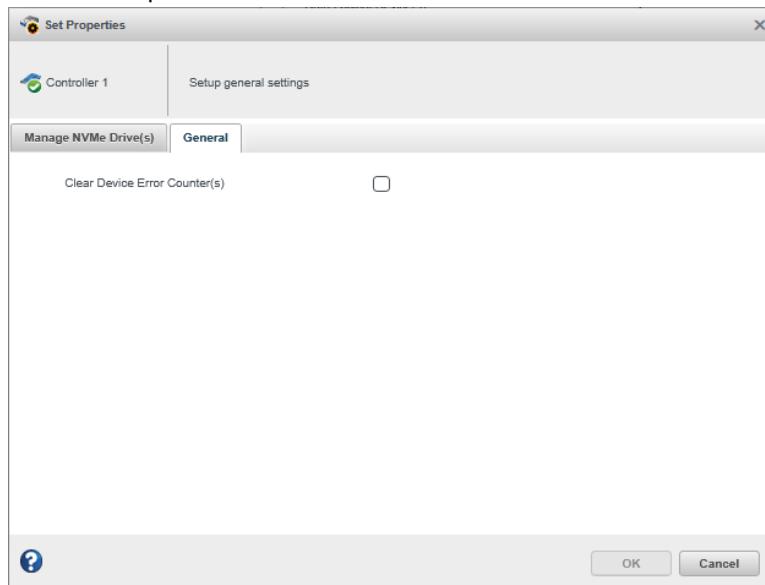
Use this option to clear the device error counters of all the physical devices from controller.

To clear 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**.

9.4 Working with Failed or Failing Physical Drives

This section describes how to use maxView Storage Manager to manage failed or failing physical drives in your storage space.

9.4.1 Replacing Disk Drives in a Physical Drive

You can replace one or more physical drives in a logical drive. You may want to replace a drive to upgrade to larger disk drives, or to make physical drive size uniform across the logical drive.



If another physical drive in the logical drive fails during rebuild (see [Rebuilding Logical Drives](#)), you may lose data. For help solving physical drive problems, see [Recovering from a Disk Drive Failure](#).

To replace a physical drive in a logical drive:

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

9.4.2 Setting a Physical Drive to ‘Failed’

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

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

- The physical drive is not part of a logical drive, or
- The physical 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.



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

To set a physical drive to Failed:

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



The Force Offline window opens.

3. Click **Force**.

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

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

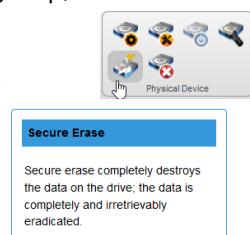
9.5 Erasing a Physical Drive

You can use maxView Storage Manager to *securely* erase existing data on any NVMe 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.

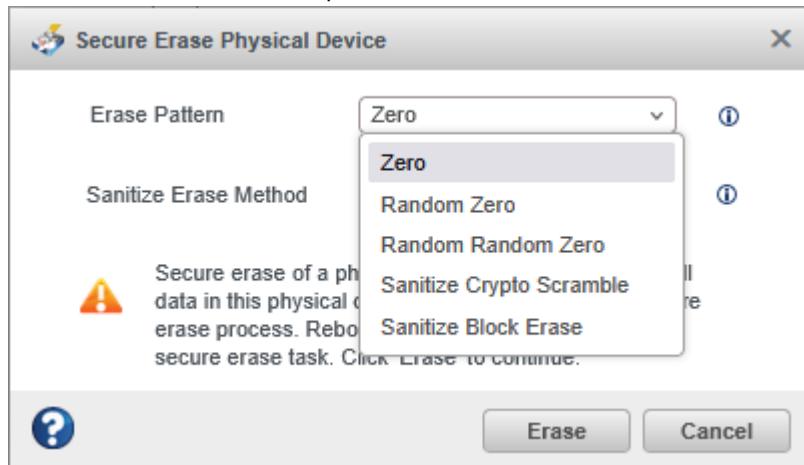
To securely erase an NVMe SSD:

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



The Secure Erase Physical Device window opens.

3. From the drop-down list, select the erase pattern:



- **Zero** (default)—Initializes all blocks to zero.
- **Random Zero**—Initializes block to random value then zero.
- **Random Random Zero**—Initializes block to random value, next block to random value, then zero.
- **Sanitize Block Erase**—(NVMe 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 NVMe SSD devices when supported by the device.

4. Click **Erase** to erase the drive.

9.5.1 Restricted/Unrestricted Secure Erase

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

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



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

9.6 Initializing and Uninitializing Physical Drives

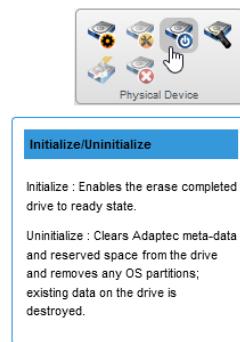
This section describes how to initialize/uninitialize disk drives to enable the erased drive, erase data and meta-data (including logical drive information) from the NVMe SSDs in your storage space. You can initialize or uninitialize individual disks, or use the wizard to initialize/uninitialize all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

9.6.1 Uninitializing a Physical Drive

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

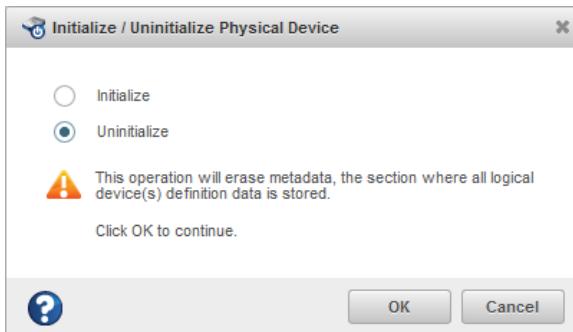
To uninitialized a physical drive:

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



The Initialize/Uninitialize Physical Device window opens.

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



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

9.6.2 Initializing/Uninitializing all Drives on a Controller

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

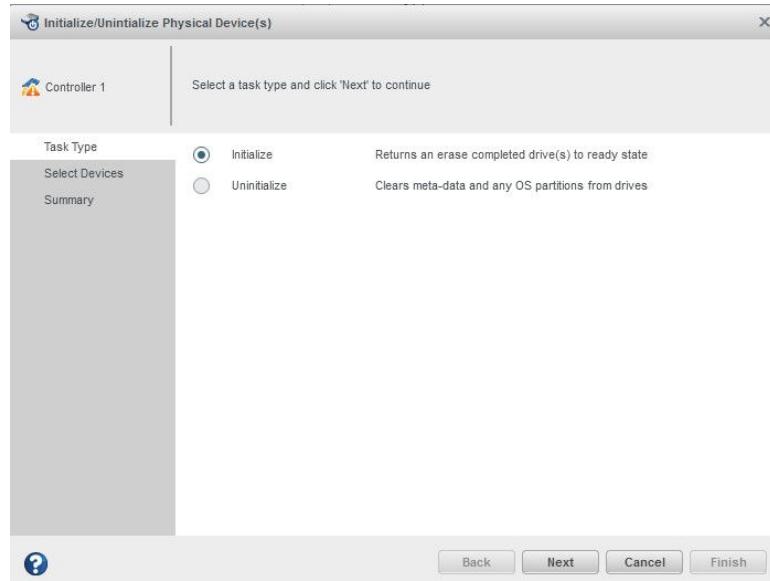
To initialize or uninitialized drives with the wizard:

1. In the Enterprise View, select a controller.
2. On the ribbon, in the Physical Device group, click **Initialize/Uninitialize**.



The Initialize/Uninitialize Physical Devices wizard opens.

3. Select Initialize or Uninitialize, then click **Next**.



4. Select drives on the controller to initialize or uninitialized, then click **Next**.

- Review the Summary, then click **Finish**.

9.7 Working with Controllers

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

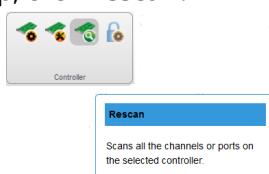
- To re-scan a controller, see [Rescanning a Controller](#).
- To optimize controller performance, see [Optimizing Controller Performance](#).

9.7.1 Rescanning a Controller

After you connect a physical 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:

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



The Rescan window opens.

- Click the **Rescan** button (on the Rescan window).
- maxView Storage Manager scans all the channels or ports on the controller you selected.
- When the rescan is finished, a success message is displayed. Click **OK** to close the Rescan window.

9.7.2 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
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.

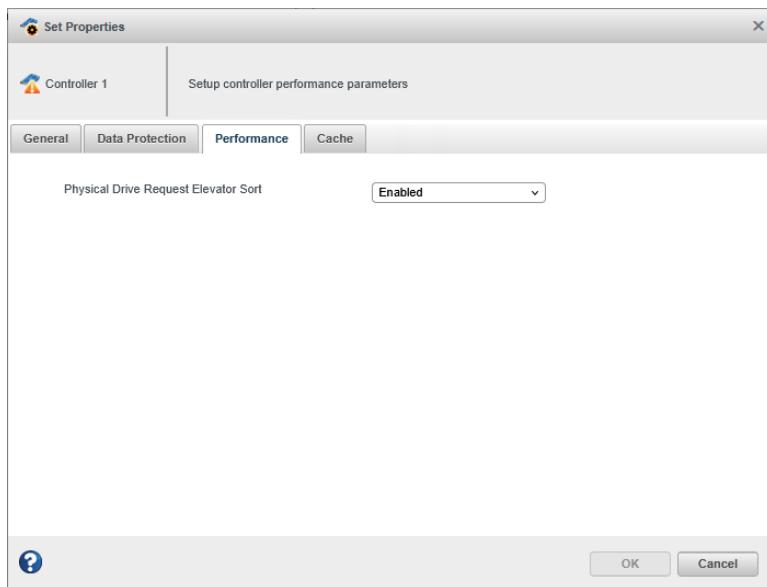
To enable/disable performance optimizations on a controller:

- 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 **Performance** tab.

- Enable/disable performance optimizations, as needed.



4. Click **OK**.

9.7.3 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.

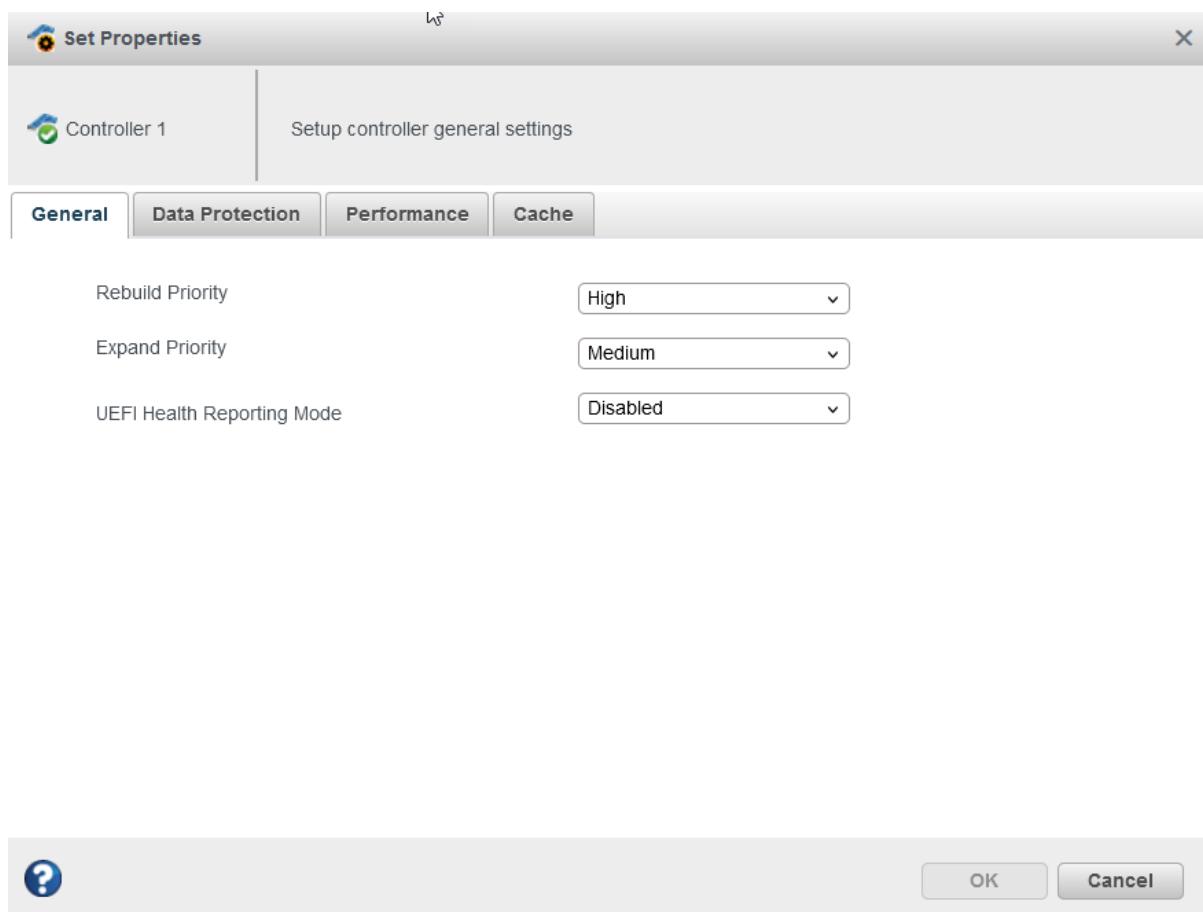
To change the UEFI Health Reporting Mode settings:

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.

9.8

Updating Accelerator and Physical Drive Firmware

Note: This task is recommended for advanced users only.

maxView Storage Manager includes a wizard to help you update the firmware on physical 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 physical drives from two different manufacturers, you must update the firmware for each manufacturer's drives separately, by running the wizard twice. Additionally, if you have more than one system in your storage space, you must run the wizard for each system separately.

To update the firmware on the physical drives in your storage space, review the prerequisites in [Before You Begin](#), then follow these sets of instructions:

- [Updating the Disk Drive Firmware](#)
- [Updating the Accelerator Firmware](#)

9.8.1 Before You Begin

Before you begin, download the latest firmware images from start.adaptec.com, or from your vendor's support site on the World Wide Web. Disk drive file names vary by manufacturer.

9.8.2 Updating the Disk Drive Firmware

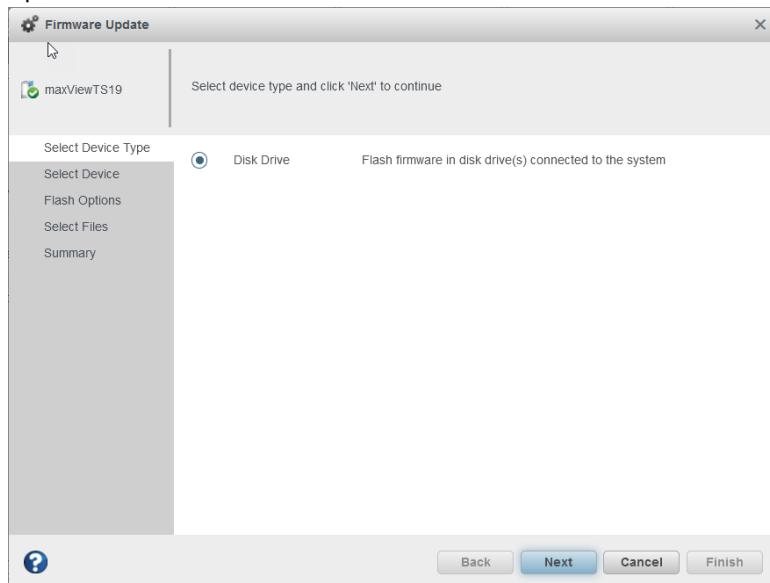
Use the Firmware Update wizard to update the firmware for one or more physical drives of the same type on the local or a remote system.

To update the physical drive firmware:

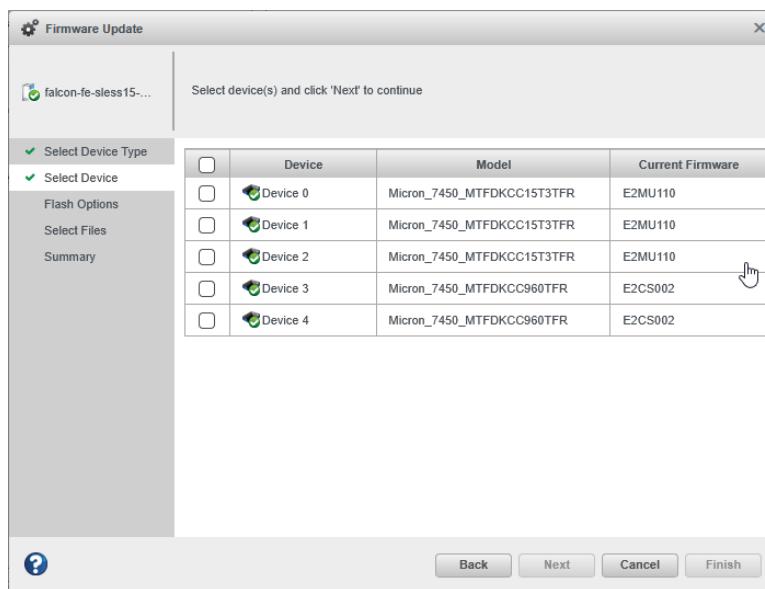
1. In the Enterprise View, select a system.
2. On the ribbon, in the System group, click **Firmware Update**.



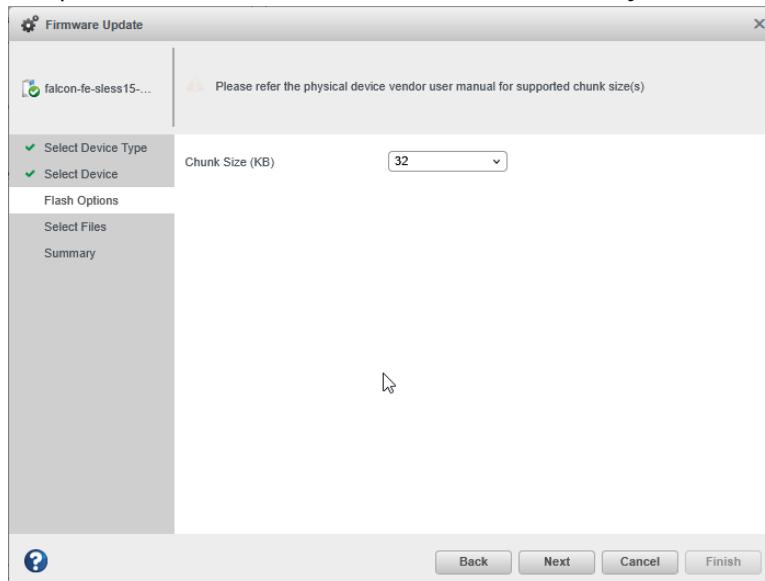
3. When the wizard opens, select **Disk Drive**, then click **Next**.



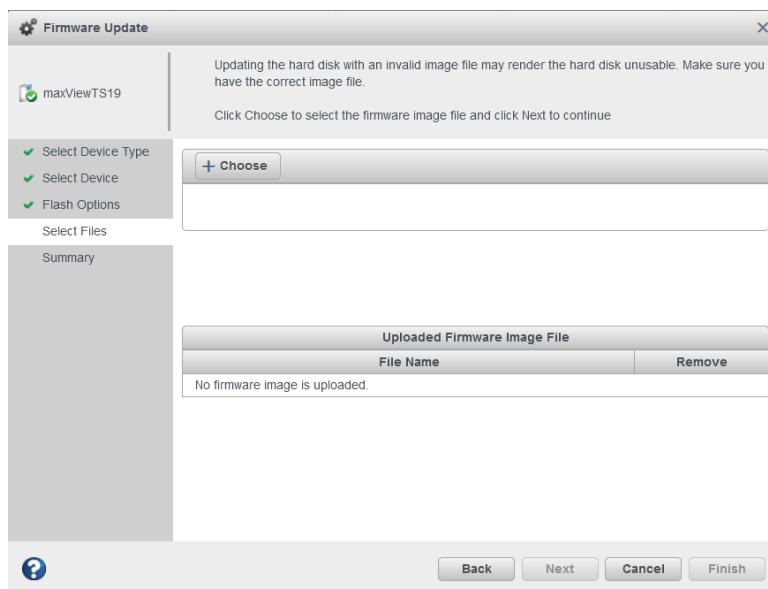
4. In the Select Devices panel, select the drive to perform firmware update operation, then click **Next**.



5. In the **Flash Options** panel, select the Chunk Size, from 1-n, in kilobytes (KB), then click **Next**.



6. 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).



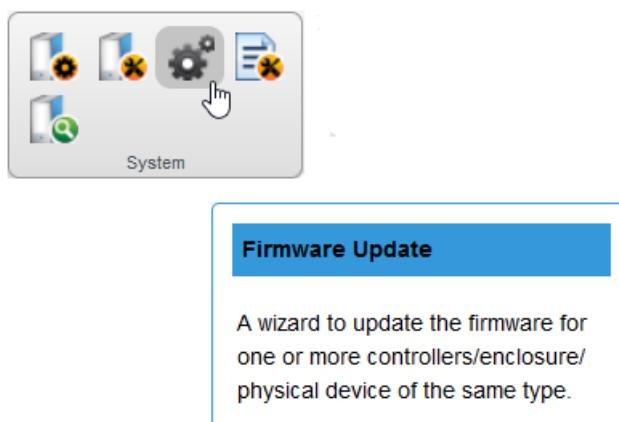
7. When the file name appears in the Uploaded Firmware Image File(s) list, click **Next**.
8. Review the update summary, then click **Finish**.

9.8.3 Updating the Accelerator Firmware

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

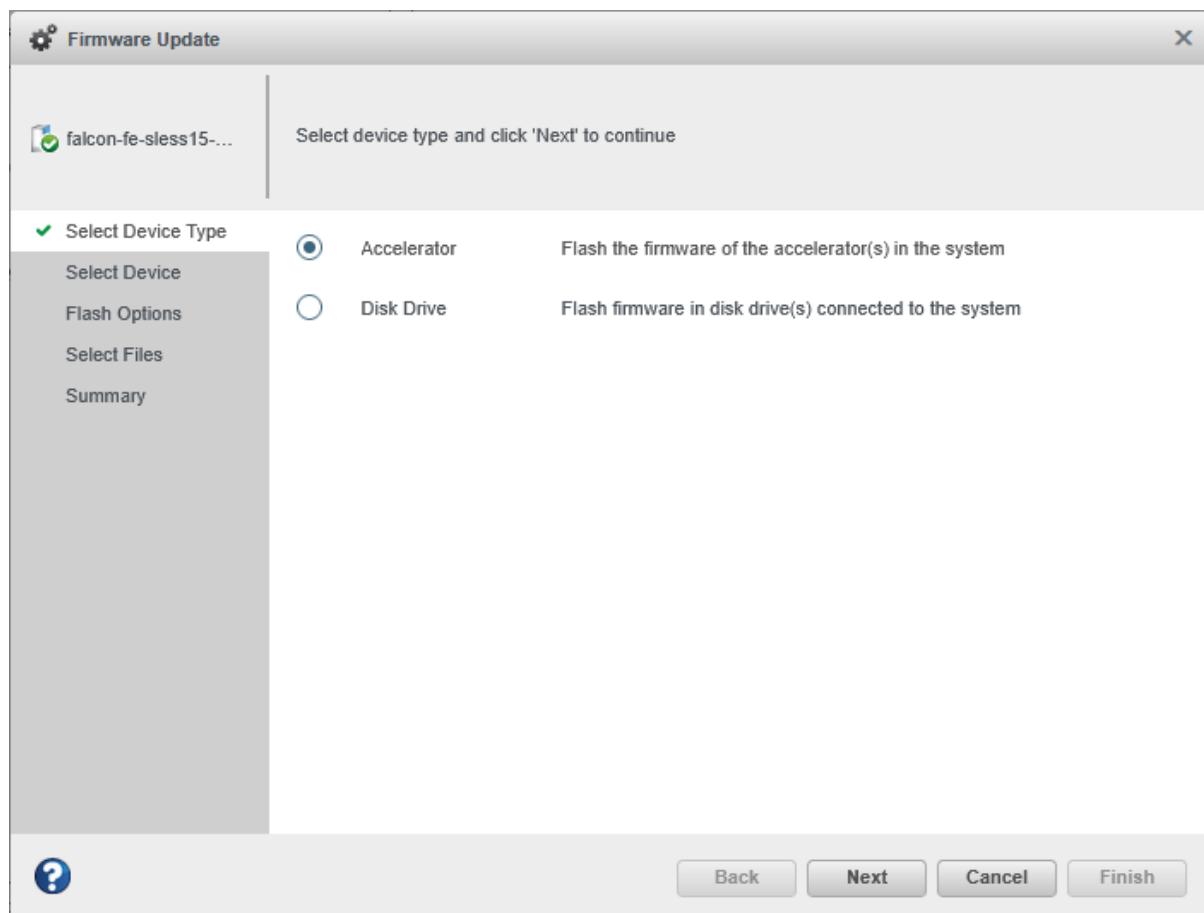
To update the accelerator firmware:

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

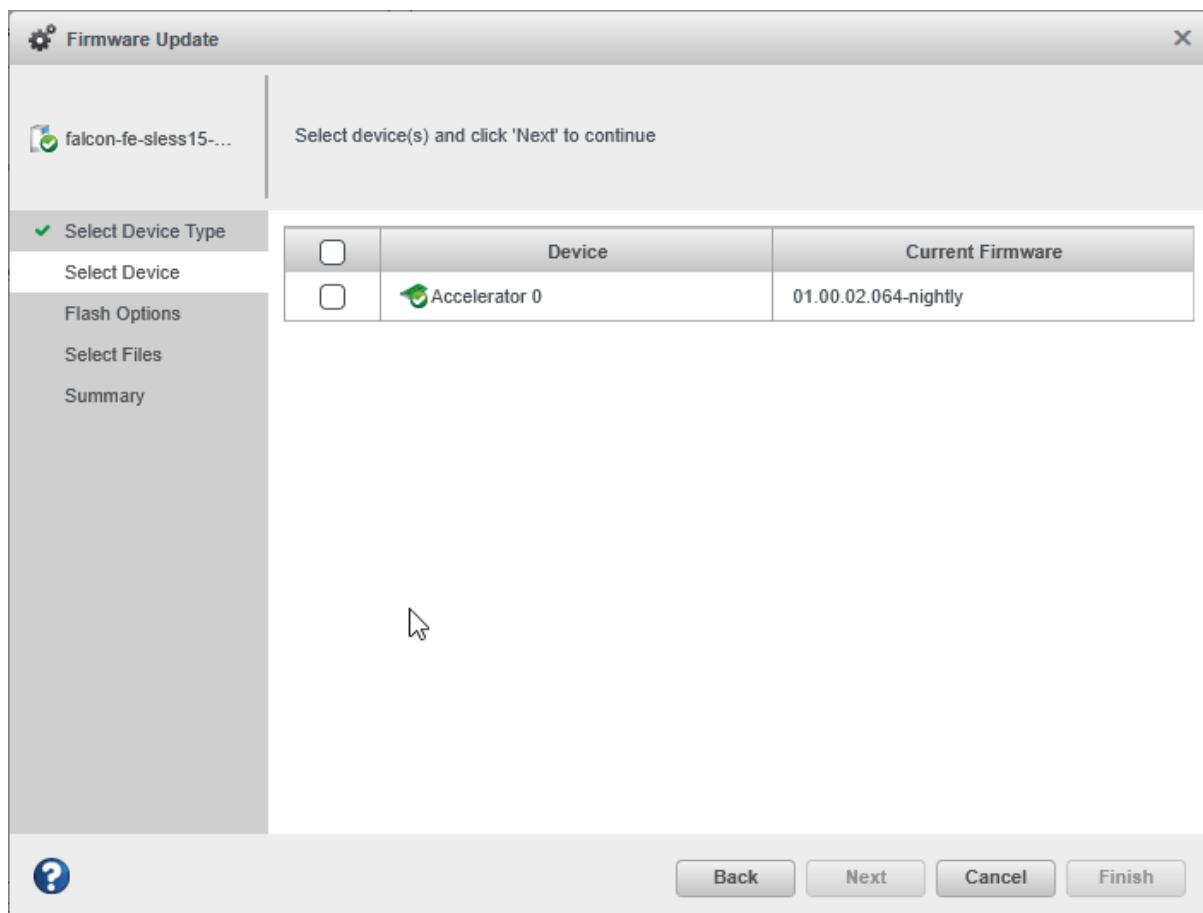


The Firmware Update window opens.

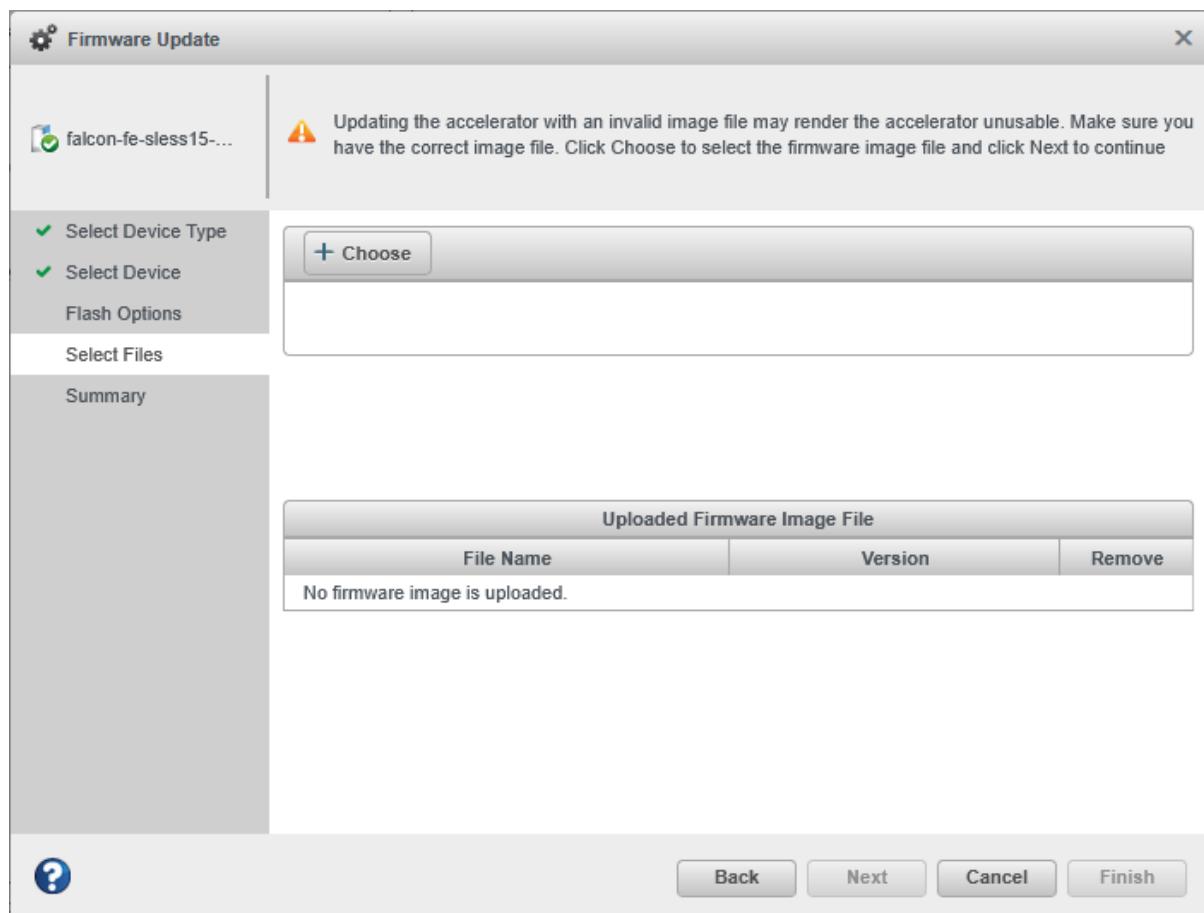
3. Select **Accelerator** from the Select Device Type panel, then click **Next**.



4. Select the accelerators that need to be updated the Select Devices panel, then click **Next**.

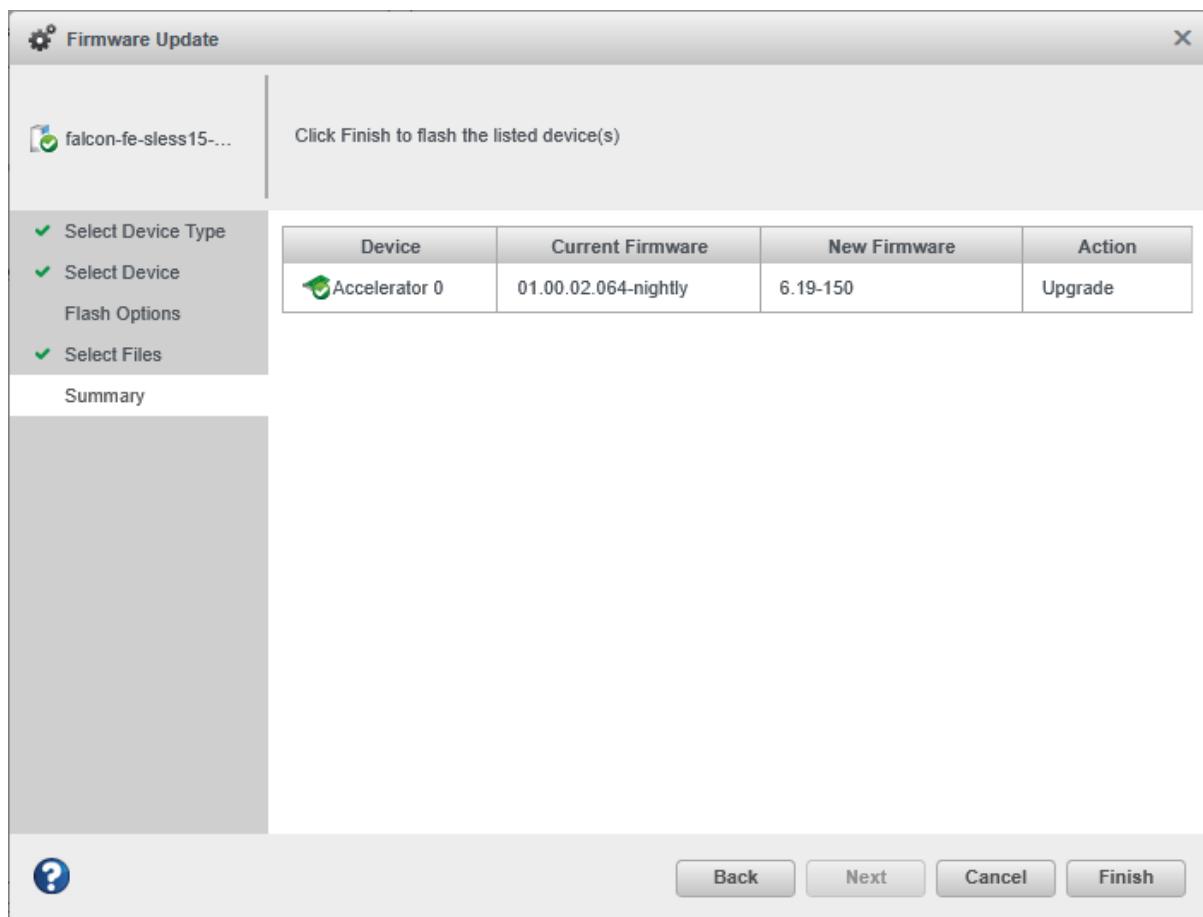


5. In the Select Files panel, click Choose to browse the file for the firmware update (typically, a .bin file). Click **Open** to select the file (the button label may be different on your browser).



The file name appears in the Uploaded Firmware File(s) list.

6. Click **Next** to review the summary, then click **Finish**.



⚠ CAUTION Do not power down the server while the update is in progress.

- When the update completes, click **OK**. Restarting the server may require activating the new firmware image.

10. Monitoring Status and Activity

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

10.1 Monitoring Options

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

- **Event Log**—The main window of maxView Storage Manager features an event log that provides at-a-glance status information about activity (or *events*) occurring in your storage space. All Warning- and Error-level events are also recorded in your *operating system's* event log. See [Viewing Activity Status in the Event Log](#) and [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 [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 NVMe SSDs. See [Viewing Component Status in the Storage Dashboard](#).
- **Chart View**—Provides a visual representation of free and used space for a system, controller, or your entire storage space. See [Viewing Storage Space Usage in Chart View](#).
- **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 physical drive failures.
 - Changes on local or remote systems, such as the creation of a hot spare.
 See [Notifying Users by Email About Status and Activity](#).
- **Audible Alarm**—A series of beeps sounds whenever a serious event occurs on your storage space.

10.2 Checking Status from the Main Window

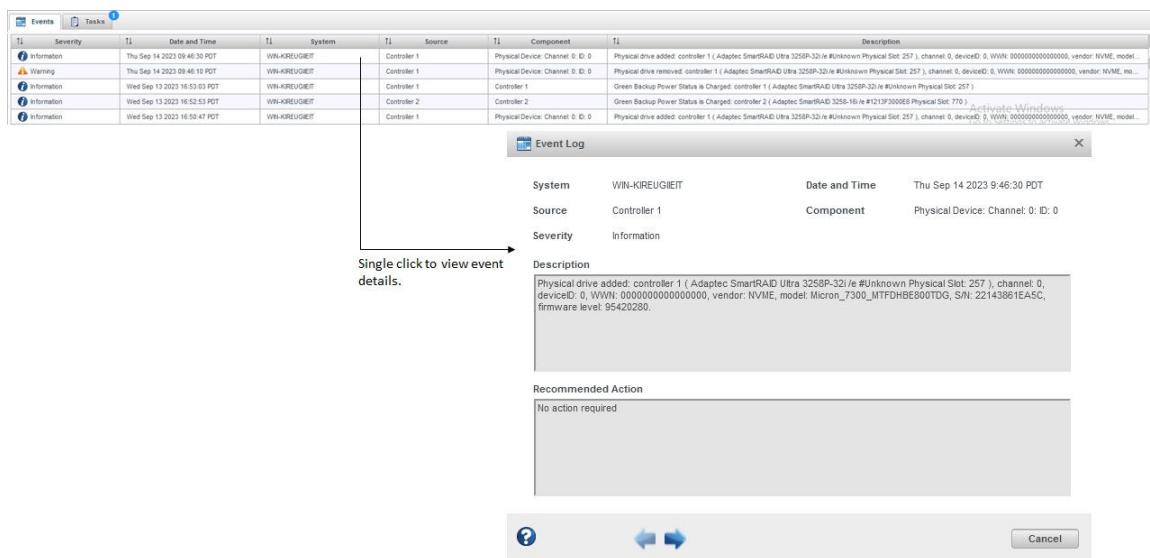
You can view status information and messages about the activity occurring in your storage space by looking at the *event log*, status icons, and *task log* in the main window of maxView Storage Manager. (You can also view all events for a system in its operating system event log; see [Changing an Operating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

10.2.1 Viewing Activity Status in the Event Log

The Event Log lists activity occurring in your storage space, with the most recent event listed at the top. Status is indicated by icons (see [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 [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.

10.2.1.1 What Do the Event Status Icons Mean?

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

Icon	Status	Examples
	Information	The local system successfully connected to a remote system. A logical drive was created. A hot spare was deleted.
	Warning	A logical drive is in a degraded state. A physical drive is being rebuilt.
	Error	A controller has failed. A logical drive has failed. A physical drive or hot spare has failed.

10.2.2 Viewing Task Status in the Task Log

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

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

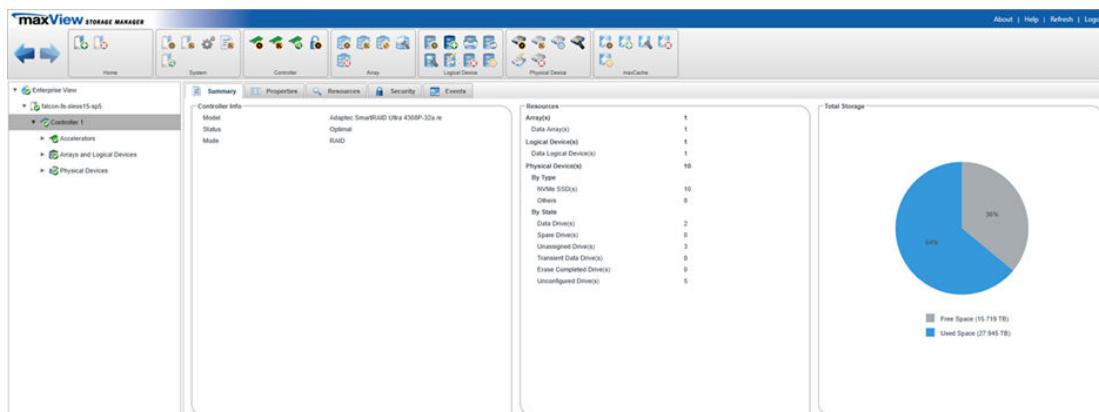
The screenshot shows the maxView Storage Manager interface. On the left, there's a table titled 'Tasks' with columns for Task ID, System, Description, State, Priority, and Progress. Two tasks are listed: 'Secure Erase (Random-Zero) physical device: controller 1, connector 0, slot 8' and 'Secure Erase (Zero) physical device: controller 2, slot 20'. Both are marked as 'Running' with 'High' priority and 0% progress. A tooltip says 'Single - click to view event details.' An arrow points from this tooltip to a 'Task Log' dialog window. This dialog has tabs for Task ID, System, Priority, and Description. It shows the same task details: Task ID S16, System WIN-KIREUGIEIT, Priority High, and Description Secure Erase (Random Random Zero) physical device: controller 1, connector 0, slot 8. The progress bar shows 1%. At the bottom of the dialog are 'Delete' and 'Close' buttons.

10.2.3 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 and NVMe SSDs. 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 [Viewing Activity Status in the Event Log](#)).

Note: For information about Chart View, on the right side of the Storage Dashboard, see [Viewing Storage Space Usage in Chart View](#).



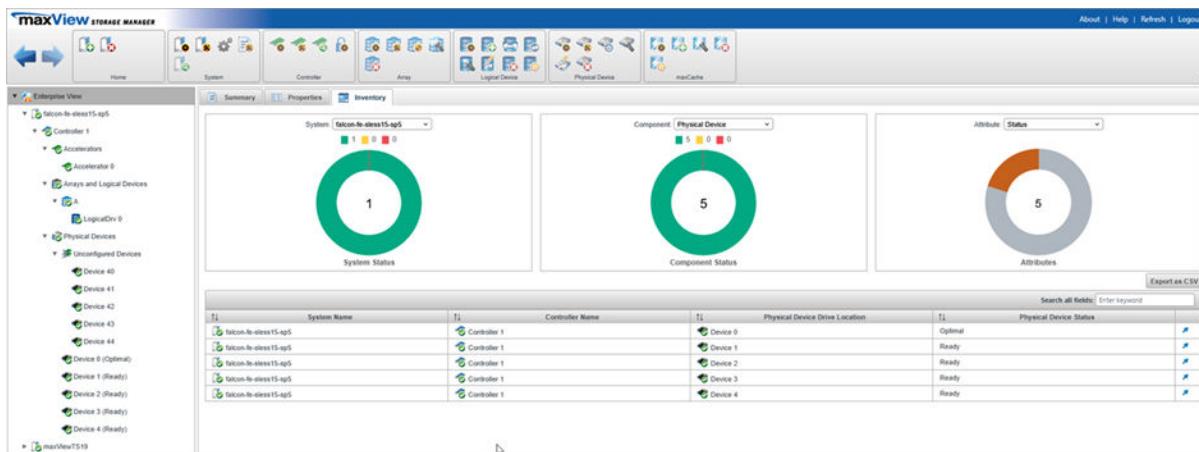
The following table lists the categories and types of information provided on the Storage Dashboard for each component in the storage space. All top-level nodes in the Enterprise View (System, Controller, Arrays, Logical Drives, Physical Devices, and so on) include a Summary tab and Events tab.

Component	Categories/Tabs	Examples
System	Summary Resources	Status, System Name, IP Address, OS Type, Number of Controller(s), Redfish Server Version, Redfish Server Port, Installation Type, Save Events to OS Log, Sound Alarm Device Model WWN State Firmware Version Driver Version
Controller	Summary Properties Resources	Model, Status, Mode, Driver Version, Driver Name, I2C Address, Reboot Required Reasons Number of physical drives, arrays, logical drives, and status Data Protection features Consistency Check Priority, Consistency Check Delay, Parallel Consistency Check Count, Consistency Check Inconsistency Notify, Spare Activation Mode Performance optimizations and other settings Physical drive assignments by logical device (see Revealing More Device Information)
Accelerator	Summary	Accelerator ID, Serial Number, WWN, Physical Slot, Temperature, Power Consumption, Negotiated PCIe Data Rate, PCI Address (Domain:Bus:Device.Function), NOR Flash Type, Firmware Version, Hardware Revision, Hardware Minor Revision, CPLD Revision
Arrays	Summary Resources	ID, Name, Device Type, Interface Type, Total Space, Used Space, Unused Size, Member Device(s) Block Size Spare rebuild mode Logical drive RAID level, size, status
Logical drives	Summary Resources	Raid level, segment and group (RAID 10 only), size, mount point, status Member drives and sizes
NVMe SSDs	Summary Properties Resources SMART Error Counter	Vendor, Model, Serial Number, Interface type (NVMe SSD), Total Size, Logical/Physical Block Size Sanitize Erase, Encryption Capability Drive state (Ready, Optimal, Hot Spare), mount point Channel number and device ID Transfer speed Drive segment allocation SMART statistics (see Viewing SMART Statistics)

10.2.3.1 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.



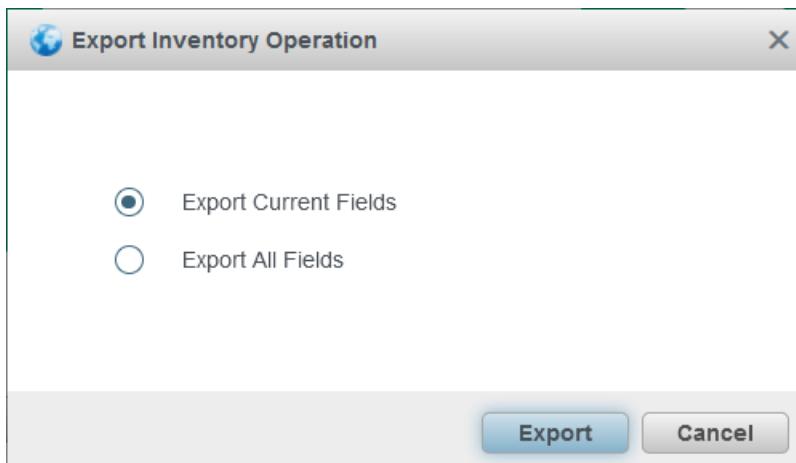
The storage inventory shows the following three charts:

- 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 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.

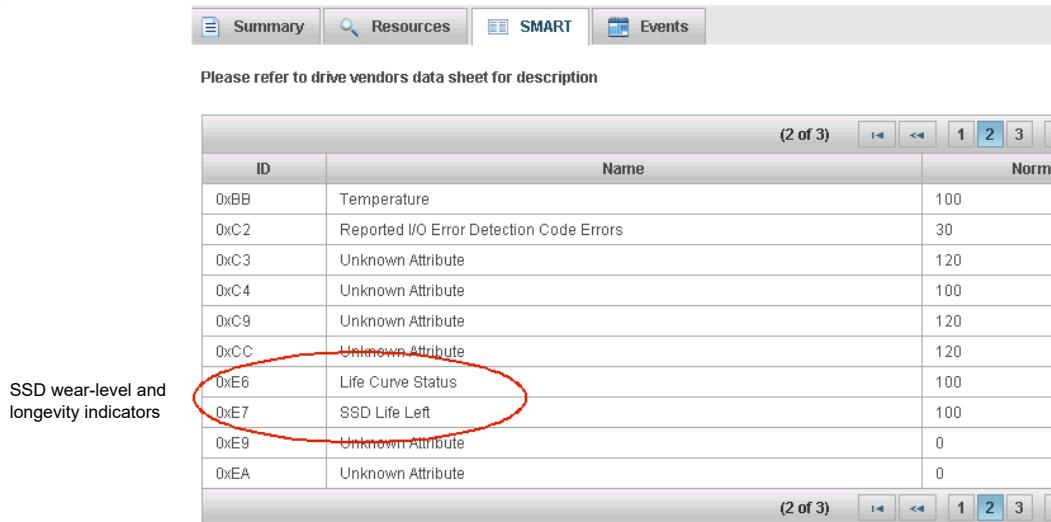


2. Select **Export Current Fields** option to export the data currently available in the table as .csv format. Or, select **Export All Fields** to export all the data in .csv format depending on the drop-down options selected on system, component, and attributes.

10.2.3.2 Viewing SMART Statistics

You can use the Storage Dashboard to view various indicators of reliability for the 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 non-spinning storage devices. You can use this information to verify the health of your NVMe SSDs and to predict drive failures.

To view the SMART statistics for an NVMe SSD, select the drive in the Enterprise View, then click the **SMART** tab on the Storage Dashboard. For NVMe 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.

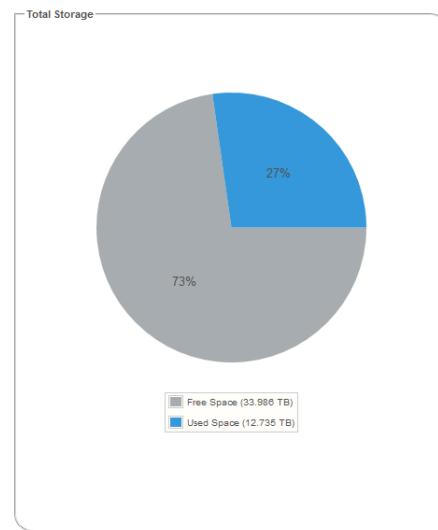


ID	Name	Normal
0xBB	Temperature	100
0xC2	Reported I/O Error Detection Code Errors	30
0xC3	Unknown Attribute	120
0xC4	Unknown Attribute	100
0xC9	Unknown Attribute	120
0xCC	Unknown Attribute	120
0xE6	Life Curve Status	100
0xE7	SSD Life Left	100
0xE9	Unknown Attribute	0
0xEA	Unknown Attribute	0

10.2.4 Viewing Storage Space Usage in Chart View

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

To view storage space usage in Chart View, simply select a component in the Enterprise View (a system, for instance); the chart view is updated immediately.



10.3 Notifying Users by Email About Status and Activity

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

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

Follow the instructions in this section to:

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

10.3.1 Setting Up Email Notifications

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

Before you begin, note this information:

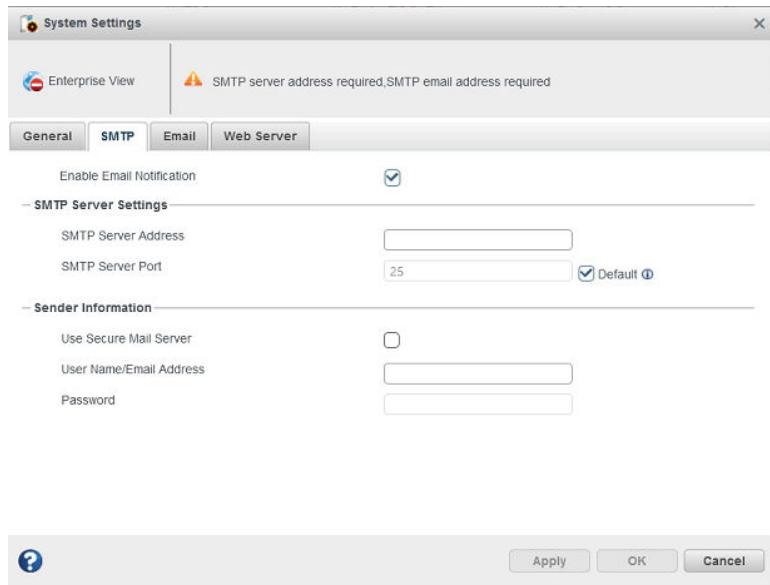
- The address of your Simple Mail Transfer Protocol (SMTP) server (host name and domain, or TCP/IP address)
- The email address of each person who will receive email notifications

To set up email notifications:

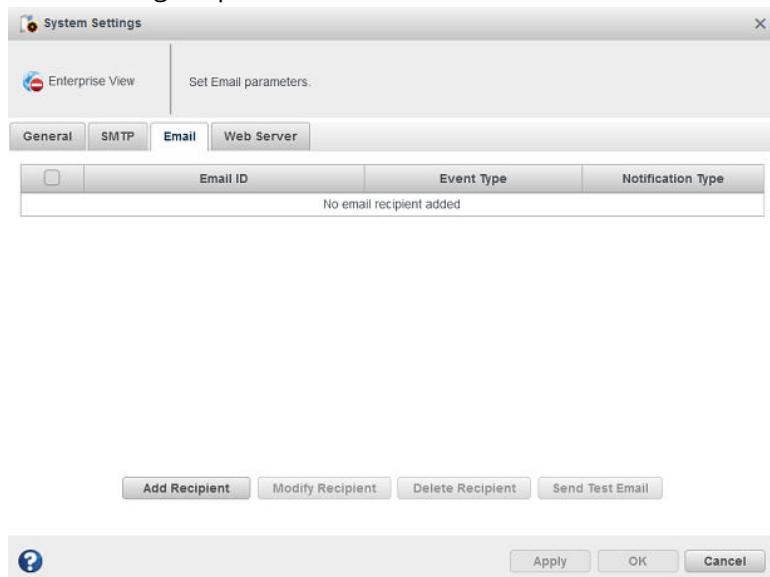
1. Select the Enterprise View node.
2. On the ribbon, in the System group, click **System Settings**.



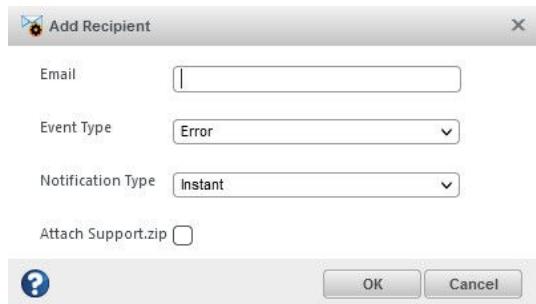
3. When the System settings window opens, click the **SMTP** tab.
4. Select **Enable Email Notifications**.
5. Enter the IP address of your SMTP server and the server's port number (or use the default port).



6. If authentication is enabled on your SMTP server (that is, the server requires authentication details before it will send messages to users), select **Use Secure Mail Server**, then enter the SMTP server's login credentials (username/password) in the space provided.
7. On the System settings window, click the **Email** tab.
The Email Notifications Manager opens.

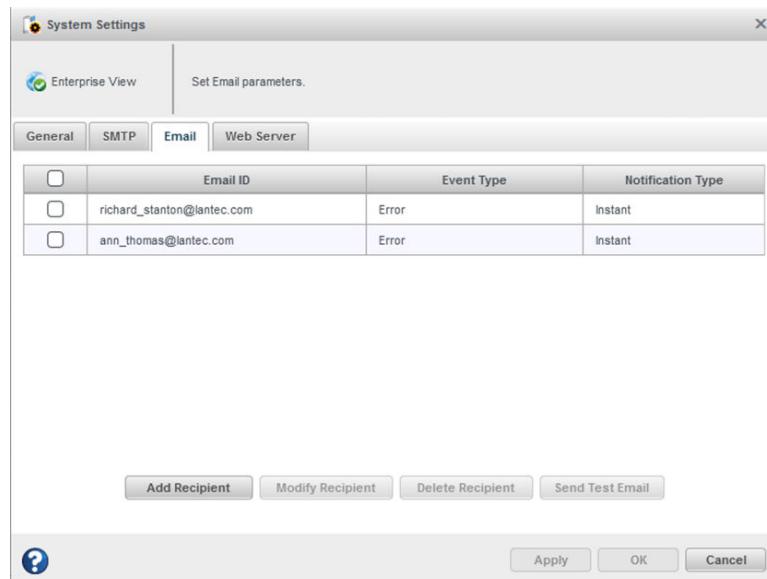


8. Click **Add Recipient**. When the Add Recipient window opens, enter the recipient's email address, select the level of events that will trigger an email notification for that recipient (Error, Error/Warning, Error/Warning/Informational), then select the notification type—Instant or Coalesced. To include a support archive file with the email, click **Attach Support.zip**, then click **OK**. (For more information about event levels, see [What Do the Event Status Icons Mean?](#); for more information about the support archive file, see [Creating a Support Archive File](#).)



Repeat this step to add more email recipients.

Each recipient appears in the Email Notifications Manager, as shown below:



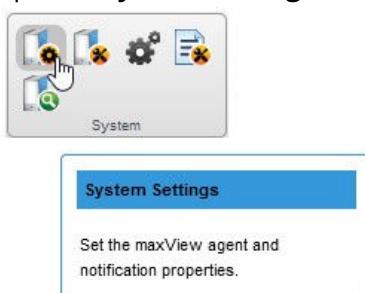
9. When you're done adding email recipients, click **OK**.
The email recipients and your SMTP server settings are saved.
10. Repeat the steps in this section *for each system* you want to monitor with email notifications, then continue by sending test messages to all recipients (see [Sending a Test Message](#)).

10.3.2 Sending a Test Message

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

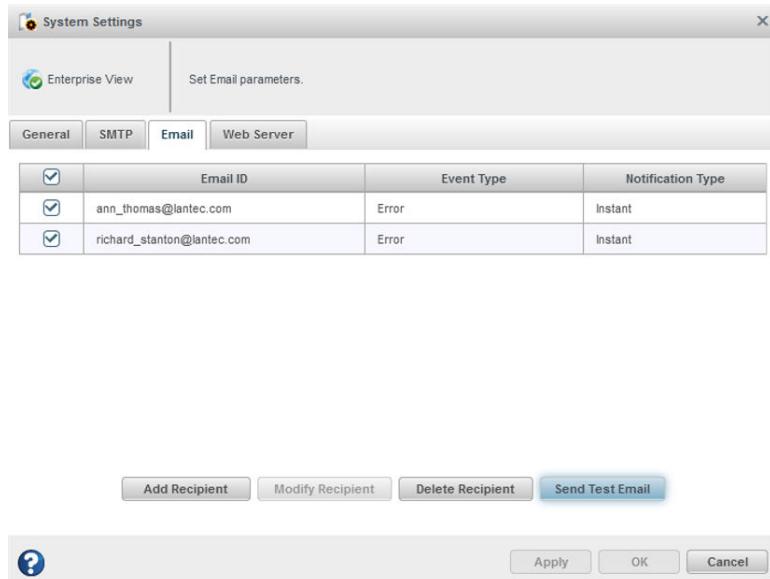
To send a test message:

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



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

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



5. Click **Send Test Email**.

If the test is successful, the email recipient(s) receive the test message. If the test fails:

- Ensure that the recipient's email address is correct. (See [Modifying or Removing an Email Recipient](#).)
- Ensure that your SMTP server address is correct. (See [Modifying Email Server Settings](#).)
- Try sending the test message again.

10.3.3 Modifying or Removing an Email Recipient

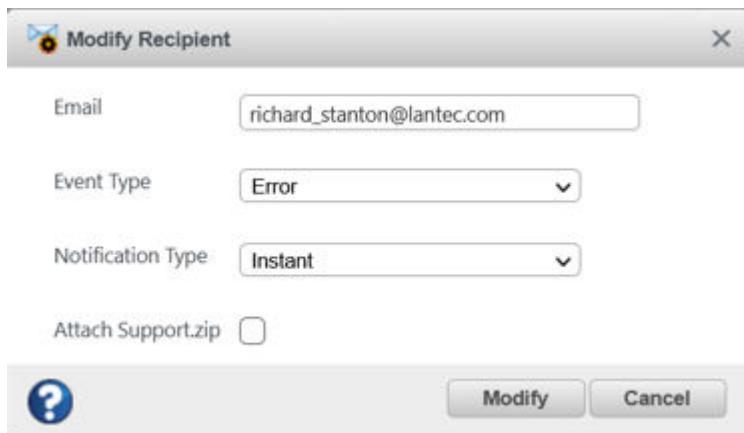
This section describes how to modify a recipient's email address, change the types of event notifications the recipient receives, or stop sending email notifications to a recipient from a selected system.

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

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



3. When the System settings window opens, click the **Email** tab.
The Email Notifications Manager opens.
4. Select the email recipient you want to modify or remove, then:
 - Click **Modify Email**, change the recipient information, as needed, then click **Modify** to save your changes.
Or,



- Click **Delete Email** to remove the recipient from the notification list.
The changes become effective immediately.
- 5. Click **OK** to close the Email Notifications Manager.

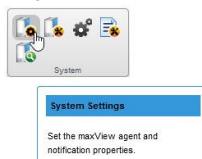
10.3.4 Modifying Email Server Settings

You can modify these email server settings, if required:

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

To modify email server settings:

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



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

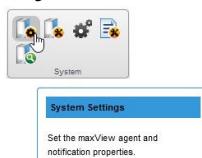
10.3.5 Disabling Email Notifications

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

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

To disable email notifications:

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



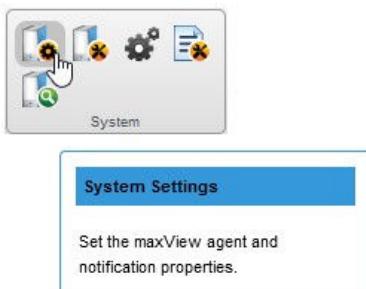
3. When the System settings window opens, click the **SMTP** tab.
4. Clear the **Enable Email Notifications** check box.
5. Click **OK** to save your changes.

10.4 Changing an Operating System's Event Log Setting

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

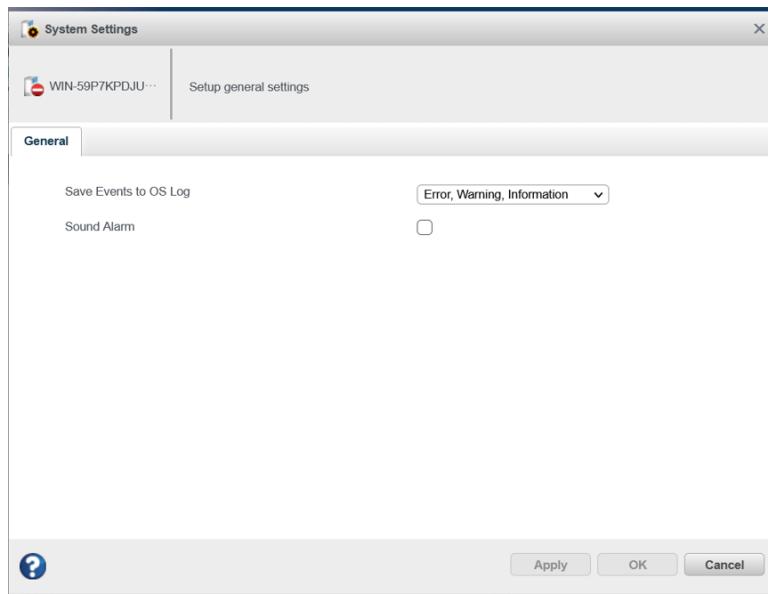
To change or disable operating system event logging on a system:

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



The System Settings window opens.

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



4. Restart maxView Storage Manager to apply the new setting.

11. Managing Your Storage Space

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

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

11.1 Deploying Servers

maxView Storage Manager helps you deploy servers in your storage space without configuring each server manually. You can select an optimally configured server in your storage space, save its configuration to a *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.

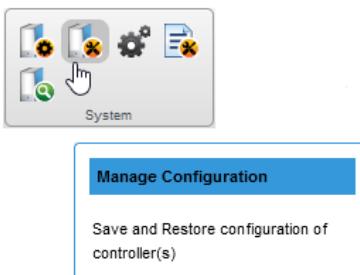
The following sections provide details on each of these steps.

11.1.1 Creating a Server Template File

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

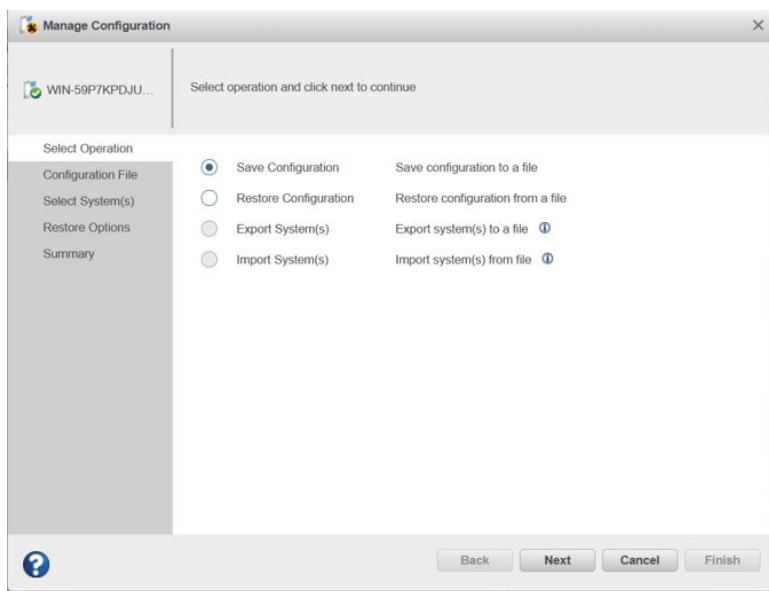
To create a server template file:

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



The Manage Configuration wizard opens.

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



4. Review the Summary information, then click **Finish**.
5. When the File Download window opens, click **Save File**, then click **OK**.
Note: The procedure for downloading and saving the template file may vary, depending on the Web browser.
6. Continue with [Duplicating the Server Template](#) to deploy the same configuration on multiple systems in your storage space.

11.1.2 Duplicating the Server Template

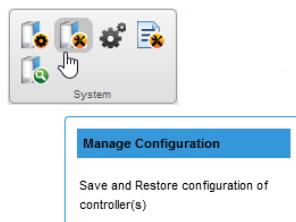
When you are ready to duplicate the server template on other systems in your storage space, you can restore the configuration from the server template file.

Keep in mind that:

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

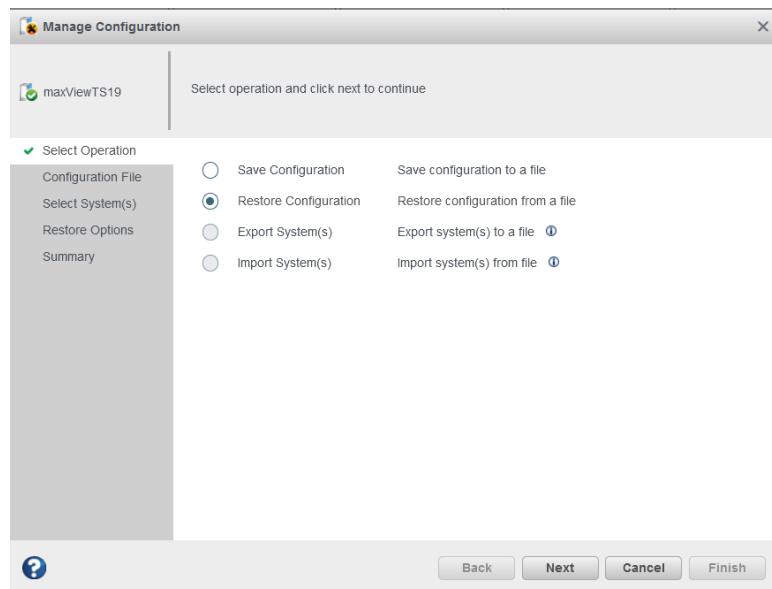
To duplicate the server template on another system:

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

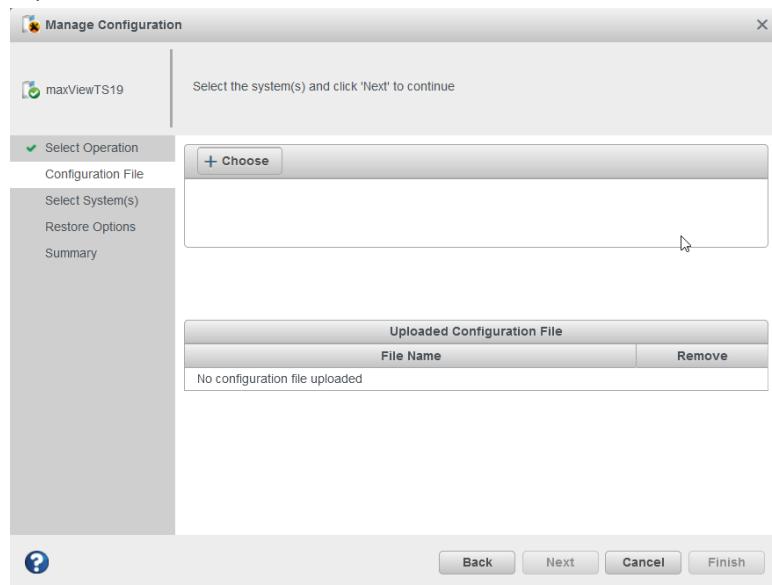


The Manage Configuration wizard opens.

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

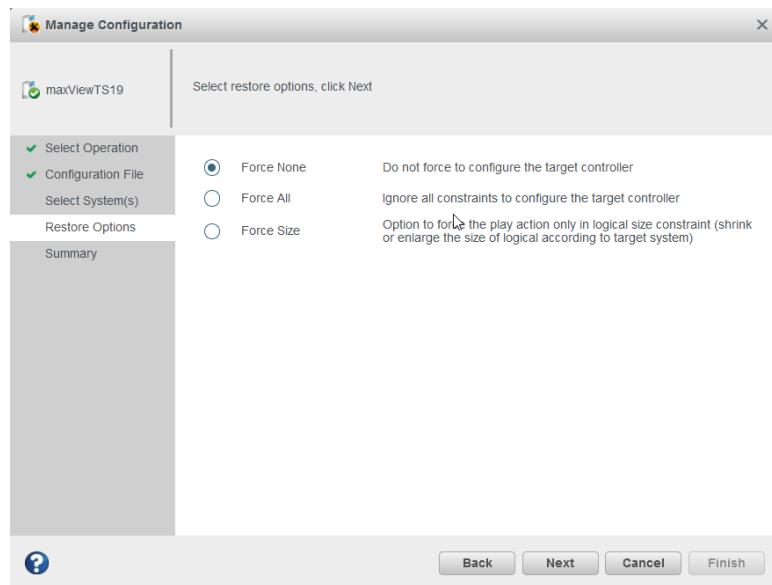


4. In the Configuration File panel, click **Choose**, navigate the file system to your server template file, then click **Open**. When the file name appears in the "selected file" area, click **Upload**, wait for the upload to complete, then click **Next**.



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

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

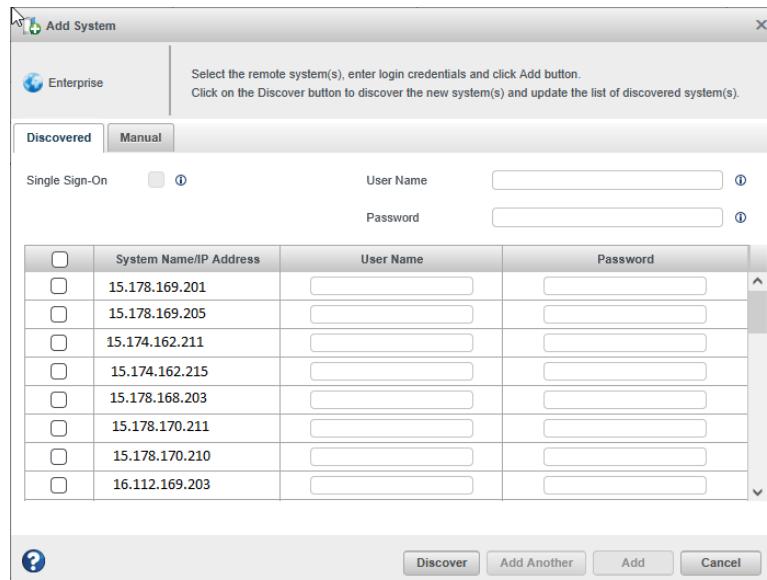


6. Click **Next**, review the summary information, then click **Finish**.
maxView Storage Manager duplicates the system configuration on the new controller.

11.2 Managing Remote Systems

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

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



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

11.2.1 Adding Remote Systems with the Wizard

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

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

11.2.2 Manually Adding a Remote System

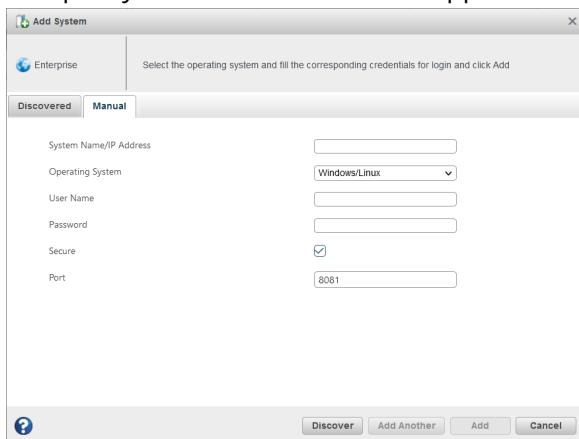
You can add a remote system manually if auto-discovery fails to find the system on your network.

To manually add a remote system:

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



2. When the Add System window opens, click **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.

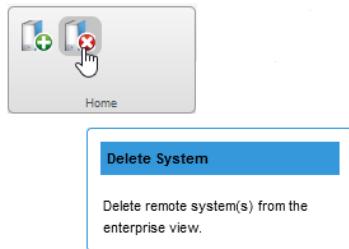
11.2.3 Removing a Remote System

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

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

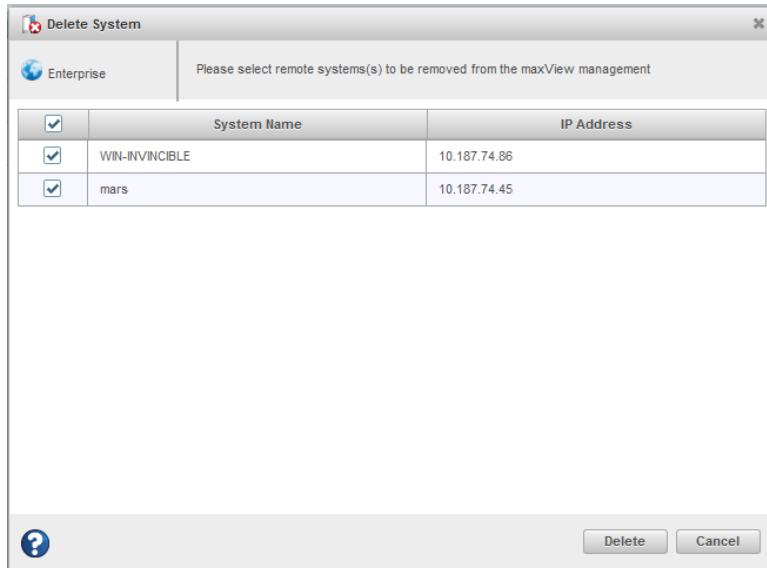
To remove a remote system:

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



The Delete System window opens.

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



3. Click **Delete**.

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

11.2.4 Changing the Auto-Discovery Settings

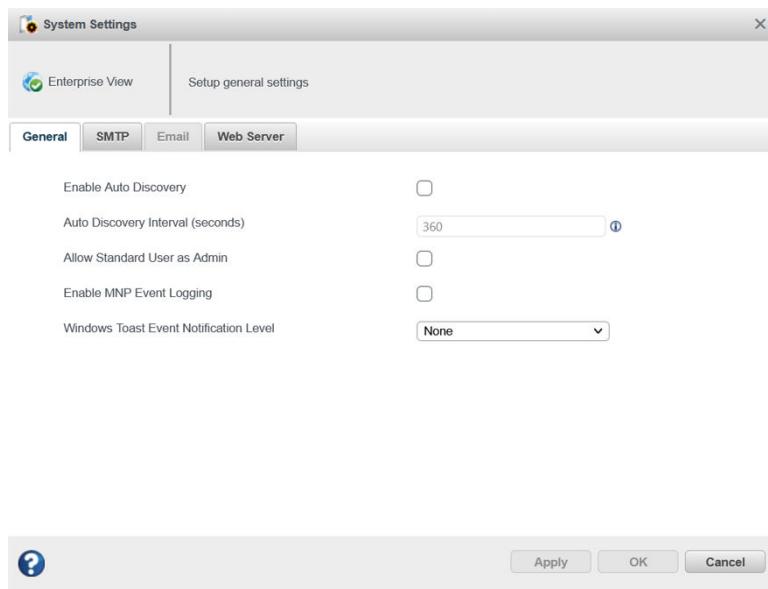
Auto-discovery, in maxView Storage Manager, is disabled by default. If enabled, the auto-discovery task runs in the background each time maxView Storage Manager is started. You can enable the auto-discovery if desired, and configure the auto-discovery settings as described in this section.

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 (seconds)** field, enter the number of seconds between each auto-discovery check. This number determines how often maxView Storage Manager checks for changes in remote system resources.
5. Click **OK** to save the changes.

11.2.5 Importing and Exporting Remote Systems

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

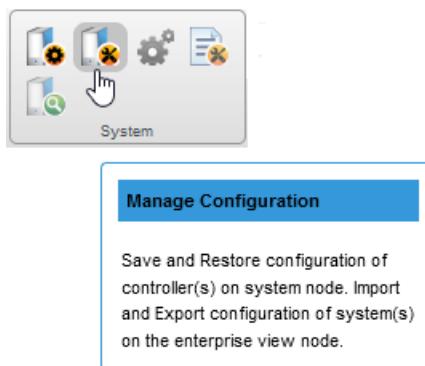
The Import and Export feature gets enabled at the "Enterprise View" level in the Manage Configuration ribbon icon.

Note:

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

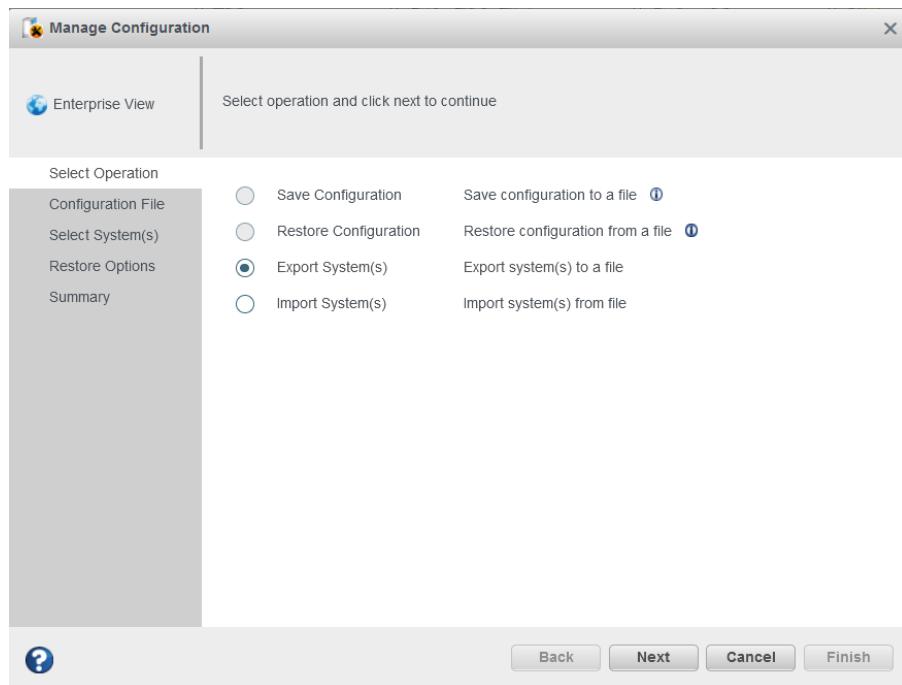
To export a system:

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

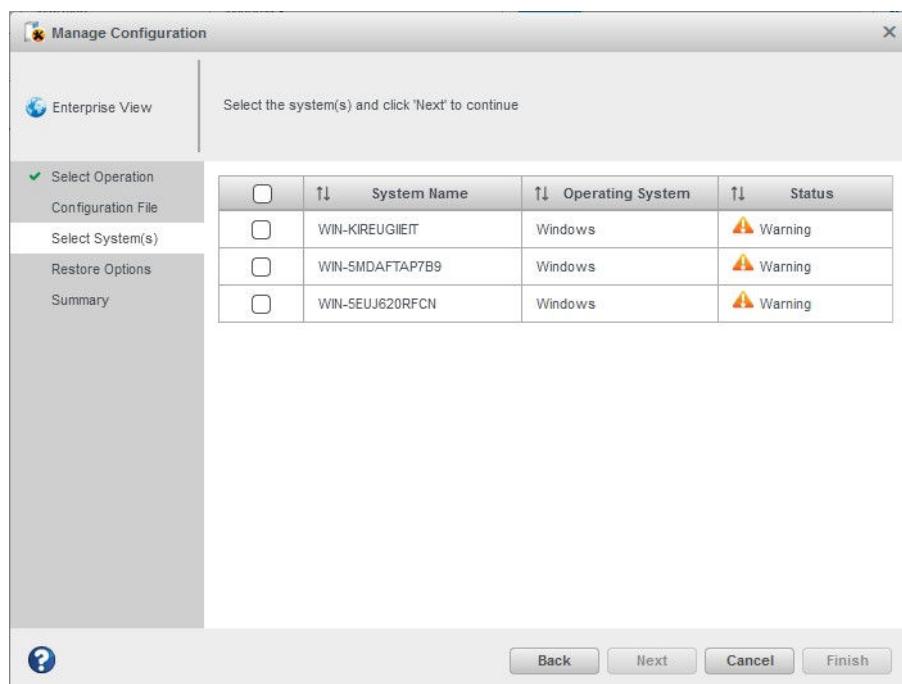


The Manage Configuration wizard opens for that system.

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



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



Note:

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

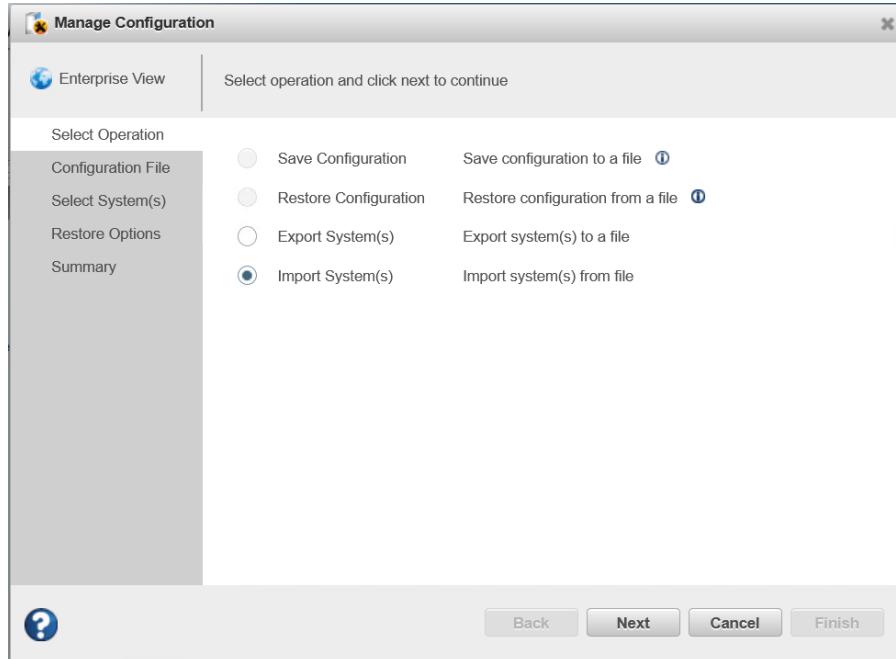
The **Manage Configuration Summary** page appears.

5. Click **Finish**.

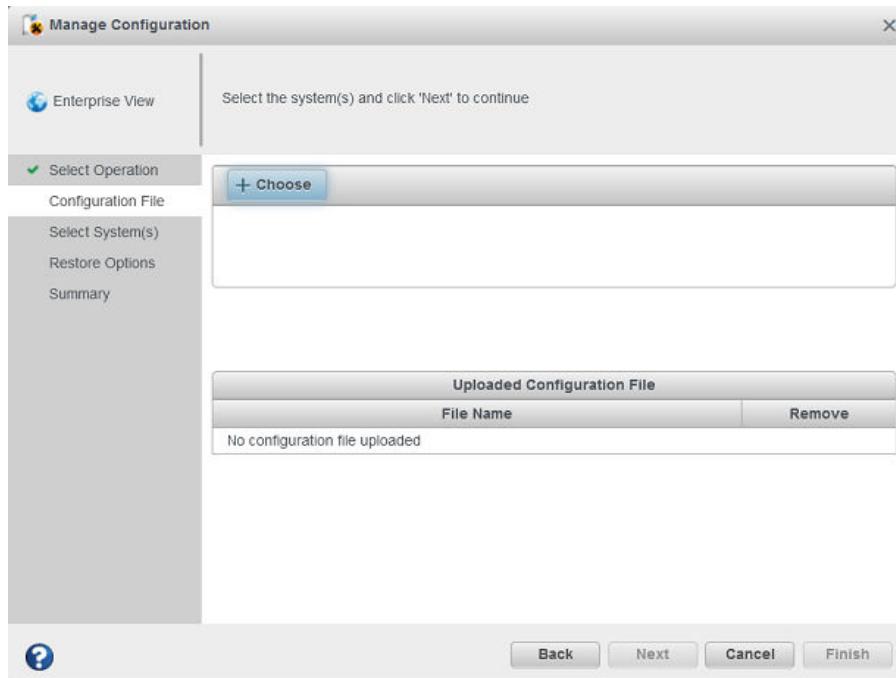
The exported systems are downloaded in a "SystemConf.json" file.

To import a system:

1. Select the Enterprise View node.
2. On the ribbon, in the System group, click **Manage Configuration**.
The **Manage Configuration** wizard opens for that system.
3. Select **Import System(s)** option, then click **Next**.



4. Click **Choose** to specify the path of the "SystemConf.json" file.



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

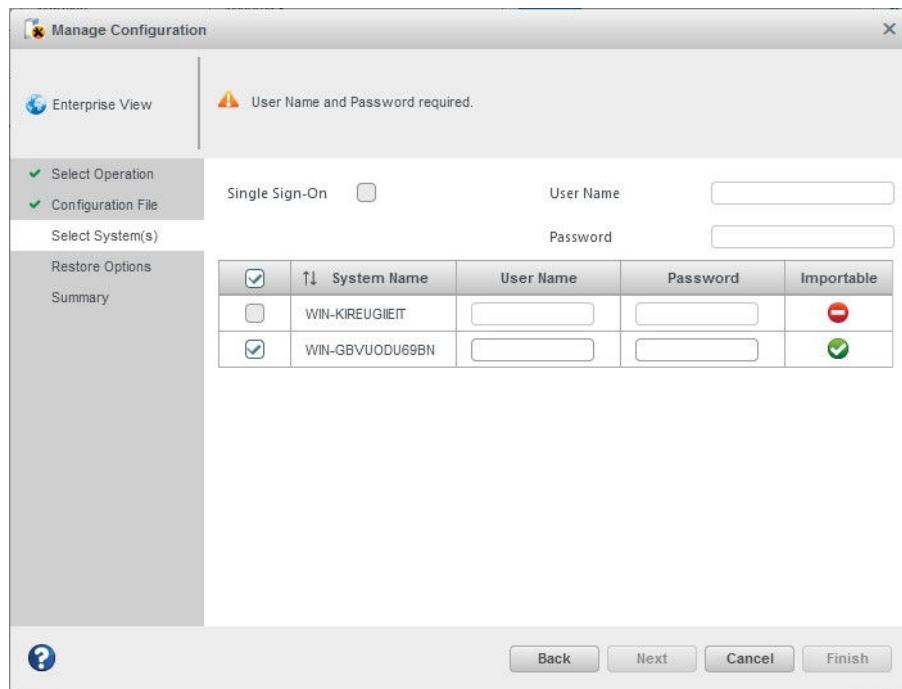
5. Click **Next**.

The **Select Systems** screen appears.

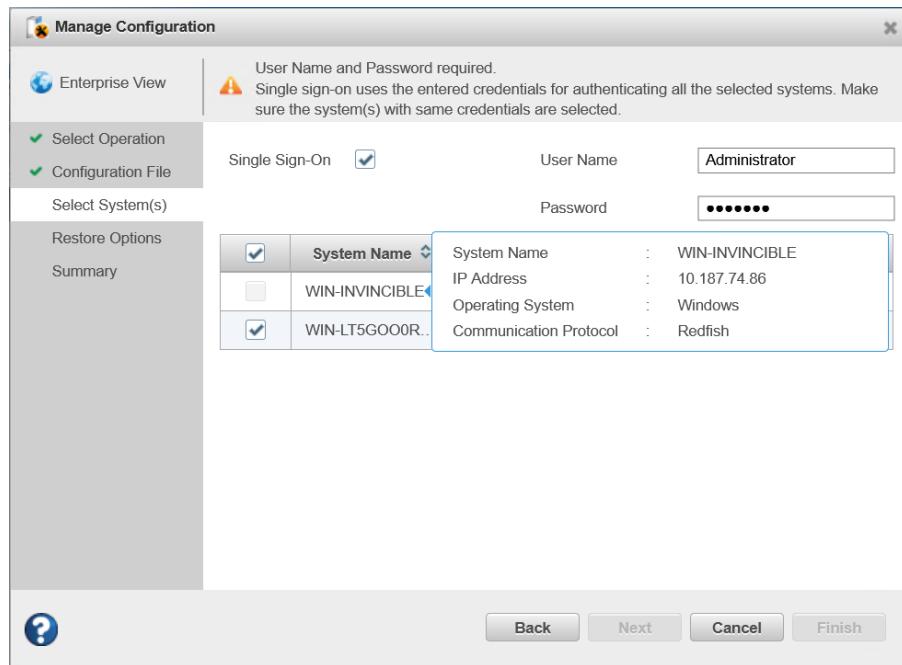
6. Select the system name(s) and specify the login credentials. Select **Single Sign-On** option to specify the **User Name** and **Password** for all the selected systems that have same credentials. Otherwise, specify each system's credentials manually.

Note:

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



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



7. Click **Next**.

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

8. Click **Finish**.

The imported systems will appear in the Enterprise View.

11.3 Clearing the Controller Configuration

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

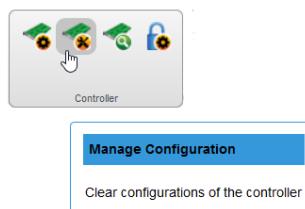


CAUTION When you clear a controller configuration, you lose all data stored on that controller. Be sure you no longer need the data on the controller before proceeding.

Note: Clear configuration option resets the user configuration.

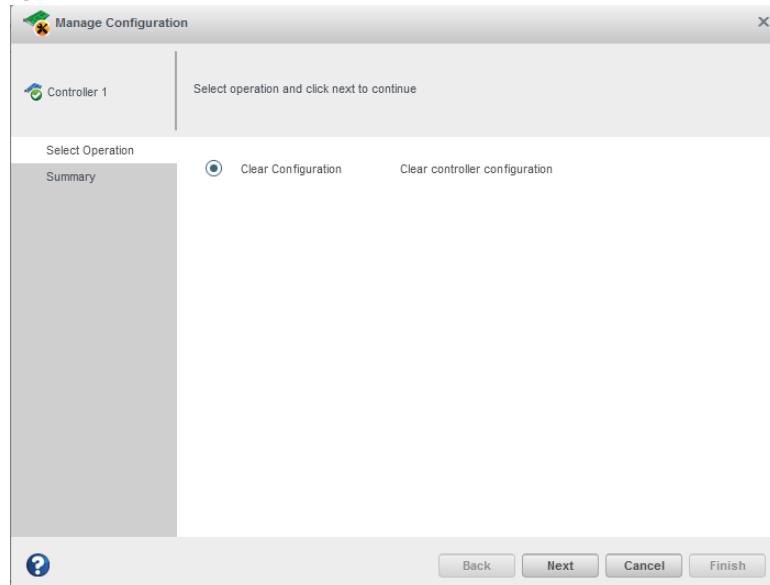
To clear the controller configuration:

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



The Manage Configuration wizard opens.

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



4. Review the Summary information, then click **Finish**.

11.4 Changing the Web Server Port

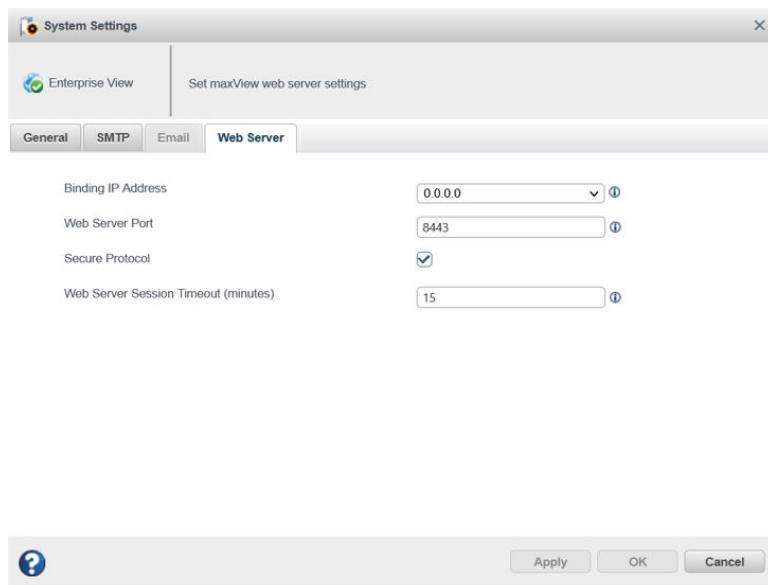
You can change the port used by the maxView Storage Manager Web Server, if needed, to accommodate changes in your network or IT requirements. The Web Server can use any open port for communication. The default port is 8443. If you change the port, you must restart maxView Storage Manager for the change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

To change the Web Server port:

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



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



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

11.5 Granting Standard Users Admin Privilege

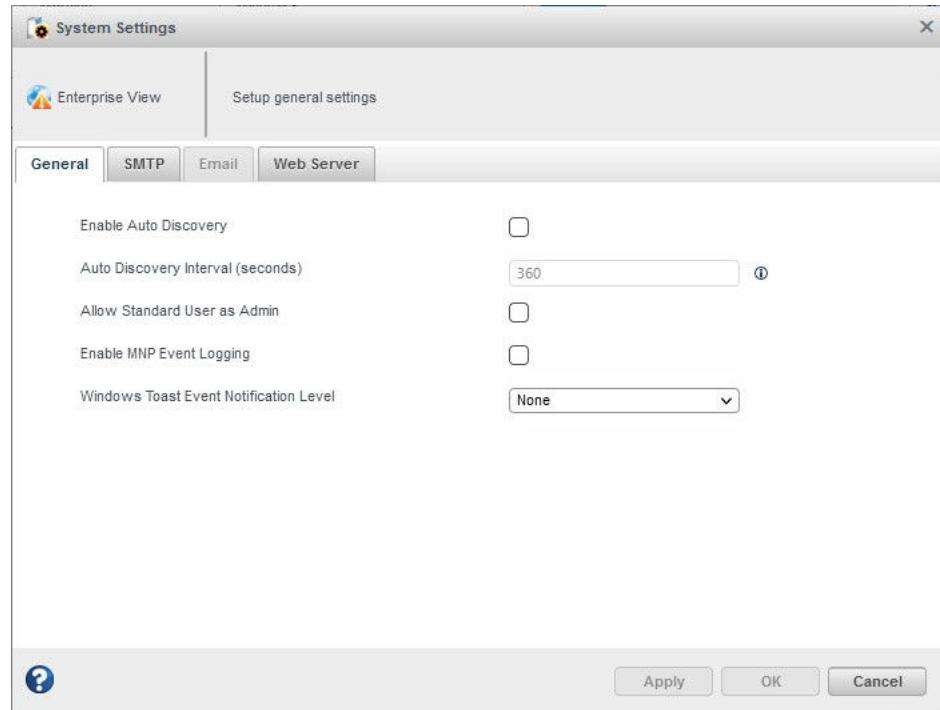
The standard users have restricted access to the storage space with limited ability to perform non-destructive operations in maxView Storage Manager (see [Working in maxView Storage Manager](#)). You can grant admin privileges to the standard users to accommodate changes in your system policies or IT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

To grant admin privilege to standard users:

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



The System Settings window opens.



3. Click the **Allow Standard User as Admin** check box, then click **Apply**.
4. Restart the webserver.

12. Solving Problems

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

12.1 General Troubleshooting Tips

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

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

12.2 Identifying a Failed or Failing Component

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

For instance, in this example, a physical drive has failed. To find the failed physical 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 maxView Storage Manager interface. The top part displays the 'Enterprise View' tree, which includes nodes for 'Controller 1' (with 'Accelerators' and 'Anaysis and Logical Devices'), 'Physical Devices' (with 'Device 0' through 'Device 44'), and a specific node for 'Device 0 (Failed)' which is highlighted. A callout box points to this node with the text: 'Error is on Local System', 'Error on Controller 1', 'affecting one logical drive', and '...and physical device.. Device 0. Click on Device 0 to check the device status on the storage dashboard and continue tracing the fault to its source...'.

The bottom part of the interface shows the 'Summary' tab of the 'Physical Device Info' panel. It details the following information for 'Device 0 (Failed)':

Vendor	NVMe
Model	Micron_T400_MTFDDCC1ST3TFR
Serial Number	2249414236ED
Interface Type	NVMe SSD
Total Size	13.873 TB
Logical / Physical Block Size	512 Bytes / 512 Bytes
Firmware Level	E2MU110
Unique ID	2A09FCCFC1F7EC7FB24F HEZ23AC...
Last Write On Disk	0
Reported Device ID	0
PCI Address (Domain Bus Function)	0000:50:00.0
Parent PCI Address (Domain Bus Device)	0000:40:01.0
XLR Configuration State	Configured
Label	Bay 1

 The 'Settings and Status' panel shows the following for 'Device 0 (Failed)':

State	Failed
Normalised Transfer Speed	PCIe 4.0 (16.0 GT/s)
Configuration Type	Data
Write Cache	Unknown
Current Temperature	Not Applicable
Maximum Temperature	27°C / 80°F
Threshold Temperature	60°C / 149°F

 The 'Progress Task' panel indicates 'Not Applicable' for Task Name, Erase Pattern, and Task Percentage. The 'Phy Information' panel lists link rates for four physical ports (Phy 0 to Phy 3):

Phy 0	Physical Link Rate: PCIe 4.0 (16.0 GT/s)
Phy 0	Logical Link Rate: PCIe 4.0 (16.0 GT/s)
Phy 0	Maximum Link Rate: PCIe 4.0 (16.0 GT/s)
Phy 1	Physical Link Rate: PCIe 4.0 (16.0 GT/s)
Phy 1	Logical Link Rate: PCIe 4.0 (16.0 GT/s)
Phy 1	Maximum Link Rate: PCIe 4.0 (16.0 GT/s)
Phy 2	Physical Link Rate: PCIe 4.0 (16.0 GT/s)
Phy 2	Logical Link Rate: PCIe 4.0 (16.0 GT/s)
Phy 2	Maximum Link Rate: PCIe 4.0 (16.0 GT/s)
Phy 3	Physical Link Rate: PCIe 4.0 (16.0 GT/s)
Phy 3	Logical Link Rate: PCIe 4.0 (16.0 GT/s)
Phy 3	Maximum Link Rate: PCIe 4.0 (16.0 GT/s)

12.3 Recovering from a Physical Drive Failure

This section describes how to recover when an NVMe SSD fails:

- If the logical drive is protected by a hot spare, see [Failed Physical 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 physical drive failure in more than one logical drive simultaneously, see [Failure in Multiple Logical Drives Simultaneously](#).
- If it is a RAID 0 logical drive, see [Physical Drive Failure in a RAID 0 Logical Drive](#).
- If multiple physical drives fail within the same logical drive, see [Forcing a Logical Drive with Multiple Drive Failures Back Online](#).

12.3.1 Failed Physical Drive Protected by a Hot Spare

If a physical 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 physical 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 physical 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 [Protecting Your Data](#) for more information about managing spares.

12.3.2 Failed Physical Drive Not Protected by a Hot Spare

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

For example, when one of the physical drives fails in a RAID 1 logical drive, the logical drive is *not* automatically rebuilt. The failed physical 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, physical drives, and controllers are properly installed and connected. Then, if necessary, follow the instructions in [Rebuilding Logical Drives](#).

12.3.3 Failure in Multiple Logical Drives Simultaneously

If a physical 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 physical drive in the array that it might replace.
- Failed physical drives are replaced with hot spares in the order in which they failed. (The logical drive that includes the physical drive that failed first is rebuilt first, assuming an appropriate hot spare is available—see the previous bullet.)

Note: If the number of physical drive failures exceeds the number of hot spares, see [Failed Disk Drive Not Protected by a Hot Spare](#).

12.3.4 Physical Drive Failure in a RAID 0 Logical Drive

Because RAID 0 volumes do not include redundancy, if a physical 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 [Setting the Spare Activation Mode](#).

12.3.5 Forcing a Logical Drive with Multiple Drive Failures Back Online

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



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

12.3.6 Healing an Array

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

The Heal Array operation is part of the Modify Array wizard . It is available in the wizard only if:

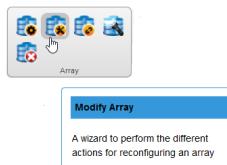
- The array has at least one failed drive.
- The array is not rebuilding to a spare.
- A sufficient number of Ready physical drives of the same type and correct size are available to replace each failed physical drive in the array.

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.

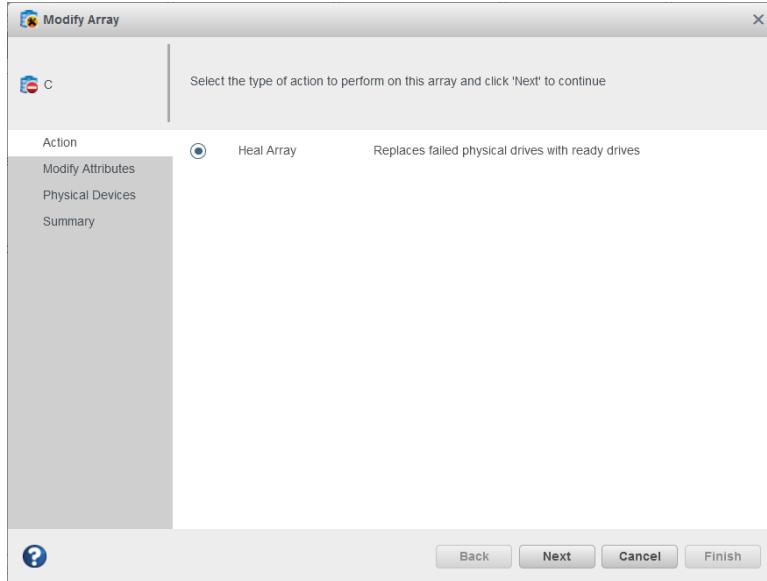
For a RAID 0 volume, the heal operation recreates the volume. For other RAID volume types, the heal operation rebuilds the volume.

To heal an array:

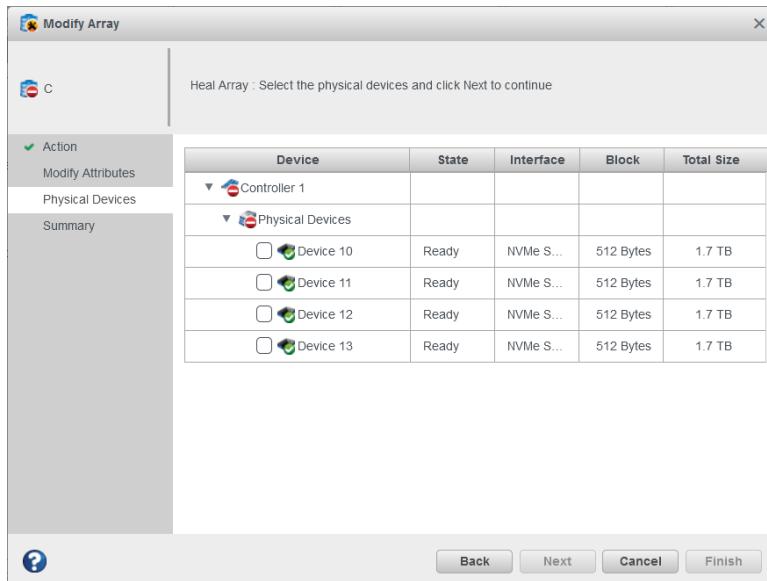
1. In the Enterprise View, select an array.
2. On the ribbon, in the Array group, click **Modify Array**.



- 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.

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

12.4 Rebuilding Logical Drives

A *hot-swap rebuild* occurs when a controller detects that a failed physical 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 .

To start a hot-swap rebuild:

1. Following manufacturer's instructions, gently pull the failed physical 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 physical drive, reinstall it, following manufacturer's instructions.
If necessary, replace the failed physical drive with a new physical drive of equal or larger size.
3. The controller detects the reinserted (or new) physical drive and begins to rebuild the logical drive.

12.5 Creating a Support Archive File

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

To create the support archive file:

1. In the Enterprise View, select the system on which the problem is occurring. (Look for the orange or red error icons in the Enterprise View.)
2. On the ribbon, in the System group, click **Archive Management**.



The Archive Management window opens.

The screenshot shows the 'Archive Management' dialog box. On the left, a sidebar lists a system named 'falcon-fe-sless15...'. To its right, a panel says 'Select log files to save'. Below this is a table with columns 'Log File' and 'Description'. All seven log files listed have checkboxes checked. At the bottom of the dialog are buttons for '?', 'Clear', 'Save', and 'Cancel'.

	Log File	Description
<input checked="" type="checkbox"/>	GUI	maxView web server logs
<input checked="" type="checkbox"/>	Redfish	Redfish server logs
<input checked="" type="checkbox"/>	Arcconf	Command line interface logs
<input checked="" type="checkbox"/>	Storlib	maxView library logs
<input checked="" type="checkbox"/>	HostStack	HostStack logs
<input checked="" type="checkbox"/>	Hardware	Hardware logs

3. Select the logs you want to save.
4. Click **Save**.
5. When the File Download window opens, click **OK**.
6. In the Archive Management window, click **Clear All Logs** to clear, or **Cancel** to exit.

13. Silent Installation on Linux

This appendix describes how to complete a silent installation of maxView Storage Manager on 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 and SLES only.

13.1 Completing a Silent Installation

This section describes the silent installation process for Linux.

13.1.1 Linux Silent Installation

To complete a silent installation on Red Hat Linux 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 [Example Command Line Installations](#).

13.2 Example Command Line Installations

This section shows typical command line installations for Linux. In the Linux examples, <x.xx>-<xxxxx>=version-build number.

- 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
```

14. Configuring SNMP Notifications on Linux

This appendix describes how to enable SNMP trap notifications on Linux.

After installing and configuring the SNMP service, you can monitor activity in your storage space with the maxView Storage Manager GUI or any OS monitoring tool, such as a Mib Browser.

14.1 Setting Up SNMP Notifications on 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
```

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
```

15. 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 physical 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.

15.1 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 physical drives and your requirements for performance and reliability.

RAID Level	Redundancy	Physical Drive Usage	Read Performance	Write Performance	Built-in Hot Spare	Minimum Physical Drives
RAID 0	No	100%	***	***	No	2
RAID 1	Yes	50%	**	**	No	2
RAID 10	Yes	50%	**	**	No	4
RAID 5	Yes	67 – 94%	***	*	No	3
RAID 50	Yes	67 – 94%	***	*	No	6

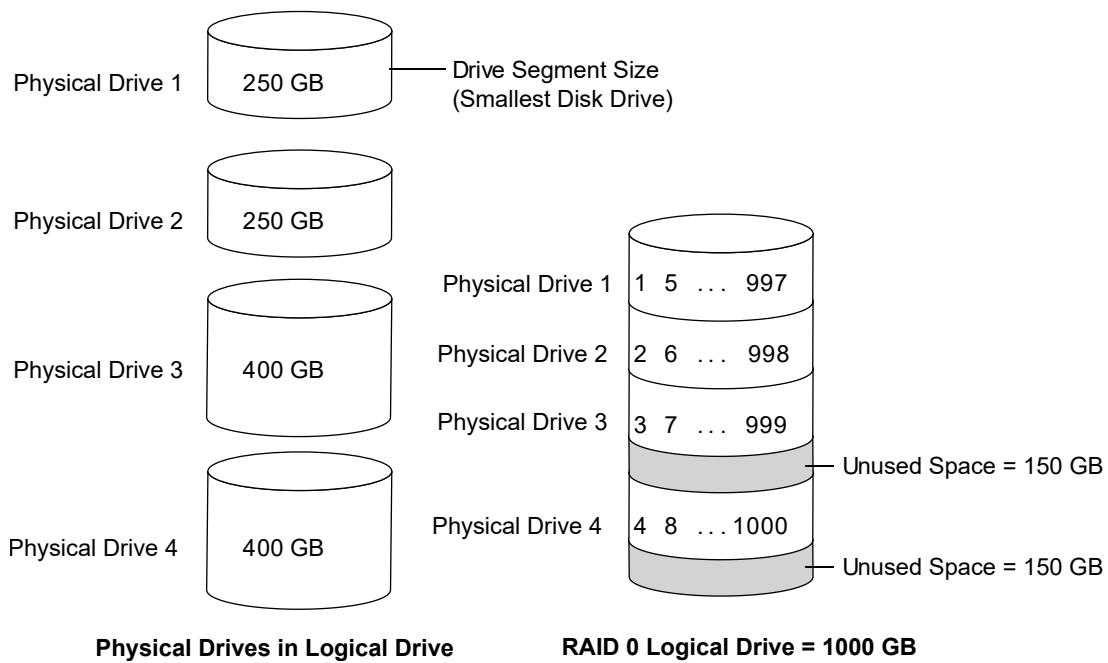
Physical drive usage, read performance, and write performance depend on the number of drives in the logical drive. In general, the more drives, the better the performance.

15.2 Non-redundant Logical Drives (RAID 0)

A logical drive with RAID 0 includes one or more physical drives and provides data *striping*, where data is distributed evenly across the physical 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 physical drives, a RAID 0 logical drives provides improved I/O performance.

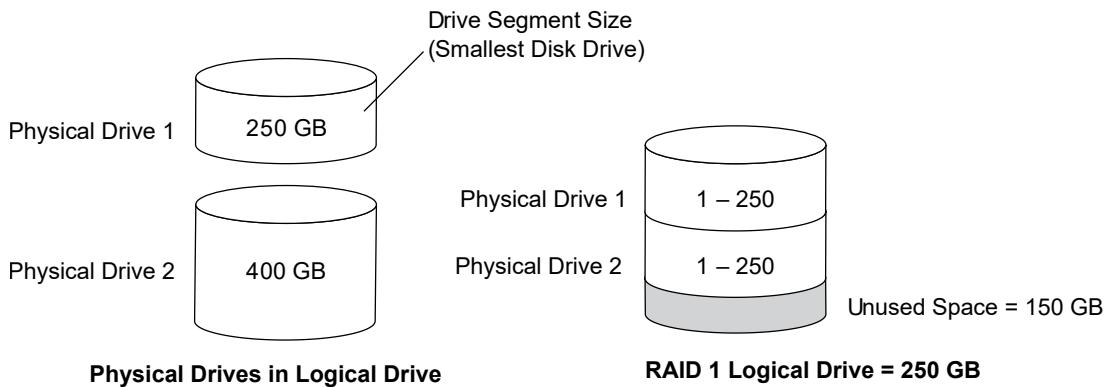
Drive segment size is limited to the size of the smallest physical drive in the logical drive. For instance, an array with two 250 GB physical drives and two 400 GB physical drives can create a RAID 0 drive segment of 250 GB, for a total of 1000 GB for the volume, as shown in this figure.



15.3 RAID 1 Logical Drives

A RAID 1 logical drive is built from two physical drives, where one physical drive is a *mirror* of the other (the same data is stored on each physical drive). Compared to independent physical drives, RAID 1 logical drives provide improved performance, with up to twice the read rate and an equal write rate of single physical drives. However, capacity is only 50 percent of independent physical drives.

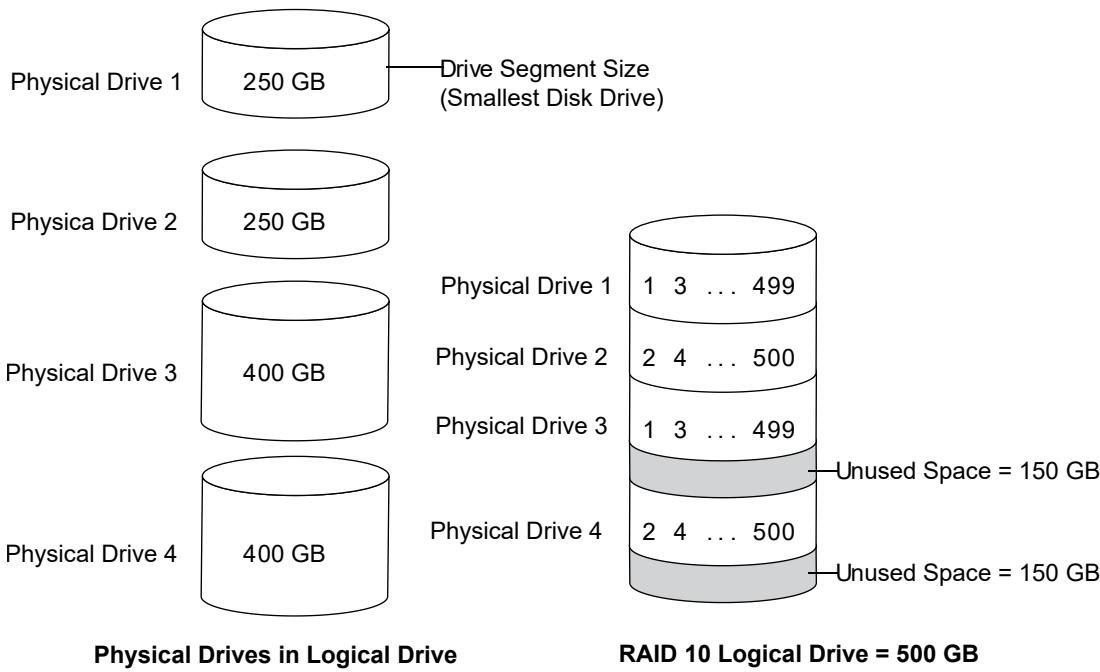
If the RAID 1 logical drive is built from different-sized physical drives, the free space, drive segment size is the size of the smaller physical drive, as shown in this figure.



15.4 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 physical drive in the logical drive. For instance, an array with two 250 GB physical drives and two 400 GB physical 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.

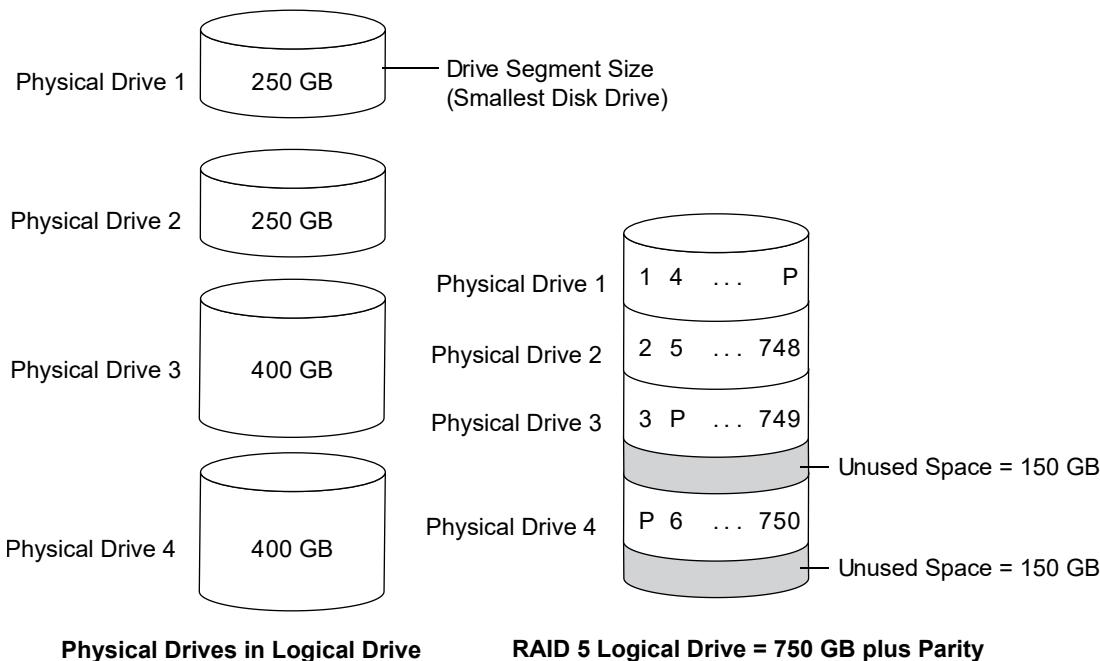


15.5 RAID 5 Logical Drives

A RAID 5 logical drive is built from a minimum of three physical 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 physical drive fails. In RAID 5 logical drives, parity data (represented by Ps in the next figure) is striped evenly across the physical 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 physical drives and two 400 GB physical drives can contain 750 GB of stored data and 250 GB of parity data, as shown in this figure.



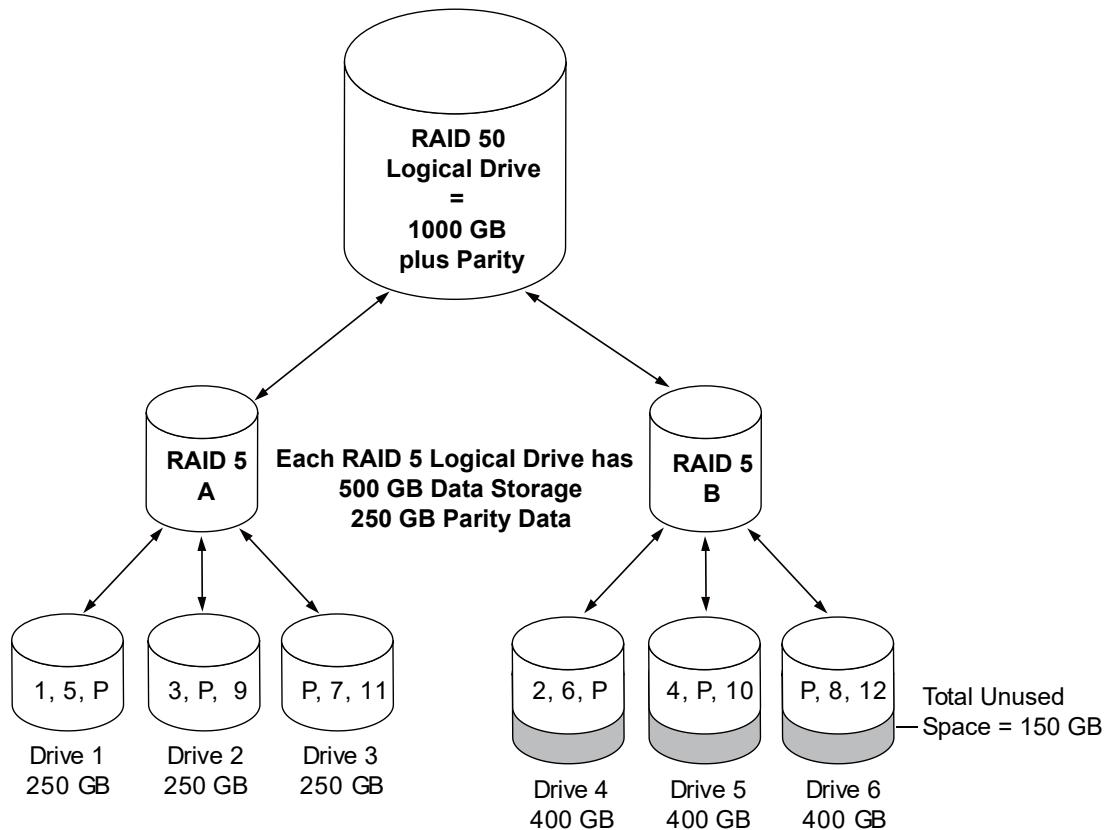
15.6 RAID 50 Logical Drive

A RAID 50 logical drive is built from six to thirty two physical drives configured as two or more RAID 5 arrays, and stripes stored data and parity data across all physical 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 physical drive in the logical drive. For example, three 250 GB physical drives and three 400 GB physical 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.



16. Icons At-a-Glance

The following is a complete list of icons used in maxView Storage Manager. It contains the icons on the ribbon, in the Enterprise View, and on tabs and dialog boxes.

See [Overview of the Main Window](#) for more information.

Ribbon Home Icons

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

Icons At-a-Glance (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 device properties
	Assign/unassign physical device as spare
	Force physical device offline
	Physical device secure erase
	Physical device 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
	Solid State drive

Icons At-a-Glance (continued)

Icon	Description
	Physical devices

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 Controller Icons

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

Enterprise View Physical Disk Icons

Icon	Description
	Physical device OK
	Physical devices OK
	Physical devices failure
	Physical devices missing
	Physical devices warning
	Physical device encrypted

Tab Icons

Icon	Description
	Summary
	Properties
	Resources
	Events
	Task

Dialog Box Icons

Icon	Description
	E-mail notification
	Chart

17. 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 XLR 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.
Has Offline Logical Drive	Array has offline 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
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

Smart Controller Device Status (continued)

Status	Description
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.
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.

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 will not be available for use until the erase operation is completed
Erase In Progress	The physical device is currently being erased and 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 physical device is offline. The physical device may now be brought online through the initialize operation.

Smart Controller Device Status (continued)

Status	Details
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.
Size Not Valid	Physical device size is not valid.

18. 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 18-1. Controller Display Properties

Property	Tooltip Details
Model	Model of the Controller
Status	Overall status of the controller based on its resources.
Mode	Mode of the controller on which it is operating.
Driver Version	Current version of driver installed on the system.
Driver Name	Driver name describes the name of the driver.
I2C Address	I2C address describes the Inter-Integrated Circuit(I2C) slave address.
Reboot Required Reasons	Indicates the reason, why a controller cold reboot is required.
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.
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.
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.

Table 18-1. Controller Display Properties (continued)

Property	Tooltip Details
UEFI Health Reporting Mode	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". 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.
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.

Table 18-2. Accelerator Display Properties

Property	Tooltip Details
Accelerator ID	Describes the unique identifier of the accelerator
Serial Number	A unique number assigned to the controller, used for identification and inventory purposes.
WWN	A World Wide Name (WWN) is an unique identifier of the controller.
Physical Slot	PCI slot number to which the controller is connected.
Temperature	Current temperature of the controller
Power Consumption	Power Consumption of the controller
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.
NOR Flash Type	Describes the NOR Flash Type 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.
CPLD Revision	Describes the CPLD revision information about the controller.

Table 18-3. Array Display Properties

Property	Tooltip Details
ID	ID describes unique array identifier within the controller.
Name	Name describes unique name of array.
Device Type	Type describes the type of the array such as data array, backup array and so on.
Interface Type	Disk drives which are the member of array can have interface type such NVMe SSD. The interface type of array is based on the member disk drives interface type.
Total Space	Total usable size is the total space available in the array for creating logical device.

Table 18-3. Array Display Properties (continued)

Property	Tooltip Details
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.
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 18-4. 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 as NVMe will also reflect as interface type of logical device.
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).
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 Note: Duplicate logical device names are not allowed.
Disk Name	Name of the logical disk drive

Table 18-4. Logical Device Display Properties (continued)

Property	Tooltip Details
Mounted	Mount points describes the Operating system device names of the 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.

Table 18-5. 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.
Logical/Physical Block Size	Specifies the unit of data that can be physically read or write to the disk. Maximum size of data block on disk drives which are RAID member of logical device (can be 512 Bytes or 4K).
Firmware Level	Firmware version of the physical device.
Unique ID	ID to uniquely identify the physical device.
Reported Channel	The channel to which the physical device is connected.
Reported Device ID	The unique identifier of a physical device reported by controller.
PCI Address (Domain:Bus:Device.Function)	The PCI address uniquely identifies the device, facilitating its management and configuration within the system.
Parent PCI Address (Domain:Bus:Device.Function)	Uniquely identifies the device, facilitating its management and configuration within the system.
XLR Configuration State	Indicates the current status of the NVMe drive, showing whether they are configured or unconfigured.
Label	Used to identify each NVMe drive.
Sanitize Erase	Specifies whether the sanitize erase is supported by this physical device.
Encryption Capability	A SED (or Self-Encrypting Drive) is a type of 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.
Has Stale RIS Data	Specifies whether the physical device has stale RIS data.
SMART	Indicates whether the physical device supports SMART or not.
S.M.A.R.T. Warning	Any SMART warning 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.

Table 18-5. Physical Device Display Properties (continued)

Property	Tooltip Details
Physical Link Rate	Physical Link Rate
Logical Link Rate	Logical Link Rate
Maximum Link Rate	Maximum Link Rate
Last Failure Reason	Indicates last known failure occurred on this device.
Unsupported Reason	Depicts the reason for why the physical device is not supported.
Power-On Hours	Indicates the number of hours the NVMe SSD has been powered on.
Usage Remaining	Indicates the percentage of the NVMe SSD that has not worn out. Usage remaining is equal to the difference of 100 and the NVMe SSD Utilization percentage.
Estimated Life-Remaining	Estimated Life Remaining based on workload to date indicates an estimate of the number of days the NVMe SSD has before NVMe SSD Utilization reaches 100%.
Smart Trip Wear-Out	Indicates the NVMe SSD's wear status.
Fifty Six Days Warning	Indicates fifty six days warning.

19. 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
B	03/2025	Preliminary Revision
A	12/2024	Initial Revision

Microchip Information

Trademarks

The "Microchip" name and logo, the "M" logo, and other names, logos, and brands are registered and unregistered trademarks of Microchip Technology Incorporated or its affiliates and/or subsidiaries in the United States and/or other countries ("Microchip Trademarks"). Information regarding Microchip Trademarks can be found at <https://www.microchip.com/en-us/about/legal-information/microchip-trademarks>.

ISBN: 979-8-3371-0940-4

Legal Notice

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

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

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

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

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 products are 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.