Quantum

User's Guide

Scalar *i*6000

6-66879-12 Rev A

Quantum Scalar i6000 User's Guide, 6-66879-12 Rev A, December 2014, Product of USA.

Contents

Preface

This guide contains information and instructions necessary for the normal operation and management of the Scalar i6000 library. This guide is intended for system administrators, operators, or anyone interested in learning about or using the Scalar i6000 library after its initial installation and configuration. Be aware that you must have administrator privileges to use many of the features that this guide describes.

Caution: Be sure to read all operating instructions in this manual and in the *System, Safety, and Regulatory Information Guide* before operating this product.

Product Safety Statements

This product is designed for data storage and retrieval using magnetic tape. Any other application is not considered the intended use. Quantum will not be held liable for damage arising from unauthorized use of the product. The user assumes all risk in this aspect.

This unit is engineered and manufactured to meet all safety and regulatory requirements. Be aware that improper use may result in

bodily injury, damage to the equipment, or interference with other equipment.

Caution: Be sure to read all operating instructions in this manual and in the *System, Safety, and Regulatory Information Guide* before operating this product.

WARNING: Before powering on or using this equipment, read THE *System, Safety, and Regulatory Information Guide*. Keep the Guide for future reference.

Note: When drive sled positions are empty, drive cover plates must be installed and in place at all times to prevent access into the empty drive sled Positions.

Mechanical Locks

The access and service doors can only be opened with a key. The key should be kept by an authorized person at your company. Access to the interior of the library is both a data-integrity and safety issue.

Power Button on the Library's Indicator Panel

Switching off the **Power** button on the indicator panel, located on the front of the library, removes power from the electronics, which causes the picker to stop immediately. This button also removes power from the drives.

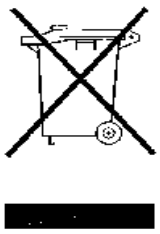
WARNING: This power button functions as a power interrupt only. To completely remove all power before servicing or in an emergency, turn off the circuit breaker on the power distribution unit, and then disconnect the power cord from the electrical source.

Mercury Statement

Projectors, LCD displays, and some multifunction printers may use lamp(s) that contain a small amount of mercury for energy-efficient lighting purposes. Mercury lamps in these products are labeled accordingly. Please manage the lamp

according to local, state, or federal laws. For more information, contact the Electronic Industries Alliance at www.eiae.org. For lamp-specific disposal information check www.lamprecycle.org.

Disposal of Electrical and Electronic Equipment



This symbol on the product or on its packaging indicates that this product should not be disposed of with your other waste. Instead, it should be handed over to a designated collection point for the recycling of electrical and electronic equipment. The separate collection and recycling of your waste equipment at the time of disposal will help to conserve natural resources and ensure that it is recycled in a manner that protects human health and the environment. For more information about where you can drop off your waste equipment for recycling, please visit our Web site at: http://qcare.quantum.com or contact your local government authority, your household waste disposal service or the business from which you purchased the product.

Product Model Number

The Scalar i6000 Regulatory Model Number is as follows: SCi6000.

Explanation of Symbols and Notes

The following symbols appear throughout this document to highlight important information.

Note: Indicates important information that helps you make better use of your system.

Caution: Indicates a situation that may cause possible damage to equipment, loss of data, or interference with other equipment.

WARNING: Indicates a potentially hazardous situation which, if not avoided, could result in death or bodily injury.

Other Documents you Might Need

The following documents are also available for this product. These documents can be found at www.quantum.com/support.

- *Scalar i6000 Planning Guide* (6-66882-xx)
- *Scalar i6000 Release Notes* (6-66883-xx)
- *Scalar i2000/i6000 Maintenance Guide* (6-66880-xx)
- *Scalar i6000 Installation Guide* (6-66881-xx)
- *Scalar i6000 Unpacking Instructions* (6-00771-xx [Gen 1] or 6-67467-01-xx [Gen 2])
- *System, Safety, and Regulatory Information Guide (*6-00618-xx)

Note: Release Notes are also available for this product. The Release Notes describe changes to your system or firmware since the last release, provide compatibility information, and discuss any known issues and workarounds. The Release Notes can be found at www.quantum.com/support.

Contacts

Quantum company contacts are listed below.

Quantum Corporate Headquarters

To order documentation on the <Product Name> or other products contact:

Quantum Corporation *(Corporate Headquarters)*
1650 Technology Drive, Suite 700
San Jose, CA 95110-1382

Technical Publications

To comment on existing documentation send e-mail to:

doc-comments@quantum.com

Quantum Home Page

Visit the Quantum home page at:

http://www.quantum.com

Getting More Information or Help

StorageCare™, Quantum's comprehensive service approach, leverages advanced data access and diagnostics technologies with cross-environment, multi-vendor expertise to resolve backup issues faster and at lower cost.

Accelerate service issue resolution with these exclusive Quantum StorageCare services:

Quantum. Global Services

- **Service and Support Website** - Register products, license software, browse Quantum Learning courses, check backup software and operating system support, and locate manuals, FAQs, firmware

downloads, product updates and more in one convenient location. Benefit today at:

http://www.quantum.com/ServiceandSupport/Index.aspx

- **eSupport** - Submit online service requests, update contact information, add attachments, and receive status updates via e-mail. Online Service accounts are free from Quantum. That account can also be used to access Quantum's Knowledge Base, a comprehensive repository of product support information. Sign up today at:

  http://www.quantum.com/osr

- **StorageCare Guardian** - Securely links Quantum hardware and the diagnostic data from the surrounding storage ecosystem to Quantum's Global Services Team for faster, more precise root cause diagnosis. StorageCare Guardian is simple to set up through the internet and provides secure, two-way communications with Quantum's Secure Service Center. More StorageCare Guardian information can be found at:

  http://www.quantum.com/ServiceandSupport/Services/GuardianInformation/Index.aspx

For further assistance, or if training is desired, contact the Quantum Customer Support Center:

United States	800-284-5101 (toll free) 949-725-2100
EMEA	00800-4-782-6886 (toll free) +49 6131 3241 1164
APAC	+800 7826 8887 (toll free) +603 7953 3010
For worldwide support: http://www.quantum.com/ServiceandSupport/Index.aspx	

Chapter 1
Description

The Scalar i6000 library automates the retrieval, storage, and control of tape cartridges. Application software on the host can use the library's robotics to mount cartridges into tape drives and retrieve them without operator intervention.

The library can be installed on a solid or raised floor. It has a standard 19-inch rack footprint and can be placed in a standard server rack space. Because the library provides access by way of the access and service doors, the library can be placed with either side against a wall or between racks.

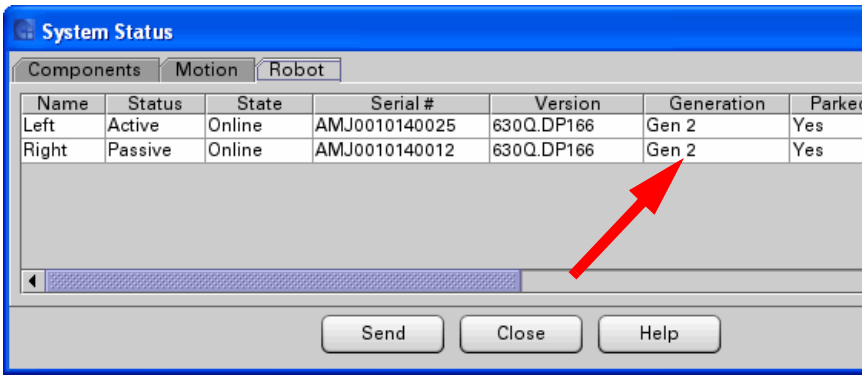
In December, 2011, the library robotics were redesigned. The redesign accommodates either a single robot or dual robotics. The original robot hardware is referred to as Gen 1; the new robot hardware is referred to as Gen 2.

With firmware version i11, robots in a dual-robot system work in an active/active manner, where both robots perform move commands and other library operations.

Dual robotics libraries require special modules on either end called parking modules, which house the robots when not in use. See Dual Robotics Configurations and Parking Modules on page 6 for more information.

You can tell which generation robot you have via the library user interface. The library displays which generation of robot hardware is installed. Select **Monitor > System** from the menu, click the **Robot** tab, and look in the **Generation** column (see Figure 1).

Figure 1 Robot Tab



For Gen 1 systems, the maximum library can be configured to accommodate from 100 LTO cartridges to 5,322 LTO cartridges (for a single-robot library) or 5,376 LTO cartridges (for a dual-robot library).

For Gen 2 systems, the maximum library can be configured to accommodate from 100 LTO cartridges to 7,146 LTO cartridges (for a single-robot library) or 7,224 LTO cartridges (for a dual-robot library).

In March of 2013, a High Density Expansion Module (HDEM) was made available to provide increased storage capabilities. A single HDEM can hold up to 720 total slots; 540 on two independent carousels and 240 on the front door.

This chapter provides a description of the following features and components:

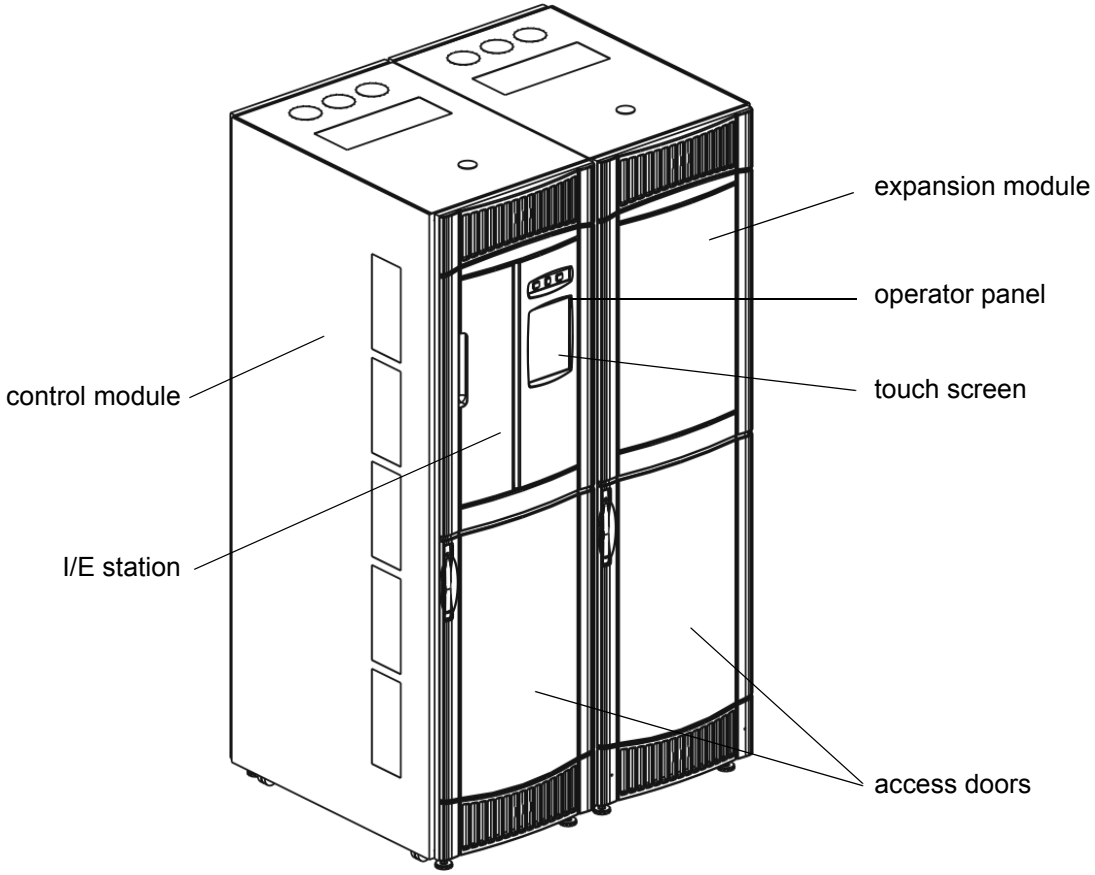
Note: The library software features described in this guide apply to both the Scalar i2000 and the Scalar i6000. However, certain features are available on Scalar i6000 only.

This chapter includes the following sections:

Front View

Figure 2 shows a front view of the library, consisting of a control module and an expansion module.

Figure 2 Front View of a Control Module and Expansion Module



Hardware Configuration Options

The library is designed for ease of installation, configuration, and field upgrades. The minimum library configuration consists of one control module. You can add up to 15 expansion modules as storage and tape drive requirements change.

Note: Expansion modules in positions nine through sixteen are no longer storage-only modules and can contain I/E stations or drives.

For LTO, the maximum library configuration can accommodate

- 1 control module,
- 0 to 15 expansion modules
- Gen 1 systems: 100 to 5322 cartridges (single robotics)
- Gen 2 systems: 100 to 7146 cartridges (single robotics), or 100 to 7224 (dual robotics). For libraries containing high-density expansion modules, the maximum capacities are 12,006 LTO cartridges (for a single-robot library) or 11,760 LTO cartridges (for dual-robot libraries).
- 1 to 96 tape drives.

An LTO library I/E Station configuration can accommodate:

- 1 to 8 24-slot Import/Export (I/E) stations in the control module and first 7 expansion modules.

  Or

- 1 24-slot I/E in the control module and up to 7 72-slot I/E stations and first 7 expansion modules.

Dual Robotics Configurations and Parking Modules

A dual robotics library requires Gen 2 robotics hardware. A dual robotics library requires, at a minimum, a control module, a left parking module, and a right parking module. See Figure 3.

The left and right parking modules have the same size and appearance as expansion modules, but they function differently. Each parking module contains a "parking space" in which the respective left or right robot resides when not in use. The "parking space" occupies four magazine columns which cannot be used for storage.

The left parking module is located to the left of the control module in position zero. It is referred to in the user interface as "module 0." The left parking module does not contain tape drives, I/E stations, or power supplies. The control module supplies its power. If you are upgrading to dual robotics, you will receive a left parking module to add onto your existing system. This increases your system size, so you must take this into account when planning for an upgrade.

The right parking module is the right-most module in the system. As of firmware version i11, a right parking module can contain drives in any position in the library and up to one 24-slot I/E station. Right parking modules may not contain 72-slot I/E stations.

Note: High-density expansion modules (HDEM) cannot be used as right parking modules.

If you are upgrading a single-robotics library to a dual-robotics library, the existing right-most expansion module can, in most cases, be converted into a right parking module. However, if the existing right-most expansion module contains a 72-slot I/E station, you may need another module to be added to the right of your system which will become the right parking module. If space considerations prohibit the addition of another module, then the right-most module will be swapped with another module in the library that does not contain a 72-slot I/E station.

Figure 3 Dual Robotics Library

Side panels, doors, and door posts have been removed for clarity.

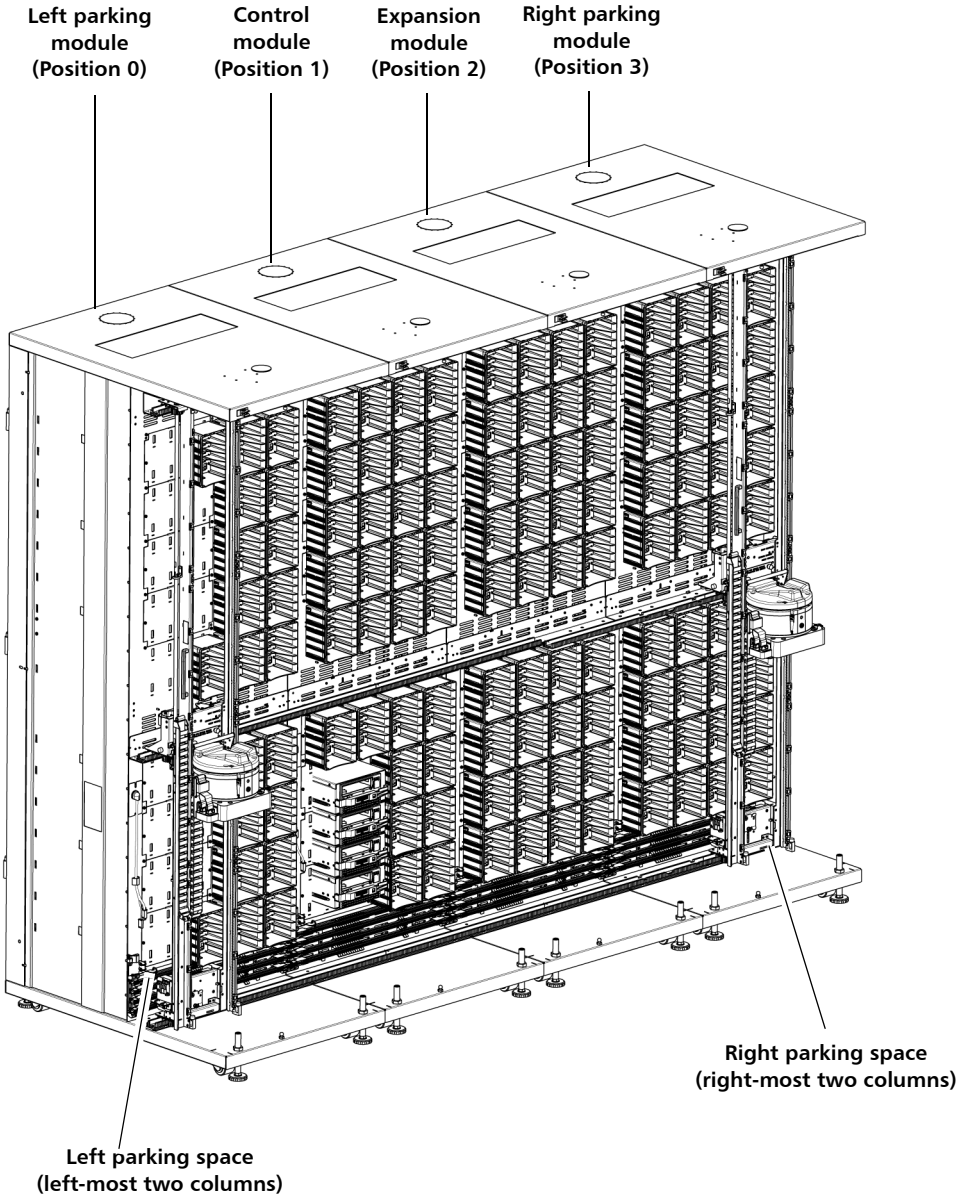


Figure 4 Left Parking Module Slot Configuration (Dual Robotics Only)

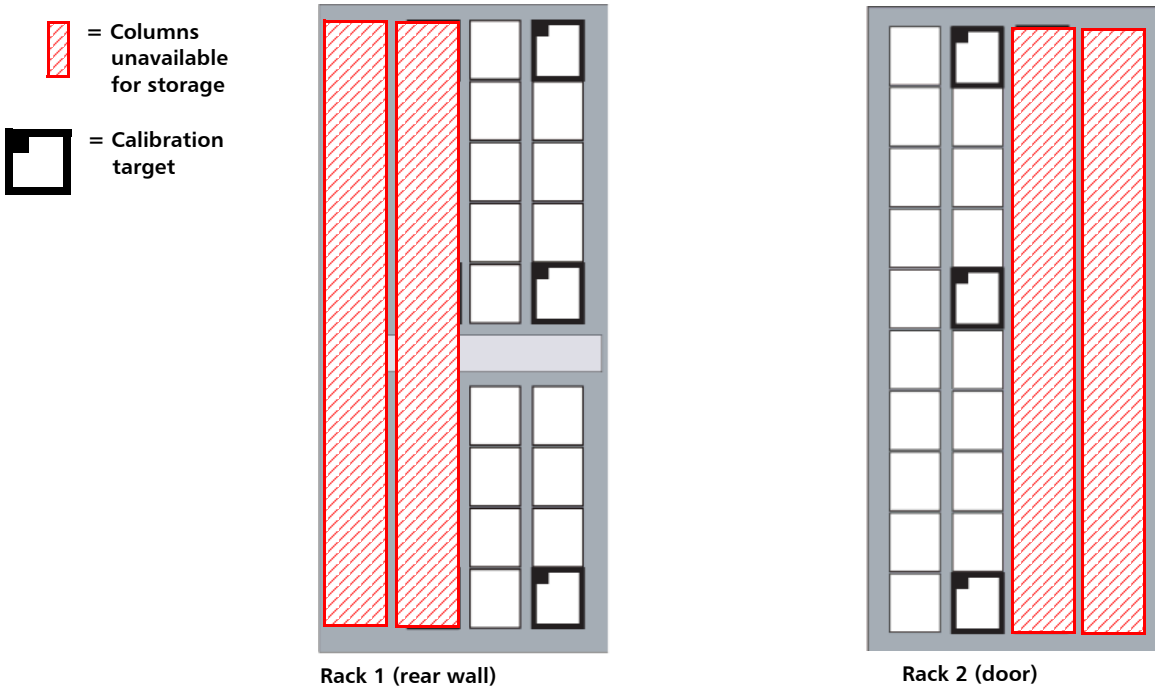
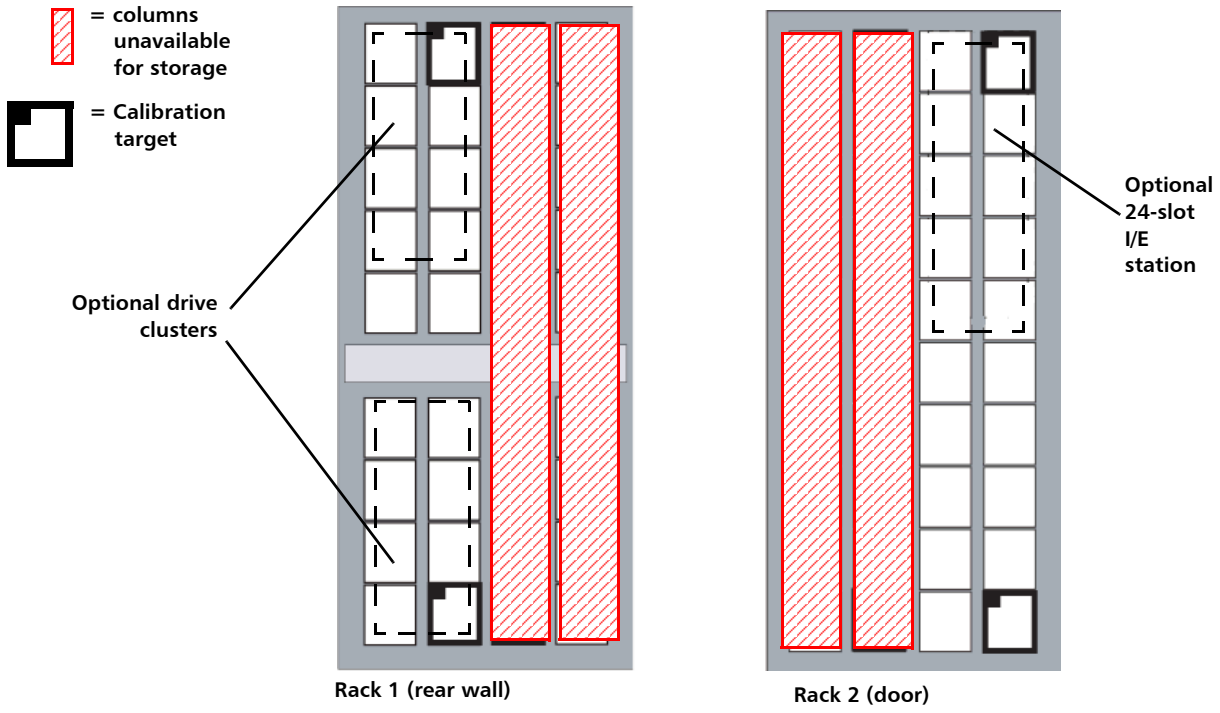


Figure 5 Right Parking Module Slot Configuration (Dual Robotics Only)



Control Module

All libraries contain a control module. A single-frame library consists of a control module only. The control module manages library operations via the library management module and includes an operator panel touch screen for local operator use. For more information, see:

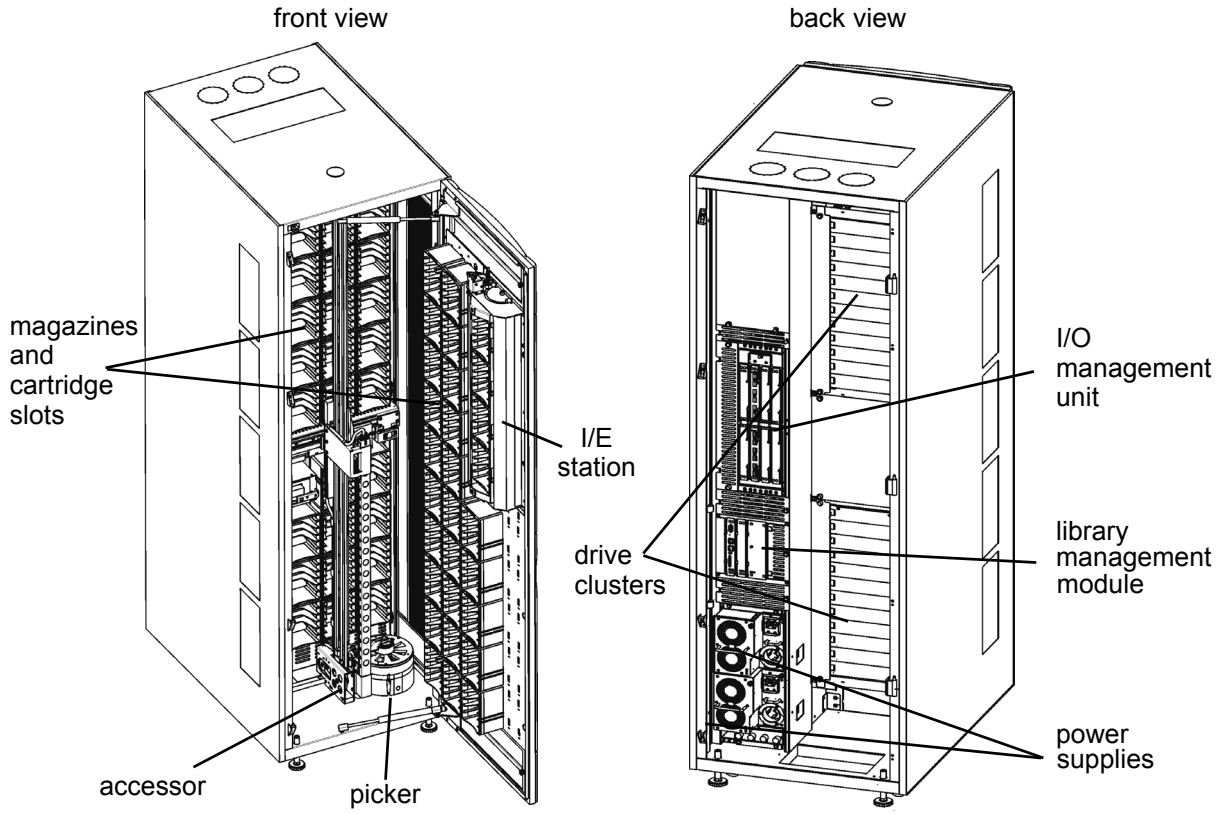
- Library Management Module on page 14
- Support for WORM on page 29

The control module also contains all of the other components common to expansion modules, including:

- Import/Export Stations on page 19
- Tape Drives and Media on page 26
- Cartridges on page 22
- Cartridge Magazines on page 23
- Power System on page 31

The control module always occupies module position 1 in the library. (In dual-robotics configurations, the left parking module is in position 0.)

Figure 6 Front and Back View of the Control Module



Expansion Modules

Expansion modules enable the library to expand by adding space for tape drives, an I/E station, and storage. Each expansion module up to the seventh expansion module adds from 300 to 456 LTO cartridge slots depending on the number of tape drives installed and whether an I/E station is installed. See Figure 7 on page 12 for location information.

In Gen 1 configurations, the library's maximum configuration includes up to 11 expansion modules for a total of 12 modules. in Gen 2 configurations, up to 16 modules can be added. Expansion modules can be added only to the right of the control module.

In firmware version i11, all standard expansion modules can accommodate the following functional units:

- I/O Management Unit on page 16
  - Control Management Blade on page 16
  - Fibre Channel I/O Blades on page 17
  - Ethernet Expansion Blades on page 17
- I/O Management UnitRobot on page 18
- Import/Export Stations on page 19 (optional)
- Tape Drives and Media on page 26 (drives are optional)
- Cartridge Magazines on page 23
- Support for WORM on page 29
- Power System on page 31 (required only if drives are installed; if an expansion module contains only cartridges, all power is derived from the control module).

High-density expansion modules can accommodate the following functional units:

- I/O Management UnitRobot on page 18
- Import/Export Stations on page 19 (optional)
- Tape Drives and Media on page 26 (media only)
- Cartridge Magazines on page 23
- Support for WORM on page 29

- Power System on page 31

Figure 7 Expansion Module with 24 Slot I/E Station

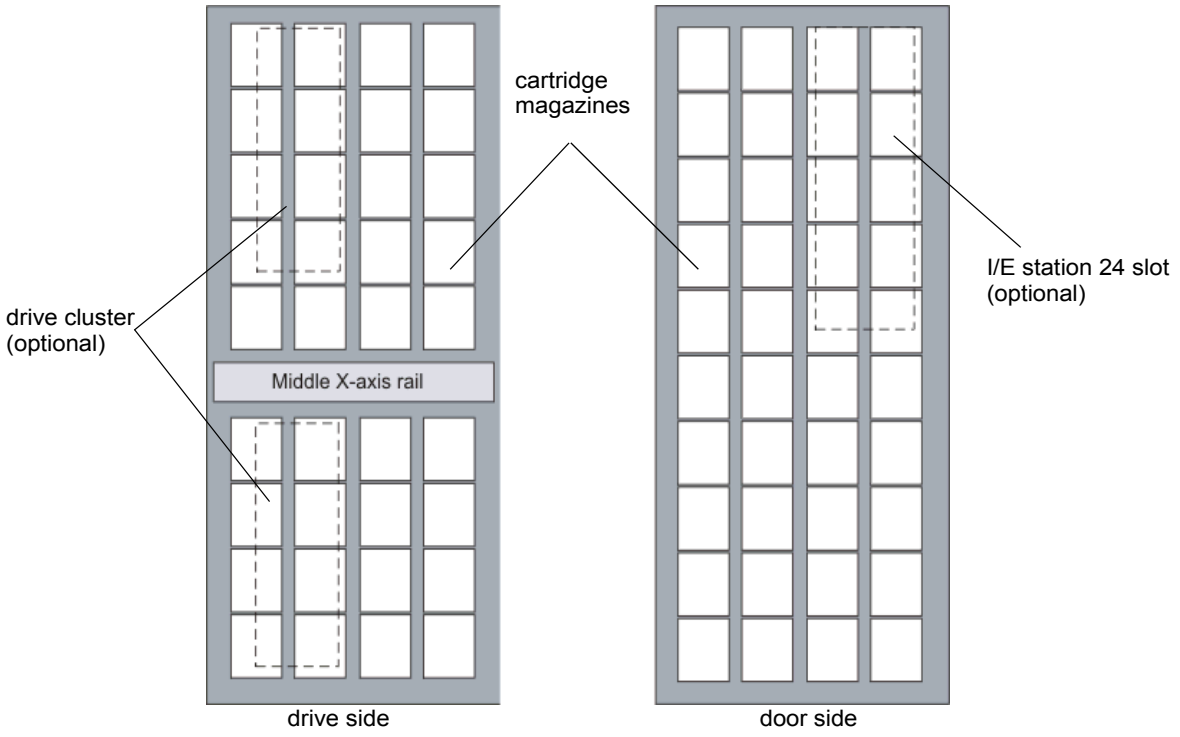
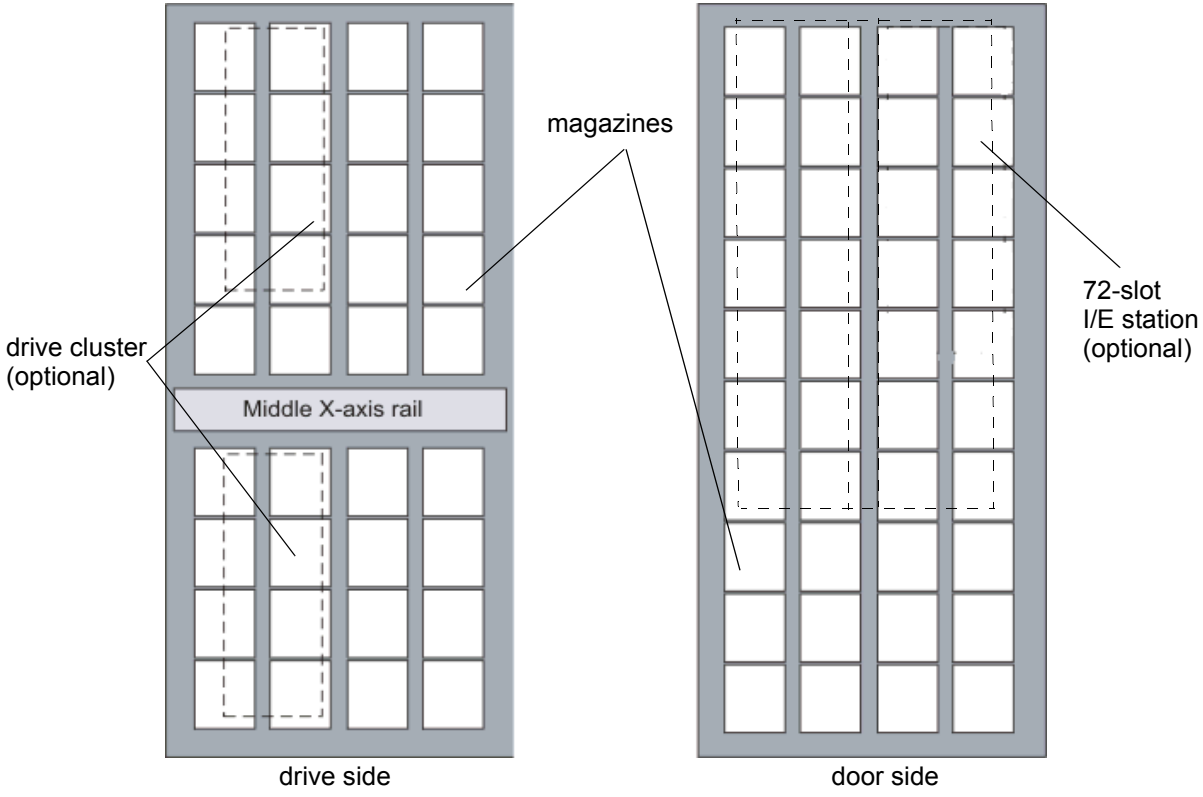


Figure 8 Expansion Module with 72 Slot I/E Station

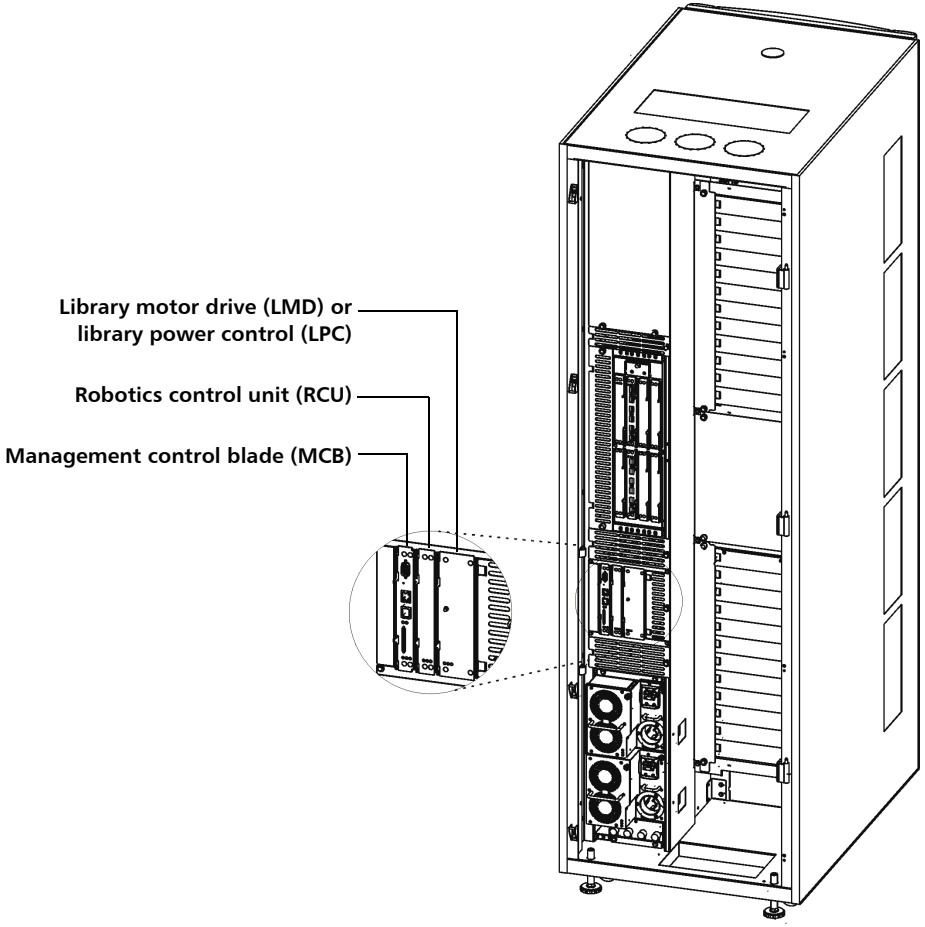


Library Management Module

The library management module is located in the control module. It controls system hardware and enables external devices to perform configuration and obtain system status. The library management module contains the following boards:

- Management control blade (MCB) - Manages the library, passing commands to and from the robotics control unit as well as the storage area network (SAN) components.
- Robotics control unit (RCU) - Controls the picker and accessor functionality.
- Library motor drive (LMD) (Gen 1 libraries only) - Distributes power to the picker along with the X and Y-axis circuits. It also distributes power to the touch screen.
- Library power control (LPC) (Gen 2 libraries only) - Distributes power to the robot through the power rails. It also distributes power to the touch screen.

Figure 9 Library Management Module Boards



I/O Management Unit

The I/O management unit is an optional component that provides connectivity and data path management to a SAN fabric and the hosts. The I/O management unit houses up to four FC I/O blades, which provide FC connections for the Fibre Channel drives in the module. The I/O management unit also houses up to two Ethernet Expansion blades, which handle internal Ethernet communication between the MCB and HP LTO-5 and LTO-6 drives. (The control module and each of the expansion modules can contain up to 12 FC drives.) The I/O management unit performs all tape drive and library host communication functions in a library that is attached to a SAN.

I/O management units may be installed in the control module and expansion modules. The I/O management unit supports the following blades:

- Control Management Blade
- Fibre Channel I/O Blades
- Ethernet Expansion Blades

When FC I/O blades or Ethernet Expansion blades are installed in the library, the following rules regarding control management blades (CMBs) apply:

- Any module (including the control module) that contains FC I/O blades or Ethernet Expansion blades must also contain a CMB.
- A CMB must be installed in the control module and all modules that contain drives. Modules that don't contain drives, blades or network chassis will contain drive and network jumpers that maintain communications between the MCB located in the control module and the modules that contain drives, FC I/O blades and EEBs.

Control Management Blade

The control management blade (CMB) performs unit status monitoring including power and I/O present conditions, and internal network switch functions connecting I/O blades with the library management module.

Fibre Channel I/O Blades

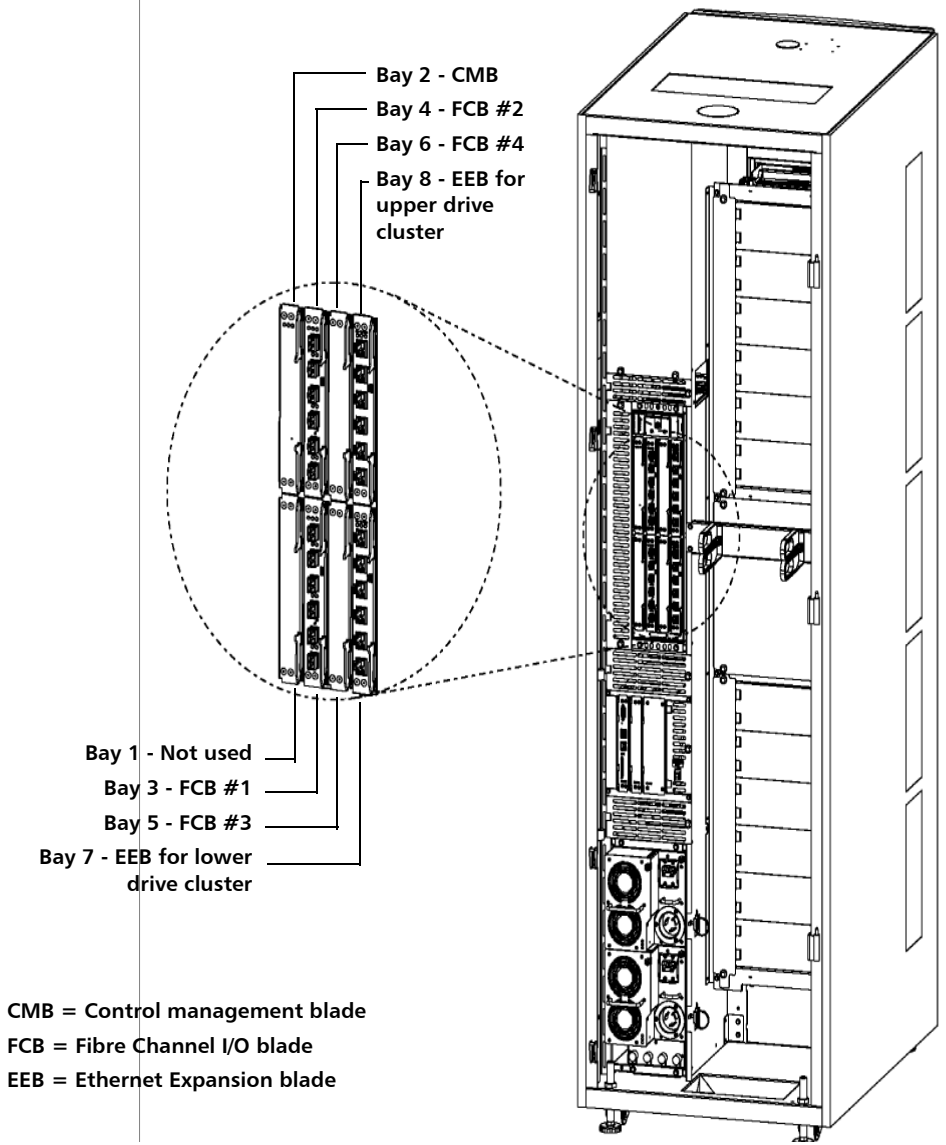
There is one Fibre Channel (FC) I/O blade type supported: 7404 that auto-negotiates up to 4 Gbps. The 7404 FC I/O blade has an embedded controller that provides connectivity and features that enhance the performance and reliability of tape operations. It also provides two host communication ports and four connection ports to drives.)

- Fibre Channel LTO-1, LTO-2, LTO-3, LTO-4, LTO-5, and LTO-6 drives can be connected to drive-aggregating Fibre Channel I/O blades or directly attached to a host, so these drives do not require an external SNC.
- We recommend that you do not connect an LTO-5 or LTO-6 drive to an FC I/O blade. These drives support speeds of 8 Gbps, but the FC I/O blade only supports 4 Gbps.

Ethernet Expansion Blades

The Ethernet Expansion Blade (EEB) provides the option for Ethernet connectivity to each LTO-5 or LTO-6 drive (for MCB-to-drive communication purposes only). The connection is at T100. The EEB provides a control path to the drive for commands as well as facilitates taking drive logs and downloading drive firmware. Each EEB has 6 Ethernet ports to allow attachment to 6 LTO-5 or LTO-6 drives. The EEB provides Ethernet connectivity to the library's internal Ethernet only and should not be connected to an external Ethernet source.

I/O Management



Unit

Robot

The robot moves cartridges between storage cells, tape drives, and the I/E station. A picker is used to get or put cartridges in a storage cell or a tape drive slot. The picker moves along an X and Y axis and can pivot 180°. A barcode scanner on the picker assembly identifies cartridges located in storage cells.

The library can be configured for either one or two robots. See Dual Robotics Configurations and Parking Modules on page 6 for more information.

Import/Export Stations

I/E stations enable you to import and export cartridges without interrupting normal library operation. There are two types of I/E stations: 24-slot I/E stations and 72-slot I/E stations.

Each 24-slot I/E station has a capacity of 24 LTO cartridges that are located in four removable magazines. The 72-slot I/E station consists of two side-by-side 36-slot I/E stations that can operate independently or as a single 72-slot I/E station. Each 36-slot I/E station provides I/E capacity of 36 LTO cartridges in six removable magazines.

The I/E station is installed on the front of the control module or any of the first seven expansion modules, including high-density expansion modules. It can be installed in a right parking module if the right parking module is in position 2 through 8. Expansion modules (and the right parking module) in positions nine through seventeen are storage-only modules and do not contain I/E stations or drives. See Figure 2 on page 4, Figure 7 on page 12, and Figure 8 on page 13 for I/E station location.

Note: The I/E station cannot be configured as a storage location, but it can be part of a logical division of library resources known as partitions. For information about partitions, see Working With Partitions on page 118.

Note: The maximum number of I/E element addresses in any partition is 240. This includes both physical slots and Extended I/E virtual slots.

I/E Station Options

An expansion module is designed for customers who have an increased need to import or export cartridges. An expansion module, including high-density expansion modules, can have no I/E station, a 24 slot I/E station, or a 72 slot I/E station. The increased capacity is achieved by increasing the overall length of the I/E station and doubling its width.

The 24-slot I/E station has a capacity of 24 LTO cartridges that are located in four removable magazines.

The 72- slot I/E station consists of two side-by-side 36-slot I/E stations that can be operate as one 72-slot I/E station or can be operated independently. Each 36-slot I/E station provides I/E capacity of 36 LTO cartridges in six removable magazines.

Extended I/E Option

The number of I/E slots in a library is usually associated with the number of I/E slots in an actual physical I/E station, but this physical slot count could limit how many I/E slots may be available to a host application.

Extended I/E configurations remove such I/E slot count limitations by increasing the I/E slot count for a partition with storage slots that will be reported to a host as I/E slots. Thus, extended I/E allows the user to configure their partitions with I/E slots beyond the number of physical I/E slots configured in the library. As a result, the host can export more media than previously allowed.

Keep in mind that as extended I/E slots are used, fewer storage slots are available. You will need to initiate move/import operations of tape cartridges into the extended I/E area for host access. Conversely, to move/export tape cartridges from extended I/E area slots to the emptied physical I/E Station slots, you need to initiate the move/export operation from the user interface for physical access to the library.

Note: By default, the extended I/E feature is disabled and is only available on Scalar i6000 libraries. Extended I/E can be enabled/disabled from the 'Physical Library' dialog (**Setup > System Settings > Physical Library**). Refer to Setting Up Policies for the Physical Library on page 170.

Note: To configure a partition with extended I/E segments, you must use the Partition Wizard (**Setup > Partition > Configure**). The extended I/E feature is only available in expert creation mode or if you are modifying an existing partition. Refer to Using Expert Mode on page 131. Extended IE is not supported on library managed partitions.

Extended I/E must be enabled before using it. When configuring extended I/E in a partition, ensure you have enough licensed slots [Capacity On Demand (COD)] to accommodate the new extended I/E slots, since extended I/E slots use the COD licensed slot count.

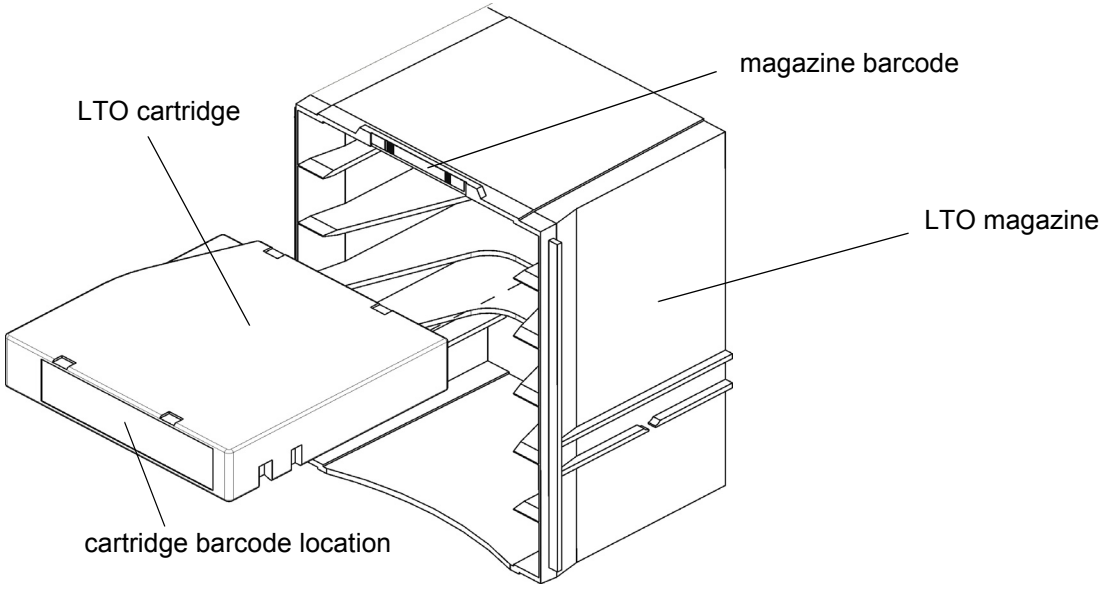
When you configure extended I/E slots you must have at least one physical I/E segment configured in the partition. The maximum number of physical and extended I/E slots per partition is 240.

The I/E area configured with the extended I/E feature will report the SCSI element addresses starting with the actual physical I/E slots, followed by the extended I/E slots. This will allow hosts to always first use the available slots in the actual physical I/E Station before “spilling” into the extended I/E area.

Cartridges

Cartridges are stored in magazines within the library, as shown in Figure 10.

Figure 10 Example of LTO Cartridge Insertion into a Magazine



Each cartridge has an operator-attached, machine-readable barcode label on it for identification purposes. The library can dynamically support barcode labels with 1 to 14 characters plus a one-character or two-character media identifier, depending on drive type. The library currently supports Code 39 (3 of 9) type barcode labels. For more information about tape cartridges, see Tape Drives and Media on page 26. For additional specification information, see Barcode Label Requirements on page 679. For details about the use of drives and cartridges, see Mixed Media Support and Rules on page 28.

Note: Media must contain valid barcode labels. The library will not support tapes without valid barcode labels.

Note: A 14-character barcode label length may not be printable according to the Code 39 label specifications for the tape cartridge area to which the label is attached. The effective tape cartridge barcode label length, including any media ID, may be limited to a maximum of 12 characters.

Cartridge Magazines

The cartridge magazine is a storage assembly that installs on the drive side or door side of the control module or expansion module, as shown in Figure 11. It contains the cartridge slots and provides flexibility when adding storage cartridges to a module.

Figure 11 Magazine and Drive Locations in the Control Module

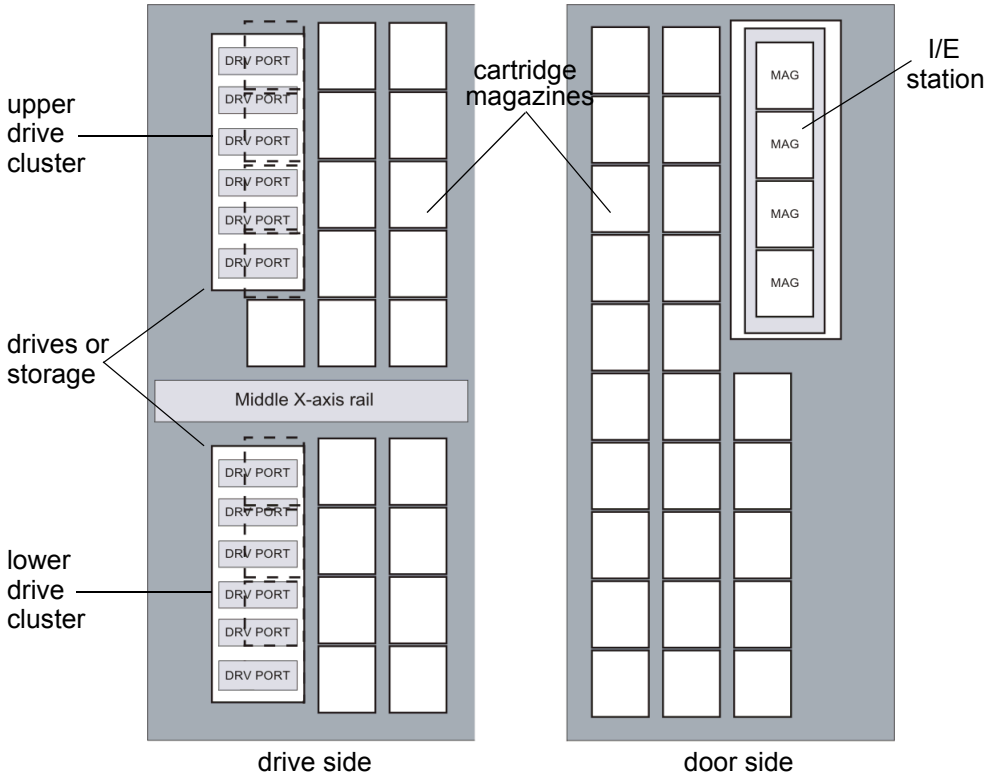


Table 1 Cartridge Capacities in Library Modules

Type	Magazine Capacity	Cartridge Capacity
Magazine (LTO)	--	6
Control module (single-robotics)[a]	44 min/51 max	264 min/306 max
Control module (dual-robotics)[a]	50 min/64 max	300 min/384 max
Standard Expansion module[c]	48 min/76 max	288 min/456 max
Drive Ready Expansion Module[b]	32 min/76 max	192 min/456 max
High-Density Expansion Module[c]	102 min/130 max	612 min/780 max
Left parking module (dual-robotics)[d]	38	228
Right parking module (dual-robotics)[e]	12 min/38 max	72 min/228 max

a. Control module: The minimum is based on having 12 drives and one 24-slot I/E station installed. The maximum is based on having one drive and one 24-slot I/E station installed.
b. Drive Ready Expansion module: The minimum is based on having 12 drives and one 72-slot I/E station and 12 drives installed. The maximum is based on having no drives or an I/E station installed.
c. Standard and HDEM: The minimum is based on one 72-slot I/E station and 12 drives installed. The maximum is based on having no drives or an I/E station installed.
d. Left parking module: No drives or I/E stations are allowed. The left parking space takes up 4 columns of storage. There are six empty magazines located in the unusable 4 columns which are used for calibration only. These six magazines are not counted toward the total capacity.
e. Right parking module: The minimum is based on having 12 drives and one 24-slot I/E station installed. The maximum is based on no drives or I/E station installed. The right parking space takes up 4 columns of storage.

Each magazine has a barcode label that the scanner reads for identification and inventory. An optional, snap-on dust cover is available for the magazines. Magazines with the dust cover have interlocked stacking that enables easier storage of the media when they are removed from the library for external storage.

Tape Drives and Media

Note: Library firmware versions 630Q (i10) and later do not support DLT tape drives, media, or magazines. If you upgrade to these library firmware versions, make arrangements to remove and/or replace all DLT tape drives, media, and magazines in your library. If you want to continue to use DLT tape drives and media, your library firmware must be at version 617Q.GS01001 (i8.4) or earlier.

Tape drives are enclosed in a universal drive sled. You can hot swap and hot add all supported drives, regardless of type. The library supports the following types of tape drives:

- IBM LTO-1 or LTO-2 LVD–SCSI
- IBM LTO-1, LTO-2, LTO-3, LTO-4, LTO-5, or LTO-6 FC Multi-mode
- HP LTO-3, LTO-4, LTO-5, and LTO-6 FC Multi-mode

Caution: A single partition can have a mixture of drive types and interface types within the same domain (for example, LTO-1 and LTO-2 with SCSI or Fibre Channel interfaces). For more information, see Mixed Media Support and Rules on page 28 and Understanding Partition Media Policy Settings on page 121.

The control module and expansion modules have upper and lower drive clusters. Each library must have at least one tape drive. Each drive cluster can house up to six tape drives for a total of 12 drives. Additional drives can be added to any expansion modules in the configuration, except high-density expansion modules. This enables you to have a total of 96 drives. In dual-robot systems, the left parking module cannot contain drives.

Note: When you add drives, you lose storage slots.

As of firmware version i11, drives can be installed in any module in the library except a left parking module or high-density expansion module. However, it is still recommended that drives be installed in bottom-to-top order.

Note: The term **drive cluster** defines a grouping of up to six tape drives below or above the middle X-axis rail.

Figure 11 on page 24 shows the locations of drives in the control module. For details about the use of drives and cartridges, see Mixed Media Support and Rules on page 28.

Fibre Channel LTO-1, LTO-2, LTO-3, LTO-4, LTO-5, and LTO-6 drives can be connected to drive-aggregating Fibre Channel I/O blades or directly attached to a host, so these drives do not require an external SNC. More detailed information about LTO drives follows.

LTO Drives

Six generations of LTO drives are supported, but they are not fully compatible as shown in Table 2. (N/C = Not Compatible)

Table 2 LTO Drive and Cartridge Compatibility

	LTO-1	LTO-2	LTO-3	LTO-3 WORM	LTO-4	LTO-4 WORM	LTO-5	LTO-5 WORM	LTO-6	LTO-6 WORM
LTO-1 Drives	Reads/ Writes	N/C	N/C	N/C	N/C	N/C	N/C	N/C	N/C	N/C
LTO-2 Drives	Reads/ Writes[a]	Reads/ Writes	N/C	N/C	N/C	N/C	N/C	N/C	N/C	N/C
LTO-3 Drives	Reads[b]	Reads/ Writes[c]	Reads/ Writes	Write Once, Read Many[d]	N/C	N/C	N/C	N/C	N/C	N/C
LTO-4 Drives	N/C	Reads	Reads/ Writes	Write Once, Read Many	Reads/ Writes	Write Once, Read Many[e]	N/C	N/C	N/C	N/C
LTO-5 Drives	N/C	N/C	Read	Read Many	Reads/ Writes	Write Once, Read Many	Reads/ Writes	Write Once, Read Many	N/C	N/C

	LTO-1	LTO-2	LTO-3	LTO-3 WORM	LTO-4	LTO-4 WORM	LTO-5	LTO-5 WORM	LTO-6	LTO-6 WORM
LTO-6 Drives	N/C	N/C	N/C	N/C	Read	Read Many	Reads/ Writes	Write Once, Read Many	Reads/ Writes	Write Once, Read Many

a. LTO-2 drives do not reformat LTO-1 cartridges. The drives will write to the cartridges in the LTO-1 format (100 GB capacity).
b. LTO-3 drives only read LTO-1, they do not write to the LTO-1.
c. LTO-3 drives do not reformat LTO-2 cartridges to contain the same density as the LTO-3 cartridges (400 GB). The LTO-3 drives will write to the LTO-2 cartridges in the LTO-2 format (200 GB capacity).
d. LTO-3 WORM requires the installation of library firmware and WORM-supported LTO-3 tape drive code.
e. LTO-4 WORM requires the installation of the library firmware and WORM-supported LTO-4 tape drive code.

All LTO cartridges are the same physical size, which means they use the same magazines in the library.

LTO drives can be directly attached to hosts, the SAN, or to FC I/O blades in the I/O management unit. SCSI drives must be directly attached to hosts or to the SAN.

Mixed Media Support and Rules

The library supports LTO cartridges and drives in the same configuration, provided that you adhere to the following rules:

Note: Libraries with Gen 2 hardware do not support DLT drives or media.

Note: Libraries with firmware at version 630Q or later do not support DLT drives or media.

- When purchasing a library with mixed media, the new orders must specify the base system technology and the number of magazines, the number of drives, and the number of I/E station magazines for each media type required. The base system is considered the primary media type used in the library.

- Multiple generations of LTO media can be mixed at the magazine level.
- The supported multiple media are LTO-1, LTO-2, LTO-3, LTO-3 WORM, LTO-4, LTO-4 WORM, LTO-5, LTO-5 WORM, LTO-6, and LTO-6 WORM.
- Drives can be installed in any frame.

Support for WORM

The Scalar i6000 library supports WORM (write once, read many) technology in LTO-3, LTO-4, LTO-5, and LTO-6 tape drives. WORM requirements include:

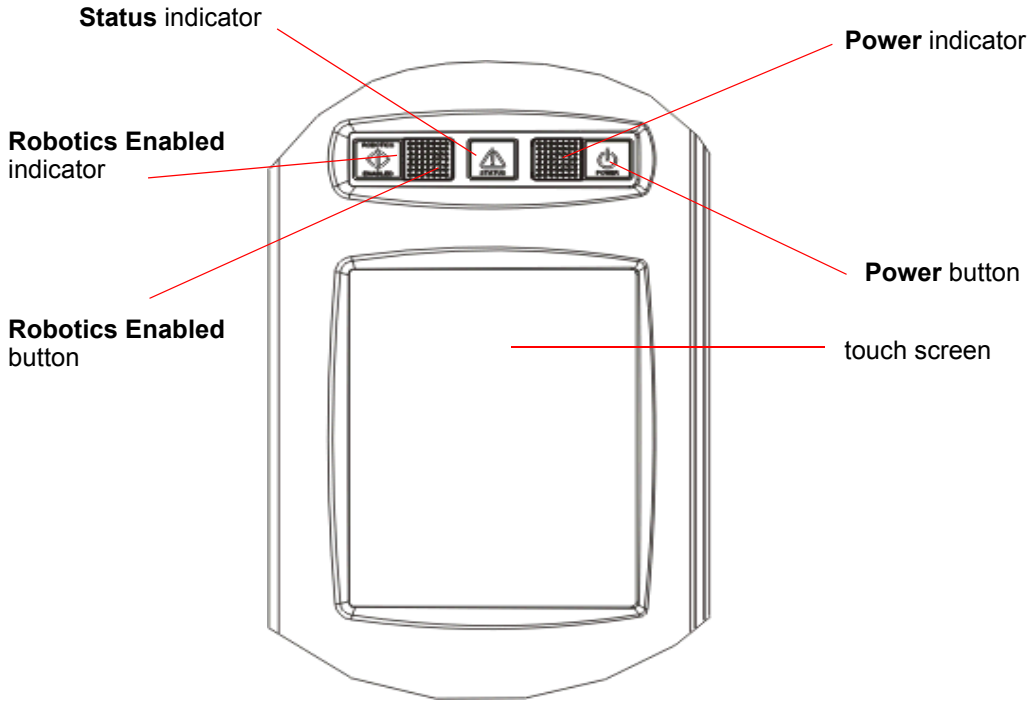
- Cartridges
- Firmware
- WORM-supported LTO-3 tape drives
- WORM-supported LTO-4 tape drives
- WORM-supported LTO-5 tape drives
- WORM-supported LTO-6 tape drives

WORM allows non-erasable data to be written once and provides extra data security by prohibiting accidental data erasure. When the library firmware and WORM-supported LTO-3, LTO-4, LTO-5, or LTO-6 tape drive code are installed on a library with LTO-3, LTO-4, LTO-5, or LTO-6 tape drives, the WORM feature is supported whenever the operator uses WORM cartridges.

Operator Panel

The operator panel is located on the front of the control module and consists of indicators and a touch screen (see Figure 12). The buttons are for library control and power, and the indicators provide library status.

Figure 12 Operator Panel



The touch screen is the library navigation point and provides access to the LMC. For more information about the touch screen and the LMC, see Library Management Console (LMC) on page 432.

Power System

The library supports single and redundant power configurations. The single configuration has a single AC line input and single DC power supply. The redundant configuration has dual AC line input and dual DC power supplies. You can hot swap a power supply if you have a redundant power supply. You can hot add a second power supply.

The power system consists of the following:

- Power supply
- Power distribution unit
- AC power cord

A single power switch, located on the front door of the control module, turns on and off all power for the control module and attached expansion modules. Each power distribution unit has a second circuit breaker, located in the rear of the module, that controls the module power supply output. The power supply has three LEDs that provide status information. The power system also has four fuses for system protection.

The control module and all expansion modules or right parking modules that contain drives must contain a power system. If an expansion module or right parking module contains only cartridges, its power is derived from the control module and a power system is not needed.

High-density expansion modules have their own AC power systems that can supply power to up to six (6) additional HDEMs if redundant power is installed. The additional HDEMs must be in consecutive positions to receive power from a single HDEM. Each power distribution unit has a circuit breaker located at the rear of the module.

Library Features

This section describes several library features.

Density

The library provides a storage density of 720 cartridges (LTO) per square meter. Each module, also referred to as a frame, has two storage racks: one on the drive side and another on the door side. A rack consists of up to 10 horizontal sections and three or four columns of magazines, depending on the rack configuration. Each magazine, located at the intersection of a particular section and a particular column, consists of five or six cartridge slots, depending on the type of media (DLT or LTO).

Centralized Management

The Library Management Console (LMC) gives you a single point from which to view all library components, including robotics, drives, storage, I/E stations, and network connectivity. You can use this graphical user interface both locally from the library's touch screen and remotely from a remote client. The LMC communicates with the LMC server that runs on the library. The LMC uses a simple and intuitive graphical style that is secure and provides library managers with native partitioning ability.

Proactive Availability

The library can alert you about problems before they occur. The library checks the complete data path at user-defined intervals to make sure that it is functioning properly before backups begin. The library also monitors its six major subsystems (drives, power, robotics, cooling, connectivity, and control). You can configure the library to send notifications of problems to one or more e-mail accounts, including Quantum service personnel. For more information about the library's monitoring and reporting capabilities, see Maintaining Your Library on page 505.

Serviceability and Reliability

The library has extensive serviceability and reliability features. You can hot swap drives, power supplies (in redundant power configurations only), Input/Output (I/O) blades, and fans. Host port failover, an advanced feature that moves a host's communication stream from a failed connection to a working connection without disrupting the backup operation, maintains connectivity whether the failure occurs on the host, the switch, or the library.

Your backup system and data path are idle most of the time. When backups begin, the system is used intensively at maximum bandwidth. The library provides you with notifications and a robust ticket system that notifies you of any problems it identifies, enabling you to solve

them before backups begin. For more information about the library's notification system, ticket system, and other troubleshooting help, see Troubleshooting Your Library on page 35.

Data Path Conditioning

Quantum provides an automatic means of verifying, monitoring, and protecting data path integrity between hosts and library drives. This feature is referred to as data path conditioning. Using this feature, administrators can proactively detect and resolve data path problems before they affect backups, restore operations, and other data transfer operations. Data path conditioning makes sure that data transmissions are optimized and reliable, resulting in improved system availability.

Data path conditioning occurs in two separately managed areas:

- Between host and Fibre Channel (FC) I/O blades
- Between FC I/O blades and library drives

The FC I/O blade manages data path conditioning along the path between itself and the library drives. Data path monitoring automatically occurs at regular, configurable intervals. The FC I/O blade generates a RAS ticket if monitoring tests fail for two intervals. This indicates either loss of connectivity or drive failure. The FC I/O blades include the data path conditioning feature. Administrators can use the LMC to configure data path conditioning.

Host Attachment

Requests issued from the host application result in cartridge movement in the library. The primary requests issued are for mounting and dismounting cartridges in and out of the tape drives and for importing and exporting cartridges in and out of the library. The library manages the physical location. In addition to requesting cartridge movement in the library, the host application can use the FC command interface to obtain status information, configuration information, and cartridge storage information from the library.

Hosts can be attached to the library in the following ways:

- FC drives can be directly attached to host systems or to the SAN. In these configurations, the management control blade (MCB) has one library control port (FC) connecting to the controlling host computer.

- FC drives can be attached to FC I/O blades in the I/O management unit. There are two ports on each FC I/O blade that can be connected directly to the host or to the SAN.

Remote Management

The library can be managed locally or remotely using the LMC. Locally, the LMC appears on the touch screen on the front of the library. Remotely, the LMC is accessed through a client instance of the LMC software on any computer on the network. For more information about accessing Logging On From a Web Browser (Remote Client) on page 426. For more information about the LMC, see Library Management Console (LMC) on page 432.

The LMC provides additional monitoring of a SAN-attached library over the network to a management server by using Simple Network Management Protocol (SNMP). This includes library subsystem health and status information and early fault notification. For more information, see the *Intelligent Libraries Basic SNMP Reference Guide*.

The library also supports the Common Information Model (CIM) server based on the Storage Management Initiative Specification (SMI-S) on the MCB. A CIM client can use the CIM server to monitor the SAN-attached library. For more information, see the *Intelligent Libraries SMI-S Reference Guide*.

Capacity on Demand

If you purchased capacity on demand, the library is initially licensed for a default configuration of 102 LTO storage slots.

Capacity on Demand allows you to license physical slots in 100-slot blocks. Any number of slots can be licensed between 100 and 12,000. You do not need to license all the physical slots, but only licensed slots can be assigned to host managed partitions. It is often desirable to have more physical slots installed than will be licensed.

Capacity on Demand allows you to purchase capacity for your library as needed. As your storage needs change, you can add storage in blocks of 100. Scalar i6000 licensing begins at 100 cartridges and can be increased to as many as 7,146 LTO cartridges (for a single-robot library) or 7,224 LTO cartridges (for a dual-robot library).

Expansion modules are sold separately from the slot licensing. This separation provides the flexibility to order the exact modules needed (DREM, SEM or HDEM).

Chapter 2

Troubleshooting Your Library

This chapter describes how the library informs you of issues that it detects within its subsystems. It also provides information about working with tickets to resolve issues, running verifications tests to check whether they have been resolved, interpreting LEDs, viewing command history logs, and accessing Online Help.

This chapter consists of the following sections:

How Does the Library Report Issues?

The library has advanced problem detection, reporting, and notification functionality. The library has many processors and sensors that monitor conditions and operations, such as temperatures, voltages, current, calibrations, firmware versions, and so forth.

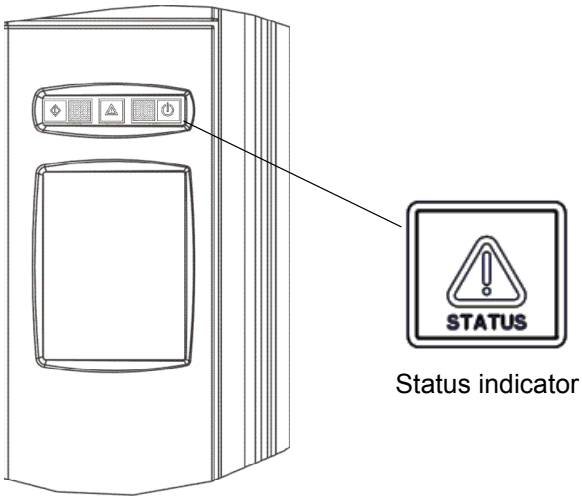
The library reports issues in several ways, which are described below:

- Status Indicator on page 36
- System Status Button Indicators on page 38
- E-mail Notifications on page 39

Status Indicator

The first indication of issues is the status indicator on the indicator panel, as shown in Figure 13.

Figure 13 Status Indicator



- If the **Status** indicator light is solid green, the library currently has no tickets in an **Open** state.
- If the **Status** indicator light is flashing amber, at least one of the six subsystems has a ticket in an **Open** state.

When the library detects an issue, it creates a ticket for it. A ticket includes the following types of information:

- Details about the issue
- Reports that are associated with the ticket
- A repair page that provides corrective actions

In most cases, tickets indicate operational failures that do not always point to a single CRU/FRU as having failed or causing an issue. IN such

cases, customer repair instructions are provided to isolate the issue and recover from the failure. Only if the library is able to clearly identify a failing CRU/FRU will the repair instruction request service or specific CRU/FRU replacement.

Note: Tickets can indicate failures or other serious problems, but they also can indicate warning conditions that you should investigate. For example, opening the library's access door or intentionally disconnecting drive fibre channel connections, causes the library to create a ticket, but if such operation is performed intentionally this condition would not indicate serious problems. However, you should still investigate the tickets to make sure no issue has been caused inadvertently by an aisle access operation or SAN configuration.

The library assigns a severity level to each ticket that it creates, and it notifies users of the ticket. Table 3 describes possible severity levels for tickets.

Table 3 Severity Levels Assigned to Tickets

Severity Level	Description
1 (Failed)	Indicates that a failure or serious condition has occurred within a library subsystem that requires immediate corrective action. In some cases, a hardware component is no longer functioning at an acceptable level or has failed. In other cases an operation may not have completed without a component having actually failed. Examples of failure situations include a FRU that is not functioning, a temperature threshold that may affect operations, or an Ethernet or FC connectivity issue that requires resolutions to network or SAN fabric connectivity issues before operations function normally again.
2 (Degraded)	Indicates that a degraded condition exists within a library subsystem that impacts system performance or redundancy. Typical library operations can continue without immediate corrective action, but an administrator should investigate the condition and correct the problem soon. Examples of degraded situations include a redundant power supply that has failed or a connectivity problem that has caused failover to occur.

Severity Level	Description
3 (Warning)	Indicates that a condition exists within a library subsystem that has some or little effect on system operations. Typical library operations can continue without immediate corrective action, but you should investigate the condition and correct the problem when possible. Examples of warning situations include a FRU that is functioning less reliably, or drives that cannot unload a tape while other drives are still available to service other requests, or a temperature threshold that has been reached that does not affect reliable operations.

The library has three ways of notifying users that it has discovered issues and has created tickets for them:

- Status indicators on Library Management Console (LMC) system status buttons
- E-mail notifications
- SNMP TRAP notifications

System Status Button Indicators

System status buttons are located in the **Overall System Status** area at the bottom of the LMC display. Each button displays a status indicator for the library subsystem it represents. For more information about the buttons, see System Status Buttons on page 447. When the library creates a ticket, the status indicator button for the affected subsystem automatically changes from the following icon:

Good (green)

to one of the following icons:

Warning *or* Degraded (yellow)

Failed (flashing red)

The meanings of these status indicators correspond to the severity levels described in Table 3 on page 37. If a system status button indicates anything other than a Good state, clicking it displays a list of open tickets for the subsystem. To access tickets by using the system status buttons, see Working With Tickets on page 40.

E-mail Notifications

The library collects status information on its components and, if the appropriate e-mail notifications have been set up in the LMC, the library can send notifications whenever tickets with severity levels 1, 2, or 3 are created. For information about severity levels, see Table 3 on page 37. The library assigns a severity level to each ticket it creates. If the ticket's severity level matches one of an e-mail address' severity codes (as set up in e-mail notifications), the library sends a notification to that particular e-mail address. The library also sends a notification if a ticket's severity level escalates to a more severe level. The library does not send one when an ticket's severity level becomes less severe.

By default, the only e-mail address to which the library sends e-mail notifications is techsup@quantum.com (Quantum technical support). When configured for Quantum technical support notification, the library notifies Quantum technical support only of those severity 1 issues that suggest a component failure requiring a possible CRU/FRU replacement. Severity 1 tickets that do not identify a library component failure, such as customer network connection issues and SAN fabric connection problems, do not automatically notify Quantum technical support, but allow customer issue analysis and customer-initiated support calls. To set up other e-mail addresses to receive any severity 1, and/or severity 2 and severity 3 ticket notification, see Configuring E-mail on page 177 and Setting Up E-mail Notifications on page 180.

Note: Even though you can remove the Quantum technical support e-mail address so that Quantum does not receive severity level 1 notifications, Quantum recommends that you do not remove it. Also, do not include the Quantum technical support e-mail address for severity level 2 or 3 notifications.

The subject line of the e-mail notification indicates "Scalar i6000," the library's serial number, and the severity level of the ticket. The body of the message states that the library sent the message automatically. The message body also includes the following information, which provides details about the ticket and library conditions at the time of the event:

- Ticket summary
- Ticket details, including status information
- Firmware versions, including MCB, RCU, CMB, and drive bricks
- Physical library configuration
- Library states, such as physical library online or offline, partitions online or offline, or robotics varied on or varied off
- Time stamps of recent activity
- Report summary
- Report details for the ticket

The notification also includes a repair page attachment. This page provides a problem description and corrective actions you or a customer service engineer (CSE) can perform. For more information about repair pages, see Viewing Ticket Repair Pages on page 58.

Note: A notification e-mail contains helpful information about a ticket and how to resolve it. However, the notification represents a condition that existed at a certain time in the past. The notification might not reflect the current situation. The notification indicates a specific ticket ID, so you should find and examine that specific ticket in the LMC. The ticket reflects the real-time status of the issue. For more information about accessing tickets, see Working With Tickets on page 40.

SNMP TRAP Notification

The library can be configured for SNMP TRAP receiver addresses which to send RAS subsystem change event notification and other library event as discussed in the *Basic SNMP Reference Guide for the Scalar i2000/ i6000 Library*.

Working With Tickets

Tickets are your primary troubleshooting tool when you experience problems with the library. A ticket provides details and reports about

the issue and library conditions at the time of the event. It also provides guidance on how to resolve the issue. If you are an administrator or a service representative, you can access the tickets through the LMC. This section explains how to display ticket lists, view ticket and report details, view repair pages, and resolve and close tickets.

Ticket Guidelines

To help you quickly troubleshoot an issue by using tickets, read the following guidelines.

What is the issue and its cause?

You became aware of a library issue because either the library sent an e-mail notification, an LMC system status button indicated a subsystem status of Warning, Degraded, or Failed, or a backup/archive software application indicated a problem. Tickets include details about the issue and library conditions at the time of the event. They also include reports, any history tickets that the library has created in the past for the same FRU, and a repair page that provides a detailed description of the issue and its possible causes. The repair page also provides corrective actions that you or a CSE can perform. To use a ticket to determine an issue and its cause, you can perform the following general steps:

1. Display a list of tickets (see Displaying Ticket Lists on page 44).
2. View the details for the appropriate ticket (see Viewing Ticket Details on page 49).
3. View the reports that are associated with this ticket (see Viewing Ticket Details Reports on page 54.
4. View the ticket's repair page (see Viewing Ticket Repair Pages on page 58).

Where did the issue occur in the library?

The **Status Group** field on the **Details** tab of the **Ticket Details** dialog box indicates the library subsystem that caused the ticket. For more information about the **Details** tab, see Viewing Ticket Details on page 49 The **FRU ID** field on the **Report** tab of the **Ticket Details** dialog box indicates the type of FRU that is affected, and the **FRU Instance** field indicates the specific FRU by its location in the library. For more

information about the **Report** tab, see Viewing Ticket Details Reports on page 54.

When did the issue first occur?

The **Posted** field on the **Details** tab of the **Ticket Details** dialog box indicates the date and time on which the library first reported the issue and created a ticket for it. For more information about the **Details** tab, see Viewing Ticket Details on page 49.

Has the issue occurred repeatedly?

The **Duplicates** field on the **Details** tab of the **Ticket Details** dialog box indicates how many times the library has reported the same issue while the ticket has been open. In addition, you can determine whether the same issue has occurred and been resolved in the past. The **FRU History List** area on the **Details** tab lists tickets that have been opened for the same FRU in the past, but have been resolved and are now in the Closed or Verified state. By selecting a history ticket and then clicking **Show**, you can investigate the ticket history of a particular FRU. For more information about the **Details** tab and viewing history tickets, see Viewing Ticket Details on page 49.

Does the issue involve drives or tapes?

You can determine if the issue involves a particular drive or tape by viewing tape alerts and generating tape alert reports.

Tape alerts are issued by a drive whenever there is a problem in the drive that relates to a tape cartridge. The problem can be with the drive or with the tape cartridge. You can view tape alerts on the Media Integrity Analysis tab of the Ticket Details dialog box for tickets in the drive group. For more information on the Media Integrity Analysis tab, see Viewing Tape Alerts and Generating Media Integrity Analysis Reports on page 59.

Tape alert reports enable you to cross-reference tape alerts for drives and tape cartridges over a specified period of time, in order to determine if the problem belongs to the drive or to a specific tape cartridge. You generate tape alert reports using the Report Criteria dialog box. You need an Advanced Reporting license in order to use view tape alerts reports. For more information on using the Report

Criteria dialog box, see Viewing Tape Alerts and Generating Media Integrity Analysis Reports on page 59.

Has the FRU been replaced before?

You can determine whether a specific FRU has been replaced in the past by examining the **FRU SN** field on the **Details** tab of the **Ticket Details** dialog box for the open ticket and the history tickets. Because the history tickets associated with an open ticket are for the same specific instance of a FRU, and because a FRU instance is identified by its location in the library, the FRU serial number, which is uniquely assigned to each FRU, will change if the unit has been replaced in the past. For more information about the **Details** tab and viewing history tickets, see Viewing Ticket Details on page 49.

How do I resolve the issue?

The repair page provides comprehensive, step-by-step procedures for resolving the issue. Both user and CSE procedures are provided. When the procedures require a CSE to perform them, contact technical support. For more information, see Viewing Ticket Repair Pages on page 58.

How can I know whether the issue is resolved?

Some issues require you to determine whether they are resolved and others the library will detect automatically.

- In some cases, the library can automatically detect that an issue is resolved (for example, an open door that is now shut). For these, the library automatically transitions the ticket to the Verified state.
- In other cases, the library cannot automatically detect that an issue is resolved (for example, a faulty tape cartridge). You must determine whether the issue is resolved by running a verification test or, if an applicable test does not exist, by following the repair page instructions. If you run a test and the results are all good, the library automatically transitions the ticket to the Verified state. If you cannot run a test, you should physically examine the FRU, and then manually transition the ticket to the Closed state after determining that the issue is resolved. After you close the ticket, the library transitions it to the Verified state if it is able to do so. For

more information, see Running Verification Tests to Determine Issue Resolution on page 73 and Closing Tickets on page 74.

The library reopens tickets that receive failed, degraded, or warning reports within 30 minutes of transitioning to the Closed or Verified state. If a Closed or Verified ticket remains free of failed, degraded, or warning reports for 30 minutes, the library locks them from transitioning back to the Open state. A failed, degraded, or warning report that is received beyond 30 minutes causes the library to open a new ticket.

What do I do if I cannot resolve the issue?

Contact Quantum technical support. See Getting More Information or Help on page xiii. Technical support personnel might ask you to send them an electronic copy of the ticket. For instructions, see Mailing, Saving, and Printing Ticket Information on page 71.

How do I view the number of tickets that occurred in a certain time range?

The Tickets Report lets you see how many tickets occurred in a particular time period. You can choose to group tickets by subsystem, module, or FRU, and the results can be presented as a rollup summary or as a trend so you can see if the number of issues is increasing or decreasing over time. Also, the report results can be presented in different chart formats, such as bar graphs or pie charts. For more information, see Generating the Tickets Report on page 75.

Displaying Ticket Lists

The LMC provides three ways to display ticket lists:

- By clicking a system status button that indicates a Warning, Degraded, or Failed state

  This option displays a list of open tickets for the associated subsystem. See Using System Status Buttons to Display Ticket Lists on page 45.

- By clicking **Tools** > **Tickets**

  This option displays the **Tickets** dialog box from which you can obtain a list of all tickets or a partial list of tickets according to

selection criteria. See Using the Tickets Command or the Tickets Button to Display Ticket Lists on page 47.

- By clicking the **Tickets** button on the toolbar

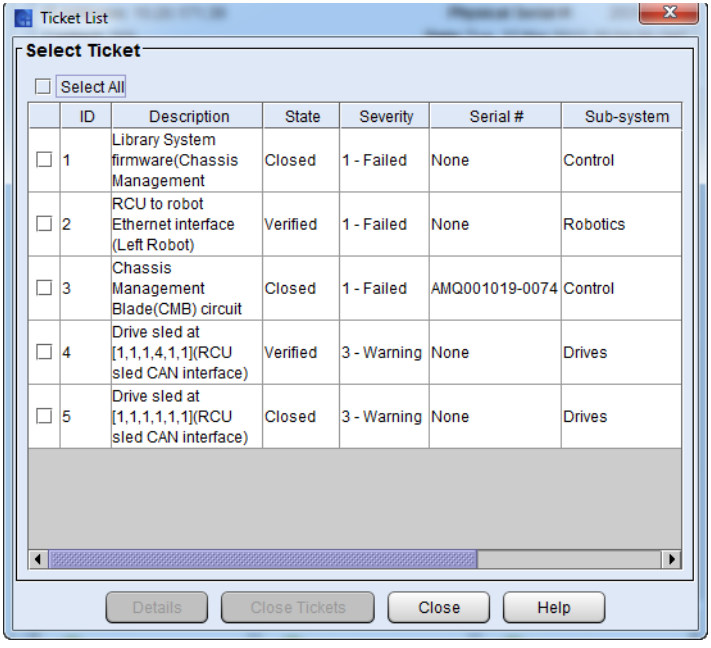
  This option displays the same **Tickets** dialog box as the **Tools** > **Tickets** command does. See Using the Tickets Command or the Tickets Button to Display Ticket Lists on page 47.

From the ticket list, you can select a ticket to view ticket details, associated reports, and a repair page.

Using System Status Buttons to Display Ticket Lists

To display a list of tickets by using a system status button, the button must indicate a Warning, Degraded, or Failed state. Clicking a system status button that indicates a Good state either displays a list of subsystem tickets that are in Closed or Verified states or informs you that no tickets exist for the subsystem.

1. Click the system status button that corresponds with the subsystem for which you want to display a list of open tickets. The **Ticket List** dialog box appears with a list of open tickets for the subsystem.



The following table describes the elements on the **Ticket List** dialog box.

Element	Description
In the **Select Ticket** area:	
Check Box	To close multiple tickets, select each ticket you want to close by clicking the check box.
ID	The library-assigned identifier for the ticket.
Description	A summary description of the ticket. The description identifies the FRU that caused the ticket and includes reason text that describes the cause of the ticket.
State	The current state of the ticket. Possible states are: **Open** — indicates that an issue, whether problem or warning condition, has occurred in the library that requires attention **Closed** — indicates that a user has closed the issue **Verified** — indicates that the library has successful operational results or positive data that verifies that the problem is resolved
Severity	The severity level of the ticket. Possible levels are: • 1 (Failed) • 2 (Degraded) • 3 (Warning) • 5 (Good)
Serial #	The serial number that the manufacturer assigns to the particular FRU.
Sub-system	The subsystem that caused the ticket. Possible subsystems are: • Connectivity • Drives • Control • Power • Cooling • Robotics
Posted Date	The date and time on which the library created the ticket.

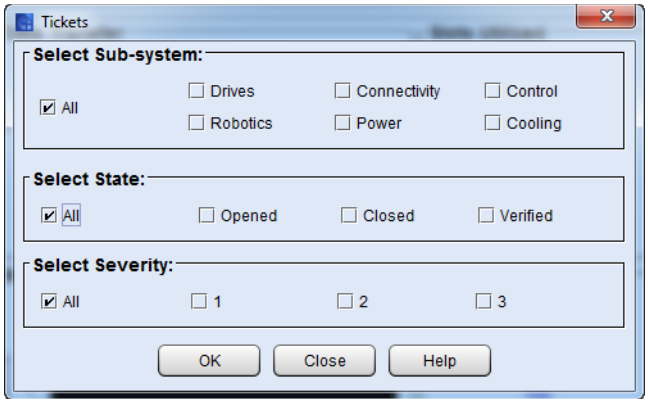
The **Details** button displays the **Ticket Details** dialog box. For more information, see Viewing Ticket Details on page 49.

2 By default, the ticket list is sorted by ticket ID in ascending order with the oldest ticket at the top and the newest one at the bottom. To change the sorting (for example, by state or severity), click the column heading by which you want the tickets sorted. Repeatedly clicking a column heading toggles between ascending and descending order.

Using the Tickets Command or the Tickets Button to Display Ticket Lists

1 Make sure that you are viewing the physical library. From the **View** menu, click the name of the physical library.

2 Click **Tools** > **Tickets** or click the **Tickets** button on the toolbar. The **Tickets** dialog box appears.



The **Tickets** dialog box enables you to specify the kinds of tickets that will appear in the ticket list. For example, you can do the following:

- To display all tickets in the library, select **All** for state, severity, and subsystem.
- To display all open tickets with a severity level 2 status for the drives and control subsystems, select **Opened** for state, **2** for severity, and **Drives** and **Control** for subsystem.
- To display all tickets that users have manually closed for the robotics subsystem, select **Closed** for state, **All** for severity, and **Robotics** for subsystem.

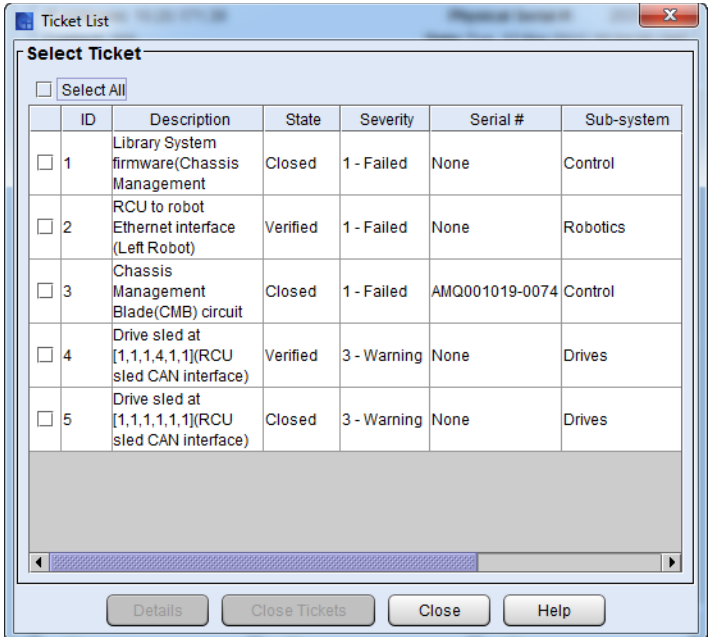
- To display all tickets that the library has automatically determined as having been resolved, select **Verified** for state, **All** for severity, and **All** for subsystem.

  If you select a combination that does not produce a ticket list, a **No Tickets Found** error message appears.

  By default, this dialog box is set to **Opened** for state, **All** for severity level, and **All** for subsystem.

Note: Tickets that the library has automatically verified and closed are in the Verified state. Tickets that users have manually closed are in the Closed state.

3 Select the appropriate check boxes in the **Select State**, **Select Severity**, and **Select Sub-system** areas, and then click **OK**. The **Ticket List** dialog box appears.



For descriptions of elements on the **Ticket List** dialog box, see Using System Status Buttons to Display Ticket Lists on page 45.

4 By default, the ticket list is sorted by ticket ID in ascending order with the oldest ticket at the top and the newest one at the bottom. To change the sorting (for example, by state or severity), click the

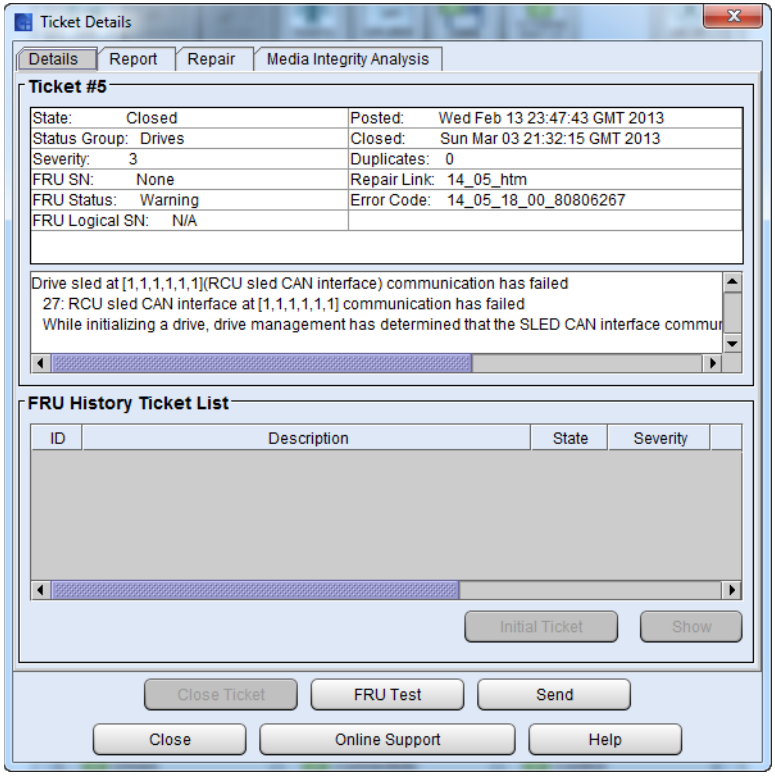
column heading by which you want the tickets sorted. Repeatedly clicking a column heading toggles between ascending and descending order.

Viewing Ticket Details

Tickets provide detailed information about the ticket itself, the reports that are associated with it, and a repair page that gives guidance for resolving the issue. These tickets provide important information about library conditions from which the issue emerged and helpful information for resolving it.

To display the detailed information for a particular ticket, perform the following steps:

1. On the **Ticket List** dialog box in the **Select Ticket** area, click the appropriate ticket row to highlight it.
2. Click **Details**. The **Ticket Details** dialog box appears with the **Details** tab displayed.



The **Ticket #** area of the **Ticket Details** dialog box displays detailed information about the ticket. The **FRU History Ticket List** area lists all tickets that were ever opened in the past and that see the same specific FRU (based on the FRU's location in the library) as the one reported by this ticket.

Table 4 on page 50 describes the elements on the **Details** tab.

Table 4 Details tab

Element	Description
In the **Ticket #** area:	
State	The current state of the ticket. Possible states are: **Open** — indicates that an issue, whether problem or warning condition, has occurred in the library that requires attention **Closed** — indicates that a user has closed the issue **Verified** — indicates that the library has successful operational results or positive data that verifies that the problem is resolved
Posted	The date and time on which the library created the ticket.
Status Group	The subsystem that caused the ticket. Possible subsystems are: • Connectivity • Drives • Control • Power • Media • Robotics
Closed	If the ticket is closed, the date and time on which it was closed.
Severity	The severity level that is associated with the status group (subsystem). Possible levels are: • 1 (Failed) • 2 (Degraded) • 3 (Warning) • 5 (Good)

Element	Description
Duplicates	The number of times that the library has reopened the ticket. If a ticket is in the Closed or Verified state and the identical problem occurs again within 30 minutes, the library reopens the ticket and increments the ticket's duplicate count. If the library has not reopened the ticket, the value is zero (0). Tickets that are in the Closed or Verified state for more than 30 minutes cannot be reopened. In this case, if the identical problem occurs again, the library creates a new ticket.
FRU SN	The serial number of the particular FRU.
Repair Link	The name of the repair page that is associated with the ticket.
FRU Status	The status of the FRU. Possible statuses are: • Failed • Degraded • Warning • Good
Error Code	A number that is associated with a particular issue that caused the ticket report. Because more than one issue can cause a report, an error code provides another level of detail to what the report provides. The error code maps to a portion of library firmware code, which a trained analyst can examine to determine the root cause of an issue. If the ticket is in the Closed or Verified state, this field is set to N/A. This information is for technical support use only.
FRU Logical SN	The logical serial number that the library assigns to a drive in a specific location. This is not the serial number of the particular FRU (see **FRU SN** in this table). If a drive is replaced by another drive in the same library location, the logical serial number remains the same. From the host's perspective, the replacement drive is the same as the original one. This field appears for all drive-related tickets only. If the logical serial number addressing feature is disabled for the library, **Disabled** appears in this field.
Description area	A summary description of report information that is associated with the ticket. It includes reason text that describes the cause of the ticket.
In the **FRU History Ticket List** area:	
ID	The library-assigned identifier for the history ticket.

Element	Description
Description	A summary description of the history ticket. The description identifies the FRU that caused the ticket and includes reason text that describes the cause of the ticket. All tickets that appear on the **Details** tab, including the ones in the **FRU History Ticket List** area and the **Ticket #** area, see the same specific FRU.
State	The current state of the history ticket. All history tickets are in the Closed or Verified state.
Severity	The historical ticket's current severity level.
Serial #	The serial number of the particular FRU.
Sub-system	The subsystem that caused the ticket. Possible subsystems are: • Connectivity • Drives • Control • Power • Media • Robotics
Posted Date	The date and time on which the library created the ticket.

From the **Ticket Details** dialog box, you can perform the following tasks:

- Display detailed information for a history ticket by using the **Show** button, and then redisplay the original ticket details using the **Initial Ticket** button (see Viewing History Ticket Details on page 53)
- Connect to online service and support resources by clicking **Online Support**. Online service and support resources include free, secure access to KnowledgeBase articles and the Online Service Request tool. (If clicking **Online Support** does not connect you to the online service and support website, try disabling your Web browser's pop-up blocker.)
- Mail, save, or print ticket information by using the **Send** button (see Mailing, Saving, and Printing Ticket Information on page 71)

- Determine whether the issue is resolved by using the **FRU Test** button. **FRU Test** is available only if the ticket's FRU has an applicable verification test that you can run. (FRUs that belong to the Accessor, Picker, Drive, I/E Assembly, or Bar Code Label categories have applicable verification tests.) When you click **FRU Test**, the **Verification Tests** dialog box appears with the appropriate verification test already selected and ready to start. If you run a verification test and the results are all good, the library automatically transitions the ticket to the Verified state. For more information, see Working With Verification Tests on page 608.

  Note: If the library does not have a verification test for the FRU, after you resolve the issue, you must manually transition the ticket to the Closed state by using the **Close Ticket** button. After you close the ticket, the library transitions it to the Verified state if it is able to do so. For more information about manually closing a ticket, see Closing Tickets on page 74.

- Display report information (see Viewing Ticket Details Reports on page 54)
- Display the repair page (see Viewing Ticket Repair Pages on page 58)

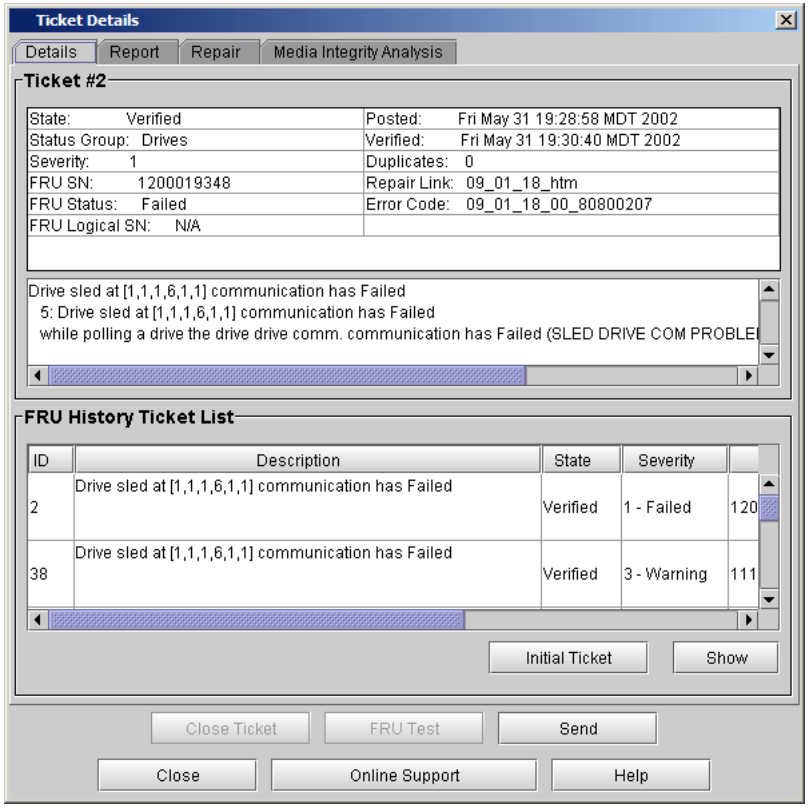
Viewing History Ticket Details

To display the detailed information for a particular history ticket, perform the following steps:

1. On the **Ticket List** dialog box in the **FRU History Ticket List** area of the **Details** tab, click the appropriate ticket row to highlight it and click **Show**.

   The history ticket details appear in the **Ticket #** area. However, the list of tickets in the **FRU History Ticket List** remains the same as what the initial ticket displayed. This list does not change. The **Report** and **Repair** tabs show information that is specific to the history ticket, but the **Close Ticket** and **FRU Test** buttons at the

bottom of the **Ticket Details** dialog box are grayed out because the history ticket is in the Closed or Verified state already.

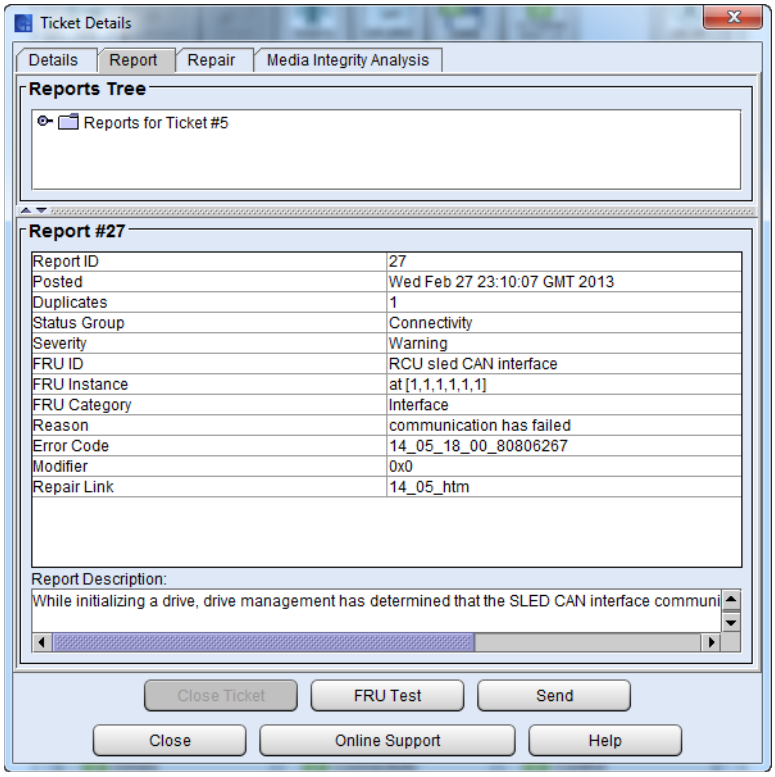


2 To return to the non-history ticket that appeared initially, click **Initial Ticket**.

Viewing Ticket Details Reports

The library creates a key report for each issue that occurs. As updates to the issue occur, the library creates subordinate reports that it associates with the key report. Typically, you should examine the key report because it represents the earliest time at which the ticket reached its highest severity level. It often isolates the most significant problem.

To display all report information that is associated with a ticket, click the **Report** tab on the **Ticket Details** dialog box.



By default, the **Report #** area displays report details for either the key report or, if subordinate reports exist, the most recent subordinate report.

Table 5 on page 56 describes the elements on the **Report** tab.

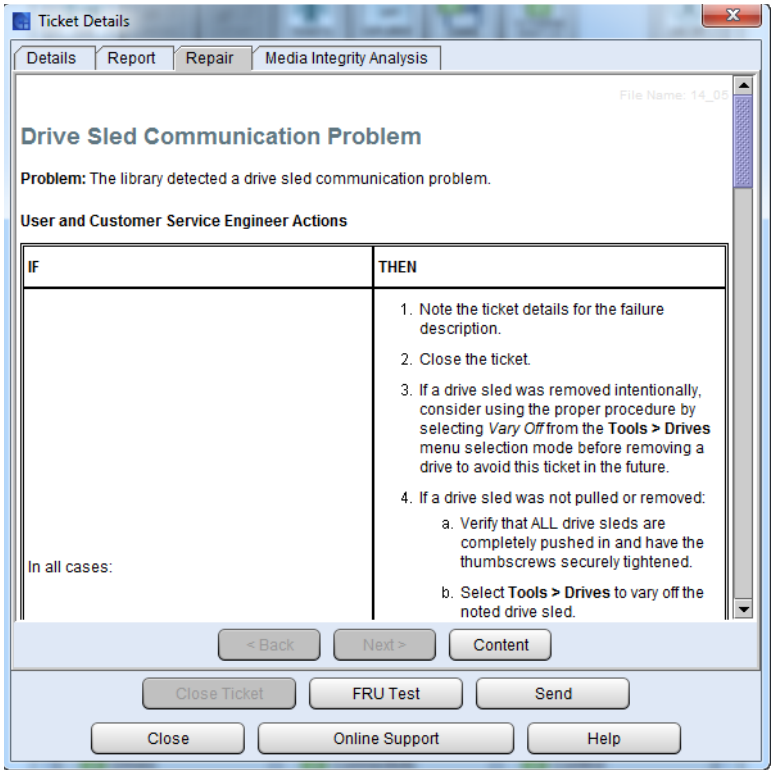
Table 5 Report tab

Element	Description
In the **Reports Tree** area:	
Report tree area	Provides a hierarchy of report information that is associated with the ticket. Descriptions includes reason text that describes the cause of the report. Initially, only the highest level of the report tree appears. Clicking this level (**Reports for Ticket #**) reveals one or more second-level reports, and clicking a second-level report reveals one or more third-level reports. Second-level reports function essentially as containers of third-level reports. A ticket in the Open state has one or more third-level reports, including one key report. The key report represents the earliest time at which the ticket reached its highest severity level. It often isolates the most significant problem. A ticket in the Closed or Verified state does not have a key report.
In the **Report #** area:	
Report ID	The library-assigned identifier for the report.
Posted	The date and time on which the library created the report.
Duplicates	For open tickets only, the number of times that the library created the same report. If the identical issue occurs while the ticket remains open, the library creates an identical report and increments the report's duplicate count. If the library has not created duplicate reports, the value is zero (0).
Status Group	The subsystem that caused the ticket. Possible subsystems are: • Connectivity • Drives • Control • Power • Media • Robotics

Element	Description
Severity	The severity level that is associated with the status group (subsystem). Possible levels are: • Failed • Degraded • Warning • Good
FRU ID	The identifier for the FRU.
FRU Instance	In libraries with multiple FRUs of the same kind, the specific FRU that caused the report. This field usually identifies a particular FRU by its location in the library (for example, [1,1,1,8,1,1] for a drive sled). If the library has only one instance of the FRU, this field is blank.
FRU Category	The category to which the FRU belongs.
Reason	A brief explanation of why the FRU caused the report. Reasons describe the causes of issues.
Error Code	A number that is associated with a particular issue that caused the ticket report. Because more than one issue can cause a report, an error code provides another level of detail to what the report provides. The error code maps to a portion of library firmware code, which a trained analyst can examine to determine the root cause of an issue. This information is for technical support use only.
Modifier	A numerical qualifier, in hexadecimal format, that provides context for an error condition. A modifier adds another level of detail to what the error code provides. If a modifier does not exist for the error condition, this field is set to "0x0". This information is for technical support use only.
Repair Link	The name of the repair page that is associated with the report.
Report Description	A summary description of the report.

Viewing Ticket Repair Pages

Repair pages provide problem descriptions and corrective actions that you or a CSE can perform. To display the repair page that is associated with a ticket, click the **Repair** tab on the **Ticket Details** dialog box.



The repair page provides the following information:

- The title at the top of the repair page is a brief description of the issue.
- The **Problem** section describes the issue in more detail.
- The **User and Customer Service Engineer Actions** section provides corrective actions that the user or the CSE can perform.
- The **Customer Service Engineer Actions** section provides additional corrective actions that the CSE can perform. If you are a user, do not perform these steps. Contact technical support for assistance.

Note: If you are a CSE, see the *Scalar i2000/i6000 Maintenance Guide* for detailed maintenance action plans, and removal and replacement procedures.

- The **Technical Support Information** section provides a comprehensive list of FRUs that could be involved.
- Text on the repair pages can include links to specific Online Help pages, which appear in place of the repair page when you click them. Navigation buttons near the top of the **Repair** tab enable you to access Online Help pages as follows:
  - The **Back** button returns you to the previously viewed page (either a previously viewed Online Help page or the repair page).
  - The **Next** button returns you to the page that you were viewing before you clicked the **Back** button.
  - The **Content** button displays a table of contents for the Online Help system.

Viewing Tape Alerts and Generating Media Integrity Analysis Reports

A drive issues a tape alert whenever there is a problem encountered by the drive. The problem can be with the drive, library, or with the tape cartridge. You can view tape alerts on the Media Integrity Analysis tab of the Ticket Details dialog box. You can also access Media Integrity Analysis via Reports on the LMC menu. See Viewing Tape Alerts on page 60 or Generating Media Integrity Analysis Reports on page 62.

Note: The **Media Integrity Analysis** feature (including viewing tape alerts) requires an Advanced Reporting license key to use. For more information, see Enabling Licenses on page 115.

You can use these reports to cross-reference tape alerts for drives and tape cartridges over a specified period of time, in order to determine if the problem belongs to the drive or to a specific tape cartridge. Typically, tape alerts point to a drive problem if a specific drive exhibits tape alerts against multiple pieces of media. Conversely, tape alerts point to a media problem if a specific piece of media exhibits tape alerts against multiple drives. See Generating Media Integrity Analysis Reports on page 62.

Viewing Tape Alerts

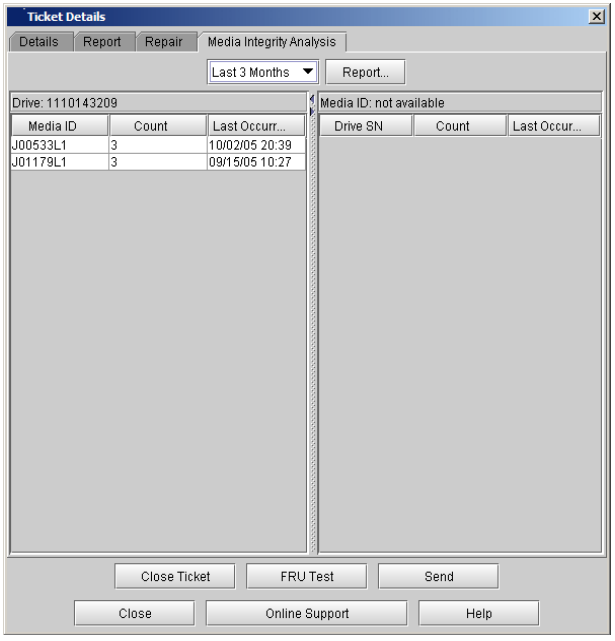
To view tape alerts:

1 Click the **Media Integrity Analysis** tab on the **Ticket Details** dialog box.

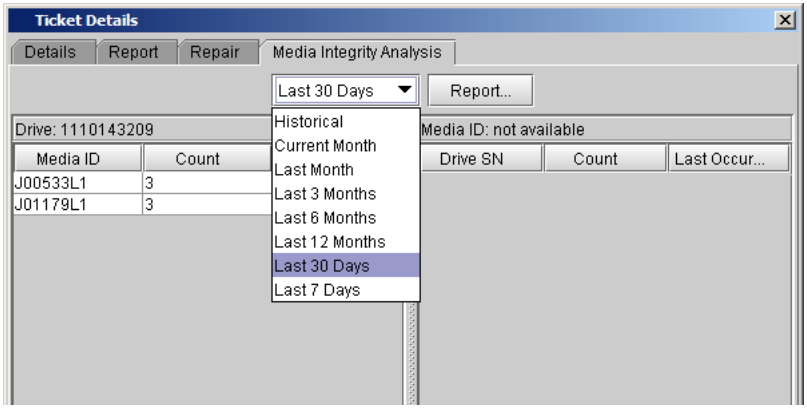
Note: The **Media Integrity Analysis** tab only appears on the **Ticket Details** dialog box for drive subsystem tickets.

The **Media Integrity Analysis** view appears, displaying one of the following:

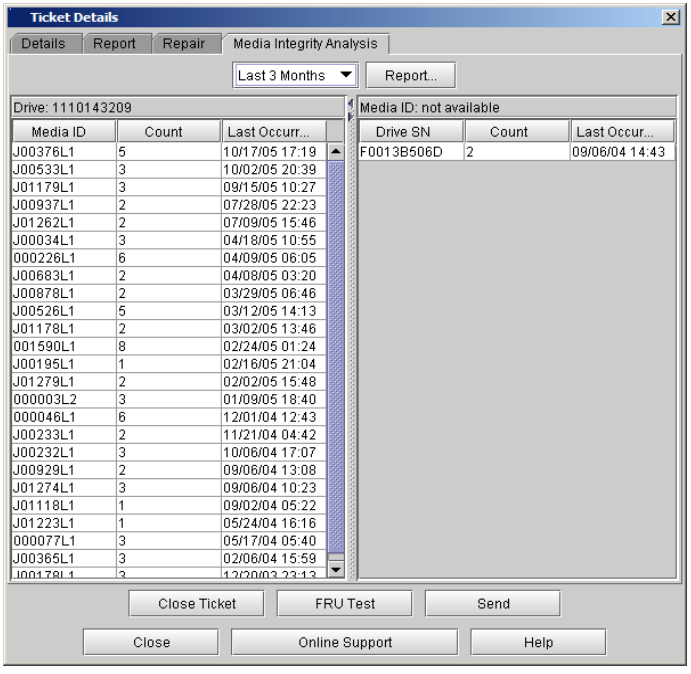
- If the ticket contains a valid drive serial number and the drive is present in the library, the view displays a list of drive SNs in the left pane and media IDs in the right pane for which tape alerts exist for the specified date range.
- If the drive serial number given in the ticket is invalid or if the drive is not present in the library, the view displays the message, "Invalid serial number or drive is no longer present."



2 To change the date range, click the down arrow next to the date box and select the range you want.



The **Media Integrity Analysis** tab displays the tape alert information available for the selected range.



3 To sort the lists, click the column heading you want to sort.

4 To generate a report, click **Report**. The **Report Criteria** dialog box appears.

Go to Generating Media Integrity Analysis Reports on page 62.

Generating Media Integrity Analysis Reports

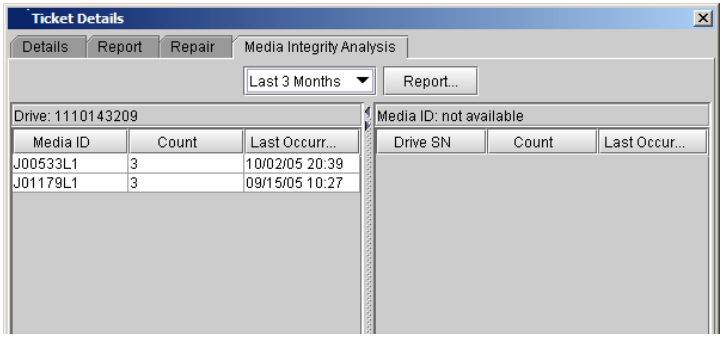
Note: The **Media Integrity Analysis** feature requires an Advanced Reporting license key to use. For more information, see Enabling Licenses on page 115.

This function allows you to generate reports using the criteria described in Table 7 on page 77.

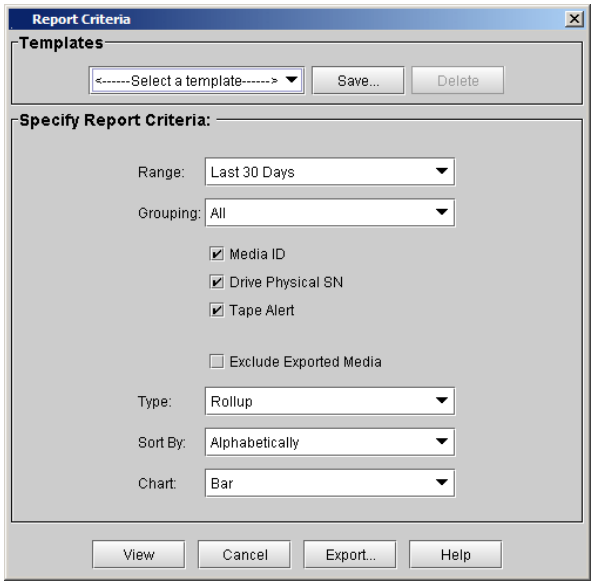
To generate **Media Integrity Analysis** reports:

1 Do one of the following:

- On the **Media Integrity Analysis** tab of the **Ticket Details** dialog box, click **Report**.



- On the menu bar, click **Tools > Reports > Media > Integrity Analysis**. The **Report Criteria** dialog box appears.



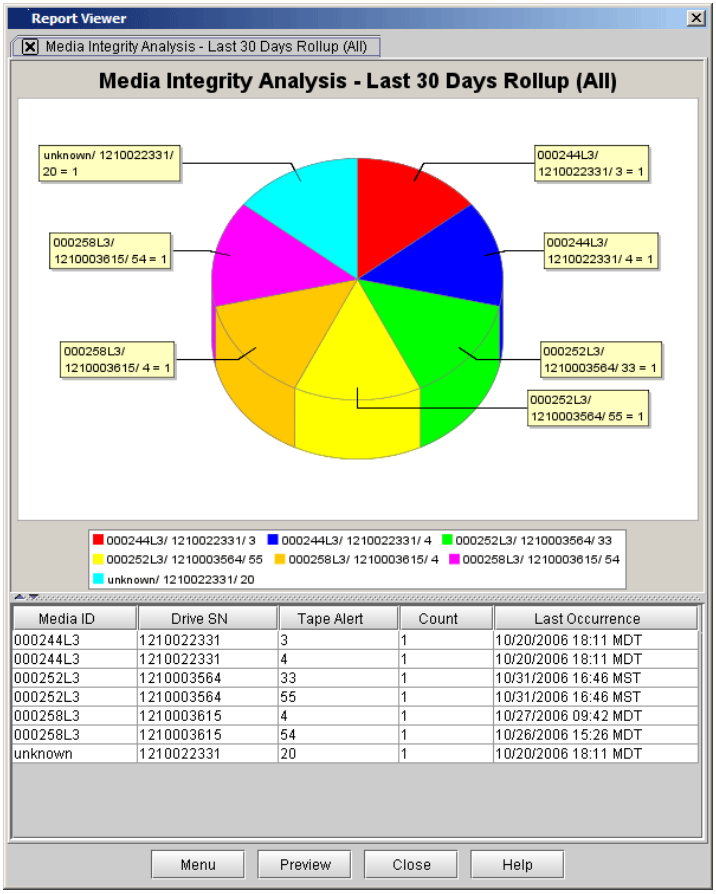
2 To view a report, select the report criteria described in Table 6 and click **View.**

Table 6 Report Criteria

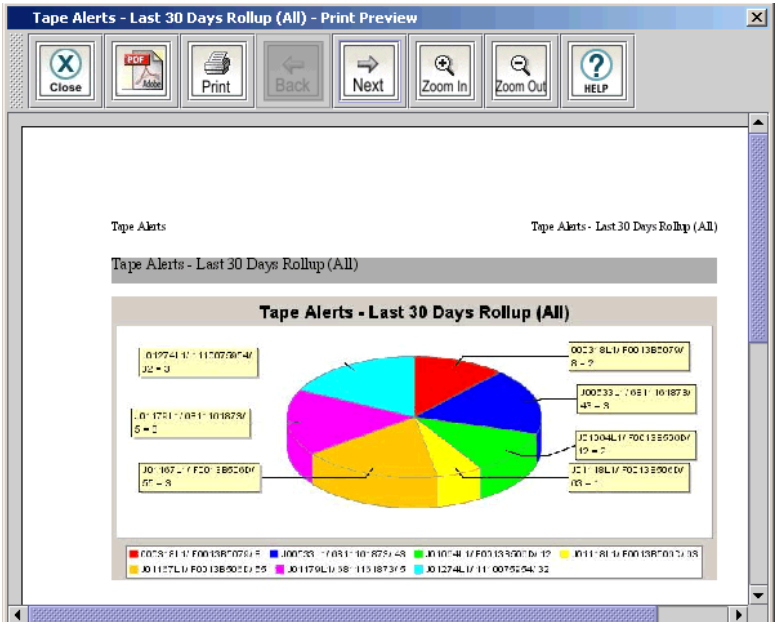
Element	Description
Range	Specifies the range of time to cover in the report. Choices include: • Historical • Current Month • Last Month • Last 3 Months • Last 6 Months • Last 12 Months • Last 30 Days (default) • Last 7 Days

Element	Description
Grouping	Determines which drive or tape cartridge to base the report. Choices include: • All (default) • Selected Drive by Physical SN—displays the **Choose Drive** dialog box • Selected Media by Media ID—displays the **Specify Media** dialog box
Media ID, Drive Physical SN, Tape Alert check boxes	Selected in any combination to determine which values are included in the report. (All=default)
Type	Type of report. Choices include: • **Rollup** — displays the values based on which of the above check boxes, **Media ID**, **Drive Physical SN**, and/or **Tape Alert**, that you have selected (default) • **Trend** — shows the occurrence of tape alerts over time
Sort By	How the report is sorted. Choices include: • Alphabetically (default) • Count • Last Occurrence
Chart	Determines the type of chart. Choices include: • Area • Bar • Bar 3D • Line • Stacked Area • Stacked Bar • Stacked Bar 3D • Pie • Pie 3D (default)

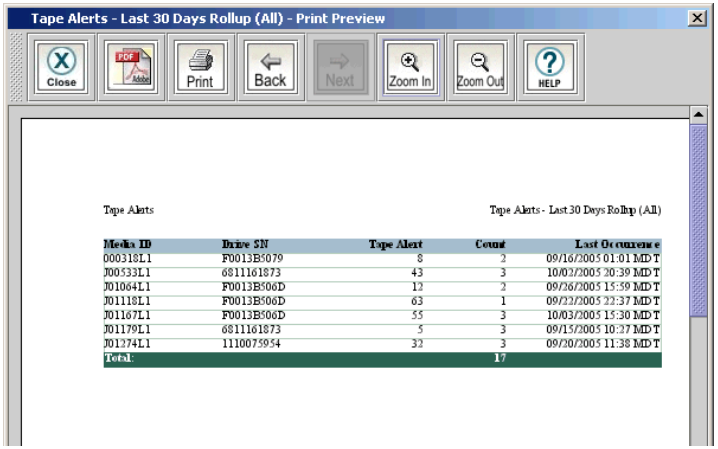
The **Report Viewer** dialog box appears. The content and appearance of the report varies depending on the selected criteria.



3 Click **Preview**. The report appears in the **Media Integrity Analysis Print Preview** window.



4 To navigate through the report, click the **Next** or **Back** icons on the toolbar. The next or previous page appears.



5 To increase or decrease the magnification of the report, click the **Zoom In** or **Zoom Out** buttons.

6 In the report viewer, you can perform the following tasks:

- To print the report, click the Print icon on the toolbar. Refer to Printing Media Integrity Analysis Reports on page 67.
- To save the report as an Adobe Portable Document Format (PDF) file, click the Adobe PDF icon on the toolbar. Refer to. Creating Report PDFs on page 67.
- To export the report, refer to Exporting a Report to an E-mail or a Text File on page 80.
- To save the report template, refer to Saving a Report Template on page 80.

Printing Media Integrity Analysis Reports

To print a tape alert report:

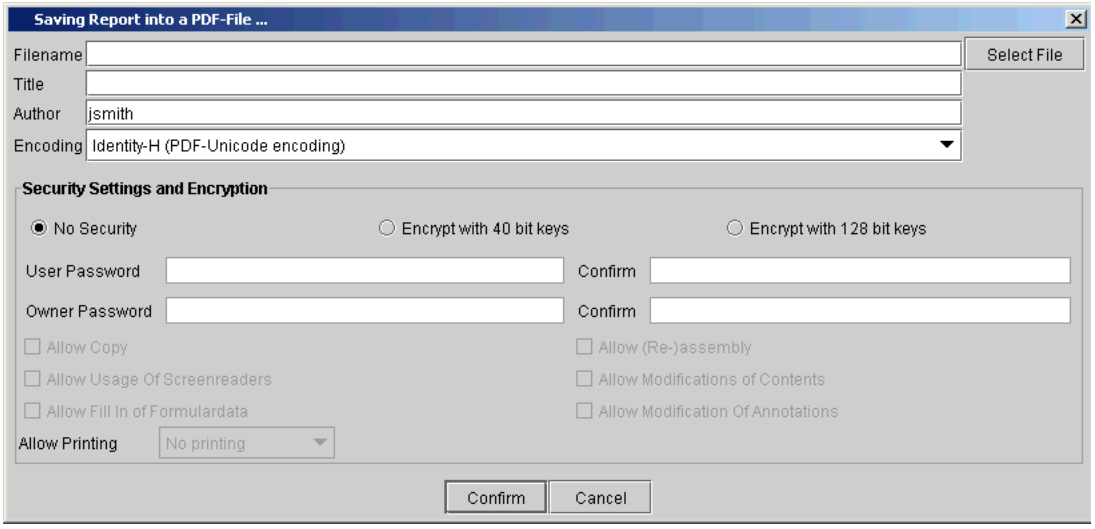
1. In the **Media Integrity Analysis Reports Print Preview** window, click the **Print** button. The local system's print dialog box appears.
2. Follow the prompts.

Note: The **Print** function is not available on the touch screen.

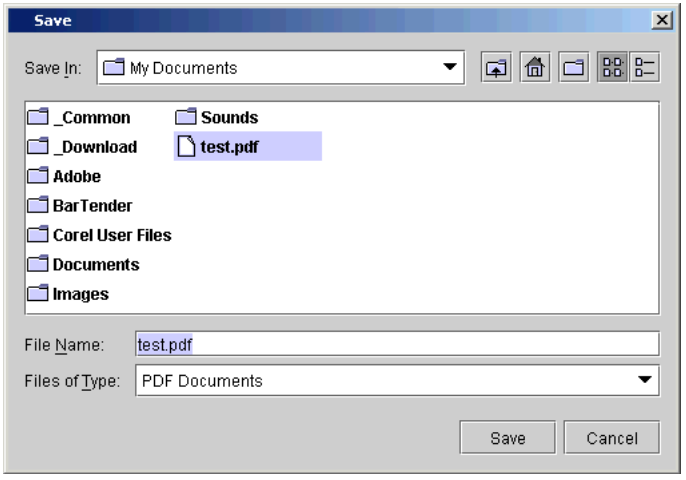
Creating Report PDFs

To create a PDF of a report:

1. In the **Media Integrity Analysis Print Preview** window, click the **PDF** button. The **Saving Report into a PDF-File** dialog box appears.



2 Click **Select File**. The **Save** dialog box appears.



3 In the **Save** dialog box, browse to the location where you want to save the file, type the filename, and click **Save**.

4 In the **Saving Report into a PDF-File** dialog box, enter the settings you want and click **Confirm**. The PDF file is saved in the specified location.

Note: The PDF function is not available on the touch screen.

Exporting Media Integrity Analysis Reports

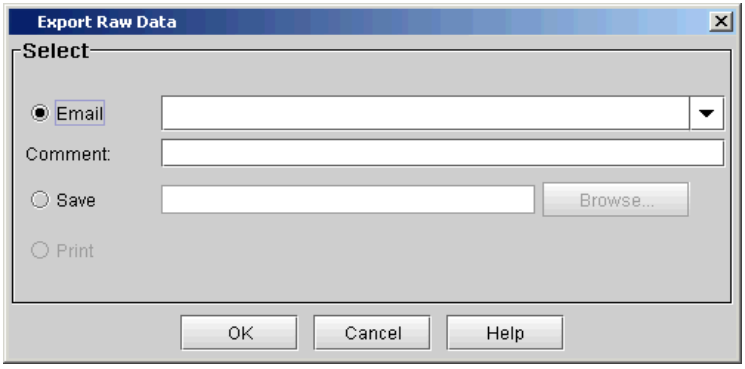
You can export the report data as a comma-delimited text (.CSV) file that you can open in Microsoft Excel. This function allows you to:

- E-mail the file as an attachment
- Save the file to a folder

To export report data:

In the **Report Criteria** dialog box, select the range and grouping you want to export and click **Export**. The **Export Raw Data** dialog box appears.

Note: The only criteria that the export function uses are range and grouping.



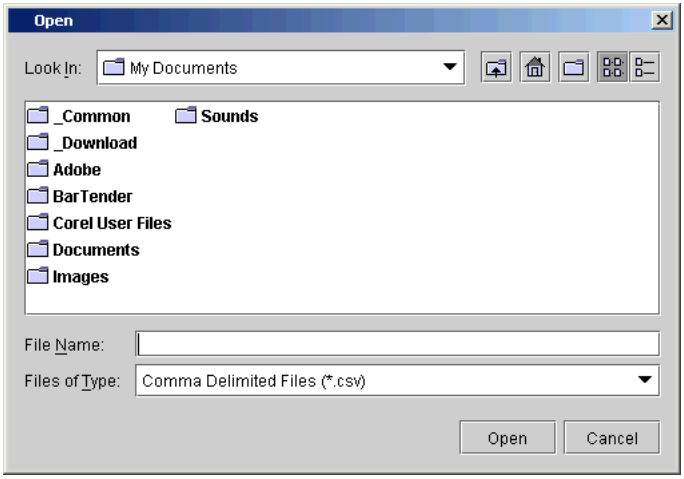
To e-mail the data:

1. Select **Email**.
2. Type the e-mail address or click the down arrow and select the e-mail address from the drop-down list.
3. If you want, type a comment.
4. Click **OK**.

To save the data to a folder:

1. Select **Save**.
2. Type the file name in the text box.

3 Click **Browse**. The **Open** dialog box appears.



4 In the **Open** dialog box, browse to the location where you want to save the file, type the file name, and click **Open**.

5 Click **OK**.

Note: The **Save** function is not available on the touch screen.

Saving a Report Template

If you frequently generate the Media Integrity Analysis Report with the same set of report criteria, save the criteria as a template. Loading the template recalls the saved report criteria and lets you quickly generate a report based on the saved criteria.

1 On the menu bar, click **Tools > Reports > Media Integrity Analysis**. The **Report Criteria** dialog box appears.

2 Under **Specify Report Criteria**, click criteria options in the lists to customize the content and appearance of the Media Integrity Analysis Report.

Table 6 on page 63 summarizes the available report criteria options.

3 Under **Templates**, click **Save**.

4 Type a name for the template, and then click **OK**. The template appears in the list under **Templates**.

To load the saved report criteria at a later time, click the template in the list, and then click **View** to generate the report.

5 To close the **Report Criteria** dialog box, click **Cancel**.

Mailing, Saving, and Printing Ticket Information

The **Send** button on the **Ticket Details** dialog box enables you to send detailed ticket information, including all report details, to e-mail addresses. If you are accessing the LMC from a remote client, **Send** also enables you to save the information to a file or print it.

Note: You can mail, save, or print ticket information from a remote client. However, you cannot save or print the information from the library's touch screen.

Ticket information that a user sends by using the **Send** button is essentially the same as the information that the library automatically provides in e-mail notifications (see E-mail Notifications on page 39). The only differences are that the subject line states "Library RAS Information" and the body of the message does not have a "REASON FOR AUTOMATED E-MAIL" section, but it has a "REPAIR AND TROUBLESHOOTING INSTRUCTIONS ATTACHED" section.

The message body also includes the following information, which provides details about the ticket and library conditions at the time of the event:

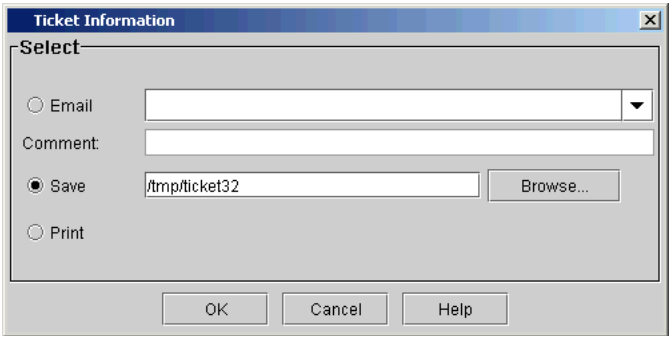
- Ticket summary
- Ticket details, including status information
- Firmware versions, including MCB, RCU, CMB, and drive bricks
- Physical library configuration
- Library states, such as physical library online or offline, partitions online or offline, or robotics varied on or varied off
- Time stamps of recent activity
- Report summary
- Report details for the ticket

  The RAS repair page attachment is in HTML format.

Note: Before you perform the following procedure, you must make sure that e-mail is appropriately configured in the LMC so that the library can send ticket details to the recipient. See Configuring E-mail on page 177.

To mail, save, or print information for a particular ticket, perform the following steps:

1. Make sure that the **Ticket Details** dialog box displays information for the ticket that you want to send. See Displaying Ticket Lists on page 44 and Viewing Ticket Details on page 49.
2. Click **Send**. The **Ticket Information** dialog box appears.



3. Perform one of the following tasks:
   - To indicate that you want to send the information as an e-mail message to a recipient, select **Email**, and then either type an e-mail address in the **Email** text box or select an existing address from the drop-down list. You can type a comment in the **Comment** text box to send with the information.
   - To indicate that you want to save the information, select **Save**, and then either type in the **Save** text box a path and a file name to which you want the information saved or click **Browse** to specify a location and a file name.

     Note: The **Save** option is available to remote client users only. It appears grayed out on the touch screen.

   - To indicate that you want to send the information to a printer, select **Print**.

Note: The **Print** option is available to remote client users only. It appears grayed out on the touch screen.

4 To send, click **OK**.

Running Verification Tests to Determine Issue Resolution

A ticket is always generated against a particular FRU when the library detects an issue. Therefore, the library provides FRU tests that you can run to determine whether the conditions that caused the ticket have been resolved. Running the FRU tests is an important part of ensuring that the system is working properly.

The library can detect issues under the following contexts:

- When the library polls at regular intervals, or
- When a host or user commands the library to perform an operation (such as occurs with GUI commands, host inventory, and host move media)

FRU tests are designed to help resolve issues under the second context.

During FRU testing, the library creates operational scenarios to evaluate the functionality of a FRU. FRU tests attempt to evaluate as many aspects of the FRU as possible, but they might not fully recreate the conditions that caused the original ticket. The library cannot recreate all conditions and, therefore, the library does not provide tests for some FRUs.

The instructions on the ticket's repair page direct you to run a FRU test if an applicable one exists. If you run the test and the results are all good, the library automatically transitions the ticket to the Verified state.

Note: If you cannot run a test, make sure that you complete the repair page instructions and, if needed, physically examine the FRU. After you determine that the issue is resolved, manually transition the ticket to the Closed state. See Closing Tickets on page 74. After you close the ticket, the library transitions the ticket to the Verified state if it is able to do so.

You can access the tests in two ways:

- On the main LMC display, click **Tools > Verification Tests**. The **Verification Tests** dialog box appears. From this dialog box, you can choose from a variety of verification tests, including the FRU tests.

- On the **Ticket Details** dialog box, click **FRU Test**.

  Note: The **FRU Test** button is available only if the ticket's FRU has an applicable verification test that you can run.

  The **Verification Tests** dialog box appears with the appropriate test already selected and ready to start.

For details about the verification tests and how to run them, see Working With Verification Tests on page 608.

Closing Tickets

Manually close a ticket if all of the following conditions are true:

- You have completed the repair page instructions to resolve the issue (for example, replaced a FRU).
- You have physically examined the FRU to make sure that the issue is resolved.
- The **FRU Test** button on the **Ticket Details** dialog box is not available. This means that an applicable verification test does not exist.

  Note: If the **FRU Test** button is available for a ticket, you should use it to access and run the verification test. You should not manually close it. The verification test determines whether the issue is resolved, and the library automatically transitions the ticket to the Verified state if the test passes without problems. See Running Verification Tests to Determine Issue Resolution on page 73.

- The issue has been resolved, but the ticket remains in an Open state (for example, when defective media has been replaced in the library).

You should manually transition a ticket to the **Closed** state after performing the resolution steps and making sure the issue is resolved.

Closing Individual Tickets

To transition a ticket to the **Closed** state, perform the following steps:

1 Make sure that the **Ticket Details** dialog box displays information for the open ticket that you want to close. See Displaying Ticket Lists on page 44 and Viewing Ticket Details on page 49.

2 Click **Close Ticket**. The ticket's state changes to **Closed**. If the library is able to do so, it automatically transitions the closed ticket to the Verified state.

Note: If the identical issue occurs again within 30 minutes after the ticket transitions to the Closed or Verified state, the library reopens the ticket and increments the ticket's duplicate count.

Tickets that are in the Closed or Verified state for more than 30 minutes cannot be reopened. In this case, if the identical problem occurs again, the library creates a new ticket.

Closing Multiple Tickets

You can use this method when you have many tickets relating to the same issue, for example, when you have many drives in a library or many tape alerts.

To transition multiple tickets to the **Closed** state, do the following:

1 On the **Ticket List** dialog box, select each ticket you want to close by clicking the check box.

See Displaying Ticket Lists on page 44 and Viewing Ticket Details on page 49.

2 Click **Close Tickets**.

3 In the **Attention** message box, click **Yes** to confirm that you want to close multiple tickets. The tickets' state changes to **Closed**. If the library is able to do so, it automatically transitions the closed tickets to the Verified state.

Generating the Tickets Report

The Tickets Report lets you see how many tickets occurred in a particular time period. You can choose to group tickets by subsystem, module, or FRU, and the results can be presented as a rollup summary or as a trend so you can see if the number of issues is increasing or decreasing over

time. Also, the report results can be presented in different chart formats, such as bar graphs or pie charts.

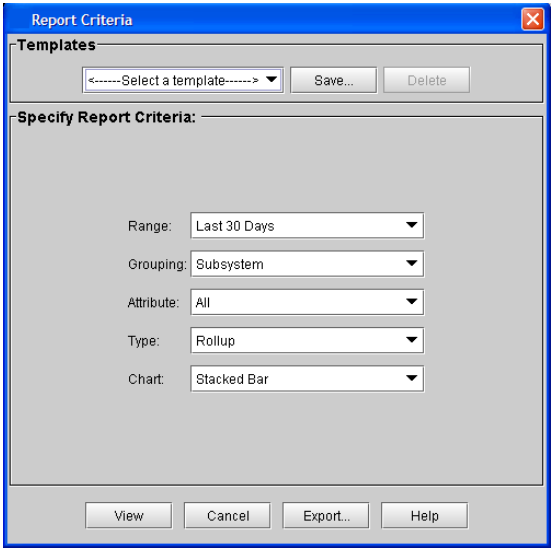
After generating a report, you can print it or save it as a PDF file. In addition, you can save a set of report criteria as a template for reports you frequently generate.

Specifying Tickets Report Criteria

To generate the Tickets Report, first specify the report criteria, and then view the report.

1 Log on as an administrator.

2 On the menu bar, click **Tools** > **Reports** > **Tickets**. The **Report Criteria** dialog box appears.



3 Under **Specify Report Criteria**, click criteria options in the lists to customize the content and appearance of the **Tickets Report**.

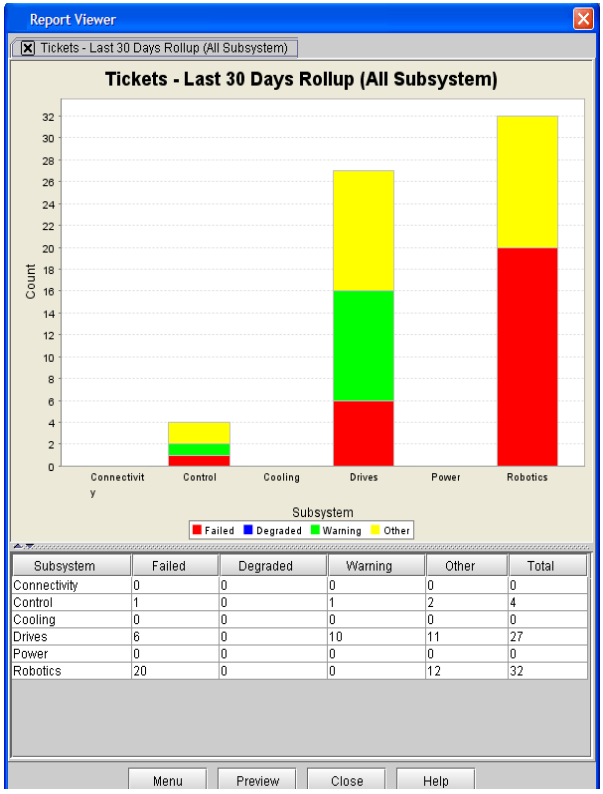
Table 7 summarizes the available report criteria options.

Table 7 Tickets Report Criteria Options

Criteria	Description
Range	Specifies the range of time to cover in the report. Choices include: • Historical • Current Month • Last Month • Last 3 Months • Last 6 Months • Last 12 Months • Last 30 Days (default) • Last 7 Days
Grouping	Determines how tickets are grouped in the report. Choices include: • Subsystem (default)—tickets are grouped according to subsystem • FRU Category—tickets are grouped according to FRU category • FRU Id—tickets are grouped according to FRU ID • Serial Number—tickets are grouped according to module serial number • Selected Drive by Physical SN—tickets are grouped according to drive serial number (displays the **Choose Drive** dialog box)
Attribute	Determines how tickets are identified in the report. Choices include: • All (default)—tickets are separated according to attribute (Failed, Degraded, Warning, or Other) • Total—tickets are not separated according to attribute
Type	Specifies the type of report. Choices include: • Rollup (default)—displays the values based on the selected grouping • Trend—shows the occurrence of tickets over time (grouping criteria is not used)

Criteria (Continued)	Description
Chart	Determines the type of chart. Choices include: • Area • Bar • Bar 3D • Line • Stacked Area • Stacked Bar (default) • Stacked Bar 3D • Pie • Pie 3D

4 Click **View**. The **Report Viewer** dialog box appears. The content and appearance of the report varies depending on the selected criteria.



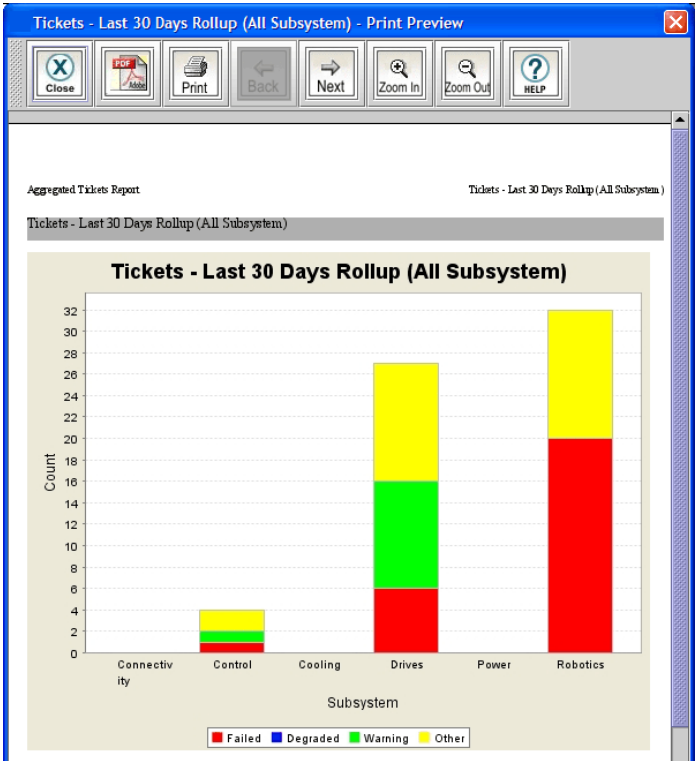
5 When you are finished viewing the Tickets Report, click **Close**.

6 To close the **Report Criteria** dialog box, click **Cancel**.

Printing or Exporting a Report to PDF

After generating the Tickets Report, you can print it or export it to a PDF file.

1 On the **Report Viewer** dialog box, click **Preview**. The **Print Preview** dialog box appears.



2 Do one or more of the following:

- To navigate through the pages of the report, click **Back** or **Next**.
- To increase or decrease the magnification of the report, click **Zoom In** or **Zoom Out**.
- To print the report, click **Print**. Specify print options, and then click **OK**.

- To save the report as a PDF file, click **PDF**. Specify a file path and file name, and then click **Confirm**.

3 When you are finished working with the **Print Preview** dialog box, click **Close**.

Note: You cannot print reports or save them to a PDF file using the touch screen.

Exporting a Report to an E-mail or a Text File

Instead of viewing the report as a chart, you can e-mail the report data to an e-mail address. Or export the report data to a comma delimited text file (***.csv**) for use in other programs.

1 On the menu bar, click **Tools** > **Reports** > **Tickets**. The **Report Criteria** dialog box appears.

2 Under **Specify Report Criteria**, click criteria options in the lists to customize the content and appearance of the Tickets Report.

Table 7 on page 77 summarizes the available report criteria options.

3 Click **Export**. The **Export Raw Data** dialog box appears.

4 Do one of the following:

- To send the report data to an e-mail address, click **Email**. Type or select the e-mail address, type an optional comment in the **Comment** box, and then click **OK**.
- To save the report data to a comma delimited text file, click **Save**. Specify a file path and file name, and then click **OK**.

5 To close the **Report Criteria** dialog box, click **Cancel**.

Saving a Report Template

If you frequently generate the Tickets Report with the same set of report criteria, save the criteria as a template. Loading the template recalls the saved report criteria and lets you quickly generate a report based on the saved criteria.

1 On the menu bar, click **Tools** > **Reports** > **Tickets**. The **Report Criteria** dialog box appears.

2 Under **Specify Report Criteria**, click criteria options in the lists to customize the content and appearance of the Tickets Report.

   Table 7 on page 77 summarizes the available report criteria options.

3 Under **Templates**, click **Save**.

4 Type a name for the template, and then click **OK**. The template appears in the list under **Templates**.

5 To load the saved report criteria at a later time, click the template in the list, and then click **View** to generate the report.

6 To close the **Report Criteria** dialog box, click **Cancel**.

Suppressing Tickets and Ticket Notifications

By default, the library provides notifications whenever a problem occurs. Notifications include:

- For Severity 1 issues, an e-mail is sent to Quantum Technical Support (techsup@quantum.com). This is set up by default in the **Setup > Notifications > System Setup** dialog box, Rules tab. See Setting Up E-mail Notifications on page 180 for more information.
- An e-mail is sent to individuals that you have set up in the **Setup > Notifications > System Setup** dialog box, Rules tab. See Setting Up E-mail Notifications on page 180 for more information.
- A ticket is generated (see Viewing Ticket Details on page 49 for more information).

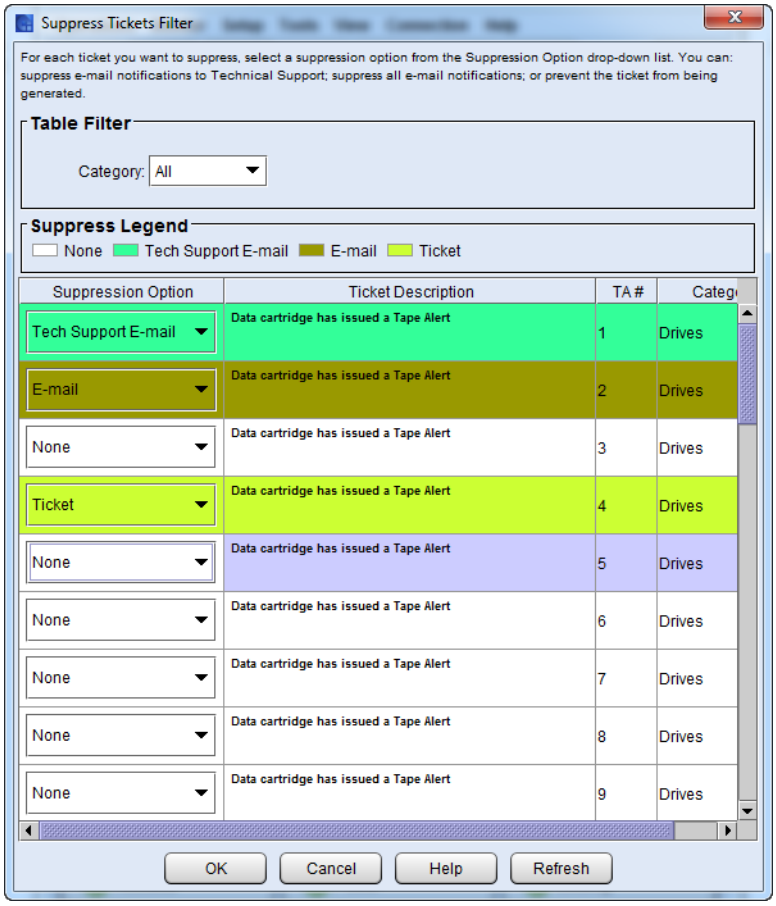
You can suppress these notifications and ticket generation as follows:

1 Select **Setup > Notifications > Tickets Filter**.

2 The **Suppress Tickets Filter** dialog box appears. The displayed table lists all tickets that have ever been issued for your library, plus all tickets pertaining to Tape Alerts (indicated by the Tape Alert number in the TA# column). Tape Alert tickets are listed even if they were not issued for the library.

Note: The list does not update dynamically. You can click the Refresh button to update the list

Figure 14 Suppress Tickets Filter



3 Filter the displayed list by selecting an option from the **Category** drop-down list in the **Table Filter** section. Options include **All** (default) or any of the six system status categories (**Connectivity**, **Control**, **Media**, **Drives**, **Power**, and **Robotics**).

4 For each ticket that you want to suppress, choose a suppression option from the drop-down list in the **Suppression Option** column. Options include:

- **Tech Support E-mail** — No e-mail notification will be sent to Technical Support for this ticket.
- **E-mail** — No e-mail notification will be sent to Technical Support or to the individuals configured in the **Setup > Notifications > System Setup, Rules** tab for this ticket.

- **Ticket** — No RAS ticket will be generated. Additionally, no e-mail notification will be sent to Technical Support or to the individuals configured in the **Setup > Notifications > System setup, Rules** tab.

5 Once you have chosen a suppression option, click somewhere else in the table and the row containing the ticket you suppressed turns a color corresponding to the suppression option (colors are identified in the legend at the top of the table).

6 Click **OK**.

Interpreting LEDs

LEDs can help you assess the state of a library component. The primary library LEDs can be grouped as follows:

- Interpreting Blade Status LEDs on page 83
- Interpreting Drive Status LEDs on page 86
- Interpreting Fibre Port Link LEDs on page 90(for Fibre drives and Fibre Channel I/O blades)
- Interpreting Ethernet Expansion Blade LEDs on page 93
- Interpreting MCB Port LEDs on page 94
- Interpreting LBX Terminator LEDs on page 96
- Interpreting Power Supply LEDs on page 101
- Interpreting Gen 2 Robot Status LEDs on page 103

Interpreting Blade Status LEDs

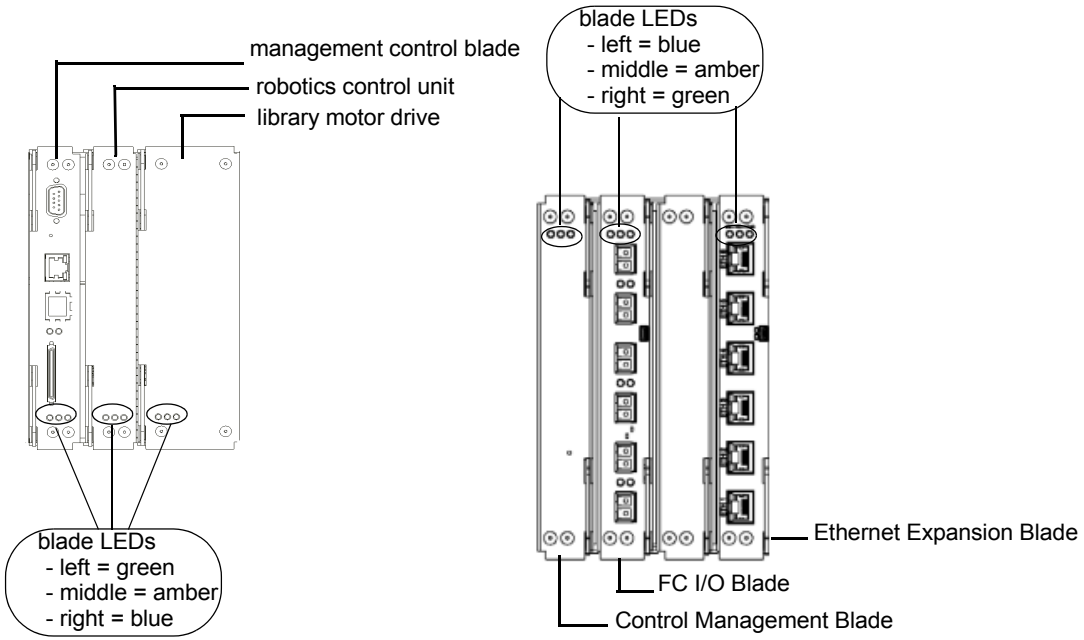
Each of the following library blades has a set of green, amber, and blue LEDs that indicate blade processor status, health status, and power control status:

- Management control blade (MCB)
- Control management blade (CMB)
- Fibre Channel (FC) I/O blade

- Ethernet Expansion blade
- Robotics control unit (RCU)
- Library motor drive (LMD)
- Library power control (LPC)

Figure 15 shows the locations and colors of the status LEDs on the five blades that can be in the library.

Figure 15 Locations and Colors of Blade Status LEDs



Blade status LEDs provide troubleshooting information that you can use in conjunction with tickets that the library creates. However, the LEDs might not directly correspond to tickets. The LEDs can indicate a firmware or hardware problem so severe that the library cannot create or display a ticket. For example, if the MCB firmware becomes inoperable, the amber LED flashes at 1 Hz, but the library might not be able to display any related tickets.

For a description of each LED color and what its state might mean, see Table 8 on page 85. For a description of how the blade status LEDs appear under normal conditions, see Table 9 on page 86.

Table 8 Explanations of Blade Status LED States

LED Color	Represents	Possible States and Explanations
Green	Processor status	• Solid off — blade's main processor is not operating (or blade is booting) • Solid on — blade's main processor is not operating (however, this does not apply to the LMD; solid on indicates that the LMD's main processor is operating normally) • Blinks one time every second (1 Hz) — blade's main processor is operating normally • Blinks 10 times every second (10 Hz) — identify mode • Solid on for three seconds, then blinks twice at 1 Hz, and then repeats — blade firmware is downloading
Amber	Health status	• Solid off — blade's power and control subsystem is operating normally • Solid on — blade's power and control subsystem has failed Solid on also can mean that the blade's power and control subsystem firmware is autoleveling. In conjunction with the blue amber LED blinking one time every 10 seconds, this is a normal condition. Autoleveling takes about three minutes for each blade, and blades within an I/O management unit autolevel in series. It can take as long as three minutes for the power and control subsystem to download. Never remove a blade when the amber LED is solid on unless it has been on continuously for at least 10 minutes.
Blue	Power control status	• Solid off — blade is not receiving power • Solid on — blade is powered down; ready to be replaced (swap mode) • Blinks one time every 10 seconds (flash) — blade is powered on; operating normally

Table 9 Blade Status LED States - Normal Conditions

LED Color	State and Explanation
Green	Blinks one time every second (1 Hz) — blade's main processor is operating normally (however, this does not apply to the LMD; solid on indicates that the LMD's main process is operating normally) Note: If there are issues during an update using an embedded flash, the green LED is solid for two seconds, and then off for one second.
Amber	Solid off — no errors are detected; blade's power and control subsystem is operating normally
Blue	Blinks one time every 10 seconds (flash) — blade is powered on; operating normally

Actions Based on LED States

When the RAS system is operating properly, service actions should be based on tickets first and foremost. However, some situations occur when the amber LED indicates problems that are not detected by the ticket system. You should always act on any amber LED that is solidly on, which indicates that the blade's power and control subsystem has failed. In this case, replace the blade.

When you replace a blade FRU or escalate a problem based on LED states, perform the following steps:

1. Observe and report the timing pattern of the blue, amber, and green LED group. Spend at least 30 seconds observing the LEDs and record the results in the service request (SR) and on any equipment failure report form that you return with the part. Proper reporting of all LED states is critical for determining the root cause of the failure.
2. Capture a system snapshot and send it to technical support for analysis.

Interpreting Drive Status LEDs

The library reports all drive issues that can affect customer operations. In addition to examining library reports, you should observe drive sled link LED and status LED activity.

Note: The blinking codes described in Table 10 on page 89 are the same for Fibre Channel and SCSI drives in the UDS-2 drive sleds.

Figure 16 shows the locations of the status LEDs and the Fibre Channel link LED on the rear of a UDS-2 drive sled.

Figure 16 Rear View of Fibre Channel Drive Sled (UDS-2)

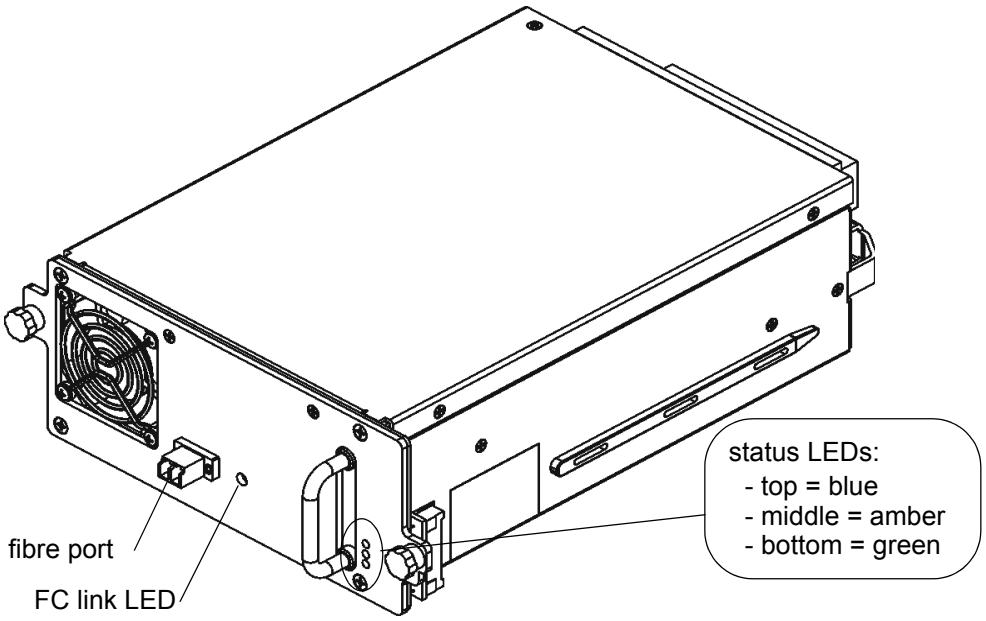


Figure 17 shows the locations of the status LEDs and the Fibre Channel link LED on the rear of a UDS-3 drive sled.

Figure 17 Rear View of Fibre Channel Drive Sled (UDS-3 LTO-4 and LTO-5 Drives)

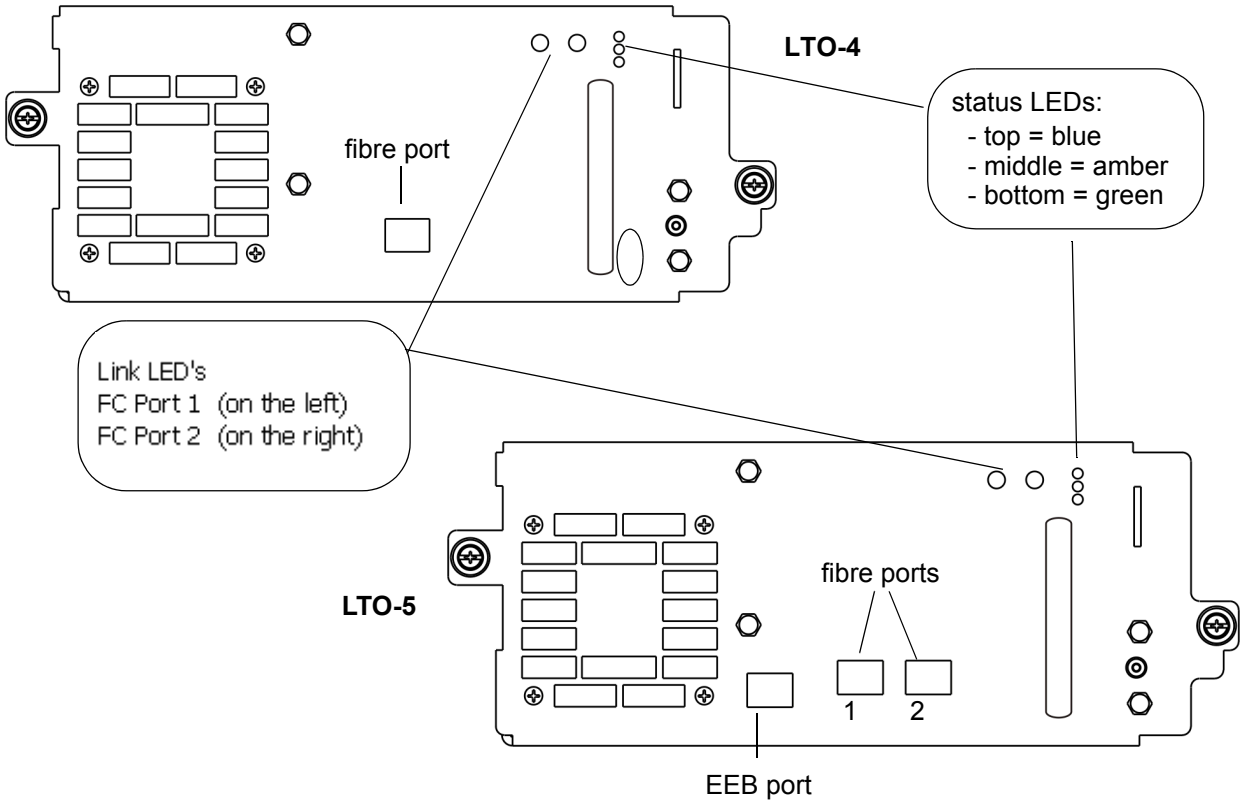


Table 10 on page 89 describes how to interpret the drive sled status LED activity that you might see on the rear of a UDS-2 or UDS-3 drive sled. For a description of how the blade status LEDs appear under normal conditions, see Table 11 on page 89. For information about interpreting the drive link LED, see Drive Sled Fibre Channel Link LED on page 90.

Table 10 Drive Sled Status LED States (UDS-2 and UDS-3)

LED Color	Represents	Possible States and Explanations
Green	Processor status	• Solid off — drive sled's main processor is not operating (or blade is booting) • Solid on — drive sled's main processor is not operating • Blinks one time every second (1 Hz) — drive sled's main processor is operating normally • Blinks 10 times every second (10 Hz) — identify mode • Solid on for three seconds, then blinks twice at 1 Hz, and then repeats — drive sled or drive brick firmware is downloading • Blinks three times in three seconds (1 Hz), then pauses (solid off), and then repeats — drive brick is activating (varying on)
Amber	Health status	• Solid off — drive sled's controller (drive DC to DC converter [DDC]) is operating normally • Solid on — drive sled's DDC has failed
Blue	Power control status	• Solid off — drive sled is not receiving power • Solid on — drive brick is powered down; ready to be replaced (swap mode) or varied on • Blinks one time every 10 seconds (flash) — drive brick is powered on; operating normally

Table 11 Drive Sled Status LED States - Normal Conditions

LED Color	State and Explanation
Green	Blinks one time every second (1 Hz) — drive sled's main processor is operating normally. The green LEDs for all drive sleds that are operating normally blink together.
Amber	Solid off — no errors are detected; drive sled's controller is operating normally.
Blue	Blinks one time every 10 seconds (flash) — drive sled is powered on; operating normally.

Interpreting Fibre Port Link LEDs

A fibre port link LED shows the state of the Fibre Channel link and whether the link is ready to transmit commands.

Drive Sled Fibre Channel Link LED

The Fibre Channel link LED for a drive sled is located on the rear of the drive sled. Figure 16 on page 87 shows the location of the Fibre Channel link LED on the rear of the UDS-2 drive sled, and Figure 17 on page 88 shows the location of the Fibre Channel link LED on the rear of the UDS-3 drive sled.

Table 12 describes how to interpret the Fibre Channel link LED activity that you might see on the rear of the UDS-2 drive sled. Table 13 on page 91 on page 135 describes the Fibre Channel link LED activity on the rear of the UDS-3 drive sled.

Table 12 Explanation of Fibre Drive Sled Link LED States (UDS-2)

LED Color	Represents	State and Explanation
Green	LIP and activity	• Solid on — loop initialization protocol (LIP) has occurred. • Blinks at irregular intervals — host command/data activity is occurring.
Amber	Online and light detected	• Solid on — the library has enabled the drive data bus; it can detect light through a fiber optic cable.
No color		• Solid off — the drive brick is varied off or the drive cannot detect light through a fiber optic cable (equivalent to no fibre cable plugged in). If the drive brick is varied off, the blue status LED will be solid on.

Table 13 Explanation of Fibre Drive Sled Link LED States (UDS-3)

LED Color	Represents	State and Explanation
Green	LIP and activity	• Solid on — loop initialization protocol (LIP) has occurred. • Blinks at irregular intervals — host command/data activity is occurring.
Amber	Online and light detected	• Solid on — the library has enabled the drive data bus; it can detect light through a fiber optic cable. • Blinks at regular intervals — the library has enabled the drive data bus, but light is not detected through the fiber optic cable.
No color		• Solid off — the library has not enabled the drive data bus or the drive brick is varied off. If the drive brick is varied off, the blue status LED will be solid on.

Note: A UDS-2 drive with no fiber optic cable plugged in is healthy if the link LED is solid off. A UDS-3 drive with no fiber optic cable plugged in is healthy if the LED is amber and blinking at regular intervals, indicating that the library has enabled the drive data bus, but no light is detected.

FC I/O Blade Fibre Port Link LED

The link LED for an FC I/O blade fibre port is located next to the port. On the I/O blade faceplate, black lines indicate how each link LED belongs to a port. Figure 18 shows the locations of the I/O blade Fibre port link LEDs.

Figure 18 Locations - Colors of I/O Blade Fibre Port Link LEDs

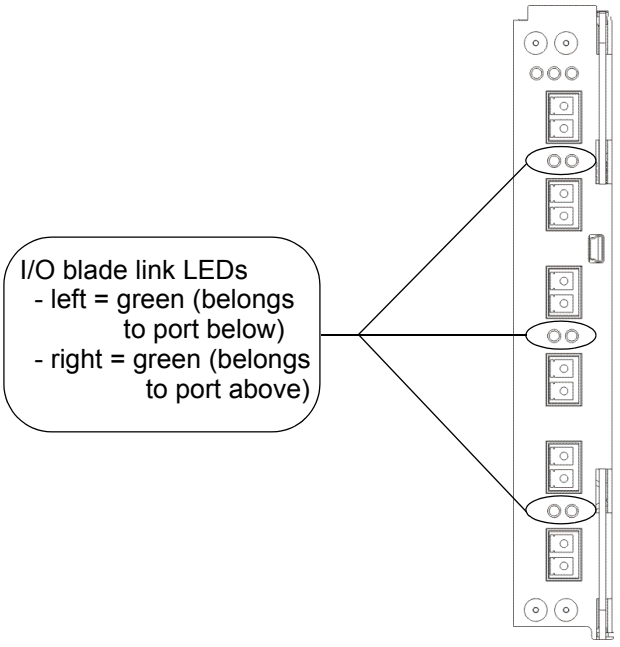


Table 14 on page 92 describes how to interpret the link LED activity that you might see. There is one supported model of FC I/O blade: 7404. LED behavior varies based on which model is installed in the library.

Table 14 FC I/O Blade Link LED States

FC I/O Blade Model	Possible Green LED States and Explanations
7404 4 gigabit/sec	• Solid on — the FC I/O blade has established a link but is not currently transporting data. • Blinks — the link is active and is currently transporting data. • Solid off — the FC I/O blade has not established a link **OR** the link is active and is currently transporting a large amount of data.

Note: For the 7404 FC I/O blade, fibre port LEDs are off while the blade is booting up.

Interpreting Ethernet Expansion Blade LEDs

The status LEDs for an Ethernet Expansion blade are located at the top of the EEB above ETH 6. Figure 19 shows the locations of the EEB status LEDs.

Figure 19 Location of Ethernet Expansion Blade Status LEDs

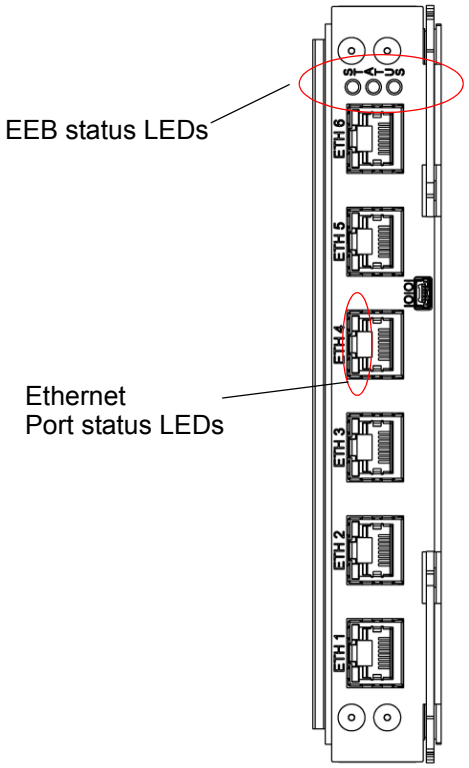


Table 15 Ethernet Expansion Blade LED States

Blue	Green	Amber	Description
Off	Off	Off	No power
1 Hz	Off	Off	Powered Down - Ready for removal

Blue	Green	Amber	Description
Off	Off	On	Booting
Flash	1 Hz	Off	Normal
Flash	10 Hz	Off	Normal - Identify

Table 16 Ethernet Expansion Blade Ethernet Port LED States

LED Color	Possible States and Explanations
Green	• Solid on — the link is up; data can be sent or received through the Ethernet port • Solid off — the link is not up; data cannot be sent or received through the Ethernet port
Amber	• Flashes at irregular intervals — data activity is occurring through the Ethernet port • Solid off — no data activity is occurring through the Ethernet port

Interpreting MCB Port LEDs

The MCB has LEDs for the Ethernet, Fibre Channel, and SCSI ports.

MCB Ethernet Port LEDs

The LEDs on the MCB Ethernet port indicate status and activity. Figure 20 shows the locations and colors of the MCB Ethernet port LEDs.

Figure 20 Locations - Colors of MCB Ethernet Port LEDs

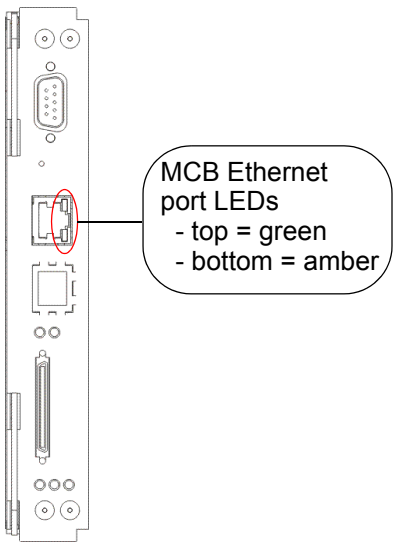


Table 17 describes how to interpret the Ethernet port LED activity that you might see.

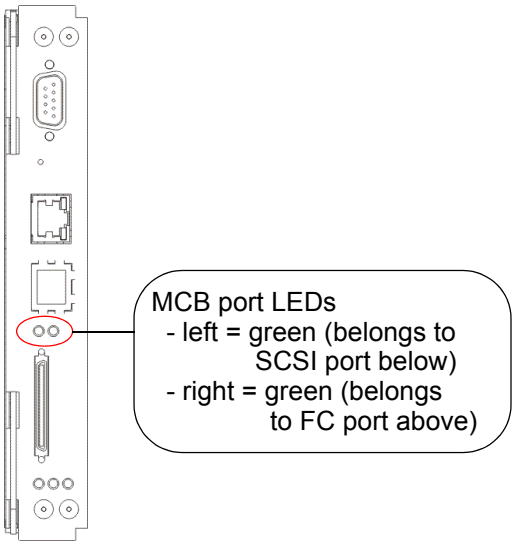
Table 17 Explanations of MCB Ethernet Port LED States

LED Color	Possible States and Explanations
Green	• Solid on — the link is up; data can be sent or received through the Ethernet port • Solid off — the link is not up; data cannot be sent or received through the Ethernet port
Amber	• Flashes at irregular intervals — data activity is occurring through the Ethernet port • Solid off — no data activity is occurring through the Ethernet port

MCB Fibre Channel and SCSI Port LEDs

The LEDs for the MCB Fibre Channel and SCSI ports are for future use. Ignore LED behaviors that might appear. Figure 21 shows the locations and colors of the LEDs.

Figure 21 Locations - Colors MCB FC / SCSI Port LEDs



Interpreting LBX Terminator LEDs

The LBX terminator has three versions. Version 01 has four LEDs and Versions 03 and 2.0 have six LEDs. For more information, see the *Scalar i2000/i6000 Maintenance Guide*.

LBX Terminator Version 01 LEDs

The LBX terminator has four green LEDs that indicate the presence of modules in the library. Figure 22 on page 97 shows the locations of the LEDs. Table 18 on page 97 describes how to interpret LED activity on the LBX terminator.

The terminator must be located in the LBX of the last expansion module. The LED status should reflect the physical installed module count of the system.

Figure 22 Locations of LBX Terminator LEDs (Version 01)

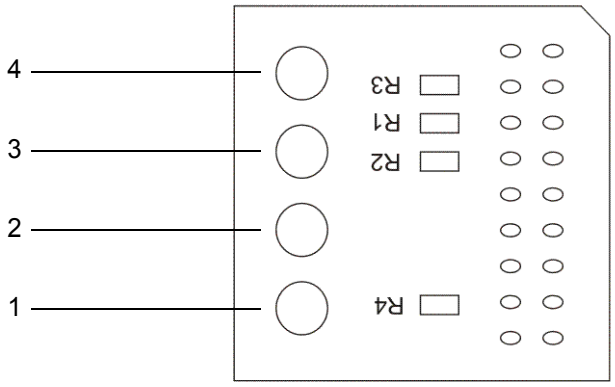


Table 18 Explanations of LBX Terminator LED States (Version 01)

LED On/Off Combinations				
1	**2**	**3**	**4**	**Explanation**
Off	Off	Off	Off	Robotics are disabled, the access door is open, or the LBX terminator is misaligned.
On	Off	Off	Off	The library has one control module and no expansion modules.
On	On	Off	Off	The library has one control module and one expansion module.
On	On	On	Off	The library has one control module and two expansion modules.
On	On	On	On	The library has one control module and three expansion modules.
On	Off	On	On	The library has one control module and four expansion modules.
On	On	Off	On	The library has one control module and five expansion modules.
On	Off	On	Off	The library has one control module and six expansion modules.
On	Off	Off	On	The library has one control module and seven expansion modules.

LBX Terminator Version 03 LEDs

The LBX terminator has six green LEDs that indicate the presence of modules in the library. Figure 23 shows the locations of the LEDs. Table 19 on page 98 describes how to interpret LED activity on the LBX terminator.

Figure 23 Locations of LBX Terminator LEDs (Version 03)

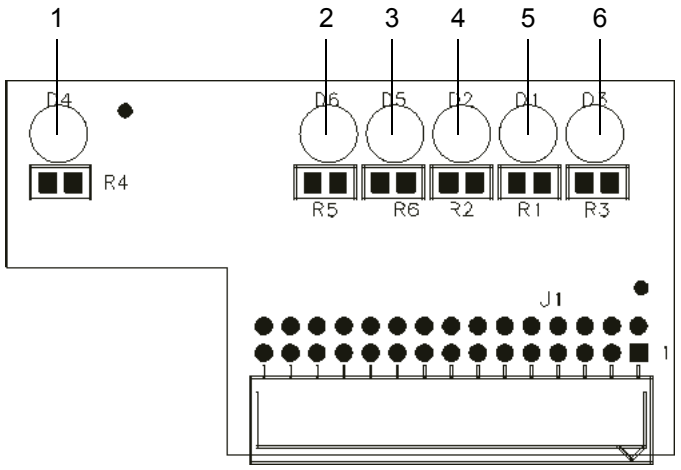


Table 19 Explanations of LBX Terminator LED States (Version 03)

LED On/Off Combinations						
1	**2**	**3**	**4**	**5**	**6**	**Explanation**
Off	Off	Off	Off	Off	Off	Robotics are disabled, the access door is open, or the LBX terminator is misaligned.
On	Off	Off	Off	Off	Off	The library has one control module and no expansion modules.
On	Off	Off	On	Off	Off	The library has one control module and one expansion module.
On	Off	Off	On	On	Off	The library has one control module and two expansion modules.
On	Off	Off	On	On	On	The library has one control module and three expansion modules.
On	Off	Off	Off	On	On	The library has one control module and four expansion modules.

LED On/Off Combinations						
1	2	3	4	5	6	Explanation
On	Off	Off	On	Off	On	The library has one control module and five expansion modules.
On	Off	Off	Off	On	Off	The library has one control module and six expansion modules.
On	Off	Off	Off	Off	On	The library has one control module and seven expansion modules.
On	On	Off	Off	Off	Off	The library has one control module and eight expansion modules.
On	On	Off	On	Off	Off	The library has one control module and nine expansion modules.
On	On	Off	On	On	Off	The library has one control module and ten expansion modules.
On	On	Off	On	On	On	The library has one control module and eleven expansion modules.
On	On	Off	Off	On	On	The library has one control module and twelve expansion modules.
On	On	Off	On	Off	On	The library has one control module and thirteen expansion modules.
On	On	Off	Off	On	Off	The library has one control module and fourteen expansion modules.
On	On	Off	Off	Off	On	The library has one control module and fifteen expansion modules.

LBX Terminator Version 2 LEDs

The LBX terminator has six blue LEDs that indicate the presence of modules in the library. Figure 24 shows the locations of the LEDs. Table 20 on page 100 describes how to interpret LED activity on the LBX terminator.

Figure 24 Locations of LBX Terminator LEDs (Version 2)

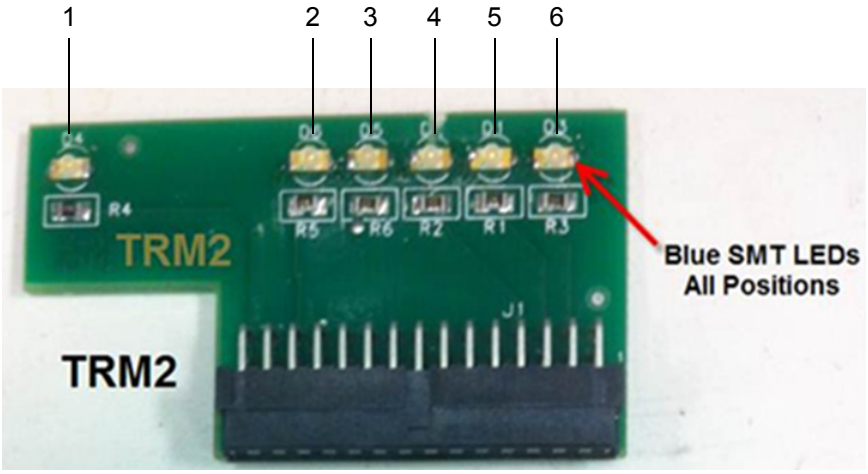


Table 20 Explanation of LBX Terminator LED States (Version 2)

LED On/Off Combinations						
1	**2**	**3**	**4**	**5**	**6**	**Explanation**
Off	Off	Off	Off	Off	Off	Robotics are disabled, the access door is open, or the LBX terminator is misaligned.
On	Off	Off	Off	Off	Off	The library has one control module and no expansion modules.
On	Off	Off	On	Off	Off	The library has one control module and one expansion module.
On	Off	Off	On	On	Off	The library has one control module and two expansion modules.
On	Off	Off	On	On	On	The library has one control module and three expansion modules.
On	Off	Off	Off	On	On	The library has one control module and four expansion modules.
On	Off	Off	On	Off	On	The library has one control module and five expansion modules.
On	Off	Off	Off	On	Off	The library has one control module and six expansion modules.
On	Off	Off	Off	Off	On	The library has one control module and seven expansion modules.

LED On/Off Combinations						
1	2	3	4	5	6	Explanation
On	On	Off	Off	Off	Off	The library has one control module and eight expansion modules.
On	On	Off	On	Off	Off	The library has one control module and nine expansion modules.
On	On	Off	On	On	Off	The library has one control module and ten expansion modules.
On	On	Off	On	On	On	The library has one control module and eleven expansion modules.
On	On	Off	Off	On	On	The library has one control module and twelve expansion modules.
On	On	Off	On	Off	On	The library has one control module and thirteen expansion modules.
On	On	Off	Off	On	Off	The library has one control module and fourteen expansion modules.
On	On	Off	Off	Off	On	The library has one control module and fifteen expansion modules.

Interpreting Power Supply LEDs

Power supply problems are reported in tickets. To physically identify a power supply, note the power supply number and module number in the ticket details. Modules can have up to two power supplies each. The top supply is #1 and the bottom supply is #2.

Figure 25 shows the locations and colors of the AC power supply LEDs.

Figure 25 Locations and Colors of Power Supply LEDs

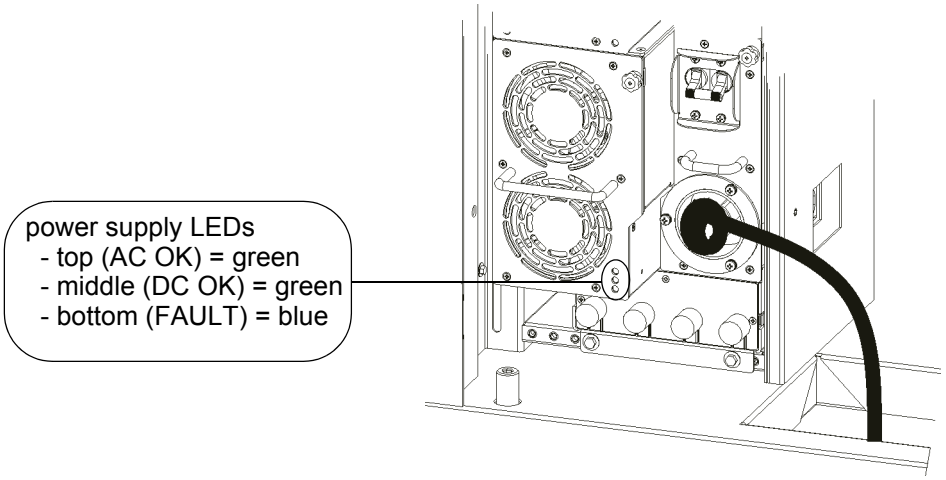


Table 21 describes how to interpret LED activity that you might see.

Table 21 Explanation of Power Supply LED States

LED Color	Represents	Possible States and Explanations
Green (top LED)	AC OK	• Solid on — power supply's AC input is above minimum requirements to operate • Solid off — power supply's AC input is below minimum requirements to operate
Green (middle LED)	DC OK	• Solid on — power supply's output voltage is within specifications • Solid off — power supply's output voltage is outside of specifications

LED Color	Represents	Possible States and Explanations
Blue (bottom LED)	Fault	• Solid on — indicates any of the following conditions: • Power supply output is outside of specifications • Current limit has been exceeded • Temperature limit has been exceeded • Fan failed while AC input is present and above minimum operating voltage • AC input is below minimum operating voltage • PDU is on, but the **Power** button on the library's indicator panel is off • Solid off — no faults are detected

Interpreting Gen 2 Robot Status LEDs

The Gen 2 robot has six status LEDs on the front plate of the picker on the robot itself (see Figure 26). These LEDs are described in Table 22.

If there are no problems with the robot, the LEDs should display as follows:

- If this is a left-side robot, the Left Position LED should be ON
- If this is a right-side robot, the Right Position LED should be ON
- The Sensors Engaged, Robot Power, and Robot Rail Engaged LEDs should all be ON
- The Sensors Disengaged LED should be OFF

If any of the LEDs are incorrectly illuminated, Quantum Support will need to troubleshoot, adjust, and possibly replace components to make sure all LEDs are correctly illuminated. Table 22 describes what the LEDs mean and how to troubleshoot them.

Figure 26 Robot Status LEDs

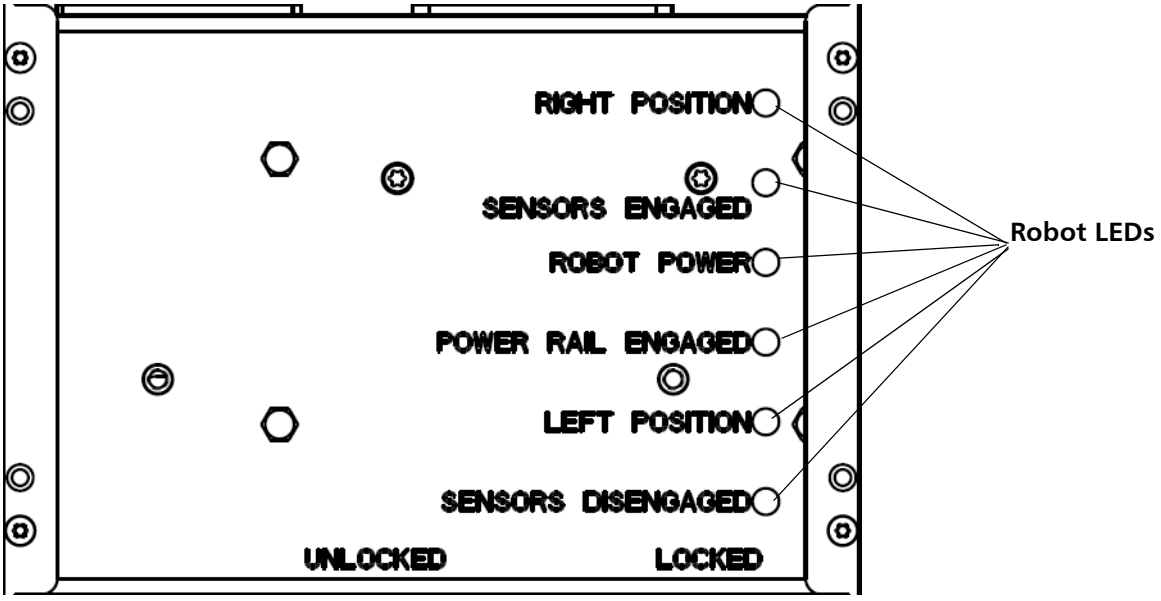


Table 22 Robot Status LEDs

LED	When ON, indicates the following
Right Position	Indicates this is a right-side robot.
Sensors Engaged	The Lock/Unlock handle is in the fully Locked position, and the home/parking sensors are positioned correctly for robot operations. It is safe to use the robot for library operations.
Robot Power	Robot control power is ON.
Power Rail Engaged	Connection to power rail is OK
Left Position	Indicates this is a left-side robot.
Sensors Disengaged	The robot's X-axis home/parking sensors are disengaged. The robot locking lever is fully unlocked. It is safe to remove the robot from the library.

Interpreting HDEM Tower Enable Button Blinking Pattern

The high-density expansion module (HDEM) operator panel contains a button that allows users to vary on and off the tower (see Figure 27 on page 105). The tower enable button has two colors: Amber (varied off) and green (varied on). Table 23 on page 105 describes what the blinking pattern mean and how to troubleshoot them.

Figure 27 HDEM Operator Panel with Tower Enable Button

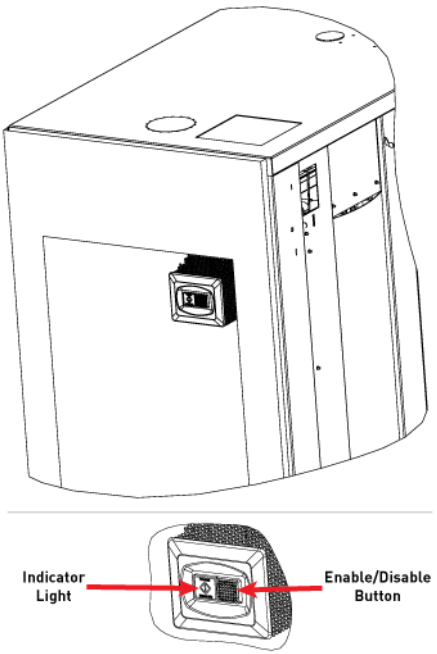


Table 23 HDEM Status LEDs

Lighting Pattern	Description
OFF, solid	Tower is not functioning properly or powered off completely
GREEN, solid	Tower is fully active, varied on and online
BLINKING GREEN (1 sec on, 1 sec off)	Tower is initializing/activating to an online or offline, varied on state

Lighting Pattern	Description
AMBER, solid	Tower is varied off, online or offline. Vary off status trumps online/offline status display. **Note:** It does not matter if the tower is offline or offline if it is varied off or being varied off.
BLINKING GREEN (3 sec ON, 1 sec OFF	Tower is varied on and UI takes the tower offline
BLINKING AMBER (10 HZ frequency)	Tower door is opened while tower is still varied on, or is currently in performing a vary-on or vary-off operation before completing the state transition, regardless of being logically online or offline, hereby interrupting tower motor control.
BLINKING (3 secs AMBER, 1 sec GREEN)	Aisle door opened while tower is varied on, regardless of being logically online or offline, hereby interrupting tower motor control. **Note:** If the tower was varied off before the aisle power was interrupted, the tower continues to display the vary off blink pattern.
10 Hz blinking pattern	Tower identification initiated

Working With Command History Logs

The **Command History Log** dialog box enables you to view command and response activity that has occurred with externally addressable library devices, including the LMC, controller LUNs, partitions, and drives. This information can help you isolate the source of an issue, such as a library device or host application.

Note: The number of selected drives affects the performance of the Command History Log.To ensure proper operations, limit drive log requests to twenty-five.

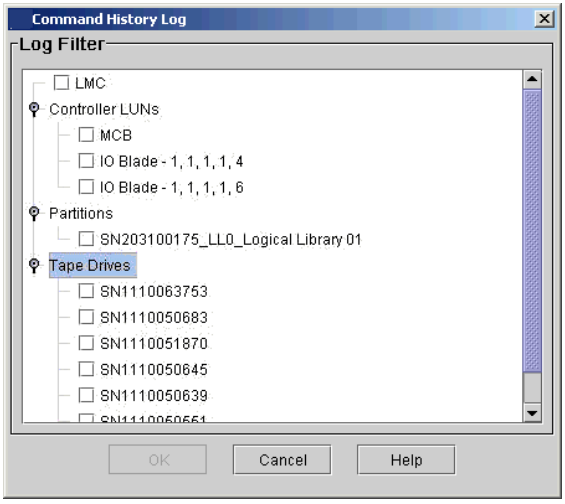
Viewing Command History Logs

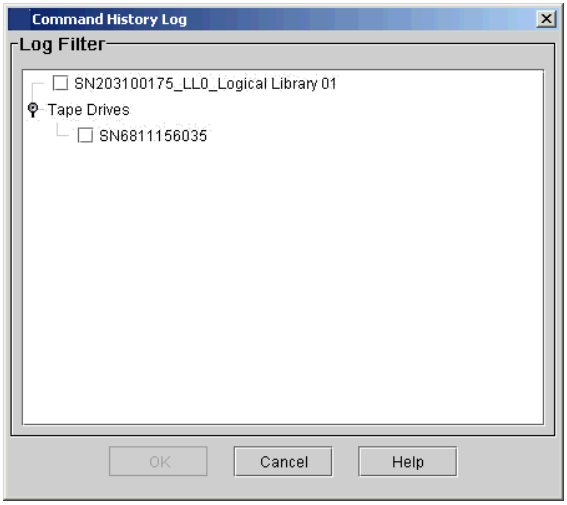
1 Log on as an administrator.

2 You can perform this procedure while viewing either the physical library or a partition. From the **View** menu, click the name of the physical library or the appropriate partition.

3 Click **Tools > Command History Log**. The **Command History Log** dialog box appears.

The first example dialog box that follows represents the physical view, and the second one represents a partition view. These examples show expanded levels for “Controller LUNs”, “Partitions”, and “Tape Drives”. Initially, these areas are not expanded. Click the highest-level items to show next-level items.





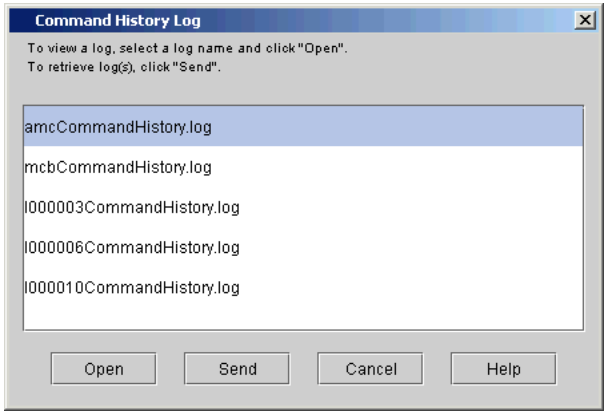
If logical serial number addressing is enabled on the **Physical Library** dialog box (**Setup > System Settings > Physical Library**), tape drives are listed according to their logical serial numbers. If logical serial number addressing is disabled, the drives are listed according to their physical serial numbers.

Also notice that command history logs for the LMC and the controller LUNs are available only from the physical view.

Note: The library is a multi-LUN device. To meet SCSI standards, a LUN 0 is allocated as a controller LUN on each blade, including the MCB and the I/O blades. The command history log for a controller LUN includes commands intended for the blade, not a specific logical unit connected to the blade.

---

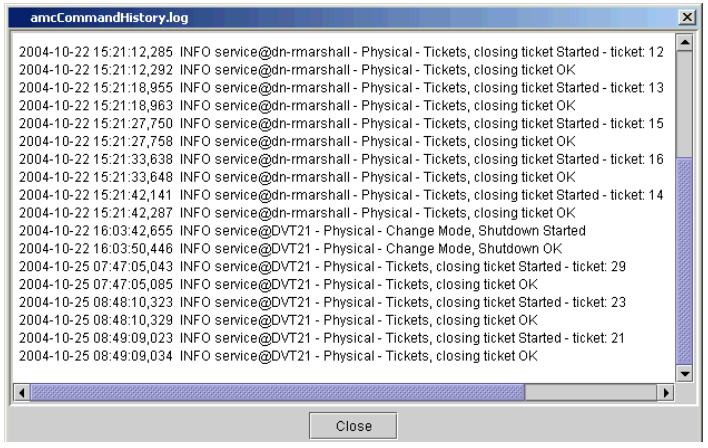
4 To access the command history logs (for LMC, controller LUNs, partitions, or tape drives), select one or more device check boxes, and then click **OK**. A list of log files appears in the **Command History Log** dialog box.



From this log-list view of the **Command History Log** dialog box, you can perform the following tasks:

- Display the contents of a log by clicking the **Open** button (proceed to the next step)
- Mail or save a log by clicking the **Send** button (see Mailing and Saving Logs on page 110)

5 Click a log file to highlight it, and then click **Open**. The contents of the log file appear.



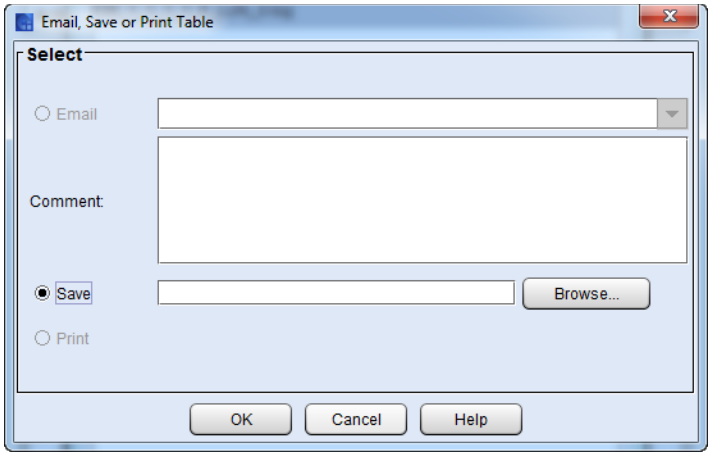
Mailing and Saving Logs

The **Send** button on the log-list view of the **Command History Log** dialog box enables you to send logs to e-mail addresses. If you are accessing the LMC from a remote client, **Send** also enables you to save the information to a file.

Note: You can mail or save logs from a remote client. However, you cannot save logs from the library's touch screen.

Note: Before you perform the following procedure, you must make sure that e-mail is appropriately configured in the LMC so that the library can send logs to the recipient. For more information about configuring e-mail, see Configuring E-mail on page 177.

1 From the log-list view of the **Command History Log** dialog box, click a log file to highlight it, and then click **Send**. The **Email, Save or Print Table** dialog box appears.



2 Perform one of the following tasks:

- To indicate that you want to send the log as an e-mail message to a recipient, select **Email**, and then either type an e-mail address in the **Email** text box or select an existing address from the drop-down list. You can type a comment in the **Comment** text box to send with the log.
- To indicate that you want to save the log, select **Save**, and then either type in the **Save** text box a path and a file name to which

you want the information saved or click **Browse** to specify a location and a file name.

Note: The **Save** option is available to remote client users only. It appears grayed out on the touch screen.

3 To send, click **OK**.

Accessing Online Help

For further help, you can access the library's Online Help system.

- To access the entire Online Help system, click **Help > Content**.
- To access context-sensitive help, click the **Help** button on any dialog box.

Chapter 3
Configuring Your Library

You can use either the local or remote versions of the Library Management Console (LMC) to modify your library's configuration. The **Setup** menu includes most of the configuration commands.

This chapter consists of the following sections:

- Setting Up Media Security Notifications on page 186
- Configuring Devices on page 188
- Configuring Drive Cleaning on page 217
- Registering SNMP Traps on page 223
- Configuring Library Security on page 225
- Using LDAP on page 231
- Configuring Screen Saver Preferences on page 238
- Working With Data Path Conditioning on page 240
- About the Configuration Record on page 242
- Setting Aisle Lights on page 243
- Configuring a Webcam For Your Library on page 244
- Working with Towers on page 245

For a brief overview of the LMC, see Library Management Console (LMC) on page 432.

If you are configuring your library for the first time, see the *Scalar i6000 Installation Guide* for information about performing an initial library configuration.

Note: Only one administrator can be logged on and performing library configuration at any one time. If another administrator attempts to log on, a message appears, warning that only one administrator at a time is permitted on the library. If a service user logs on while an administrator or regular users are logged on already, the library automatically logs off those users.

Running the Setup Wizard

Use the **Setup Wizard** command to initially configure important settings on a library as part of the normal installation procedure. Before you can manage your library from a remote LMC client, you must initially configure the library from its touch screen by either running the **Setup Wizard** command or using individual configuration commands

from the **Setup** menu. For detailed information about initially configuring the library, see the *Scalar i6000 Installation Guide*.

Caution: Use the Setup Wizard only once to initially configure the library.

Prerequisites

Before you run the Setup Wizard, do the following:

- Note the name and IP address of your network Domain Name Server (DNS) or the IP address, subnet mask, and default gateway for your network segment.
- Verify that your network is attached to the library network connection.
- Delete the default partition. Refer to Deleting Partitions on page 145 for more information.

Accessing Setup Wizard

To access the setup wizard, log on as an administrator from the library's touch screen, make sure that you are viewing the physical library, and then click **Setup** > **Setup Wizard**.

Enabling Licenses

In addition to the standard features, the following licensable features are available:

License/Feature	For more information about this feature, see...
Active Vault	Chapter 4, Active Vault.
Advanced Reporting	Chapter 5, Advanced Reporting

License/Feature	For more information about this feature, see...
Automated Media Pool (AMP) / Partition license	The Partition license allows you to create from 2 to 16 partitions, and gives you access to the Automated Media Pool features. See Chapter 6, Automated Media Pool.
Capacity on Demand (COD)	Chapter 7, Capacity on Demand
Encryption Key Management	Chapter 8, Encryption Key Management.
Extended Data Lifecycle Management (EDLM)	Chapter 9, Extended Data Lifecycle Management.
Partition Utilization	Chapter 12, Partition Utilization Reporting
Storage Networking (SNW)	Chapter 10, Path Failover

The following situations require you to enable license keys:

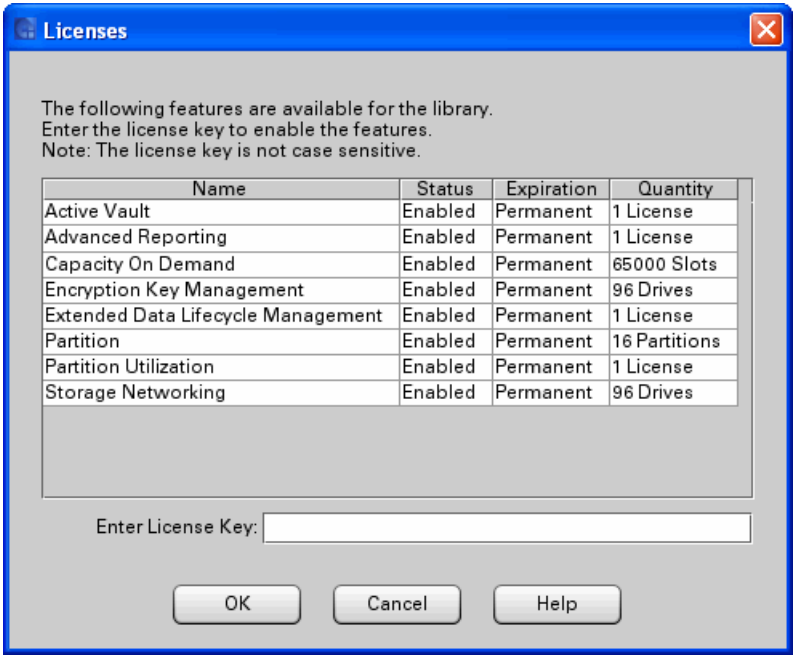
- During initial installation and configuration of the library. For more information about enabling licenses for the first time, see the *Scalar i6000 Installation Guide*
- During a feature upgrade
- When you need to activate additional storage slots in your current COD configuration

If you cannot locate the license keys shipped with the library, you can obtain them by contacting technical support or, if you are an end user, by contacting your inside sales representative.

Note: Authorized service personnel are involved in the first two situations. However, any administrator can activate additional storage slots.

1. Log on as an administrator.
2. If you are not already working from the physical library, select it from the **View** menu.

3 From the menu bar, click **Setup > Licenses**. The **Licenses** dialog box appears.



This dialog box lists the licensed features for your library, including their status, expiration date, and quantity. The following guidelines apply to the **Quantity** column:

- **Capacity on Demand** displays the number of licensed slots.
- **Encryption Key Management** and **Storage Networking** display the number of licensed drives.
- **Partition** quantity displays the number of licensed partitions.
- **Extended Data Lifecycle Management** and **Advanced Reporting** quantity is always set to 1.
- For features that are not licensed by quantity but instead apply to the entire library, such as the drive monitoring feature, the **Quantity** is always set to 1.

4 In the **Enter License Key** text box, type the appropriate license key.

Note: License keys are not case-sensitive, so if you are using the library's touch screen, enter the library key from the lowercase keyboard, which gives you access to the dash (-) character.

If you cannot locate the license keys shipped with the library, you can obtain them by contacting technical support (see Contacts on page xiii) or, if you are an end user, by contacting your inside sales representative.

5 Click **OK**.

6 If you have upgraded the library's storage capacity, the extra storage slots you just added are not assigned to a partition. You can either create a new partition to include them or manually modify an existing partition to include them by using expert partitioning mode.

Caution: Consult your service representative and see the *Scalar i6000 Planning Guide* before you reconfigure your partitions.

For more information, see Working With Partitions on page 118.

Working With Partitions

A partition is an abstraction of a single underlying physical library that presents the appearance of multiple, separate libraries for purposes of file management, access by multiple users, or dedication to one or more host applications. For example, you can choose to run one software application in one partition, and a different software application in a second partition.

There are two types of partitions in the Scalar i6000 library:

- **Standard partitions** — Standard partitions are visible to hosts and are used for normal backup operations. You can create standard partitions via the setup wizard or manually using simple or expert mode.

- **Library managed partitions** — Library managed partitions (LMPs) are similar to other partitions, except they are not visible to backup applications or hosts. The library manages the LMP, rather than the backup application. The library uses the LMP to facilitate the following value-added features, each of which requires its own license:
  - Active Vault on page 249
  - Automated Media Pool on page 263
  - Extended Data Lifecycle Management on page 317

  You can create library managed partitions via the setup wizard or manually using expert mode.

Each partition contains the following components of the physical library:

- Accessor — the robotic assembly that moves media within the library. The accessor includes the picker and reach assemblies.
- I/E station magazine — a magazine, consisting of slots for cartridges, that enables media to be moved into or removed from the physical library.

  Note: Partitions do not require I/E station slots, but if you do not assign any, you will need to bulk load/unload cartridges in the partition, which requires taking the entire library offline. I/E stations allow you to import and export cartridges to and from a partition without taking the library offline.

- Storage magazine — a static column location within a section of the physical library rack that holds removable media. For more about location coordinates, see Understanding Location Coordinates on page 449.
- Drive — the read/write device for removable media.

  Note: Partitions can be created that have zero (0) drives allocated.

  Note: Active Vault and Automated Media Pool (AMP) library managed partitions do not contain drives.

For more information about the library's physical components, see the *Scalar i2000/i6000 Maintenance Guide.* For help with planning before you configure your system, see the *Scalar i6000 Planning Guide.*

A standard partition consists, at a minimum, of one storage magazine and one drive. Neither the storage magazine nor the drive can be shared with another partition.

Note: Active Vault and AMP partitions do not contain drives; they must contain at least one storage magazine.

One 24-slot I/E station can be used by up to four partitions. One 72-slot I/E station can be used by up to twelve partitions. The maximum number of I/E station slots per partition is 240. The maximum number of partitions is determined by the lesser of the number of drives available in the physical library (assuming there are at least as many storage slots) or 16.

Note: The library is licensed for either one partition or the maximum number of partitions, which is 16. For more information about partition licensing, see Enabling Licenses on page 115.

Gen 1 libraries support multiple drive and media domains. However, drive and media domains cannot be mixed within a partition. Each Gen 1 partition can contain only one drive and media domain. Within that domain, a partition can contain multiple drive interface types (FC and SCSI) as well as multiple media types (for example, LTO-3, LTO-4, LTO-5, and LTO-6).

Gen 2 libraries only support LTO drives and media. A single partition can contain multiple drive interface types (FC and SCSI) as well as multiple media types (for example, LTO-3, LTO-4, LTO-5, and LTO-6).

Configuration controls, such as **FC Host** and **SNW** (Storage Networking) **Host Access** provide the means to permit host access to particular partitions and tape drives. Multiple hosts can share a single partition, or a partition can be restricted to one exclusive host. Host applications control access to elements within the shared partition. Each application can have a partition assigned to it. Each application uses its partition as if it were a dedicated physical library.

Note: For information about creating library-managed encryption on partitions, see Chapter 8, Encryption Key Management.

Understanding Partition Media Policy Settings

A partition's **Media Type Checking, Media Checking Policy, and Return Media Identifier** settings help determine how the library handles differing media types within the same library. You can configure media policy settings when you manually create or modify a partition.

The key concepts regarding partition media policies are the media domain, media type, media ID checking, and media identifier.

Media Domain

Gen 2 libraries only support the LTO media domain.

Media Type

The media type is a particular generation of tape technology. Several media types can exist within one media domain. For example, within the LTO media domain is the LTO-1 media type, the LTO-2 media type, and so forth. A media type has an identifier, chosen by the tape manufacturer or consortium, that enables users and libraries to distinguish between them. The LTO consortium uses L1, L2, L3, L4, L5, and L6 to identify the LTO-1, LTO-2, LTO-3, LTO-4, LTO-5, and LTO-6 media types in a volume serial number.

A single partition can contain a mixture of media types and interface types within the same domain (for example, LTO-1 and LTO-2 with SCSI or Fibre Channel interfaces).

To create or modify a partition with mixed media types, you must use **Expert** mode (select **Expert** mode on the **Partitions Wizard** dialog box). You cannot create or modify partitions with mixed media while in **Automatic** mode or **Simple** mode.

Media ID Checking

Media ID checking policy restricts the movement of tape cartridges based on the media ID on the barcode label. This policy also helps you monitor the management of tapes and drives by the host applications. When you create or modify a partition, you can enable or disable the **Media Type Checking** option. If you choose to enable media type checking, you also can use the **Media Checking Policy** option to select from two modes of operation: **Required** or **Not Required**. With either mode, the library checks whether a cartridge has a valid media ID on the barcode label.

In **Required** mode, if the library does not find a valid media ID on a cartridge, the library does not allow it to be moved into or within the library. If the library finds a valid media ID, the library allows it to be moved from an I/E station into a partition that contains magazines matching the media domain of the cartridge (for example, LTO), but the library does not allow the cartridge to be moved from storage to an incompatible drive type (for example, an LTO-2 cartridge will not be allowed to move to an LTO-1 drive).

In **Not Required** mode, if the library does not find a valid media ID on a cartridge, the library allows it to be moved into or within the library as long as the I/E station magazine, storage magazine, or drive matches the media domain of the cartridge. If the library finds a valid media ID, the library does not allow the cartridge to be moved from storage to a drive that does not have a compatible type (for example, an LTO-2 cartridge will not be allowed to move to an LTO-1 drive).

Return Media Identifier

For the media policy settings, the library makes assumptions about a media identifier and its position in a media barcode label. To be considered a media identifier, the identifier characters must be correct for the media domain and media type. Also, the identifier, which for some media types can consist of more than one character, must be complete and in the correct location. The correct characters in the wrong position are not viewed as a media type identifier. In a physical library or partition containing mixed media, the media identifier is not required for all cartridges.

Table 24 explains the media type identifiers and assumptions.

Table 24 Sampling of Media Type Identifiers

Media Domain	Media Type	Identifier
LTO	LTO-1	“L1” as the last characters in the barcode
LTO	LTO-2	“L2” as the last characters in the barcode
LTO	LTO-3	“L3” as the last two characters in the barcode

Media Domain	Media Type	Identifier
LTO	LTO-3 WORM	“LT” as the last two characters in the barcode
LTO	LTO-4	“L4” as the last two characters in the barcode
LTO	LTO-4 WORM	“LU” as the last two characters in the barcode
LTO	LTO-5	“L5” as the last two characters in the barcode
LTO	LTO-5 WORM	“LV” as the last two characters in the barcode
LTO	LTO-6	“L6” as the last two characters in the barcode
LTO	LTO-6 WORM	“LW” as the last two characters in the barcode

With a valid media type identifier present and the **Media Type Checking** setting enabled, which is the case by default, a host is prevented from executing invalid media moves across differing media types. For example, a host can be prevented from moving LTO-2 media to an LTO-1 drive. If an invalid move is attempted, the library returns an error to the host.

Regardless of whether or not partition media policies are enabled or disabled, the library always prevents host move-media commands that cross different media domains.

With the **Return Media Identifier** setting, you can control if and where a media type identifier appears in the volume serial number that is returned to the host.

Table 25 shows an example of how the return media identifier is reported to the host, depending on the setting you choose: **Disabled**, **Prefix**, **Suffix**, and **Pass Through**. The bold, underlined portion is the media identifier.

Table 25 Return Media Identifier Behavior Example

Setting	Volume Serial Number Returned to Host*
Disabled	ABC123
Prefix	**L1**ABC123
Suffix	ABC123**L1**
Pass Through	ABC123**L1**

*Based on actual LTO-1 barcode: ABC123**L1**

For more information about configuring the **Media Type Checking** and **Return Media Identifier** settings, see Creating Partitions Manually on page 126.

Creating Partitions

You can create library partitions in three ways:

- Creating Partitions Automatically on page 125
- Creating Partitions Manually on page 126, using one of the following modes:
  - Using Simple Mode on page 126
  - Using Expert Mode on page 131

The method you should choose depends on the circumstance and the level of control you want in allocating resources to the partition. When creating partitions **Automatically**, the library assigns available system resources to create the number of partitions you specify. Automatic mode is not available if a partition already exists. Creating partitions **Manually** enables you to pick specific drives, storage magazines, and magazines within an I/E station to assign to a partition.

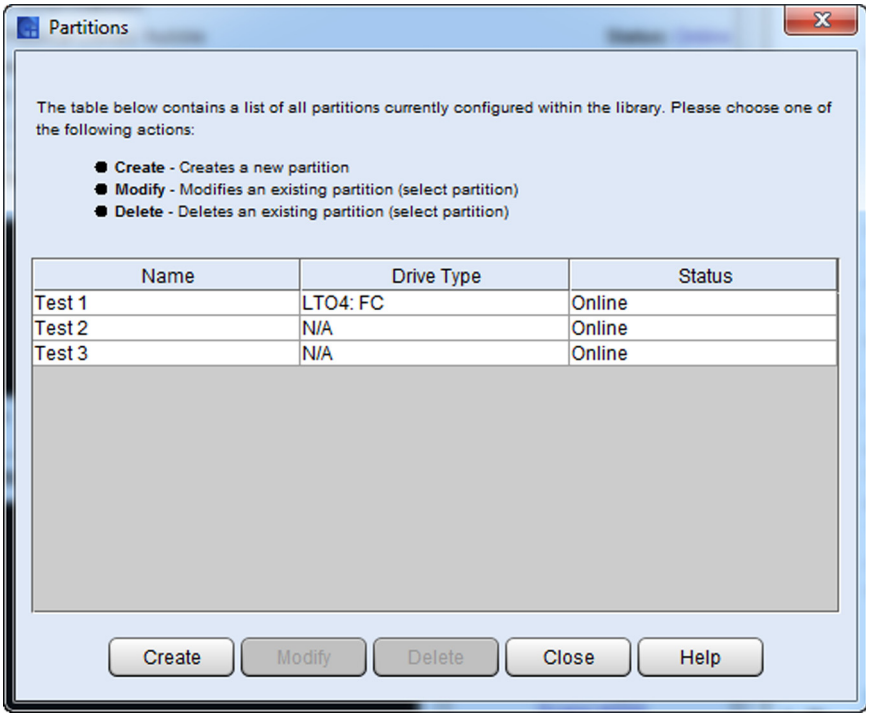
Note: Make sure that you have adequately planned for the number of partitions that you want to configure.

Creating Partitions Automatically

You can use the library's **Automatic** mode to create partitions within limits based on licensing restrictions and available resources. **Automatic** mode is available *only* if no partitions currently exist.

1. Log on as an administrator.
2. Make sure that you are viewing the physical library. From the **View** menu, click the name of the physical library.
3. Click **Setup > Partitions > Configure**. The **Partitions** dialog box appears.

Figure 28 Partitions dialog box



4. Click **Create**. The **Partitions – Step 1: Choose Creation Mode** dialog box appears.
5. Select **Automatic**, and then click **Next**. The **Partitions – Step 2: Automatic Creation** dialog box appears.

6 In the **Partitions** column, type the number of partitions you want to create for each media/drive type.

   The maximum number of partitions that you can create is determined by the number of partitions you are licensed to create and the number of drives available. See Enabling Licenses on page 115.

7 Click **Finish**. The **Partitions** dialog box appears again.

8 Click **Close**.

Creating Partitions Manually

If one or more partitions already exist in the library, you must manually create a new partition to allocate drives, storage slots, and I/E station magazines. You have two options to allocate system resources when manually creating a new partition:

- Using Simple Mode
- Using Expert Mode

In **Simple** mode, you can specify the quantity of each element you want assigned to the partition. In **Expert** mode, you can indicate which specific drives, storage magazines, I/E station magazines, or if enabled, extended I/E station magazines to assign to the partition. You can also configure library managed partitions in Expert mode.

Using Simple Mode

1 Log on as an administrator.

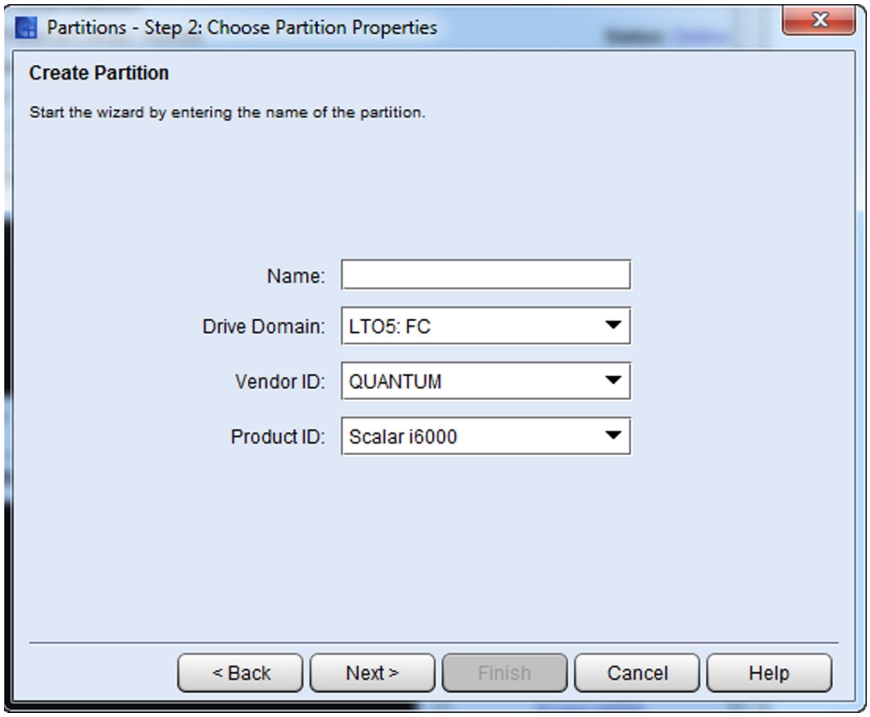
2 Make sure that you are viewing the physical library. From the **View** menu, click the name of the physical library.

3 Click **Setup > Partitions > Configure**. The **Partitions** dialog box appears, listing partitions that are currently configured within the library.

   Note: If you want to cancel the partition creation process, click **Close**. The **Close** button becomes unavailable after you click **Create** later in this procedure.

4 Click **Create**. The **Partitions - Step 1: Choose Creation Mode** dialog box appears.

5 Select **Simple**, and then click **Next**. The **Partitions - Step 2: Choose Partition Properties** dialog box appears.



6 Configure the following settings:

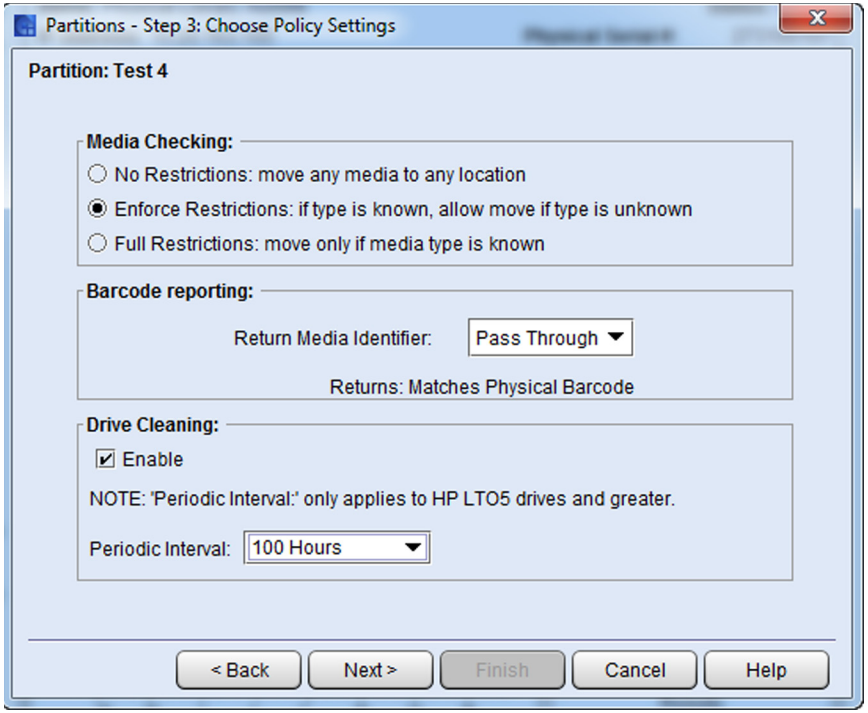
- In the **Name** text box, type a name that describes the new partition.
- In the **Drive Domain** list, select the type of drive to be used in the partition.
- From the **Vendor ID** list, select the vendor.

  The **Vendor ID** information is used in the SCSI Inquiry command. The choices are QUANTUM and ADIC. The default is QUANTUM. Some backup applications may only support or be configured for ADIC libraries, so if you configure a logical library using the vendor ID of QUANTUM, the backup application would not work with the library.

- From the **Product ID** drop-down list, click the appropriate product type.

  The **Product ID** setting controls the product ID string that is returned in a standard SCSI INQUIRY response. The library can report that it is a Scalar i500,Scalar i2000, or Scalar i6000. This feature can enable the library to be used with host applications that do not yet include the Scalar i6000 in a list of recognized devices. In addition, the various Microsoft Windows operating systems maintain a list of recognized devices. If the Scalar i6000 is not in an operating system's list of recognized devices, the library will appear as an "unknown" device in device lists. You might prevent the library from being listed as "unknown" by setting **Product ID** to a library other than Scalar i6000. This setting does not cause any library operational changes other than the SCSI INQUIRY response.

7 To continue, click **Next**. The **Partitions - Step 3: Choose Policy Settings** dialog box appears.



8 Configure the following media policy settings:

- For **Media Checking Policy**, select one of three options:
  - **No Restrictions** - Allow any media to be moved anywhere
  - **Enforce Restrictions** - If the media type is known, the barcode contains a media identifier that will enforce restrictions. For example, LTO6 supports reading LTO6, LTO5 and LTO4 media and writing to LTO6 and LTO5 drives. This setting is the default setting.
  - **Full Restrictions** - The media type identified must be known before we can import or move a media to a drive.
- From the Barcode reporting area, select an option from the **Return Media Identifier** drop-down list. Options include **Suffix**, **Pass Through**, **Prefix**, or **Disabled**. Depending on which setting you choose, you can control the use of the media type identifier in the volume serial number that is returned to the host.

Caution: After a media volume serial number has been reported to a host, changing the **Return Media Identifier** setting could cause the host to not recognize media within the library.

For more information about how media policies work, see Understanding Partition Media Policy Settings on page 121.

9 Configure the **Drive Cleaning** policy, by selecting either **Enable** or **Disable**. This setting is enabled by default.

Enabling drive cleaning allows the library to initiate drive cleaning each time a drive requests a cleaning operation. For drive cleaning to function, you must first configure drive cleaning for the library. For more information about configuring drive cleaning, refer Configuring Drive Cleaning on page 217.

Note: Drive cleaning should be enabled for partitions only if the host application does not support the coordination of drive cleaning. If drive cleaning functionality is enabled on the host application, do *not* enable automatic drive cleaning for any partitions in the library.

10 If you are enabling **Drive Cleaning**, select the number of motion hours you want the drives in the partition to be cleaned. Values include:

- 100 hours (default)
- 200 hours
- 400 hours
- 800 hours
- 1000 hours

Note: Drive cleaning settings only apply to HP LTO-5 or higher drives.

11 To continue, click **Next**. The **Partitions - Step 4: Choose Resource Quantities** dialog box appears.

12 Type the number of elements to include in the partition by specifying:

- Number of drives

Note: Partitions can be created that have zero (0) drives allocated.

- Number of storage slots
- Number of I/E slots

The quantity available for each type of resource indicates resources not yet assigned to existing partitions.

13 To continue, click **Next**. The **Partitions - Summary Information** dialog box appears.

14 Verify that the parameters you set are correct.

15 To create the partition, click **Create**. The **Partitions - Completed** dialog box appears.

Note: After you click **Create**, the **Cancel** button becomes unavailable.

16 Review the information to make sure it is correct.

17 If you want to view the drive information after creating the partition, click **Next**.

18 Click **Finish**. The **Partitions** dialog box appears again with the partition you just created listed.

19 Click **Close**.

Using Expert Mode

1 Log on as an administrator.

2 Make sure that you are viewing the physical library. From the **View** menu, click the name of the physical library.

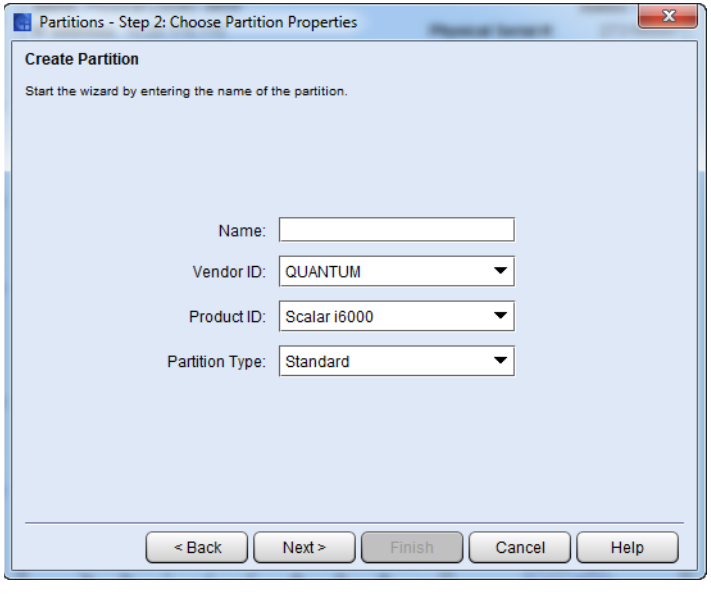
3 Click **Setup > Partitions > Configure**. The **Partitions** dialog box displays a list of partitions currently configured within the library.

Note: If you want to cancel the partition creation process, click **Close**. The **Close** button becomes unavailable after you click **Create** later in this procedure.

---

4 Click **Create**. The **Partitions - Step 1: Choose Creation Mode** dialog box appears.

5 Select **Expert**, and then click **Next**. The **Partitions - Step 2: Choose Partition Properties** dialog box appears.



6 In the **Name** text box, type a name to describe the new partition.

7 From the **Partition Type** drop-down list, select the type of partition you want to create.

- The default is **Standard**. If you are creating a standard partition, accept the default and go to Step 8.
- The other choices are for creating **library managed partitions** (LMPs). You can only select a library managed partition if it is already licensed. The choices are:
  - **Library Managed (EDLM)** — For more information, see Extended Data Lifecycle Management on page 317)
  - **Library Managed (AMP)** — For more information, see Automated Media Pool on page 263
  - **Library Managed (VAULT)** — For more information, see Active Vault on page 249

  When you select a library managed partition, the Vendor ID, and Product ID fields become disabled. If you are creating a library managed partition, make your selection and continue to Step 9.

8 If you are not creating a library managed partition, do the following:

a From the **Vendor ID** drop down list, select the vendor.

The **Vendor ID** information is used in the SCSI Inquiry command. The choices are QUANTUM and ADIC. The default is QUANTUM. Some backup applications may only support or be configured for ADIC libraries, so if you configure a logical library using the vendor ID of QUANTUM, the backup application would not work with the library.

b From the **Product ID** drop-down list, click the appropriate product type.

The **Product ID** setting controls the product ID string that is returned in a standard SCSI INQUIRY response. The library can report that it is a Scalar 24, Scalar 100, Scalar i500, Scalar 1000, Scalar i2000, Scalar i6000, or Scalar 10K. This feature can enable the library to be used with host applications that do not yet include the Scalar i6000 in a list of recognized devices.

In addition, the various Microsoft Windows operating systems maintain a list of recognized devices. If the Scalar i6000 is not in an operating system's list of recognized devices, the library will

appear as an “unknown” device in device lists. You might prevent the library from being listed as “unknown” by setting **Product ID** to a library other than Scalar i6000. This setting does not cause any library operational changes other than the SCSI INQUIRY response.

9 To continue, click **Next**. The **Partitions - Step 3: Choose Policy Settings** dialog box appears.

Note: If you are configuring an LMP, all choices on this screen are pre-selected and you cannot change them. To continue, go to Step 12.

10 Configure the following settings:

- For **Media Checking Policy**, select one of three options:
  - No Restrictions - Allow any media to be moved anywhere
  - Enforce Restrictions - If the media type is known, the barcode contains a media identifier that will enforce restrictions. For example, LTO6 supports reading LTO6, LTO5 and LTO4 media and writing to LTO6 and LTO5 drives. This setting is the default setting.
  - Full Restrictions - The media type identified must be known before we can import or move a media to a drive.
- From the **Return Media Identifier** drop-down list, click either **Suffix**, **Pass Through**, **Prefix**, or **Disabled**. Depending on which setting you choose, you can control the use of the media type identifier in the volume serial number that is returned to the host.

  Caution: After a media volume serial number has been reported to a host, changing the **Return Media Identifier** setting could cause the host to not recognize media within the library.

  For more information about how media policies work, see Understanding Partition Media Policy Settings on page 121.
- For **Drive Cleaning**, click either **Enable** or **Disable**.

  Enabling drive cleaning allows the library to initiate drive cleaning whenever a drive in the partition recommends or

requires cleaning. For drive cleaning to function, you must first configure drive cleaning for the library. For more information about configuring drive cleaning, refer Configuring Drive Cleaning on page 217.

Note: Drive cleaning should be enabled for partitions only if the host application does not support the coordination of drive cleaning. If drive cleaning functionality is enabled on the host application, do *not* enable automatic drive cleaning for any partitions in the library.

11 If you are enabling **Drive Cleaning** for a partition containing HP LTO-5 and later drives, select the number of motion hours after which the drive will recommend cleaning. Values include:

- 100 hours (default)
- 200 hours
- 400 hours
- 800 hours
- 1000 hours

12 To continue, click **Next**. The **Partitions - Step 4: Select Drives** dialog box appears.

Note: If you are creating a library managed Automated Media Pool (AMP) or Active Vault partition, this screen is skipped because drives are not allowed in these partitions. Go to Step 16.

Note: If you are creating an EDLM partition, only EDLM-capable drives are shown.

13 In the left column, select the location of one or more drives.

Make sure that you select the appropriate module because the library can have drives in the control module and any of the eleven expansion modules.

Note: With the release of version i12, you can create partitions that have zero (0) drives allocated.

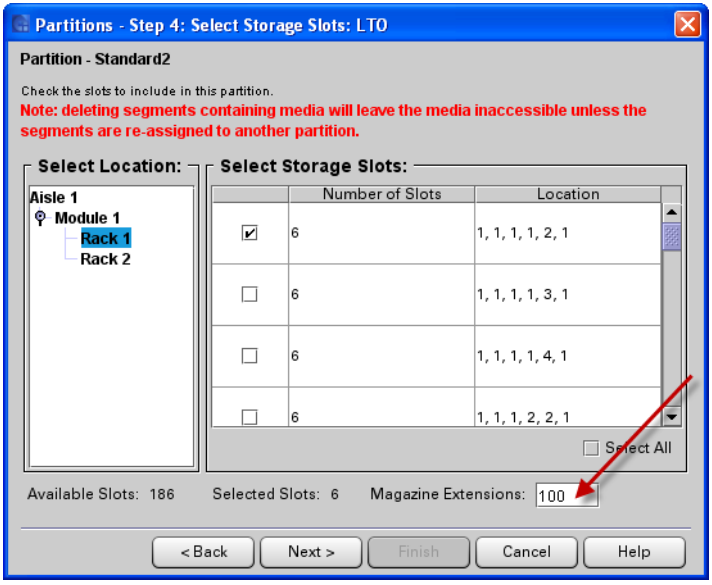
14 To assign a drive to the partition, select the appropriate check box. You can identify a drive by its serial number and location coordinates. For more information, see Understanding Location Coordinates on page 449.

15 To continue, click **Next**. The **Partitions - Step 5: Select Storage Slots** dialog box appears.

16 Storage slots are assigned by magazine. In the left column, select the location of one or more storage magazines.

17 To assign a storage magazine, select the appropriate check box. You can identify a magazine by its location coordinates. The number of slots available is determined by the drive media type.

18 If this is a standard partition and you are using Automated Media Pool (AMP), you can add logical element extensions to the partition for possible later use. Type the number of magazines by which you would like to extend the standard partition in the **Magazine Extensions** field. For more information, see Create Magazine Extensions in Standard Partitions on page 266.



19 To continue, click **Next**. The **Partitions - Step 6: Select I/E Slots** dialog box appears.

20 Select the location of one or more I/E station magazines.

a To assign an I/E station magazine, select the appropriate check box. You can identify an I/E station magazine by its location coordinates.

b Make sure that you select the appropriate module because the library can have I/E stations in the control module and expansion modules.

Note: The maximum number of I/E element addresses in any partition is 240. This includes both physical slots and Extended I/E virtual slots.

---

21 To continue, click **Next**.

Note: Depending on whether Extended I/E is enabled, **Step 6: Select Extended I/E Slots** may appear. If Extended I/E is enabled, go to Step 22. If Extended I/E is not enabled, go to Step 24.

To enable Extended I/E, go to **Setup > System Settings > Physical Library**, and select the feature. For more information about Extended I/E, see I/E Station Options on page 20.

---

22 In the **Partitions - Step 6: Select Extended I/E Slot**s dialog box, do the following:

a In the left column, select the location of one or more Extended I/E station magazines.

b To assign an Extended I/E station magazine, select the appropriate check box. You can identify an I/E station magazine by its location coordinates.

Note: The maximum number of I/E element addresses in any partition is 240. This includes both physical slots and Extended IE virtual slots.

---

23 To continue, click **Next**. The **Partitions - Summary Information** dialog box appears.

24 In the **Partitions - Summary Information** dialog box, verify that the parameters you set are correct.

To create the partition, click **Create**. The **Partitions - Completed** dialog box appears.

Note: After you click **Create**, the **Cancel** button becomes unavailable.

25 Review the information to make sure it is correct.

26 If you want to view the drive information after creating the partition, click **Next**.

27 Click **Finish**. The **Partitions** dialog box appears again with the partition you just created listed.

28 Click **Close**.

Modifying Partitions

You can use the **Modify** process to change the allocation of drives and storage magazines in existing partitions without having to delete the entire partition and then recreate it. You also can use **Modify** to change partition properties, partition settings and I/E elements.

Caution: Modifying partitions improperly, particularly when deleting partition elements, can disrupt host applications.

Before you modify any partitions, understand the configuration changes you plan to make and the potentially disruptive effects that those changes could have on the host application(s). Be careful whenever you add or delete partition elements that include drives, storage magazines, and I/E station magazines.

For best results, follow these guidelines when adding or deleting partition elements:

- Shut down the host application
- Update the inventory in the library
- Reconfigure the library in the application
- Update the inventory in the application

Note: This procedure includes instructions for downloading new drive firmware images. You can modify partitions from either the library's touch screen or a remote client. However, if you want to download drive firmware images, you must do so from a remote client.

To modify an existing partition, perform the following steps:

1. Log on as an administrator.
2. Make sure that you are viewing the physical library. From the **View** menu, click the name of the physical library.
3. Click **Setup > Partitions > Configure**. The **Partitions** dialog box appears.

   Note: If you want to cancel the partition modification process, click **Close**. The **Close** button becomes unavailable after you click **Modify** later in this procedure.

4. Select the partition you want to change, and then click **Modify**. The **Partitions - Step 1: Choose Partition Properties** dialog box appears.

   Note: For Library Managed Partitions, you cannot modify these properties; all options are disabled.

5. On this dialog box, you can modify the partition Name, Vendor ID, and Product ID.
6. To continue, click **Next**. The **Partitions - Step 2: Choose Policy Settings** dialog box appears.

   Note: For Library Managed Partitions, you cannot modify these properties; all options are disabled.

7. On this dialog box, you can modify the following settings:
   - For **Media Type Checking**, select either **Enable** or **Disable**. This setting is enabled by default.
   - From the **Media Checking Policy** drop-down list, click either **Required** or **Not Required**.

- From the **Return Media Identifier** drop-down list, click either **Suffix**, **Pass Through**, **Prefix**, or **Disabled**. Depending on which setting you choose, you can control the use of the media type identifier in the volume serial number that is returned to the host. When you have made your modifications, including adding or deleting elements, your proposed changes to the partition are highlighted in the **New Value** column of the table that appears on the **Partitions – Summary Information** dialog box.

  Caution: After a media volume serial number has been reported to a host, changing the **Return Media Identifier** setting could cause the host to not recognize media within the library.

  For more information about how media policies work, see Understanding Partition Media Policy Settings on page 121.

- For **Drive Cleaning**, click either **Enable** or **Disable**. This setting is enabled by default.

  Enabling drive cleaning allows the library to initiate drive cleaning each time a drive requests a cleaning operation. For drive cleaning to function, you must first configure drive cleaning for the library. For more information about configuring drive cleaning, refer Configuring Drive Cleaning on page 217.

  Note: Drive cleaning should be enabled for partitions only if the host application does not support the coordination of drive cleaning. If drive cleaning functionality is enabled on the host application, do *not* enable automatic drive cleaning for any partitions in the library.

8 To continue, click **Next**. The **Partitions - Step 3: Select Drives** dialog box appears.

  Note: If you are creating an Automated Media Pool (AMP) library managed partition or an Active Vault library managed partition, this screen is skipped because drives are not allowed in these partitions. Go to Step 16.

9 Select the location of one or more drives.

Make sure that you select the appropriate module because the library can have drives in the control module and in any of the expansion modules.

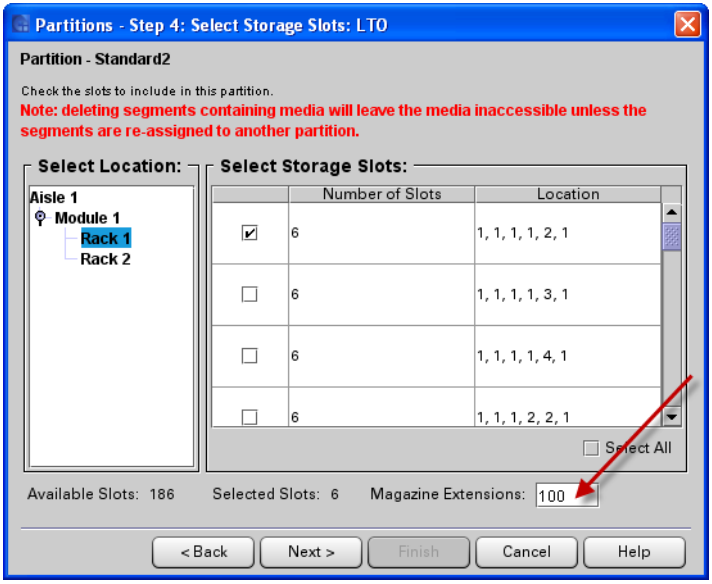
10 You can add a drive to the partition by selecting the appropriate drive check box. You can delete a drive from the partition by clearing the drive's check box. You can identify a drive by its serial number and location coordinates.

11 To continue, click **Next**. The **Partitions - Step 4: Select Storage Slots** dialog box appears.

12 Select the rack you want to modify.

13 You can add a storage magazine by selecting the appropriate check box. You can delete a storage magazine by clearing its check box. You can identify a storage magazine by its location coordinates.

14 If this is a standard partition and Automated Media Pool (AMP) is configured on the library, you can add virtual storage to the partition for possible use later by adding magazine extensions. Type the number of magazines to add in the **Magazine Extensions** field. For more information, see Create Magazine Extensions in Standard Partitions on page 266.



15 To continue, click **Next**. The **Partitions - Step 5: Select I/E Slots** dialog box appears.

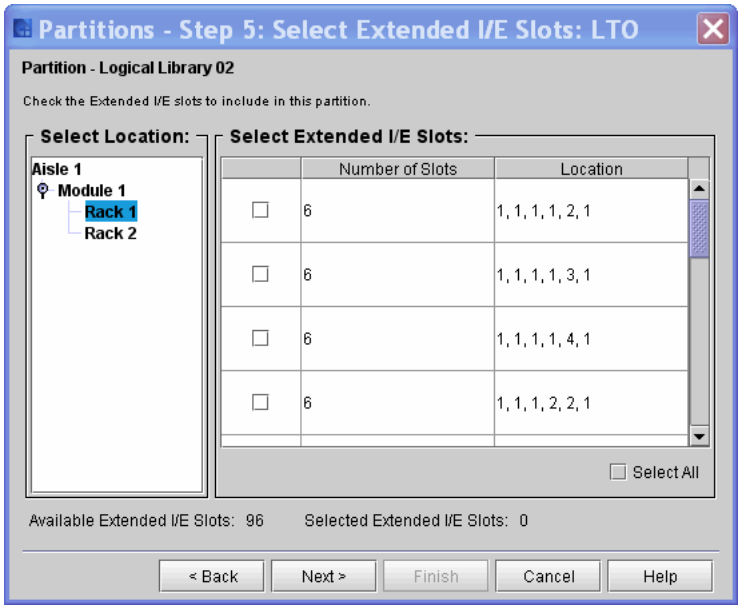
16 Select the location of one or more I/E station magazines.

- Make sure that you select the appropriate module because the library can have I/E stations in the control module and in expansion modules.
- You can add an I/E station magazine by selecting the appropriate check box. You can delete an I/E station magazine by clearing its check box. You can identify an I/E station magazine by its location coordinates.

Caution: If you delete magazines that contain media, the media will be inaccessible unless you reassign the magazines to another partition.

Note: The maximum number of I/E element addresses in any partition is 240. This includes both physical slots and Extended I/E virtual slots.

17 To continue, click **Next**. If Extended I/E is configured, the **Extended I/E Slots** dialog box appears.



Otherwise, the **Partitions - Step 6: Configure Drive Firmware Autoleveling** dialog box appears.

Note: The **Partitions - Step 6: Configure Drive Firmware Autoleveling** dialog box appears only if the drives are connected via an FC I/O blades or an Ethernet Expansion blade. If this dialog box does not appear, the **Partitions - Summary Information** dialog box appears instead. See Step 19 on page 143.

The **Partitions - Step 6: Configure Drive Firmware Autoleveling** dialog box enables you to set up drives to participate in autoleveling operations. Drives are autoleveled whenever they are reset, such as when the library is power cycled or rebooted.

18 To enable autoleveling for the partition, perform the following steps:

a From the **Drive Type** drop-down list, click the type of drives that you want to list in the table. Listed drive types use the following format:

<vendor>_<product>_<interface>

Drives of the specified type within the partition appear in the table.

Note: All drives of the specified type within the partition are listed, regardless of whether they are attached to an FC I/O blade or Ethernet Expansion blade.

If you need to download a new drive firmware image to use with drives that you want to participate in auto leveling operations, perform the procedure under Updating Drive Firmware on page 578, and then proceed with the next substep. Otherwise, proceed directly to the next substep.

After you download a new image, the new drive firmware version is automatically added to the **Firmware Version** drop-down list.

b In the left-most column of the table in the **Selected Drives will be Autoleveled** area, select one or more check boxes that correspond to drives that you want to update with the same drive firmware version, and then click the version in the **Firmware Version** drop-down list.

Note: Only drives that are attached to an FC I/O blade or an Ethernet Expansion blade can participate in drive firmware autoleveling operations.

19 To continue, click **Next**. The **Partitions - Summary Information** dialog box appears.

20 Verify that the parameters you set are correct.

21 If the summary information is correct, click **Modify**. The **Partitions - Completed** dialog box appears.

Note: After you click **Modify**, the **Cancel** button becomes unavailable.

22 Review the information to make sure it is correct.

23 If you want to view the drive information after modifying the partition, click **Next**.

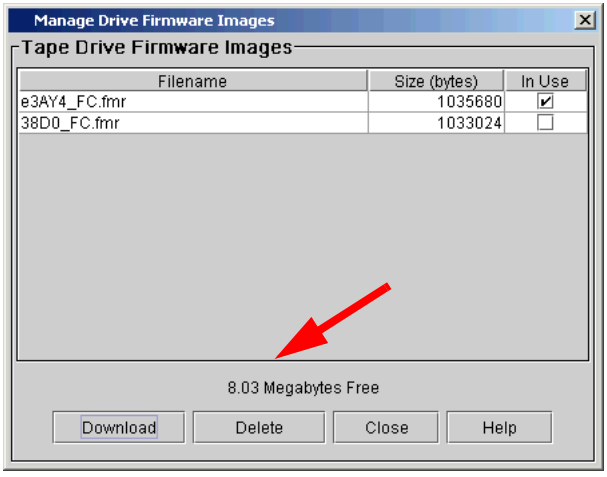
24 Click **Finish**. The **Partitions** dialog box appears again.

25 Click **Close**.

Downloading Drive Firmware for Autoleveling

Note: Before you begin the following procedure, make sure that you have obtained the new drive firmware image from Quantum technical support and placed it in an accessible location on your laptop.

1 On the **Partitions - Step 6: Configure Drive Firmware Autoleveling** dialog box, click **Manage Images**. The **Manage Drive Firmware Images** dialog box appears.



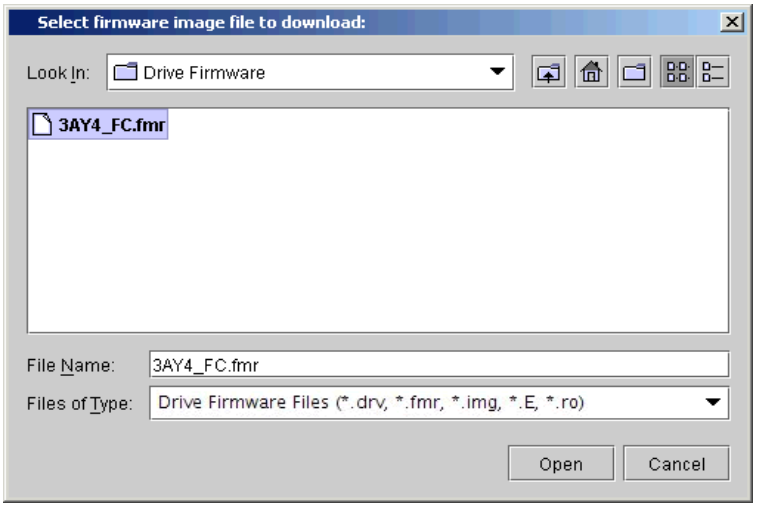
The library sets aside space for drive firmware. You can load multiple firmware images. The library screen indicates how much space is free. Quantum recommends you use the latest firmware available (as specified in the Release Notes). A check mark in the **In Use** column indicates one of the following conditions:

- An autoleveling policy exists that uses this drive firmware image.
- A pending autoleveling policy exists that uses this drive firmware image.
- A pending firmware update exists that uses this drive firmware image.

Under these conditions, you cannot delete the drive firmware image. If the check box for a drive firmware image is clear, you can

delete the image by clicking it to highlight it, and then clicking **Delete**.

2 To download a new drive firmware image, click **Download**. The **Select firmware image file to download** dialog box appears.



3 Navigate to the location of the drive firmware image file (with either a **.drv**, **.fmr**, **.img**, **.E,** or **.ro** extension) you want to download, and then click the image file to highlight it.

4 Click **Open**.

The download process copies the drive firmware image from the remote file system to the MCB. When the download process completes, the **Partitions - Step 6: Configure Drive Firmware Autoleveling** dialog box appears again.

Deleting Partitions

Caution: For the host application to have access to the written data on the partition that you want to delete, you must recreate a partition that includes the same media type, interface, I/E station magazines, and a host at the same SCSI ID and LUN.

To delete a partition, perform the following steps:

1 Log on as an administrator.

2 Make sure that you are viewing the physical library. From the **View** menu, click the name of the physical library.

3 Click **Setup > Partitions > Configure**. The **Partitions** dialog box appears.

4 Click the partition you want to delete.

Note: You can delete only one partition at a time.

5 Click **Delete**.

Note: If the physical library is not offline, you receive a message that asks you whether you want to take the library offline and delete the partition. Click **Yes**. If the partition is already offline, you receive a message that asks you whether you want to delete the partition. Click **Yes**.

6 The library deletes the selected partition. Repeat the process to delete another partition, or click **Close**.

Configuring Control Paths

You must define a control path for each library partition. The control path is used to connect a partition to a host application. The i6000 does not automatically assign a control path when you create a partition. Each partition control path can occur through one of several different physical connection points depending on the hardware configuration of your library.

The procedure for setting up and defining the control path for a partition depends on which physical connection point you choose to use. Table 26 describes how to set up different types of control paths.

Note: Only IBM and HP LTO-5 or LTO-6 drives can be configured for control path bridging (using a drive as the control path for a partition), and in order to do so, they must be connected to an Ethernet Expansion blade.

Note: Both IBM and HP LTO-5 or LTO-6 drives with SNW licenses can be configured for control path failover.

Note: A partition can be LUN mapped through any FC I/O blade, but you must manually configure LUN mapping to present the partition to specific hosts.

Caution: When configuring a control path using an FC I/O blade connection, the partition LUN can be presented multiple times through any FC I/O blade and even the MCB at the same time. In a direct attached control path configuration, you can choose the drive to present the partition and it remains dedicated to the drive until you change it to another drive.

Note: IO blades connected to drives configured with a control path may report certain library ready conditions differently than drives without a control path configured.

Table 26 Control Path Matrix

GUI Menu Path	Procedure References	MCB Direct Connection	FC I/O Blade Connection	LTO-5 or LTO-6 EEB Direct Connection[a]	LTO-5 or LTO-6 EEB Connection w/ SNW License[b]
Setup > Partitions > Configure	Creating Partitions on page 124	Step 1	Step 1	Step 1	Step 1
Setup > Blades > Connectivity	Configure FC I/O Blade Port Configuration on page 163 FC Host Port Failover on page 167 Enabling a Target Port on page 169 Configuring Datapath Conditioning on page 240		Step 2		
Setup > Blades Connectivity	Port Configuration on page 163	Step 2			
Setup > Blades > Access	FC Host LUN Mapping on page 199 Channel Zoning on page 198 Using the LUN Mapping Wizard on page 205	Step 3	Step 3		

GUI Menu Path	Procedure References	MCB Direct Connection	FC I/O Blade Connection	LTO-5 or LTO-6 EEB Direct Connection[a]	LTO-5 or LTO-6 EEB Connection w/ SNW License[b]
Setup > Drives > Access > SNW Wizard **~OR~** **Setup > Partitions > Control Path**	Use the Storage Networking Wizard on page 348 ~OR~ Configuring Control Paths on page 146			Step 2	Step 2
Setup > Drives > Access > SNW Wizard	License Drives for Path Failover on page 349				Step 3
Setup > Drives > Access > SNW Wizard	Configure Control Path on page 351				Step 4 (HP drives only)

a.Only IBM and HP LTO-5 or LTO-6 drives support control path bridging.

b.Only HP LTO-5 or LTO-6 Storage Networking licensed drives can be configured for control path failover. See License Drives for Path Failover on page 349.

Configuring an IBM or HP LTO-5 or LTO-6 Drive as the Control Path

You can configure IBM and HP LTO-5 or LTO-6 FC drives as the control path for a partition. The drive must not be connected to an FC I/O blade, but it must be connected to an Ethernet Expansion blade.

Note: The control path drive and control path failover settings are configured on the same screen. You do not need an SNW license to configure a drive for control path. However, you do need an SNW license to configure control path failover (see Configure Control Path on page 351).

The instructions that follow only describe how to configure a drive as the control path for a partition. If you would like to configure both the control path and control path failover, see Configure Control Path on

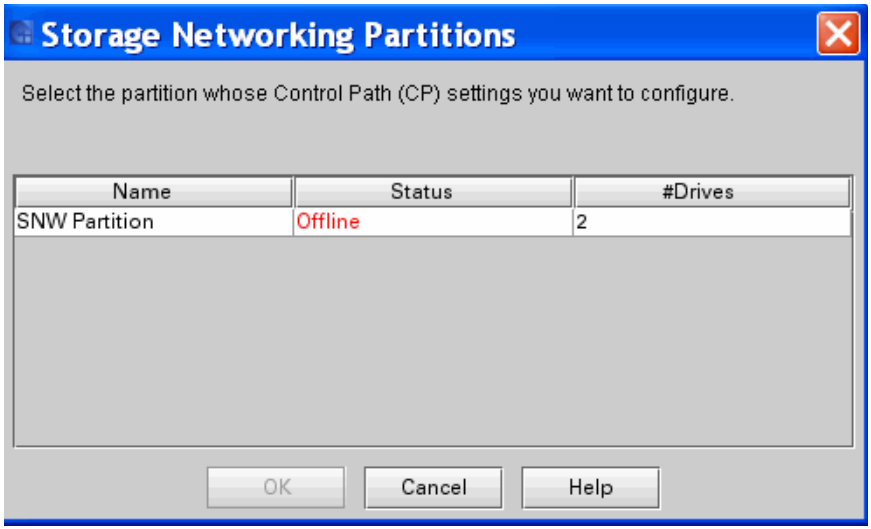
page 351 instead.

1 Log on as an administrator.

2 Access the appropriate screen in one of two ways:

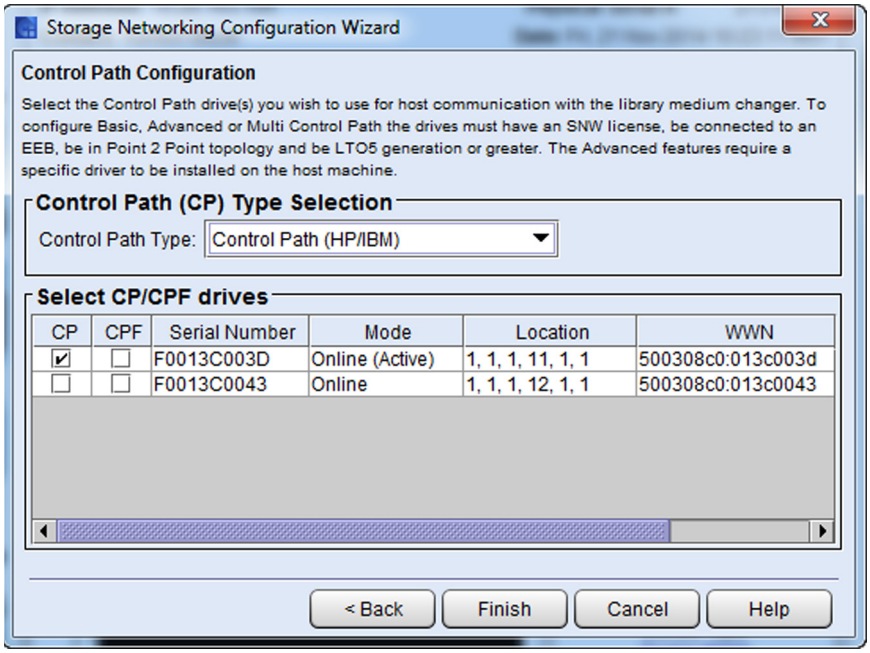
- Select **Setup > Partitions > Control Path** from the main console.
- Select **Setup > Drives > Access > SNW Wizard**. Click **Next**. From the Select Storage Networking Option screen, select **Control Path** and click **Next**.

  The **Storage Networking Partitions** dialog box appears, displaying all partitions that contain drives eligible to for control path bridging (HP LTO-5 or LTO-6 drives connected to an Ethernet Expansion blade).



3 Click to highlight the row containing the partition whose control path settings you want to configure.

4 Click **OK**. The **Control Path** dialog box appears.



5 From the **CP Drive** drop-down list select the drive you want to configure as the control path. The primary CP drive you selected is highlighted in yellow.

6 IN the CPF Mode area, select the radio button for the type of control path failover you want to configure.

Note: If you want to configure control path failover, you must have a SNW license with sufficient licensed drive counts to configure a CPF drive. For more information, see Configure Control Path on page 351.

7 Click **OK**. An **Operation in Progress** dialog box appears.

8 The control path drive is configured.

Setting Up the Network Configuration

If your library has an MCB2 installed, you can configure two (2) network settings for your library. When looking at the Setup > Network Settings menu, you'll notice two (2) interface options. Depending on what you have enabled, you'll see IPv4 or IPv6 listed.

The intended use of these settings is twofold:

- Interface 1 is for configuring a gateway to go outside the network.
- Interface 2 is for accessing devices on it's own network, encryption keys and for security. You cannot configure a gateway and cannot access any devices outside the network. You can access the library from a browser, however.

Make sure that your library is attached to a network before you use the **Network Configuration** command.

Caution: When configuring both interface settings, the IPs must be on separate subnets. If you configure the second interface with the same IP, you will not be able to save the configuration settings.

Caution: You must fully understand all network issues before you change the network configuration for an already configured library. It is recommended that you consult with your network administrator before changing your network configuration.

Note: To set up an iPv6 network connection, make sure that the **IPv6** option is enabled on the **Physical Library** dialog, as described in Setting Up Policies for the Physical Library on page 170.

Note: For all site-to-site customer firewall network settings, see Appendix B, Network Port Settings.

1 Log on as an administrator.

2 If you are not already working from the physical library, select the physical library from the **View** menu.

3 Do one of the following, depending on whether IPv6 is enabled or disabled and the protocol of the network connection you want to configure:

- **IPv4 Configuration** — Proceed to Setting up IPv4 Network Configuration on page 153.
- **IPv6 Configuration** — Proceed to Setting up IPv6 Network Configuration on page 157.

  Note: The IPv6 Configuration sub-menu only appears if you have enabled IPv6 for the physical library, as described in Setting Up Policies for the Physical Library on page 170.

- **DNS Configuration** — Proceed to Configuring DNS on page 160.

Setting up IPv4 Network Configuration

After completing the steps listed in Setting Up the Network Configuration on page 152, select **Setup > Network Configuration > Interface (#) > IPv4 Configuration**. The **IPv4 Network Configuration - Interface #** dialog box appears.

Figure 29 Network Configuration - Interface 1

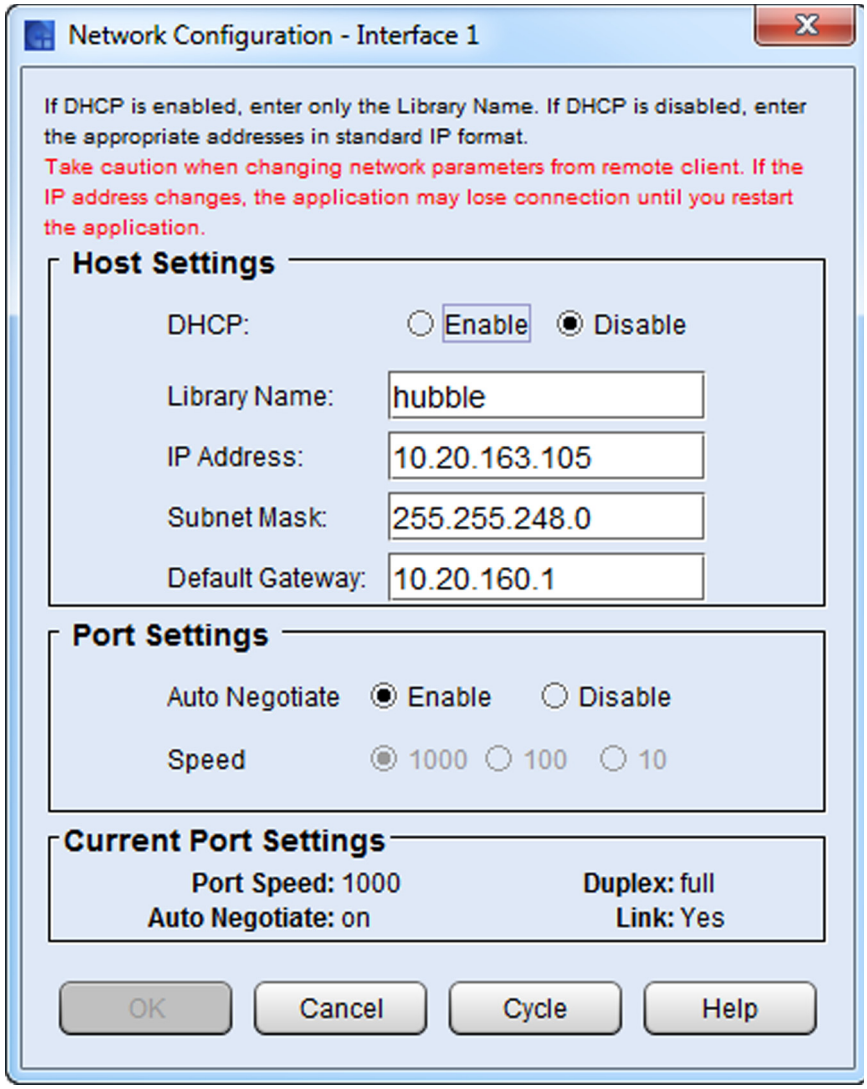
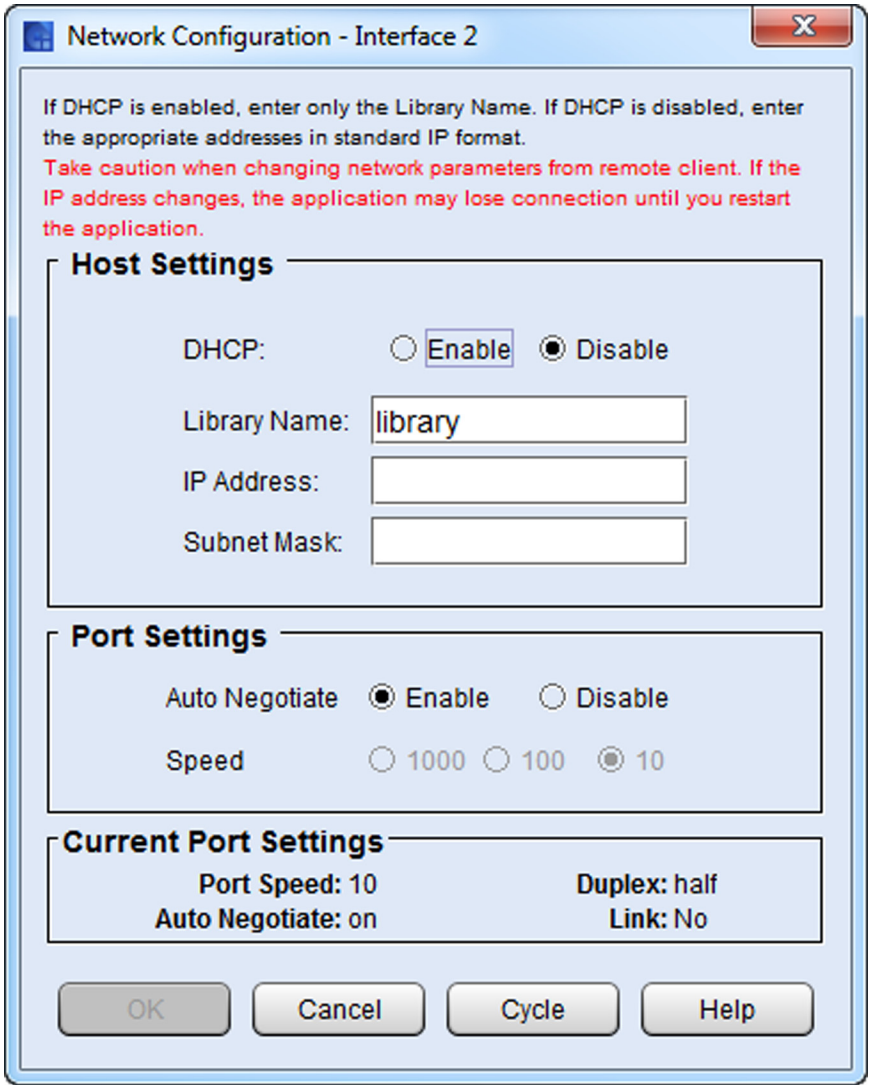


Figure 30 Network Configuration - Interface 2



4 Use the following table to assist you in completing the elements on the IPv4 **Network Configuration** dialog box.

Element	Description
In the **Host Settings** area:	
DHCP	If Dynamic Host Configuration Protocol (DHCP) is enabled on your network, do one of the following: • Select **Enable** to have DHCP automatically configure the library network settings. **Enable** makes the **IP Address**, **Subnet Mask**, and **Default Gateway** text boxes unavailable. • Select **Disable** to make the **IP Address**, **Subnet Mask**, and **Default Gateway** text boxes available for you to manually set the library network settings.
Library Name	The network name that you want to assign to the library.
IP Address	The IP address of the library. This text box is available only if **DHCP** is disabled.
Subnet Mask	The subnet mask. This text box is available only if **DHCP** is disabled.
Default Gateway	The IP address of the default gateway for your portion of the Ethernet network. This text box is available only if **DHCP** is disabled only for Interface 1.
In the **Port Settings** area:	
Auto Negotiate	• Select **Enable** to have the library automatically negotiate port speeds. **Enable** makes the **Speed** options unavailable. • Select **Disable** to make the **Speed** options available for you to manually set the port speed.
Speed	The port speed (10, 100 or 1000 Mbps). **Speed** options are available only if **Auto Negotiate** is disabled.

The current port settings are listed in the **Current Port Settings** section. For more information, see Viewing the Current Network Port Settings on page 161.

The **Cycle** button enables you to cycle the external Ethernet interface without rebooting the library.

5 Make the appropriate network configuration changes, and then click **OK**. A message appears that informs you that network connectivity will be lost temporarily, and asks whether you want to proceed.

6 Click **Yes**.

Setting up IPv6 Network Configuration

After completing the steps listed in Setting Up the Network Configuration on page 152, select **Setup > Network Configuration > Interface (#) > IPv6 Configuration**. The **IPv6 Network Configuration - Interface #** dialog box appears.

Figure 31 Network Configuration - Interface 1

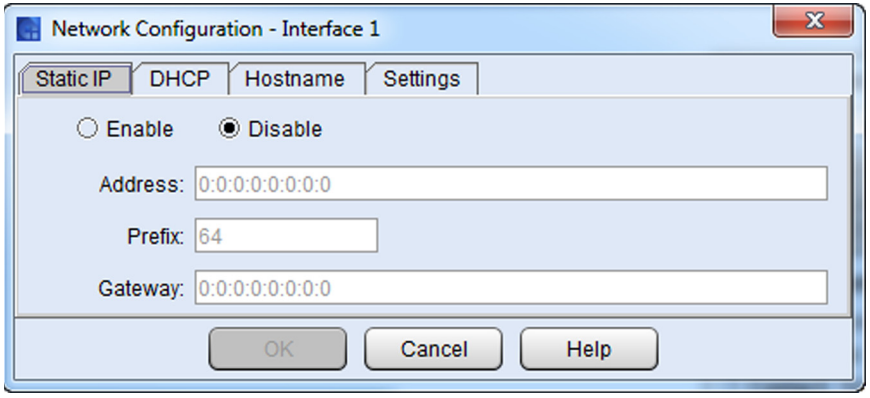
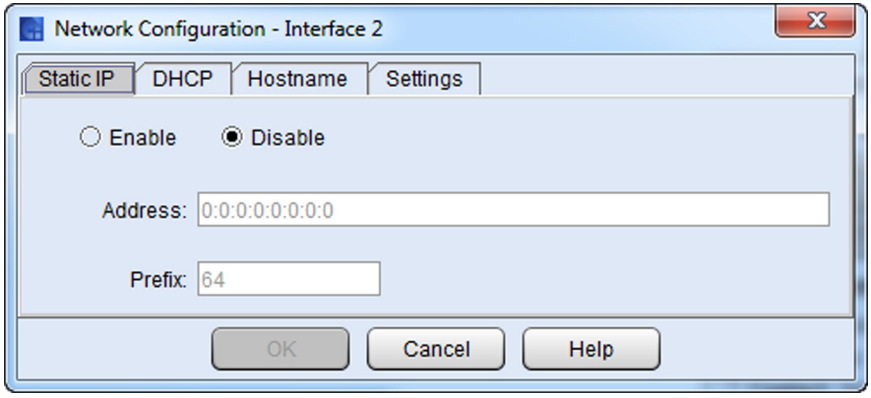


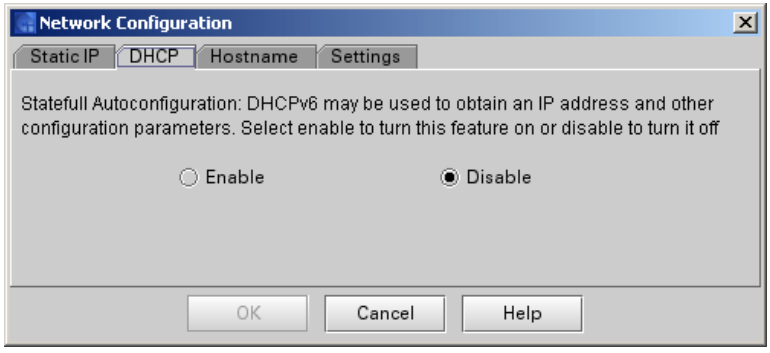
Figure 32 Network Configuration - Interface 2



7 Use the **Static IP** tab to disable or to enable and specify a static IP address. Valid static IP addresses include link local, site local, and global unchaste.

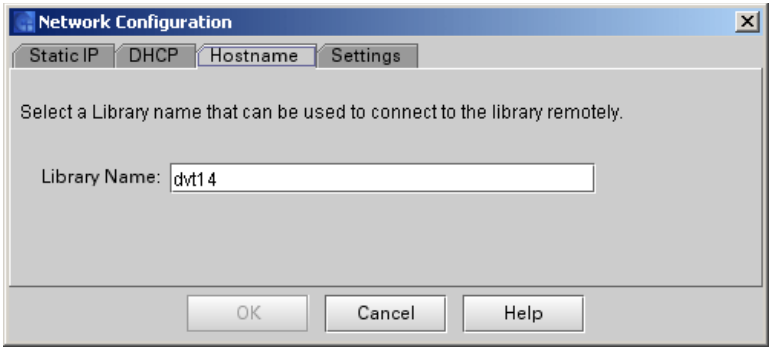
Caution: The IP address for Interface 2 must be on a different subnet than Interface 1.

8 Click **DHCP** to display the **DHCP** tab.



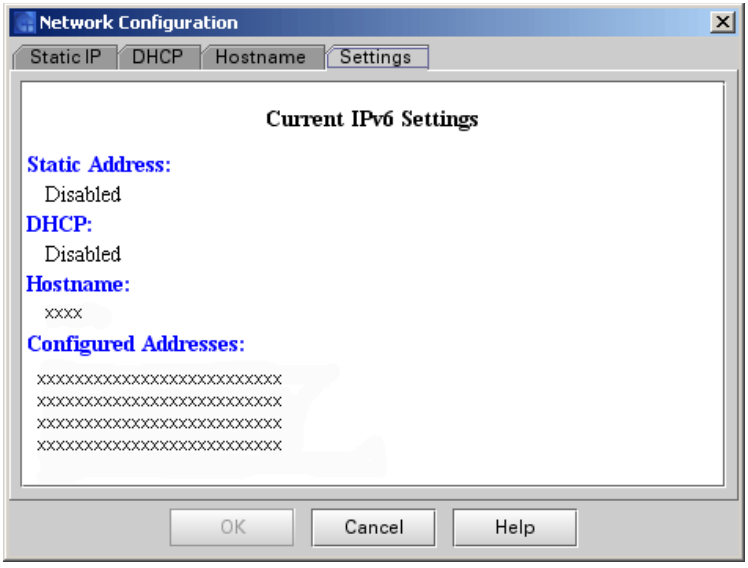
9 As prompted, use the **DHCP** tab to enable or disable the Dynamic Host Configuration Protocol (DHCP) auto configuration function.

10 Click **Hostname** to display the **Hostname** tab.



11 Use the **Hostname** tab to specify a library name that can be used for remote connections to the library.

12 Click **Settings** to display the **Settings** tab.



13 Use the **Settings** tab to view the current IPv6 configuration settings.

14 After you make the appropriate network configuration changes, click **OK**. A prompt appears informing you that network connectivity will be temporarily lost and asks whether you want to proceed.

15 Click **Yes**.

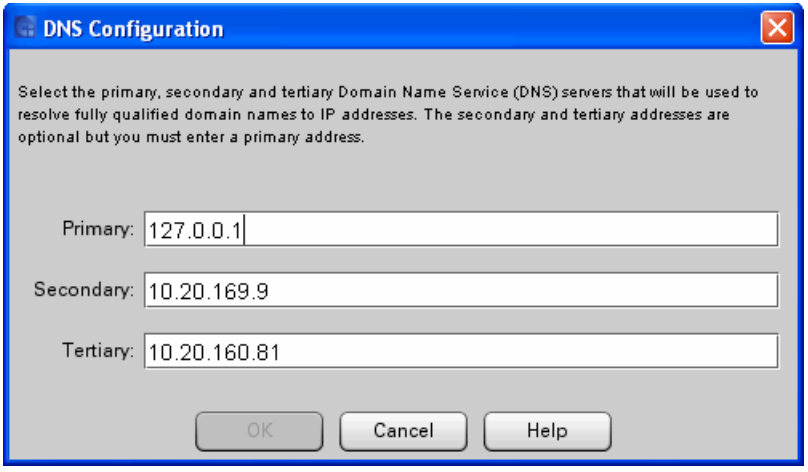
Configuring DNS

If DHCP is disabled, you can specify primary, secondary, and tertiary Domain Name System (DNS servers). DNS servers provide IP address resolution of fully qualified domain names. DNS settings are optional.

Caution: You must fully understand all network issues before you change the network configuration for an already configured library. It is recommended that you consult with your network administrator before changing your network configuration.

To configure DNS servers:

1. Log on as an administrator.
2. If you are not already working from the physical library, select the physical library from the **View** menu.
3. Click **Setup > Network Configuration > DNS Configuration**. The **DNS Configuration** dialog box appears.



4. Enter a primary DNS server IP address. Optionally, enter secondary and tertiary addresses.
5. Click **OK**.

Viewing the Current Network Port Settings

To view the current settings on the library's network Ethernet port, select **Setup > Network Configuration > IPv4 Configuration**. The Current Port Settings section of the dialog displays the following information:

- **Port Speed** — Current speed
- **Auto Negotiate** — On or off
- **Duplex** — Half or full
- **Link** — Indicates whether the Ethernet link is up (yes or no)

Changing the Internal IP Network Address

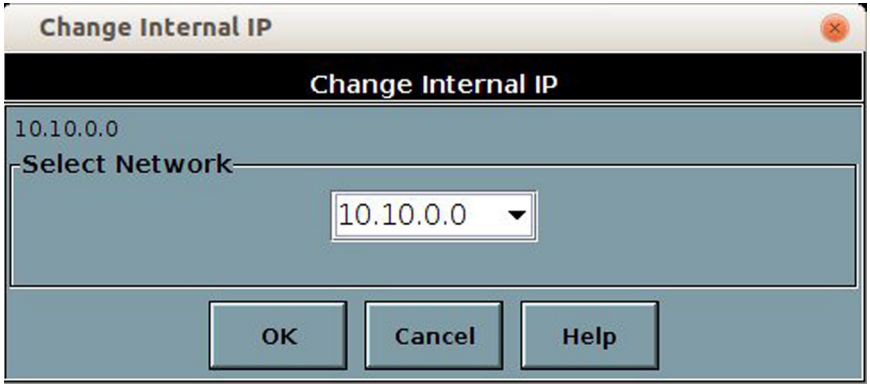
Note: The **Change Internal IP** dialog box is accessible only from the library's touch screen.

The default internal network subnet setting for the library is 10.20.X.X. Attaching the library to a 10.20.X.X external network can cause library and network problems. The **Change Internal IP** dialog box enables you to change the library's internal IP addressing so that conflicts do not occur.

Keep in mind the following considerations:

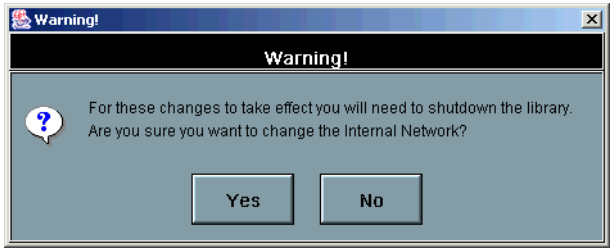
- You only need to change the default internal IP setting if your external network is 10.10.X.X.
- Do not set up internal IP addressing to conflict with existing external IP addressing. If you set up the same IP subnet for both the internal and external IP networks (for example, 10.10.X.X), the library will become unusable.
- If you change the internal IP addressing, and then later a user uses the **Network Configuration** dialog box (**Setup > Network Configuration**) to assign to the library a static IP address that conflicts with the internal network, the assignment request will fail and the library will issue a ticket.
- If you change the internal IP addressing, and if Dynamic Host Configuration Protocol (DHCP) is enabled and DHCP assigns to the library an IP address that conflicts with the internal network, address conflicts could occur between internal library devices and external customer devices and the library will issue a ticket.

1 From the local operator panel only, select **Setup > Network Configuration** > **Internal IP**. The **Change Internal IP** dialog box appears.



By default, the internal IP subnet address that is automatically selected on the **Change Internal IP** dialog box is not the one to which your internal network is currently set. In the example shown, the current internal network IP setting is 10.10.x.x,. The drop-down menu has multiple subnet options from 10.10.x.x to 10.90.x.x.

2 To accept the automatic internal IP setting, click **OK**. The following warning message appears.



Caution: Setting the internal IP network to be on the same subnet that the external IP network is on causes library failure and results in the management interface (the MCB) becoming unusable. For example, if you set 10.10.X.X as the internal IP network and your external IP network is also 10.10.X.X, a conflict occurs. If you are unsure about whether the change is appropriate, select **No**.

3 If you are sure that you want to make the change, select **Yes**.

4 After the library processes the request successfully, a message appears that asks you whether you want to shut down the library. You must shut down and restart the library in order for the changes to take effect.

Managing Connectivity

The **Connectivity** command on the **Setup** menu enables you to access three connectivity-related commands for the library: **Port Configuration**, **Datapath Conditioning**, and **FC Host Port Failover**.

For information about configuring data path conditioning monitoring levels and intervals, see Configuring Datapath Conditioning on page 240.

Port Configuration

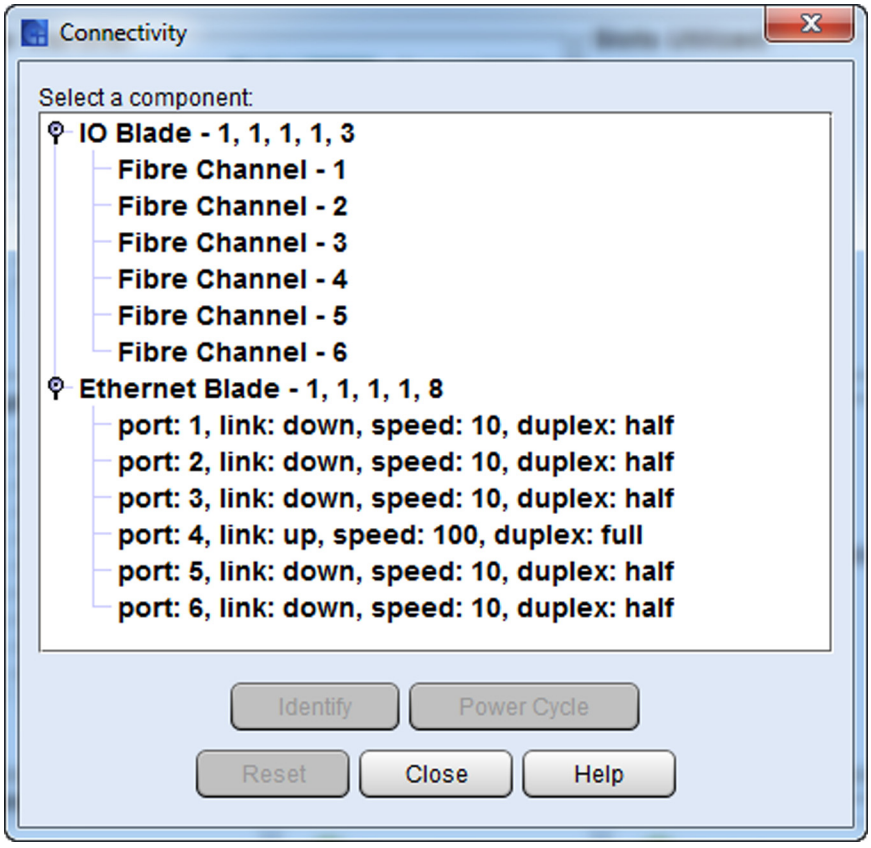
Use the **Port Configuration** command to view and configure connectivity parameters for FC ports. **Port Configuration** gives you access to the FC ports on the I/O blades.

Note: You can only view EEB port connection status and configure or view I/O blade port connections status.

1 Log on as an administrator.

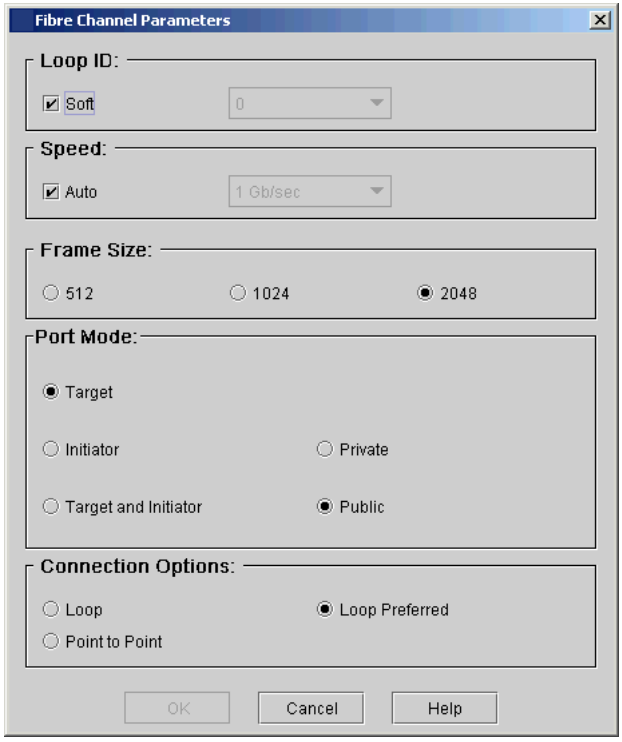
2 Make sure that you are viewing the physical library. From the **View** menu, click the name of the physical library.

3 Click **Setup > Blades > Connectivity > Port Configuration**. The **Connectivity** dialog box appears.



4 Click the highest-level items to show next-level items.

5 Click a port to highlight it, and then click **Configure**. For an FC port on an I/O blade, the **Fibre Channel Parameters** dialog box appears.



You can configure all settings for an I/O blade connection. The figure above shows an FC port configured for target mode and a loop preferred connection.

a In the **Loop ID** area of the **Fibre Channel Parameters** dialog box, repeatedly selecting **Soft** acts as a toggle, checking and clearing the box. If the box is not checked, you can click a hard loop ID (within the range from 0 to 125) from the drop-down list. Some operating systems require hard ID settings. Consult your service representative before making changes to this setting.

b Select **Auto** to automatically set the interface speed. To configure the speed manually, uncheck the **Auto** check box and use a setting from the drop-down list.

c FC **Frame Size** is specified by each receiving node and need not match any other node. The frame size is typically set to 2048. (You can use another frame size if it is required by a particular software application.)

d FC ports support **Private** and **Public** Fibre Channel attachments. The default port mode setting for FC ports 1 and 2 is **Target Public**, and the default port mode setting for FC ports 3 through 6 is **Initiator Public**. With **Public**, the loop is scanned for Fabric devices and allows the Fabric to have access to all available target devices that are attached to it. With **Private**, the local loop is scanned for devices except for Fabric devices. In **Target** mode, the port is set to receive connections from another FC initiator, such as a host or FC switch. In **Initiator** mode, the port scans for storage devices. In **Target and Initiator** mode, the port operates in both modes simultaneously.

e The default connection mode for both target and initiator ports is **Loop Preferred**. For target ports, other options include **Loop** and **Point to Point**. For initiator ports, other options include **Loop** and **Loop Preferred**. If you change a target port that is set to **Point to Point** to initiator mode, the port connection type automatically changes to **Loop Preferred**. Consult your service representative before making changes to this setting.

For reference purposes, the following table shows the default FC I/O blade port settings as initially set up at installation.

Table 27 FC I/O Blade Port Settings

Port	Loop ID	Speed	Frame Size	Port Mode	Connection Option	Private/Public
FC-1	Soft	Auto	2048	Target	Loop preferred	Public
FC-2	Soft	Auto	2048	Target	Loop preferred	Public
FC-3	Soft	Auto	2048	Initiator	Loop preferred	Public
FC-4	Soft	Auto	2048	Initiator	Loop preferred	Public
FC-5	Soft	Auto	2048	Initiator	Loop preferred	Public
FC-6	Soft	Auto	2048	Initiator	Loop preferred	Public

6 After you finish selecting the port configuration settings, click **OK**. A message appears that asks whether you want to make the change.

7 Click **Yes**.

FC Host Port Failover

Configure the optional FC Host Port Failover (HPF) feature so that an alternate "standby" target port on an I/O blade can assume the identity and LUN mapping configuration of the primary "active" target port if the primary port fails. HPF enables the library to continue operations without requiring you to reconfigure the host or the SAN.

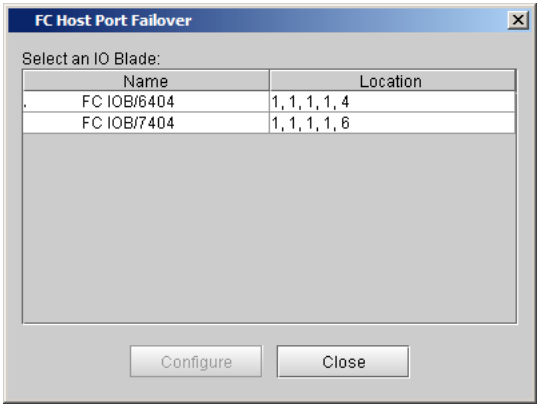
To enable HPF, you must make sure that two ports on the FC I/O blade are in target mode and point-to-point connection. Use ports 1 and 2, which are ports that are traditionally configured to be host targets. FC I/O blade ports are numbered from bottom to top as the blade sits in the I/O management unit.

Both ports must be attached to the same SAN fabric to provide host access. The active primary port is used for host communications, while the passive standby port is kept idle. The way that you configure the recovery settings determines how the failed port behaves after it is restored from a failed state.

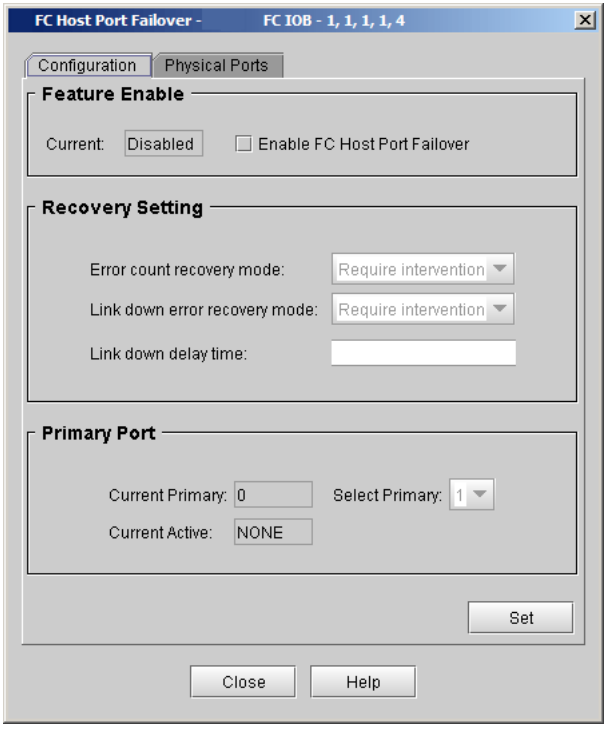
The library generates a ticket when port failover occurs. Examine the ticket and the repair page associated with the ticket to determine the reason for the failover.

To configure HPF, perform the following steps:

1. Log on as an administrator.
2. Make sure that you are viewing the physical library. From the **View** menu, click the name of the physical library.
3. Confirm that there are two ports on the I/O blade in target mode and point-to-point connection. For more information, see Port Configuration on page 163.
4. Click **Setup > Blades** > **Connectivity > FC Host Port Failover**. The **FC Host Port Failover** dialog box appears, showing all the FC I/O blades found in the library. Each blade is identified by name and by location.



5 Click a blade to highlight it, and then click **Configure**. The **FC Host Port Failover** dialog box appears



6 In the **Feature Enable** area, select **Enable FC Host Port Failover**, and then click **Set** to make the **Configuration** tab available.

On the **Configuration** tab, settings are unavailable if the current state of the tab is set to **Disabled**.

Be aware that there might be incompatibilities with channel zoning configuration on the I/O blade if you enable host port failover.

7 Accept the recovery setting default values unless an authorized representative advises you otherwise.

8 Before you set recovery settings, understand the following elements in the **Recovery Setting** area:

- **Error count recovery mode** sets the recovery scenario for all ports when port failure is caused by excessive errors on the port. The only setting option is **Require Intervention**.
- **Link down error recovery mode** sets the recovery scenario for all ports when port failure is caused by the port going offline for more time than the threshold specified in the **Link down delay time** text box. The only setting option is **Require Intervention**.
- **Link down delay time** sets the timeout threshold before link down status applies. The default value is zero (0) seconds. There is no maximum value. **Require Intervention** means that a user must manually use the **Physical Ports** tab to bring a failed port that has recovered back online.

9 Configure the **Primary Port**. Only ports that are in target mode and point-to-point connection can participate in host port failover. The primary port becomes active by default and the alternate port will go on passive standby until a failover occurs. Use the **Select Primary** drop-down list to select from the target ports that are online and available. You must select a primary port. **Current Active** indicates the currently active port.

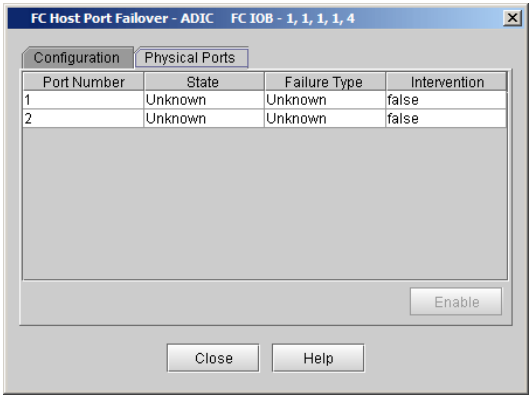
10 Click **Set**. If your configuration has errors, a warning message appears.

Enabling a Target Port

Use the **Physical Ports** tab to manually enable an online target port that was disabled because of a previous connection error. If the **Intervention** column displays “true,” you must manually bring the recovered port back online using **Enable**. If the port state is “disabled,” the port's connection is repaired and it is ready to be re-enabled. If the **Configuration** tab itself is disabled, the table on the **Physical Ports** tab will be empty.

Note: If the target port state is offline, the port's connection has not been repaired. The error condition that caused the port to fail still exists.

On the **FC Host Port Failover** dialog box, click the **Physical Ports** tab. The dialog box shows you each target port on the I/O blade, the port's state, and the type of failure that has occurred, if applicable.



11 Click the port you want to enable.

12 Click **Enable**.

Note: **Enable** is available only if the port is disabled.

13 To return to the main **FC Host Port Failover** dialog box, click **Close**.

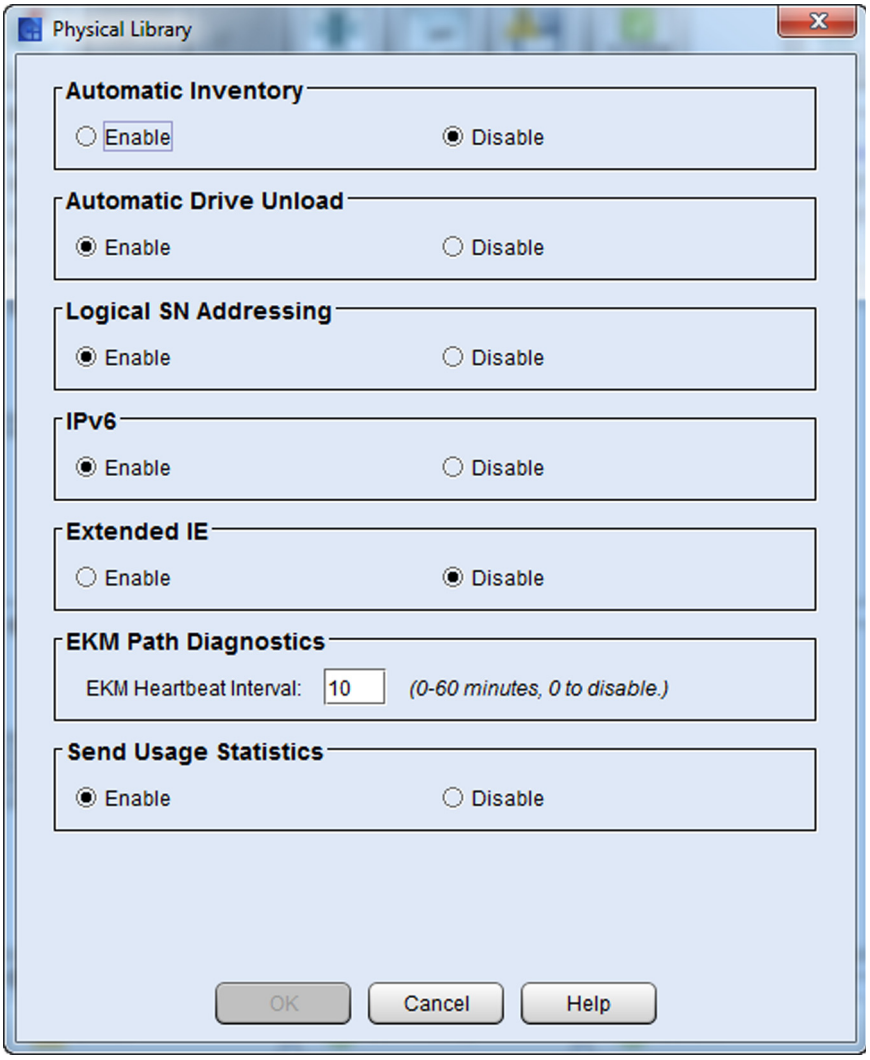
Setting Up Policies for the Physical Library

The **Physical Library** dialog box enables you to configure various operating modes:

Policy	Settings
Automatic Inventory	**Enabled**: automatically inventories all library content whenever the library powers up or when a main library access door closed and robotics are enabled (except for UI initiated Aisle Access or Robot Replacement operations). In this mode, individual I/E stations are always scanned upon I/E station door closure detection, and individual tower modules will automatically be scanned if varied on after a tower door closure, independent of the tower having a scanner installed or not. **Disabled (default)**: requires the user to initiate inventory scan operations whenever the tape cartridge inventory is manually manipulated in drives, linear storage magazines, and tower modules without scanners while the library is powered off or a library access door is opened and closed. In this mode, only I/E stations and tower modules with scanners are automatically scanned upon library power-up, and also scanned when an I/E station door is closed or a tower module with an installed scanner is varied on after a tower door closed. **Note:** Tower modules with configured but inoperable scanners will be scanned by a robot. Tower modules without scanners will not be inventoried.
Automatic Drive Unload	**Enabled (default)**: will automatically initiate unload operations to a drive if a SCSI move request is received and the drive is not already unloaded. **Disabled:** Drives need to be unloaded by allocated host applications. SCSI move requests from drives that are not already unloaded will fail.
Logical SN Addressing	**Enabled (default):** Drive are configured to report a library unique, drive position unique drive serial number. This methodology allows drive replacements without affecting host configured drive serial number re-configurations as the repeated drive serial number will not change if a drive is replaced. **Disabled:** Installed drives report their physical serial number to attached hosts. Drive replacement operations will cause the replacement drive to report its assigned physical serial number and host applications may have to re-configure drive support if the drive serial number changes.

Policy	Settings
IPv6	**Enabled:** will support the configuration of IPv6, as well as IPv4, network settings. **Disabled (default):** will not support the configuration of IPv6 network settings and only allow IPv4 network configuration.
Extended I/E	**Enabled:** will support the configuration of storage slots as I/E slots, extending the number of available I/E slots for host configurations that require non-I/E elements not physically provided in I/E stations. **Disabled (default):** will not allows I/E slot extensions to be configured.
EKM Path Diagnostics	**Enabled (default):** EKM server connectivity and functionality are performed in regular intervals to alert of connectivity or operational issues. **Disabled:** EKM path connectivity and functionality tests are not performed.
Send Usage Statistics	**Enabled (default):** If e-mail notification settings are configured, library usage and performance data will be sent to Quantum for statistical review purposes. **Disabled:** Usage statistics are not sent regardless of e-mail notification settings.

1. Log on as an administrator.
2. Make sure that you are viewing the physical library. From the **View** menu, click the name of the physical library.
3. Click **Setup > System Settings > Physical Library**. The **Physical Library** dialog box appears.



4 Select **Enable** in the **Automatic Inventory** area to schedule automatic inventories of library contents when the library powers up or when the library door is opened and closed.

Note: **Automatic Inventory** is disabled by default.

5 Select **Enable** in the **Automatic Drive Unload** area to cause the library to issue unload commands when host applications issue move media commands to the library. If you set this to **Disable**,

proper library operation requires host applications to issue unload commands to the drives. **Automatic Drive Unload** is enabled by default.

Note: The Logical SN Addressing area is available only to CSEs. You cannot enable or disable logical serial number addressing for drives. If a CSE enables this feature, the library assigns logical serial numbers to all drives in the library. Specifically, the library assigns a logical serial number to a drive in a specific location. This is not the serial number of the particular drive. If a drive is replaced by another drive in the same library location, the logical serial number remains the same. From the host's perspective, the replacement drive is the same as the original one.

6 Select **Enable** in the **IPv6** area to enable the **Network Configuration** dialog that you can use to configure the settings for an IPv6 network connection.

Note: **IPv6** is disabled by default.

Note: Enabling **IPv6** adds a sub-menu to the **Network Configuration** command on the **Setup** menu that you use to display the IPv4 or IPv6 **Network Configuration** dialog.

7 Select **Enable** in the **Extended I/E** area to enable the Extended I/E feature.

Note: **Extended I/E** is disabled by default.

Note: Extended I/E allows the user the capability to increase the number of I/E slots presented to the host. For more information, refer to I/E Station Options on page 20

8 Select **Enable** in the **EKM Path Diagnostics** area to enable Encryption Key Management background diagnostics.

The diagnostics test determines whether the EKM servers are connected and operating properly. The test runs in the background at regular intervals and generates a RAS ticket if key server connectivity issues are found. For more information about the tests included in the diagnostics, see Using EKM Path Diagnostics on

page 302.

Default configurations are as follows:

- **Q-EKM** — Not available.
- **SKM** — Enabled by default. You can disable it for SKM but it is not recommended unless directed by a service technician. The background diagnostic should always be enabled so the library can monitor SKM server status and report issues as soon as they arise.
- **RKM** - Enabled; cannot be disabled.
- **KMIP** key managers - Enabled; cannot be disabled.

9 When finished, click **OK**.

Specifying the Date and Time

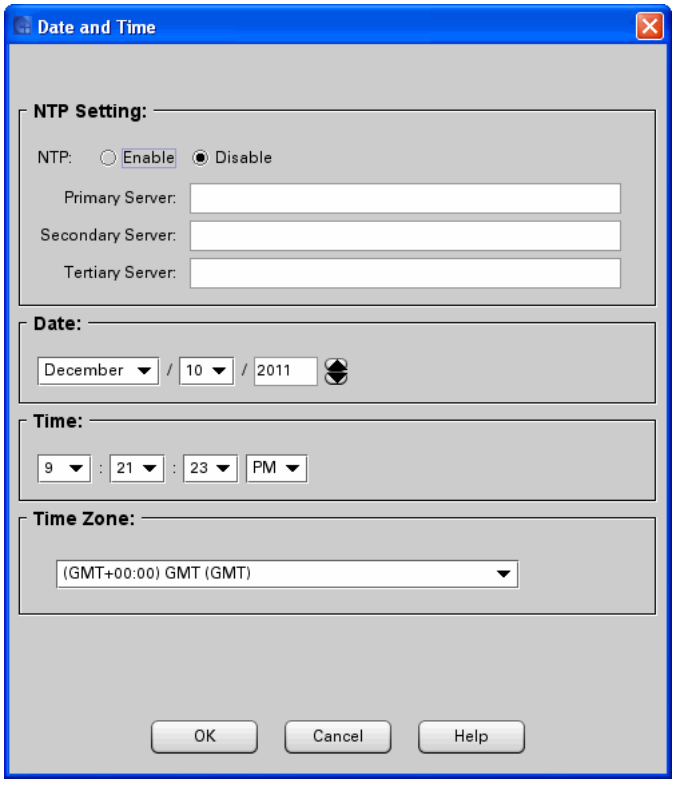
You can use the **Date and Time** command to set or reset the system time. If you want to synchronize the library over a network, you can use the Network Time Protocol (**NTP**) setting. The default date and time is Greenwich Mean Time (GMT).

To set the date and time or to use NTP:

1 Log on as an administrator.

2 Make sure that you are viewing the physical library. From the **View** menu, click the name of the physical library.

3 Click **Setup > Date and Time**. The **Date and Time** dialog box appears.



4 In the NTP section

- If you choose to enable NTP, click **Enable**.

  The **Date and Time** sections of the dialog box are grayed out.

- Type valid IP addresses for the **Primary Server** and optionally the **Secondary Server** and **Tertiary Server**.

  - If the DNS Server has not been configured in the LMC, type valid numeric IP addresses that are accessible from the library (example 111.11.11.111). Go to step 7.

  - If the DNS Server has been configured through the LMC (**Setup > Network Configuration > DNS Configuration**), type the valid alpha/numeric IP Addresses that are accessible from the library. Go to step 7.

- If NTP is enabled and you no longer want to use this setting, click **Disable**.

If you choose to disable NTP, you must manually set the date and time. Go to the next step.

5 Use the **Date** drop-down lists to select the month, date, and year.

6 Use the **Time** drop-down lists to select the hour, minute, and whether the time is A.M. or P.M.

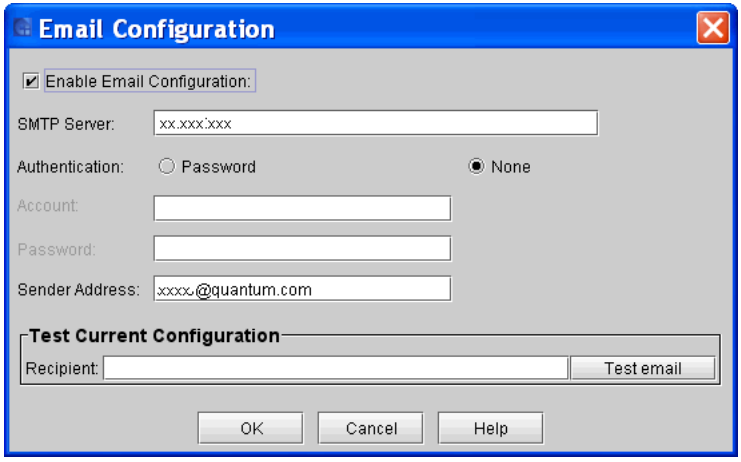
7 Use the **Time Zone** drop-down list to select the appropriate time zone.

The default time zone is GMT. The time zone that you select appears only on your library information panel. Regardless of your selection, the system operates on the GMT zone.

8 Click **OK**.

Configuring E-mail

The library uses the e-mail settings on the **Email Configuration** dialog box whenever library e-mail services are used, such as when you use the **Send** command to e-mail snapshots or logs and when the library automatically sends e-mail notifications of library problems.



Use the procedures in the following subsections for:

- Setting Up or Changing the E-Mail Configuration on page 178
- Testing the Current E-Mail Configuration on page 179

Note: Any undeliverable emails will be sent to the email address listed in the Contact Information tab of the System Setup Notifications dialog. See Setting Up E-mail Notifications on page 180.

Setting Up or Changing the E-Mail Configuration

To set up or change the e-mail configuration:

1. Log on as an administrator.
2. Make sure that you are viewing the physical library. From the **View** menu, click the name of the physical library.
3. Click **Setup** > **Email Configuration**. The **Email Configuration** dialog box appears.
4. In the **SMTP Server** text box, type the iPv4 or iPv6 address of the SMTP server (for example, 192.16.96.201).

   Caution: You must identify the SMTP server by its server address.

5. If your SMTP server requires authentication of accounts and passwords, select **Password** in the **Authentication** field. If it does not, select **None**.
6. In the **Account** text box, type the name of a valid account on the SMTP server (for example, Jay.User).

   Note: The **Account** text box is not available if **None** is selected in the **Authentication** field.

7. In the **Password** text box, type the password for the account that you specified in the **Account** field.

   Note: The **Password** text box is not available if **None** is selected in the **Authentication** field.

8. In the **Sender Address** text box, type an e-mail address for the library (for example scalari6000@mycompany.com).

The library uses this address in the **From** field of e-mail messages that it sends out, indicating the originator of the message. For example, if you type **scalari6000**, the library appends the domain information (for example, **@mycompany.com**). If you type **scalari6000@mycompany.com**, the library does not append any additional information.

9 To test the e-mail configuration, type an e-mail address in the **Recipient** box of the **Test Current Configuration** area and click **Test email**.

10 Confirm that the library displays a message indicating that the test completed successfully and sends a test message to the specified e-mail address.

The subject of the test message should be **Test email from Scalar i6000** and the message text should include the library name, version, and serial number, along with the date and time that the message was sent.

11 To finish, click **OK**.

Testing the Current E-Mail Configuration

To test the current e-mail configuration:

1 Log on as an administrator.

2 Make sure that you are viewing the physical library. From the **View** menu, click the name of the physical library.

3 Click **Setup > Email Configuration**. The **Email Configuration** dialog box appears.

4 Type an e-mail address in the **Recipient** box of the **Test Current Configuration** area and click **Test email**.

5 Confirm that the library displays a message indicating that the test completed successfully and sends a test message to the specified e-mail address.

The subject of the test message should be T**est email from Scalar i6000** and the message text should include the library name, version, and serial number, along with the date and time that the message was sent.

6 Click **OK** to close the **Email Configuration** dialog box.

Setting Up E-mail Notifications

You can set up notifications in the LMC so that the library automatically sends an e-mail message to specified e-mail addresses whenever an issue of a particular severity level occurs. The information in the e-mail notification provides details about the issue and the library conditions at the time of the error.

Note: Before you set up notifications, you must configure e-mail in the LMC so that the library can send notifications to the recipients. See Configuring E-mail on page 177.

Table 28 describes the severity levels for which the library can send notifications if e-mail addresses are set up appropriately to receive them.

Table 28 Severity Levels Assigned to Issues

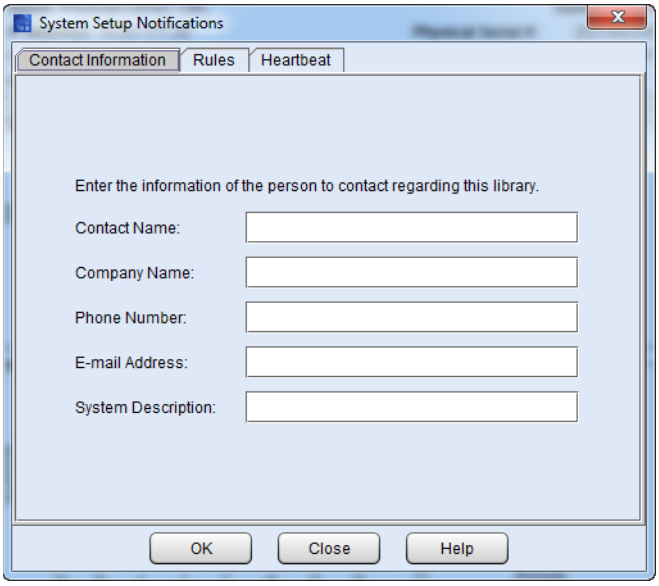
Severity Level	Description
1 (Failed)	Indicates that a failure has occurred or a different serious condition exists within a library subsystem that requires immediate corrective action. In most cases, a hardware component is no longer functioning at an acceptable level or has failed. Typical library operations are either impossible or highly unreliable. Examples of failure situations include a FRU that is not functioning, a temperature threshold that has been reached that causes unreliable operations, or a partition that the library has automatically taken offline.
2 (Degraded)	Indicates that a degraded condition exists within a library subsystem that impacts system performance or redundancy. Typical library operations can continue without immediate corrective action, but an administrator should investigate the condition and correct the problem soon. Examples of degraded situations include a redundant power supply that has failed or a connectivity problem that has caused host port failover to occur.

Severity Level	Description
3 (Warning)	Indicates that a condition exists within a library subsystem that has little effect on system operations. Typical library operations can continue without immediate corrective action, but you should investigate the condition and correct the problem when possible. Warnings also can provide helpful information, such as indicating that a door is open. Examples of warning situations include a FRU that is functioning less reliably or a temperature threshold that has been reached that does not affect reliable operations.

The body text in the e-mail notification provides details about the issue and library conditions at the time of the event. The e-mail notification also includes an attachment, referred to as a repair page, that provide a problem description and corrective actions you or a customer service engineer (CSE) can perform. For more information about e-mail notifications, see E-mail Notifications on page 39.

To set up e-mail recipients for notifications, perform the following steps:

1. Log on as an administrator.
2. Make sure that you are viewing the physical library. From the **View** menu, click the name of the physical library.
3. Click **Setup > Notifications > System Setup**. The **System Setup Notification** dialog box appears with the **Contact Information** tab displayed.



4 Enter the contact information you want included in an e-mail notification if an error occurs in the library.

5 Click **OK**. A message is displayed asking you to perform a Save Configuration operation.

6 Click **Yes**. The **Save and Restore Library Configuration** dialog box appears.

7 Click **Save** and then save the file to a desired location. The configuration is saved.

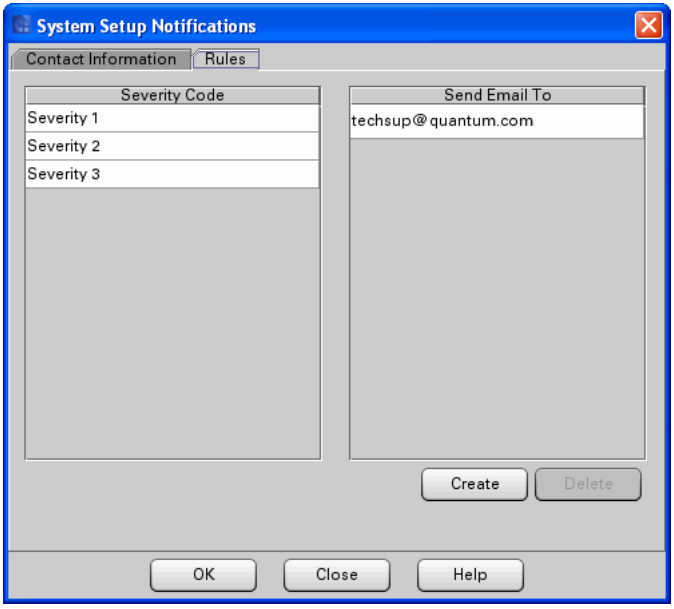
8 Click **Close**.

9 Set up the rules.

   a Click **Setup > Notification > System Setup**. The **System Setup Notification** dialog box appears with the **Contact Information** tab displayed.

   The **Notification** dialog box displays the **Rules** tab.

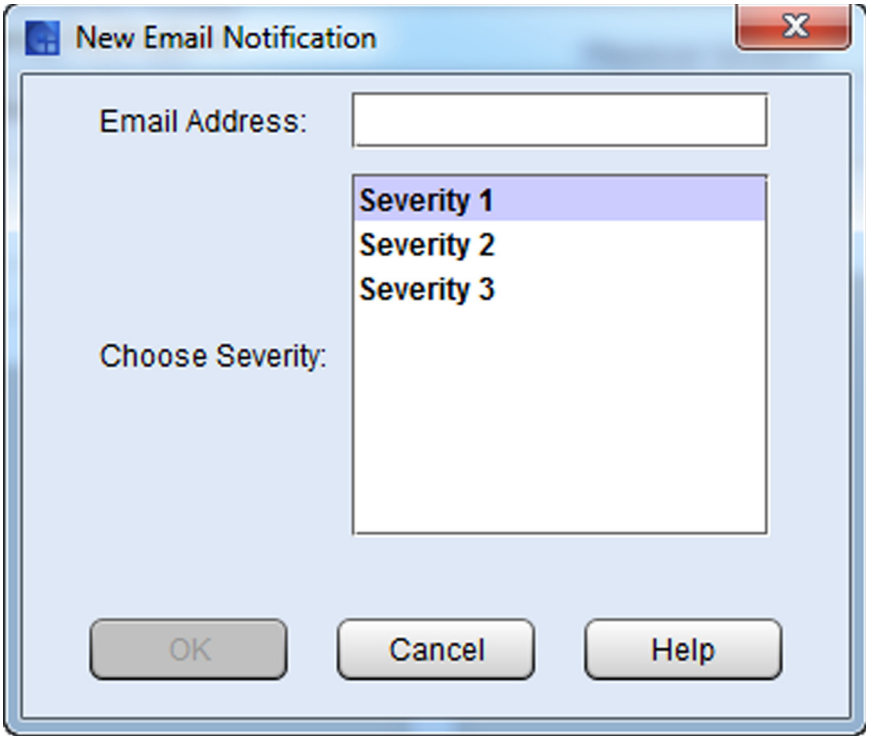
   This dialog box shows all notification recipients that are set up currently in the LMC. By default, the only e-mail address to which the library sends e-mail notifications (severity level 1 [Failed] issues only) is techsup@quantum.com (Quantum technical support), as shown in this **Notification** dialog box example.



Note: Even though you can remove the Quantum technical support e-mail address so that Quantum does not receive severity level 1 notifications, Quantum recommends that you do not remove it. Also, do not include the Quantum technical support e-mail address for severity level 2 or 3 notifications.

Note: The remaining steps in this procedure guide you through setting up new e-mail notification recipients. To delete an existing e-mail address, click the e-mail address in the **Send Email To** column, and then click **Delete**.

10 To set up a new e-mail notification recipient, click **Create**. The **New Email Notification** dialog box appears.



11 In the **Email Address** text box, type the e-mail address to which you want to send notifications.

Note: Do not enter more than one address in the **Email Address** text box. Continue to Step 7 and Step 8 for this address, and then repeat Step 5 through Step 8 for each additional address.

---

12 In the **Choose Severity** box, click the severity level you want to assign to this e-mail address.

Note: If you are using the remote client LMC, you can assign more than one severity level. While pressing the **Ctrl** key, click the severity levels you want to assign. The touch screen on the library enables you to select only one severity level.

---

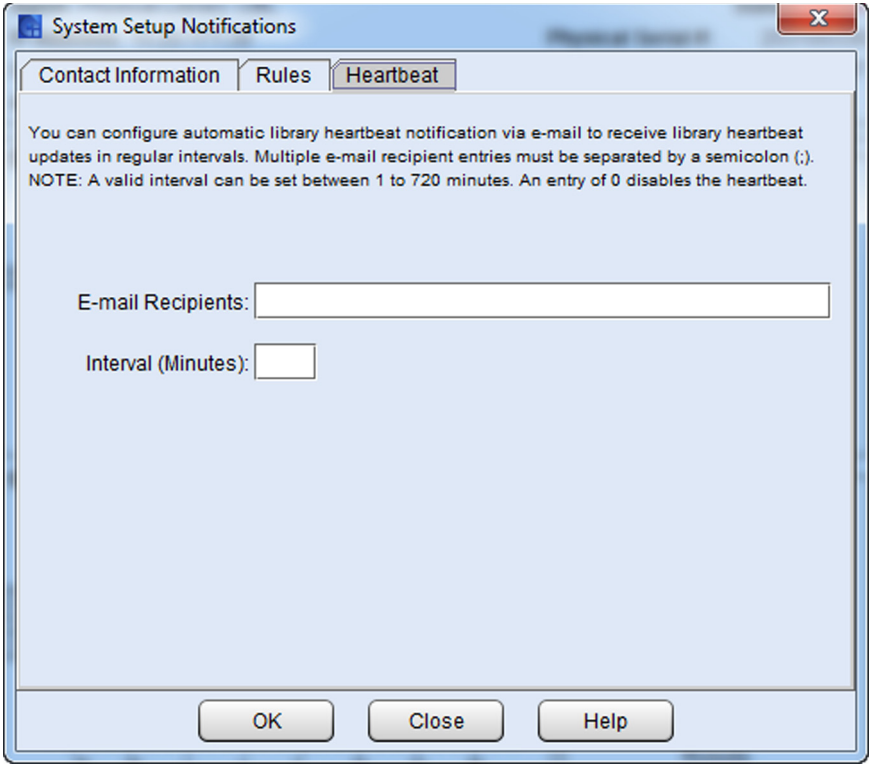
13 To accept this notification setup, click **OK**. The **System Setup Notification** dialog box reappears.

14 Setup the heartbeat.

a Click **Setup > Notification > System Setup**. The **System Setup Notification** dialog box appears with the **Contact Information** tab displayed.

The **Notification** dialog box displays the **Heartbeat** tab.

This tab allows users to assign an email address to notify someone of the status of the library at regular intervals. Users can designate the interval in minutes.



15 After you finish setting up all notifications, click **OK**.

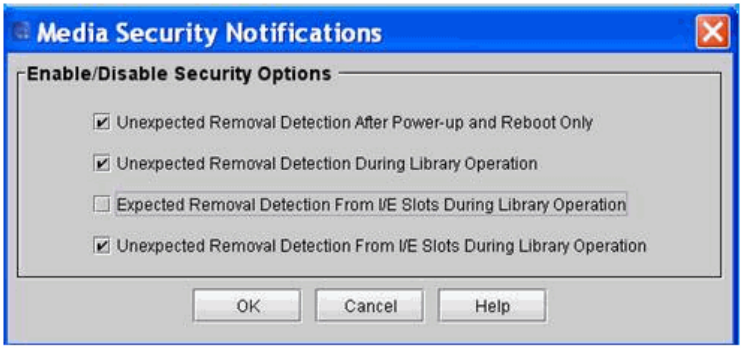
Setting Up Media Security Notifications

Note: You need an Advanced Reporting License installed on the library in order to use media security notifications. See Enabling Licenses on page 115.

You can configure the library to automatically notify you via a RAS ticket when media is moved in or out of the library, either intentionally or unintentionally. First, you must choose under which circumstances you wish to be notified, and then you must enable automatic inventory on the library.

1 Log on as administrator.

2 Click **Setup > Notifications > Media Security**. The **Media Security Notifications** dialog box appears.



3 Check the box to the left of your media security notification choices. You can select as many as you want:

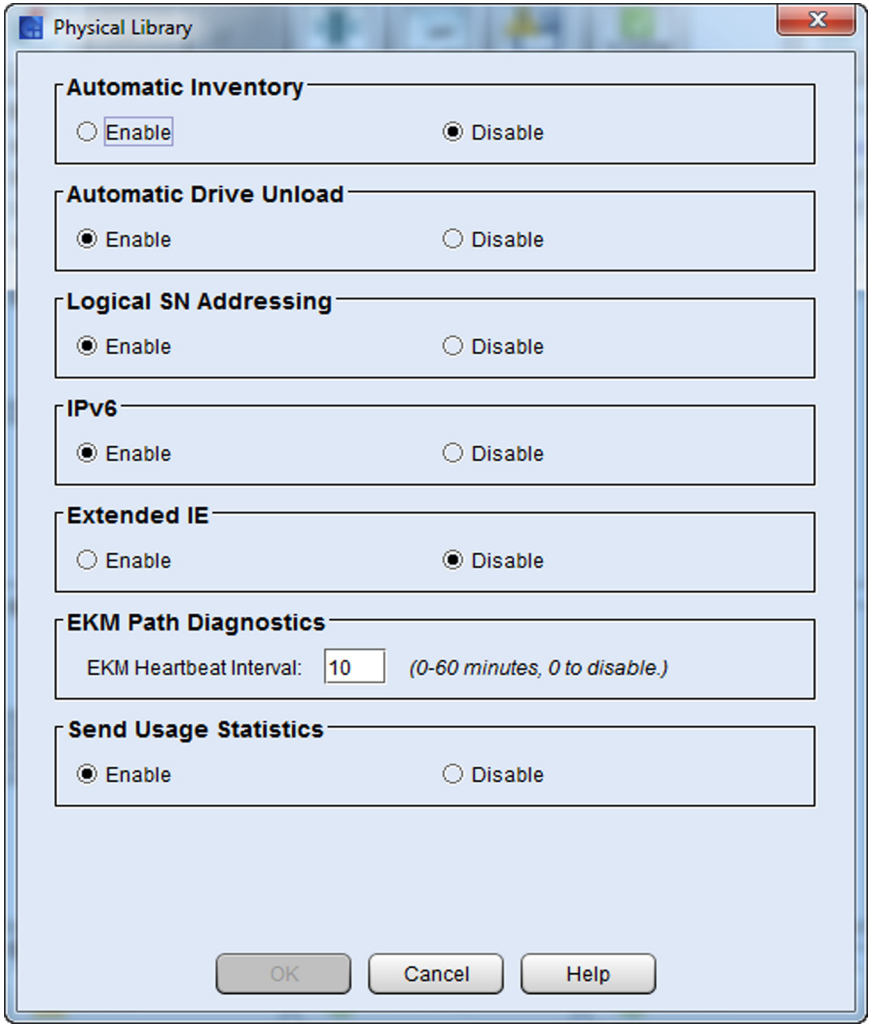
- **Unexpected Removal Detection After Power-up and Reboot Only** — Media were physically removed from the library when it was powered down.
- **Unexpected Removal Detection During Library Operation** — While library is powered up someone opens the door of the library and removes media.
- **Expected Removal Detection From I/E Slots During Library Operation** — Media are exported to the I/E (via backup

application or LMC) and are then physically removed from the I/E station.

- **Unexpected Removal Detection From I/E Slots During Library Operation** — Someone puts media in the I/E station for import, the robot scans the media, and then the media are physically removed from the I/E station.

4 Click **OK** to close the dialog.

5 From the main console, select **Setup > System Settings > Physical Library**. The **Physical Library** dialog box appears.



6 For **Automatic Inventory**, click **Enable**.

7 Click **OK**.

Viewing the Media Security Events Report

You can view a report of media security events by selecting **Tools > Reports > Media > Security**.

The log displays events which met the criteria you selected in the **Media Security Notifications** dialog box (see Setting Up Media Security Notifications on page 186).

Configuring Devices

You can change the way library components appear to the hosts. The **Setup > Device** command enables you to change the way system components appear to the hosts.

The **Setup > Drives > SCSI IDs** command is available while viewing a partition. Use this command to set the SCSI ID for a SCSI-attached drive. All hosts that view the drive will see the same SCSI ID associated with the drive.

The **Setup > Drives > FC Settings** command is available when viewing the physical library and allows you to configure speed, topology, or Loop ID for a Fibre-attached drive.

The **Setup > Blades > Access** command gives you access to the **Channel Zoning**, **FC Host**, and **LUN Mapping Wizard** commands, which are available while viewing the physical library.

The **Setup > Drives > Access > SNW Wizard** is available when viewing the physical library and gives you access to the **SNW Drive Licenses, Control Path, Data Path Failover, and Host Access.**

- Use the **Channel Zoning** command to restrict host access to particular I/O blade ports.
- Use the **FC Host** commands to configure access to partition accessors and drives on a per-host basis. If you have connected your host to the FC port on the MCB, or to a port on one of the FC I/O blades, you must map the appropriate partitions by using the **FC Host** command. If you have connected your hosts directly to the

drives, use third-party software of your choice to manage media from the host itself.

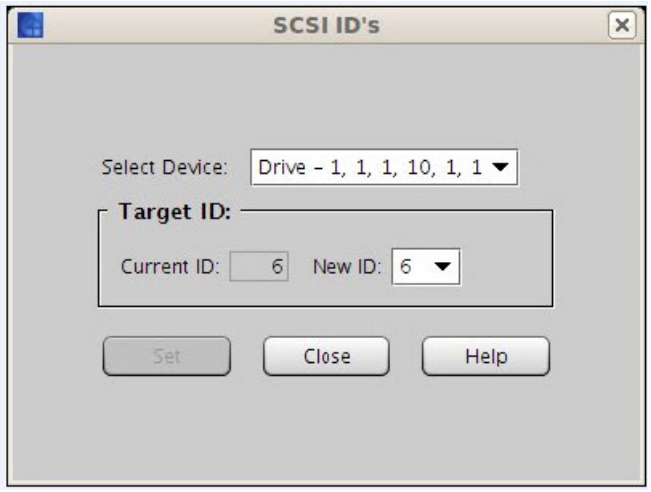
- Use the **SNW Wizard** to select the drives you want managed by the Storage Networking (SNW) feature. The selected drives can be configured so client hosts can be granted or denied access. Only IBM or HP LTO-5 or LTO-6 drives are supported. Each drive selected will consume a SNW license.
- Use the LUN Mapping Wizard command to set up LUN Mapping for your Fibre Channel hosts

If you have not otherwise restricted access, **FC Host** has full control of all LUNs on all FC and SCSI channels. Each FC host attached to an FC I/O blade can be configured to access a maximum of 255 LUNs, up to an overall system total of 2,048.

Configuring Drive SCSI ID

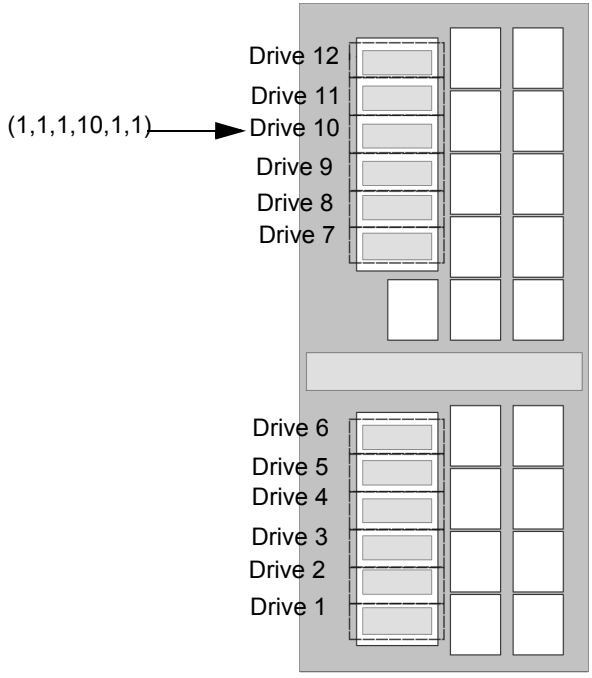
From a partition, you can change the SCSI ID for a SCSI-attached drive. For example, the default SCSI ID for a drive that you are installing might conflict with the assigned SCSI ID of an existing drive. You might be using an application that expects to communicate with a device at a specific SCSI ID, but that ID might already have been configured for use in another partition. Use the **Setup > Device > IDs** command to correct these situations.

1. Log on as an administrator.
2. Make sure that you are viewing the partition that includes the drive you want to configure. From the **View** menu, click the name of the appropriate partition.
3. Click **Setup > Drives > SCSI ID's**. The **SCSI ID's** dialog box appears.



4 Select the drive who's SCSI ID you want to change from the **Select Device** drop-down list. The drop-down list uses the drive's location coordinates to identify the drive.

For example, in the figure above, the drive is in position 10. The following figure shows its location in the control module. For more information about location coordinates, see Understanding Location Coordinates on page 449.



5 To specify a particular ID for a drive, click a new ID number from the **New ID** drop-down list.

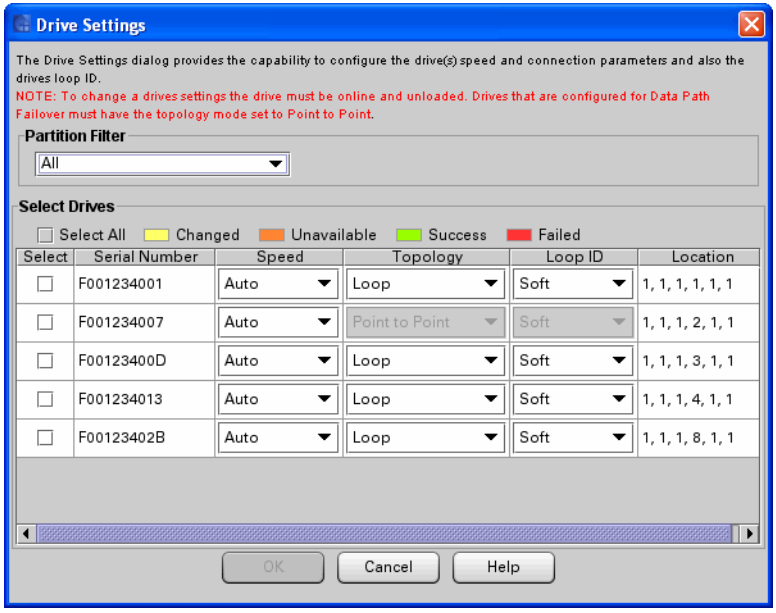
6 Click **Set**.

Configuring Fibre Channel Drive Speed, Topology, and Loop ID

Administrators can view and modify Speed, Topology, and Loop ID settings for Fibre Channel tape drives.

If the affected partition is online, it will be taken offline before the parameters are set, and brought back online after they are set.

1 Click **Setup > Drives > FC Settings**. The **Drive Settings** dialog box appears.



2 From the **Partition Filter** drop-down list, select all partitions or a single partition whose drive settings you want to set.

3 Configure the settings as described below:

Speed

The requested interface speed can be set to Auto (default; autonegotiates to highest speed possible), 1 Gb/s, 2 Gb/s, 4 Gb/s, or 8 Gb/s (depending on drive type).

Caution: LTO-5 and LTO-6 Fibre Channel tape drives can be configured for speeds of up to 8 Gb/s. If they are configured for 8 Gb/s, you should connect them directly to a host and not to an FC I/O blade, because the FC I/O blade only allows speeds up to 4 Gb/s. If you connect an LTO-5 or LTO-6 Fibre Channel tape drive to an FC I/O blade, you must configure the tape drive speed of 4 Gb/s or less.

Note: The speed settings you choose are requested, not actual. If the requested speed setting is not supported, the next appropriate setting is negotiated.

Topology

The requested topology connection mode can be set to one of the following:

- Loop (default) — Force L-Port
- Loop Preferred — Auto-configure trying L-Port first
- Point to Point — Force N-Port

Notes about point to point

- You can use Point to Point if the tape drive is connected via a switch or directly to a host.
- You cannot use Point to Point if the tape drive is connected to an FC I/O blade.
- You must use Point to Point if the tape drive is being used for control path failover (see Configure Control Path on page 351).

Loop ID

You can only set Loop ID when the Topology is set to Loop. You cannot set the Loop ID if the Topology is set to Point to Point or Loop Preferred.

The loop ID can be set to Soft (default) or to a value from 0 to 125. When set to Soft, a unique loop ID is selected for the drive. If you change the Loop ID to a specific value, make sure that each FC tape drive has a unique loop ID.

Configuring Fibre Channel I/O Blades

FC Host

The **FC Host** command enables you to manually modify host information and set LUN mappings.

During device discovery, a particular partition or drive could map to a higher LUN space than is optimal for a particular application. The **FC Host** command enables you to create a virtual private remapping of available LUNs for a specific Fibre Channel-attached host. LUN mapping is required to give hosts access to partitions and devices. You also can make devices appear to the host as if they were at lower LUNs in order to optimize system performance.

Note: Use the **FC Host** command to map partitions when a Fibre Channel host is connected either to the MCB or to an I/O blade.

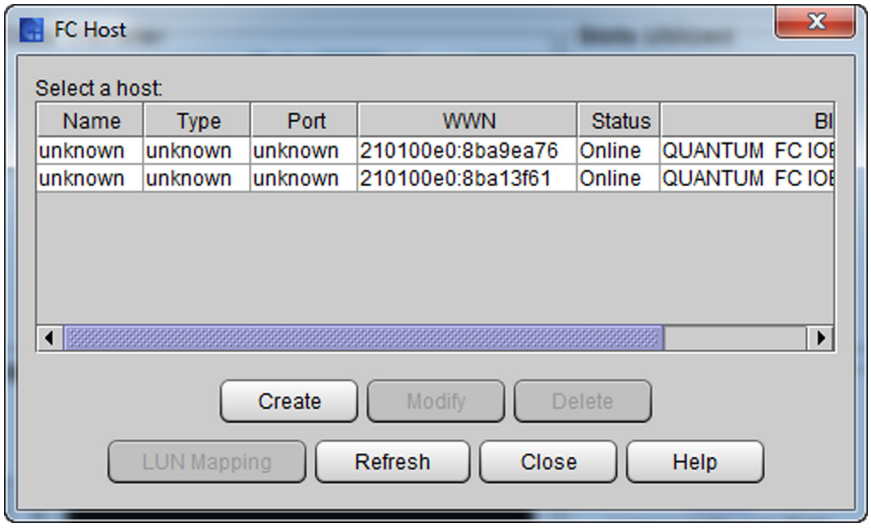
Depending on host operating system constraints, it might be necessary to reboot or reconfigure the host because of device map changes that result from using the **FC Host** command.

Caution: If you change LUN mapping after host computers or applications have already discovered devices, you must make sure that device discovery occurs again. Device discovery occurs automatically when you reboot the library. Some host computers have plug and play capability, which discovers devices automatically. In general, host applications do not discover devices automatically.

Note: EEBs connected to drives configured with a control path may report certain library ready conditions differently than drives without a control path configured.

Accessing FC Hosts

1. Log on as an administrator.
2. Make sure that you are viewing the physical library. From the **View** menu, click the name of the physical library.
3. Click **Setup > Blades > Access > FC Host**. The **FC Host** dialog box appears.



Only the host's port, blade, and World Wide Name (WWN) appear.

Note: Clicking **Refresh** allows you to update the current state of the host devices.

Adding, Modifying, and Deleting FC Hosts

You can add and configure FC hosts without powering down the system. Manually add an FC host if it was not already connected to the library when it was turned on.

Adding an FC Host

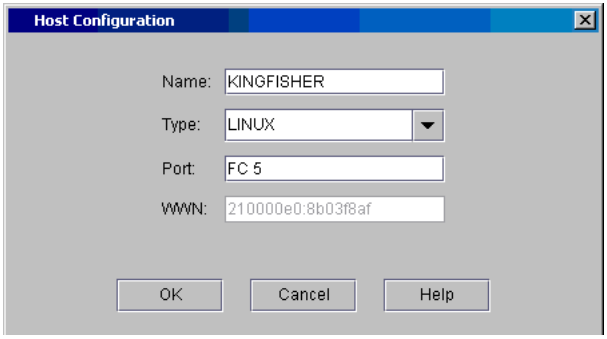
1. Log on as an administrator.
2. Make sure that you are viewing the physical library. From the **View** menu, click the name of the physical library.
3. Click **Setup > Blades > Access > FC Host**. The **FC Host** dialog box appears.
4. Click **Create**. The **Add Host Data** dialog box appears.
5. Use the check boxes under **Select Blades** to select at least one blade that the host will access.
6. Using the text boxes provided, provide the following required information:
   - In the **Name** text box, type a host device name.
   - From the **Type** drop-down list, click the appropriate host type by operating system.
   - In the **Port** text box, type the host device port.

   Note: The **Port** field can be used for any free-form text to help better describe the connectivity. This field otherwise has no configuration functionality.

   - In the **WWN** text box, type the host device World Wide Name (WWN).
7. Click **OK**.

Modifying an FC Host

1. With the host selected in the **FC Host** dialog box, click **Modify**. The **Host Configuration** dialog box appears.



2 As necessary, change the information in the **Name** and **Port** text boxes, and then click the appropriate host type by operating system from the **Type** drop-down list. You cannot change the World Wide Name (WWN).

Caution: You also must make the necessary physical changes to the name, operating system, or port connection.

3 Click **OK**.

Deleting an FC Host

1 Log on as an administrator.

2 Make sure that you are viewing the physical library. From the **View** menu, click the name of the physical library.

3 Click **Setup > Blades > Access > FC Host**. The **FC Host** dialog box appears.

Note: FC hosts can be reconfigured without powering down the system.

Click the host from the list, and then click **Delete**. A message appears that asks you whether you want to delete the host.

Note: The **Delete** button is unavailable if the host is online.

4 Click **Yes**. A message appears that indicates a successful deletion.

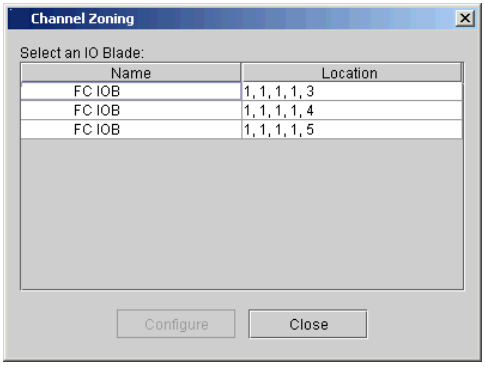
5 Click **OK**.

Channel Zoning

Channel zoning, also called port zoning, is an optional feature that configures access to an entire Fibre Channel and all the LUNs on that channel for the exclusive use of a host or group of hosts on a single port. Channel zoning enables you to control access between specific target Fibre Channel (FC) ports and initiator channels on an I/O blade in your library. If you make changes to the channel zoning settings, you must reboot the I/O blade for the new settings to take effect.

Caution: If you change channel zoning after host computers or applications have already discovered devices, you must make sure that device discovery occurs again. Device discovery could occur automatically when you reboot the library. Some host computers have plug and play capability, which can discover devices automatically. Host applications might discover devices automatically.

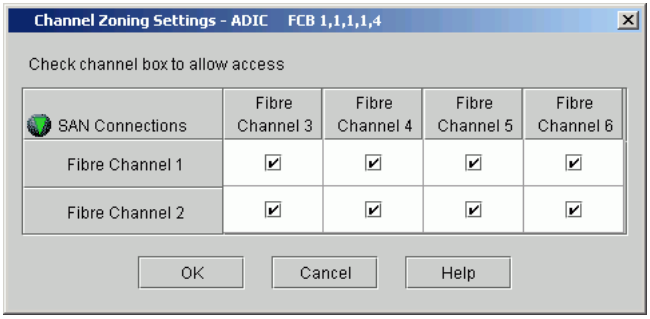
1. Log on as an administrator.
2. Make sure that you are viewing the physical library. From the **View** menu, click the name of the physical library.
3. Click **Setup > Blades > Access > Channel Zoning**. The **Channel Zoning** dialog box appears.



4. Click the I/O blade you want to configure to highlight it.

   The same I/O blade may appear multiple times in the list depending on the number of hosts assigned to the I/O blade. You only need to select one instance of the blade to zone the entire blade.

5 Click **Configure**. The **Channel Zoning Settings** dialog box appears for the selected I/O blade. By default, all FC ports have access to all channels.



6 If you want to permit access, select the check box in the cell where the target port and the initiator channel meet. If you want to restrict access, clear the check box in the cell where the target port and the initiator channel meet.

If an FC port is set to target and initiator mode, the port appears in both the horizontal row and vertical column. To prevent ghosting, the FC port is not allowed access to itself. Ghosting is a condition where hosts can see storage in two places.

Caution: When you select a check box in the cell, the entire channel is zoned. This zoning affects any host that might being accessing the I/O blade. Channel zoning settings supersede any host LUN mapping on the I/O blade.

7 To continue, click **OK**.

8 You must reboot the I/O blade for the new configuration settings to take effect. In the **Attention** dialog box, click **Yes** to proceed. If you do not want to continue with the configuration, click **No**.

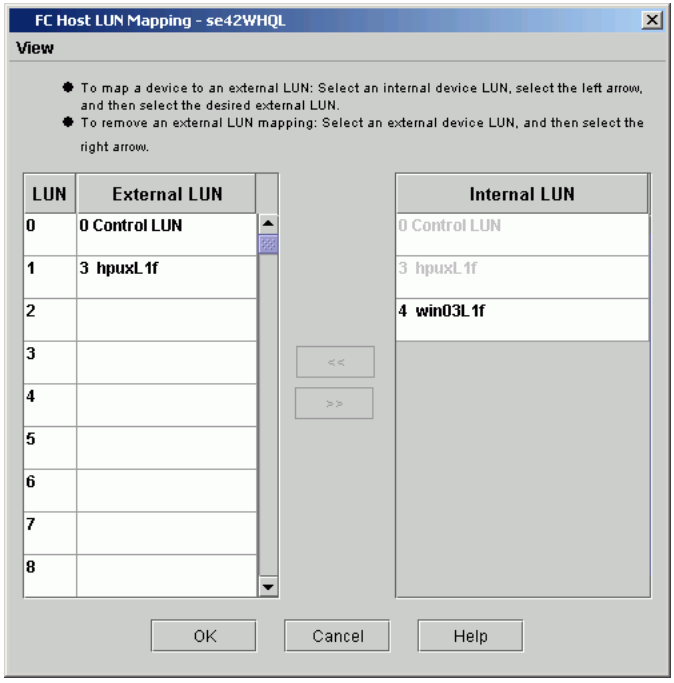
9 After you complete your configuration changes, click **Close**.

FC Host LUN Mapping

Use the **FC Host LUN Mapping** dialog box to give a selected host access to partitions and drives.

Configuring LUN Mapping

1. Log on as an administrator.
2. To ensure you are working from the physical library, from the main console, select **View** and click the name of the physical library.
3. Click **Setup > Blades > Access > FC Host**. The **FC Host** dialog box appears.
4. Select a host on the **FC Host** dialog box, click **LUN Mapping**. The **FC Host LUN Mapping** dialog box appears in its default view.

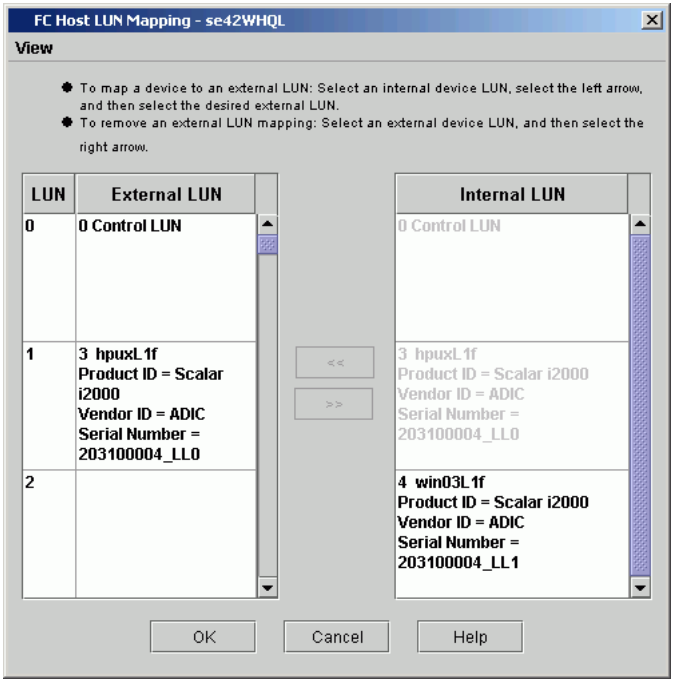


This dialog box displays all partitions and drives connected to the blade to which the host is attached.

Note: If you delete a partition that is currently displayed on the **FC Host LUN Mapping** dialog box, the internal LUN and any external LUN mappings for the partition will no longer appear on the dialog box.

Note: If a partition is already presented via Control Path it will not show up in the list of internal LUN devices.

5 Compare the default view with the **Show Details** view shown in the following figure. To change from the default view to the detailed view, see Setting the View for the FC Host Device Column on page 205.



In this figure, the **Internal LUN** column has been scrolled down. The **Show Details** view for partitions shows the partition name, product ID, vendor ID, and the serial number of the partition. For drives, the LMC displays the device LUN, connection type, port connection, vendor ID, serial number, and the associated partition.

The following table describes the descriptors that appear in the **Show Details** view for partitions.

Table 29 Show Details

Descriptor	Description
Partition Name	Name assigned during partition creation process.
Product ID	The **Product ID** setting controls the product ID string that is returned in a standard SCSI INQUIRY response. The library can report that it is a Scalar i500, Scalar i2000, or Scalar i6000. This feature can enable the library to be used with host applications that do not yet include the Scalar i6000 in a list of recognized devices. In addition, the various Microsoft Windows operating systems maintain a list of recognized devices. If the Scalar i6000 is not in an operating system's list of recognized devices, the library will appear as an "unknown" device in device lists. You might prevent the library from being listed as "unknown" by setting **Product ID** to a library other than Scalar i6000. This setting does not cause any library operational changes other than the SCSI INQUIRY response.
Vendor ID	ADIC or QUANTUM (default is QUANTUM). This information is used in the SCSI Inquiry command. Some backup applications may only support or be configured for ADIC libraries, so if you configure a logical library using the vendor ID of QUANTUM, the backup application would not work with the library.
Serial Number	Partition ID, as shown by **Monitor > System > Components** tab.

The following table describes the descriptors that appear in the **Show Details** view for drives.

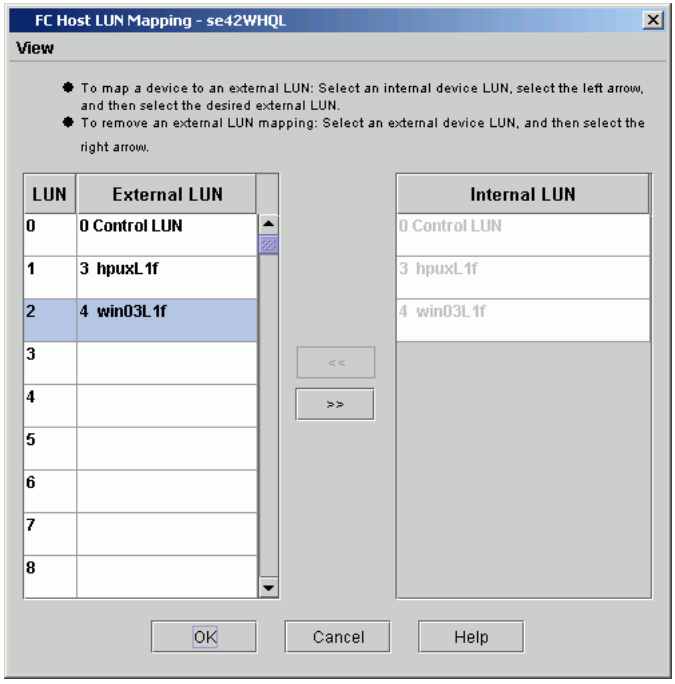
Table 30 Descriptors

Descriptor	Description
[Number] [Connection Type] [Port Connection]	[LUN] [Fibre or SCSI] [Port Number].
Vendor ID	Drive manufacturer.
Serial Number	Drive serial number.
Partition	Name of the partition with which the drive is associated.

In the default view, only the names of available partitions and the names of the devices (drives) are shown. LUN spaces from 0-255 are available. In the **Show Details** view, a partition that has not yet been manually reassigned to a new map position appears in heavy black type in the **Internal LUN** column. Partitions are treated by the system as devices. You must assign a partition to the **LUN/External LUN** column for the LMC to manage it and its media. In this example, the control LUN has already been remapped as shown in heavy black type in the **LUN/External LUN** column.

6 If you are working from the local touch screen, you must select an internal device LUN, select the left arrow, and then select the desired external LUN. If you are working from the remote client, you can use the select method or you can drag and drop the devices from the **Internal LUN** column to the appropriate LUN assignment in the **LUN/External LUN** column. Always use LUN 0 for command and control.

In the following figure, all devices have been mapped manually.



The new map locations appear in heavy black type in the **LUN/External LUN** column. The previous (default) device map position of

a remapped device is shown in gray type in the **Internal LUN** column.

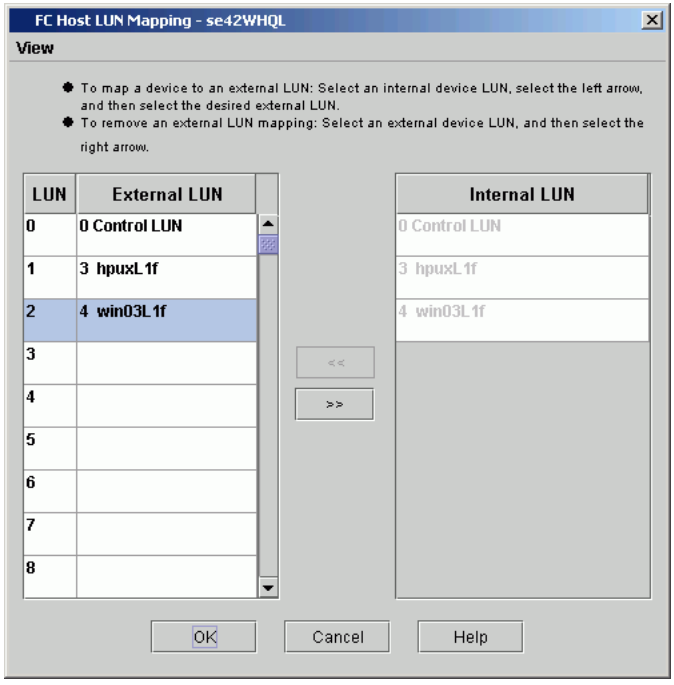
7 To save the mapping, click **OK**. The FC host map is automatically saved as part of the configuration.

For more information about device numbering in a SAN context, see the Online Help.

Modifying FC Host Mapping

When a device has been mapped, it is still listed, though unavailable, in the **Internal LUN** column.

In the following figure, the LUNs are not currently available for mapping because they have already been mapped into the **LUN/External LUN** column.



The device that was formerly found at assigned LUN 4 is now found at assigned LUN 2. Drag it back into the **Internal LUN** column to make it available for re-mapping. If you are working from the local touch screen, select an external device LUN, and then select the right arrow.

Setting the View for the FC Host Device Column

Click **View** at the top of the **FC Host LUN Mapping** dialog box. If you want to see product details, select the **Show Details** check box. If you want to see only the names of the devices available for mapping, clear the **Show Details** check box to toggle the display back to the default view.

Using the LUN Mapping Wizard

LUN mapping is required to give hosts access to partitions and devices. You can also make devices appear to the host as if they were at lower LUNs in order to optimize library performance.

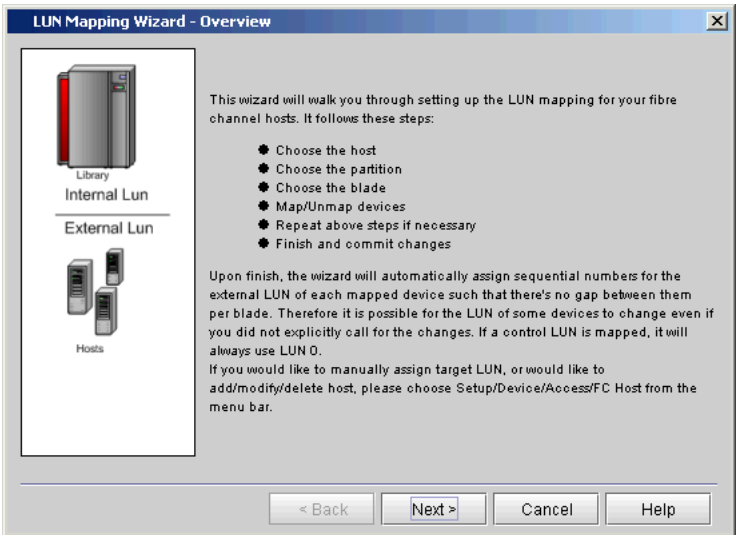
The **LUN Mapping Wizard** guides you through the setup of LUN mapping for your Fibre Channel hosts.

Note: If you want to manually assign a target LUN, or want to add/modify/delete the host, select **Setup > Blades > Access > FC Host** on the menu bar. For more information, see FC Host on page 194.

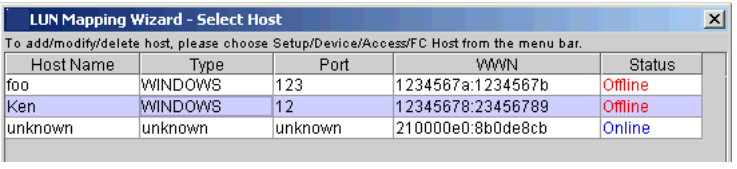
The **LUN Mapping Wizard** automatically assigns sequential numbers for the external LUN of each mapped device, without any gaps between them per blade. When using the **LUN Mapping Wizard**, the LUN for some devices may change even if you did not specify the changes. If a control LUN is mapped, it is always assigned LUN 0.

Depending upon host operating system constraints, it may be necessary to reboot or reconfigure the host as a result of device map changes resulting from the use of the **LUN Mapping Wizard**.

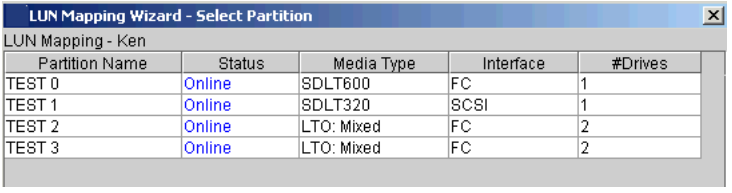
1. Click **Setup > Blades > Access > LUN Mapping Wizard**. The **LUN Mapping Wizard – Overview** dialog box appears.



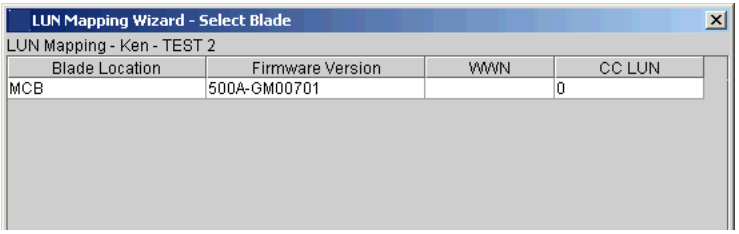
2 Review the **LUN Mapping Wizard Overview,** then click **Next** to continue. The **LUN Mapping Wizard – Select Host** dialog box appears. All available hosts are listed on this dialog box.



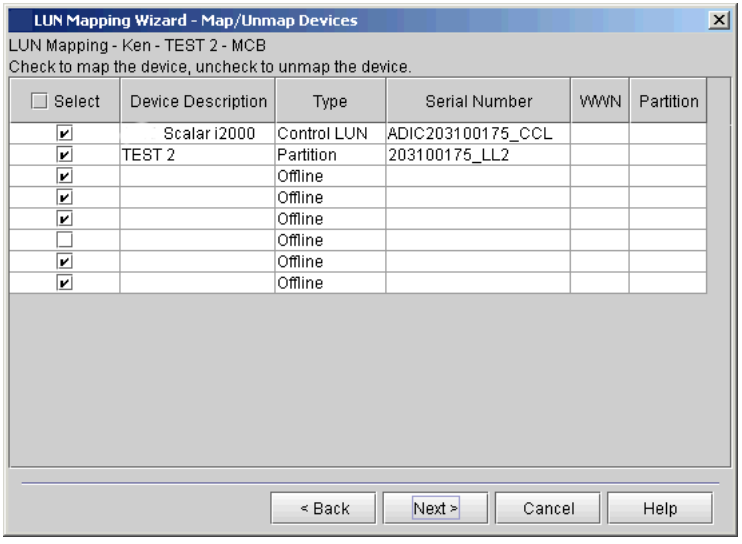
3 Select a host to configure and then click **Next** to continue. All available partitions on the selected host are listed on this dialog box. The **LUN Mapping Wizard – Select Partition** dialog box appears.



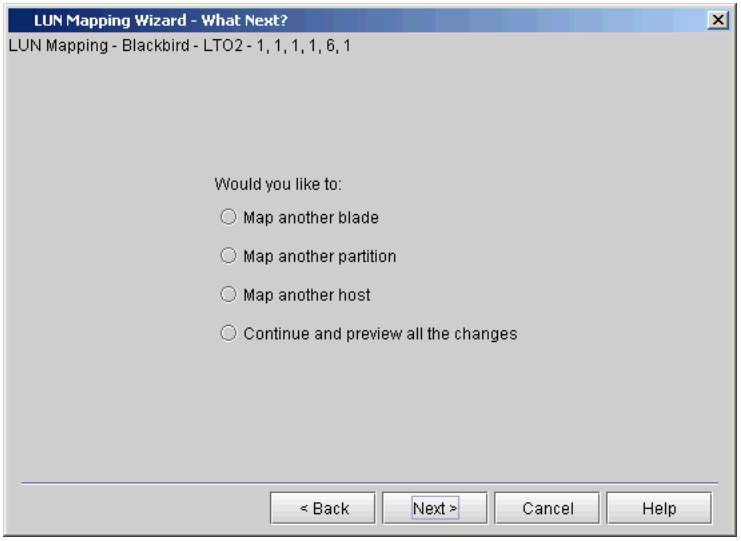
4 Select a partition to configure and then click **Next** to continue. All available blades on the selected partition are listed on this dialog box. The **LUN Mapping Wizard – Select Blade** dialog box appears.



5 Select a blade to configure and then click **Next** to continue. The **LUN Mapping Wizard – Map/Unmap Devices** dialog box appears.



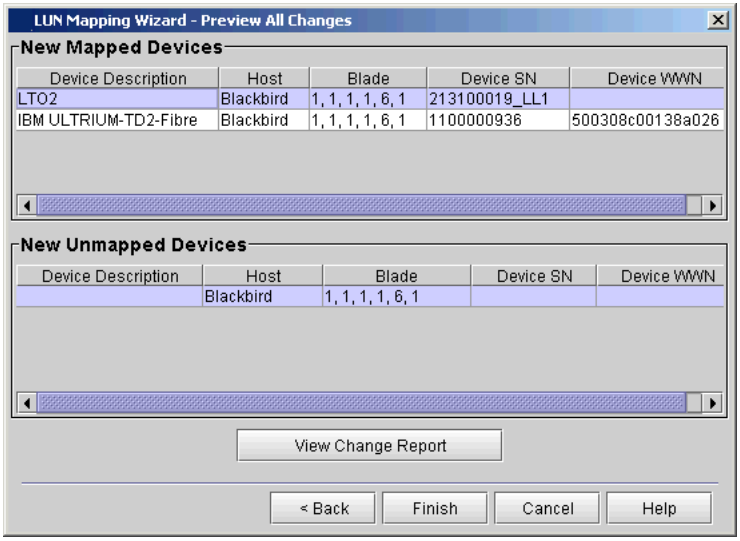
6 Select the check box to map a device or clear the check box to unmap a device, then click **Next** to continue. The **LUN Mapping Wizard – What Next?** dialog box appears.



7 Select one of the following and click **Next** to continue:

- **Map another blade** – this allows you to map another blade on the same partition.
- **Map another partition** – this allows you to map another partition on the same host.
- **Map another host** – this allows you to map another host.
- **Continue and preview all the changes** – this allows you to view an online printout of the change report which presents a preview of all changes, showing whether you added, modified or deleted any devices.

8 If your configurations are complete, select **Continue and preview all changes**. The **LUN Mapping Wizard – Preview All Changes** dialog box appears.



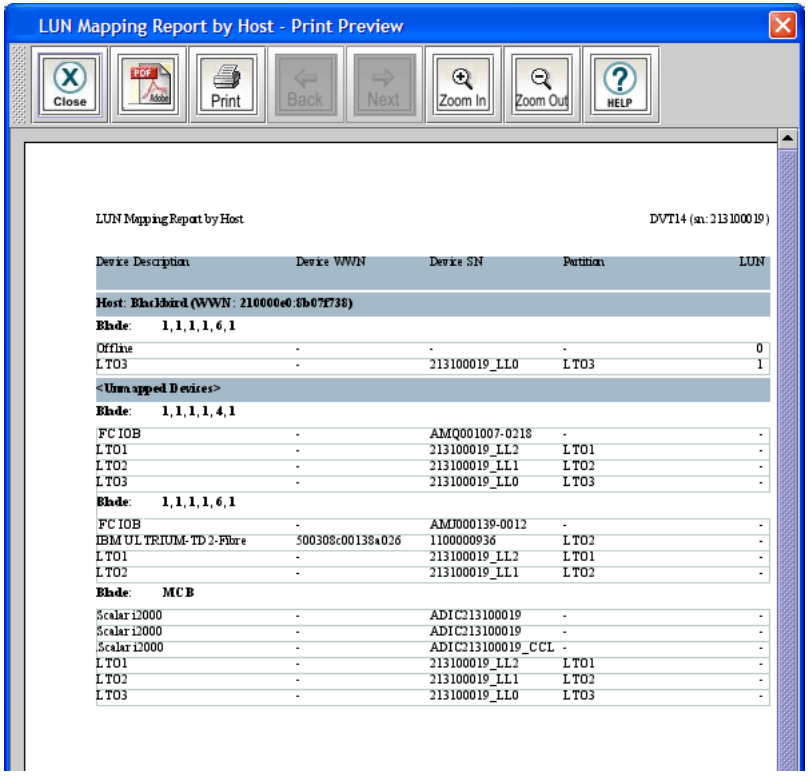
9 Prior to finishing and saving your LUN mapping configuration changes, review your newly mapped or unmapped devices in this dialog box.

- If you would like to create a report of your changes, click **View Change Report**.
- If you are satisfied with your LUN mapping changes and want complete the wizard process, click **Finish**. Your LUN mapping changes are finalized, and then you have the option of viewing the LUN Mapping Report.

The **LUN Mapping Change Preview Report – Print Preview** dialog box appears. This dialog box displays what types of changes were made to all devices.

The changes on the report include:

- Added Mapping – (**A**)
- Removed Mapping – (**R**)
- LUN Modified – (**M**)



10 On the **LUN Mapping Change Preview Report – Print Preview** dialog box, you can select the following:

- To save the report as a PDF file, click **PDF**. Specify a file path and file name, and then click **Confirm**.
- To print the report, click **Print**. Specify print options, and then click **OK**.
- To navigate through the pages of the report, click **Back** or **Next**.
- To increase or decrease the magnification of the report, click **Zoom In** or **Zoom Out**.
- To access the Online Help, click **Help.**

11 After you have reviewed the **LUN Mapping Change Preview Report**, click **Close** to return to the **LUN Mapping Wizard – Preview All Changes** dialog box.

12 If you are satisfied with your LUN mapping changes and want to complete the wizard process, click **Finish**. Your LUN mapping changes are finalized

You have the option of viewing the L**UN Mapping Report**.

Generating the LUN Mapping Report

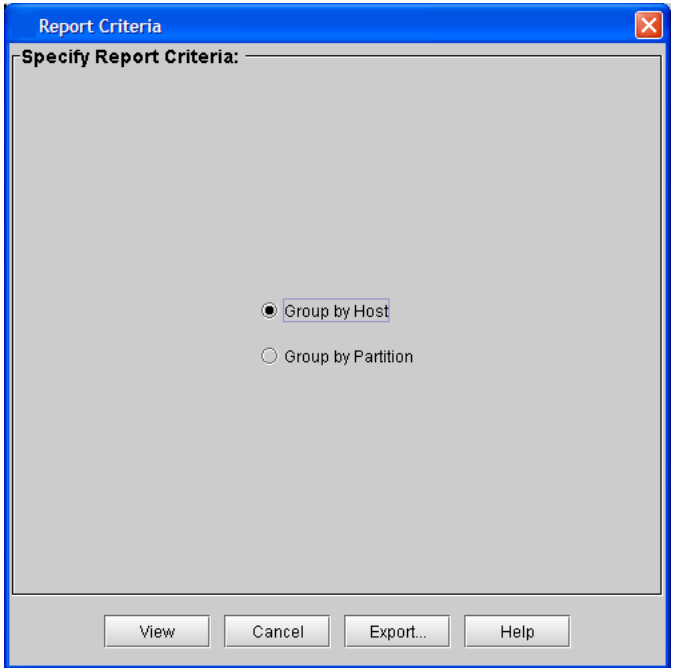
The LUN Mapping Report lets you view the current LUN configuration settings for the library. The report displays information about tape drives and other devices in the library, such as WWN (world wide name), LUN (logical unit number), and serial number.

When generating the LUN Mapping Report, you can choose to group devices by the associated host or by the associated partition.

Viewing the LUN Mapping Report

To view the LUN Mapping report, first choose a grouping criteria, then view the report.

1 On the menu bar, click **Tools > Reports > LUN Mapping**. The **Report Criteria** dialog box appears.



2 Under **Specify Report Criteria**, click a grouping option.

- **Group by Host** — The report lists the devices associated with each host.
- **Group by Partition** — The report lists the devices associated with each partition.

3 Click **View**. The **Print Preview** dialog box appears. Figure 33 on page 213 shows an example of a **LUN Mapping Report grouped by host.**

Figure 33 LUN Mapping Report grouped by host preview

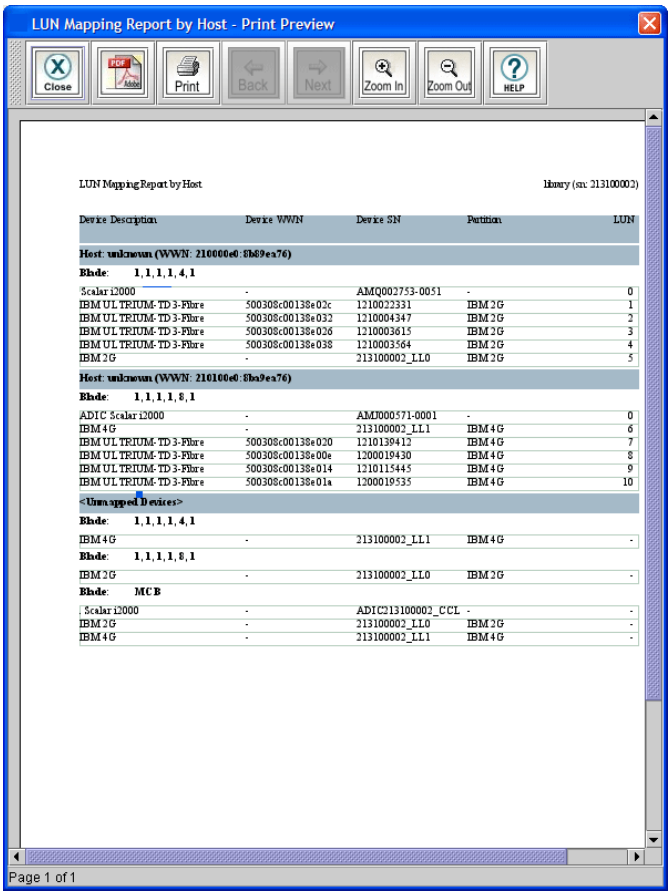
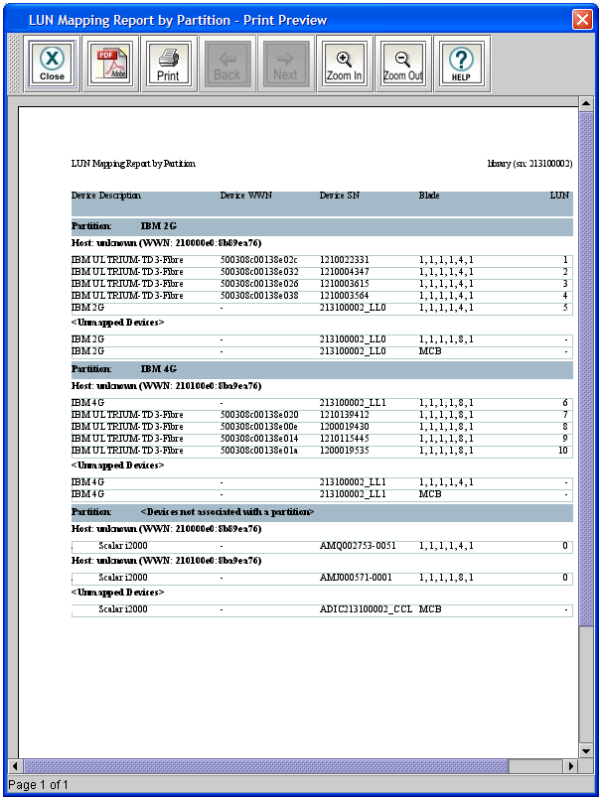


Figure 34 on page 214 shows an example of a **LUN Mapping Report grouped by partition**.

Figure 34 LUN Mapping Report grouped by partition preview



4 Do one or more of the following:

- To navigate through the pages of the report, click **Back** or **Next**.
- To increase or decrease the magnification of the report, click **Zoom In** or **Zoom Out**.
- To print the report, click **Print**. Specify print options, and then click **OK**.
- To save the report as a PDF file, click **PDF**. Specify a file path and file name, and then click **Confirm**.

Note: You cannot print reports or save them to a PDF file using the touch screen.

5 When you are finished working with the **Print Preview** dialog box, click **Close**.

6 To close the **Report Criteria** dialog box, click **Cancel**.

Exporting a Report to an E-mail or a Text File

Instead of viewing or printing the report on the **Print Preview** dialog box, you can e-mail the report data to an e-mail address. Or export the report data to a comma delimited text file (***.csv**) for use in other programs.

1 On the menu bar, click **Tools > Reports > LUN Mapping**. The **Report Criteria** dialog box appears.

2 Under **Specify Report Criteria**, click a grouping option.

- **Group by Host** — The report lists the devices associated with each host.
- **Group by Partition** — The report lists the devices associated with each partition.

3 Click **Export**. The **Export Raw Data** dialog box appears.

4 Do one of the following:

- To send the report data to an e-mail address, click **Email**. Type or select the e-mail address, type an optional comment in the **Comment** box, and then click **OK**.
- To save the report data to a comma delimited text file, click **Save**. Specify a file path and file name, and then click **OK**.

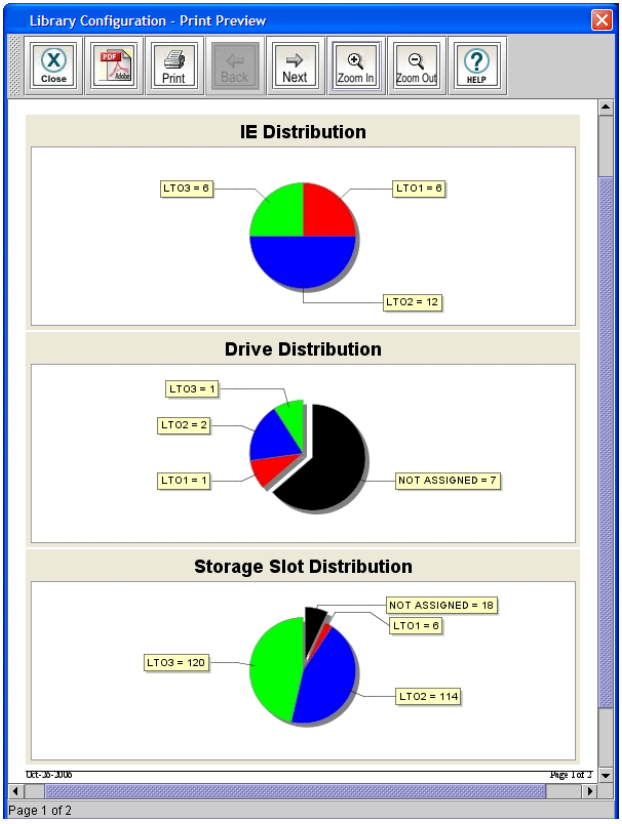
5 To close the **Report Criteria** dialog box, click **Cancel**.

Generating the Library Configuration Report

The Library Configuration report lets you view the number of I/E stations, drives, and storage slots in the library that are currently

assigned to each logical partition. Generate the Library Configuration report to help make sure you are using library resources effectively.

1 On the menu bar, click **Tools > Reports > Library Configuration**. The **Library Configuration - Print Preview** dialog box appears.



2 Do one or more of the following:

- To navigate through the pages of the report, click **Back** or **Next**.
- To increase or decrease the magnification of the report, click **Zoom In** or **Zoom Out**.
- To print the report, click **Print**. Specify print options, and then click **OK**.
- To save the report as a PDF file, click **PDF**. Specify a file path and file name, and then click **Confirm**.

Note: You cannot print reports or save them to a PDF file using the touch screen.

3 When you are finished working with the **Library Configuration - Print Preview** dialog box, click **Close**.

Configuring Drive Cleaning

When you create or modify a partition, you can specify that tape drives in that partition be cleaned each time the library requests a cleaning operation.

For drive cleaning to function, you must configure it for the library. To configure drive cleaning, first assign cleaning magazines, and then import cleaning media. Designated cleaning media can also be used when manually cleaning drives. (Cleaning magazines and media are not part of any logical partition, and so are not visible to the host application).

If cleaning magazines are no longer needed, you can unassign them. In addition, you can export expired cleaning media to remove it from the library.

Note: Slots configured for drive cleaning affect the number of licensed COD slots.

Note: Drive cleaning should be enabled for partitions only if the host application does not support the coordination of drive cleaning. If drive cleaning functionality is enabled on the host application, do *not* enable drive cleaning for any partitions in the library.

For more information about enabling automatic drive cleaning for a partition, see Working With Partitions on page 118 on page 171. For more information about manually cleaning drives, see Cleaning a Drive on page 556.

Note: For information about cleaning media, see Using Cleaning Cartridges on page 682.

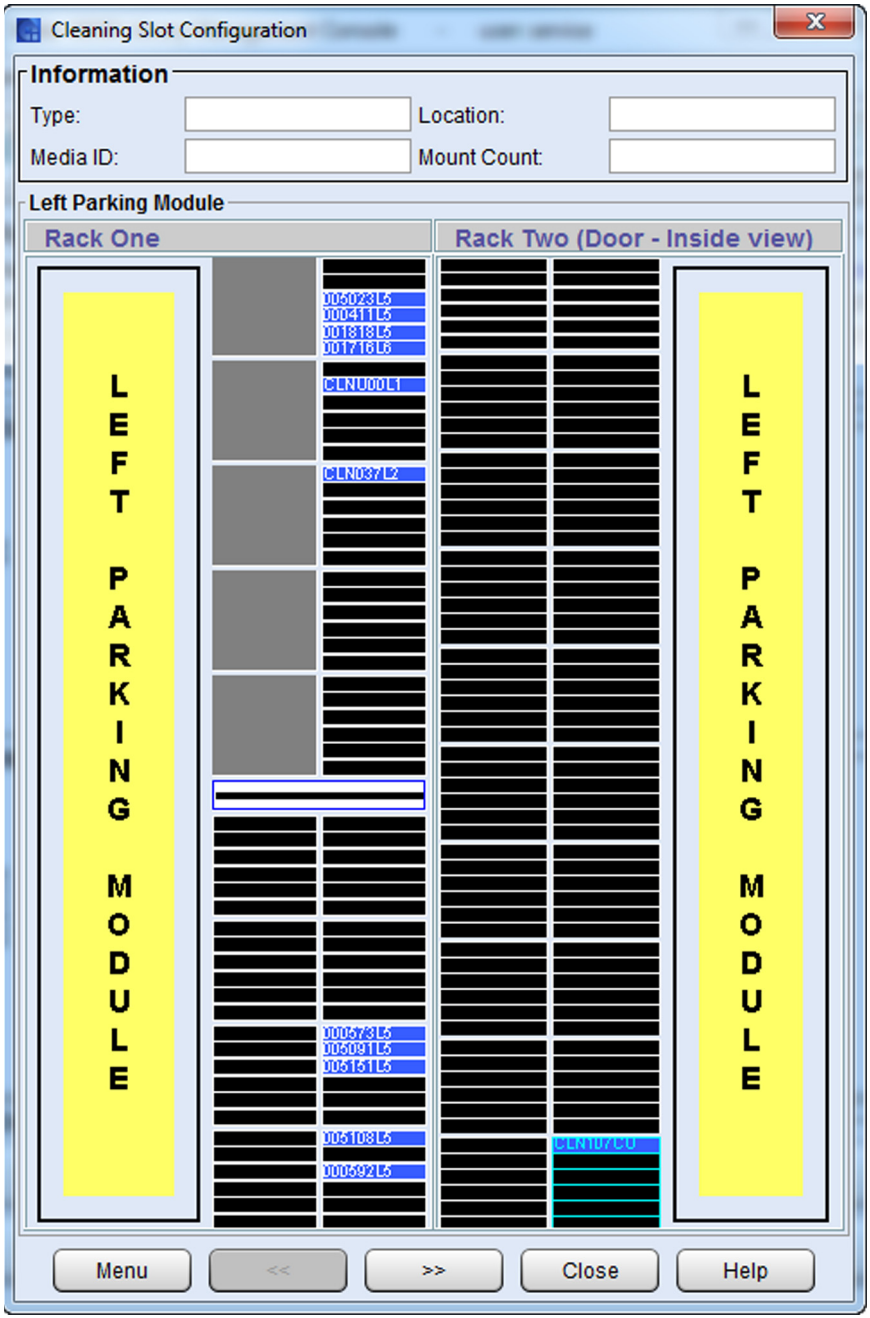
Assigning Cleaning Magazines

To configure the library for drive cleaning, you must first assign one or more magazines as cleaning magazines, and then import cleaning media (see Importing Cleaning Media on page 220).

Note: At least one magazine must be assigned for cleaning before you can import cleaning media. Also, only magazines that do not belong to a partition can be assigned for cleaning.

1. Make sure that you are viewing the physical library. From the **View** menu, select the name of the physical library.
2. On the menu bar, select **Setup > Cleaning Slots.** The **Cleaning Slot Configuration** window displays.

Figure 35 Cleaning Slot Configuration window



3 Click a magazine slot or tape cartridge to select it.

Details about the selected slot or media appear under **Information**, including the type of media, barcode number, location, and the number of times the media has been mounted in a drive.

4 If the library has more than one module, click the arrow buttons to display the next or previous module.

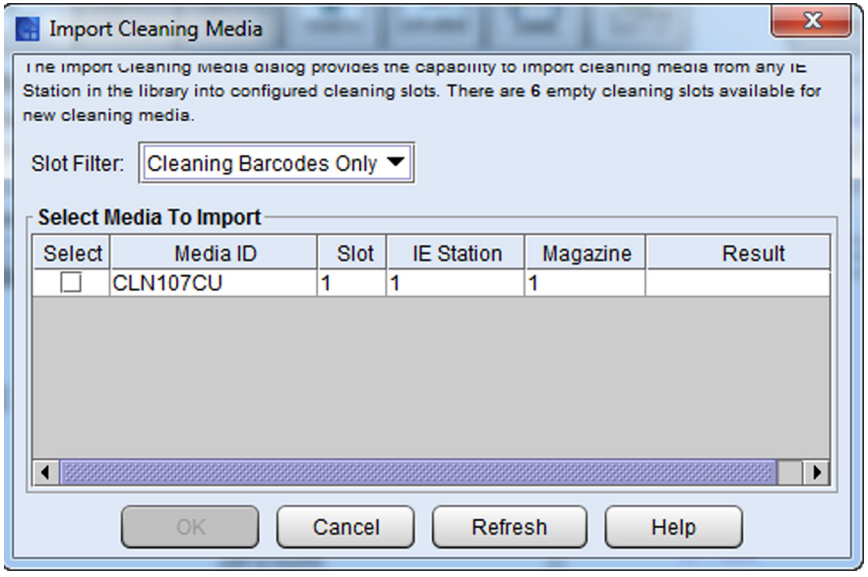
5 To assign a magazine for cleaning, click any slot in the magazine to select it. Click **Menu**, and then select **Assign magazine for cleaning**. The magazine is assigned for cleaning.

Repeat this step to assign additional cleaning magazines.

Note: You can also right click any slot in the magazine to assign it for cleaning.

Importing Cleaning Media

1 To import cleaning media, select **Operations > Import Cleaning Media...**.The **Import Cleaning Media** window displays.



2 Click the check box in the **Select** column next to the cleaning tape you want to import.

3 Click **OK**. The **Working...** dialog box displays.

4 When complete, a dialog displays indicating if the import was successful.

   The cleaning media are moved to an available cleaning magazine, and can be used for drive cleaning.

5 Click **OK**. On the **Import Cleaning Media** window, the cleaning tape will be highlighted green.

6 Click **Cancel** to close the **Import Cleaning Media** window.

Note: If you are working on the remote LMC, you can right-click a magazine slot or a piece of cleaning media to see a menu of available options.

Exporting Cleaning Media

Cleaning media can be used a limited number of times. If a cleaning tape is expired, export it and remove it from the library. There are two ways to export cleaning media:

- From the **Cleaning Slots** dialog, or
- From the **Export Cleaning Media**... dialog

Exporting Cleaning Media from the Cleaning Slots dialog

1 Make sure that you are viewing the physical library. From the **View** menu, click the name of the physical library.

2 Select **Setup > Cleaning Slots.** The **Cleaning Slot Configuration** dialog box appears. If the library has more than one module, click the arrow buttons to display the next or previous module.

   Note: To determine the number of cleanings the cleaning media has performed, click the media to select it, and then check the **Mount Count** value under **Information**.

3 Click the cleaning media in a cleaning magazine to select it, and then do one of the following:

   - To export only the selected piece of media, click **Menu**, and then click **Export cleaning media <barcode number>**.
   - To export all media in the selected magazine, click **Menu**, and then click **Export all cleaning media in magazine**.

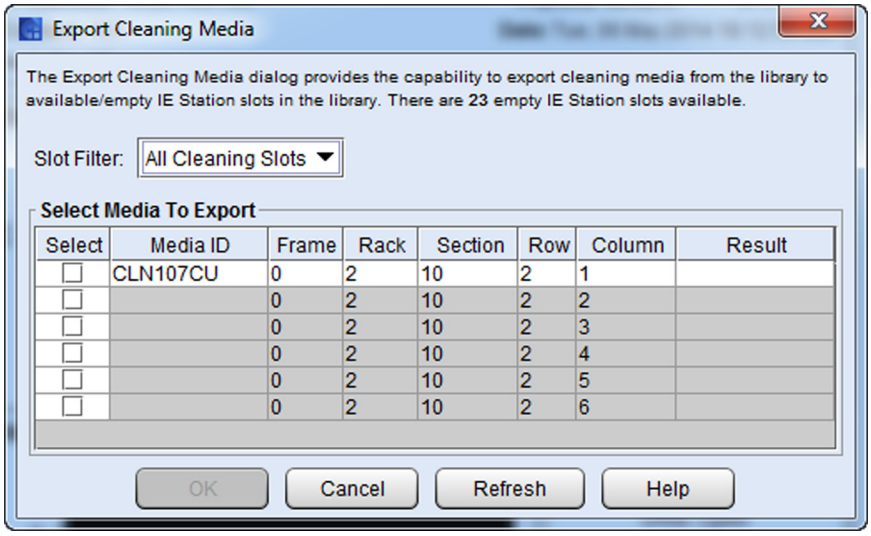
The cleaning media are moved to an available I/E station magazine.

Note: You can also right click the piece of media and select **Export cleaning media <barcode number>** or in the magazine and select **Export all cleaning media in magazine**.

4 Click **Close** to close the **Drive Cleaning Configuration** dialog box.

Exporting Cleaning Media from Export Cleaning Media dialog

1 Select **Operations > Export Cleaning Media...**.The **Export Cleaning Media** dialog box displays.



2 Click the check box in the **Select** column next to the cleaning tape you want to export.

3 Click **OK**. The **Working...** dialog box displays.

4 When complete, a dialog displays indicating if the export was successful.

The cleaning media are removed to an available slot in the I/E station.

5 Click **OK**. On the **Export Cleaning Media** window, the exported cleaning tape will be highlighted green.

6 Click **Cancel** to close the **Export Cleaning Media** window.

Unassigning a Cleaning Magazine

If a magazine is no longer needed for holding cleaning media, first export all cleaning media from the magazine, and then unassign it.

1 Make sure that you are viewing the physical library. From the **View** menu, select the name of the physical library.

2 On the menu bar, select **Setup > Cleaning Slot.** The **Cleaning Slot Configuration** dialog box appears. If the library has more than one module, click the arrow buttons to display the next or previous module.

3 If the magazine you want to unassign contains cleaning media, export all cleaning media to the I/E station.

For more information on exporting cleaning media, see Exporting Cleaning Media on page 221.

4 Click any slot in the cleaning magazine to select it.

5 Click **Menu**, and then click **Unassign magazine for cleaning**. The magazine is no longer assigned for cleaning.

Note: You can also right click in any slot in the cleaning magazine and then select **Unassign magazine for cleaning**.

6 Click **Close** to close the **Cleaning Slot Configuration** dialog box.

Note: You cannot unassign a cleaning magazine that contains valid cleaning media. You must first export the cleaning media and then unassign the cleaning magazine.

Registering SNMP Traps

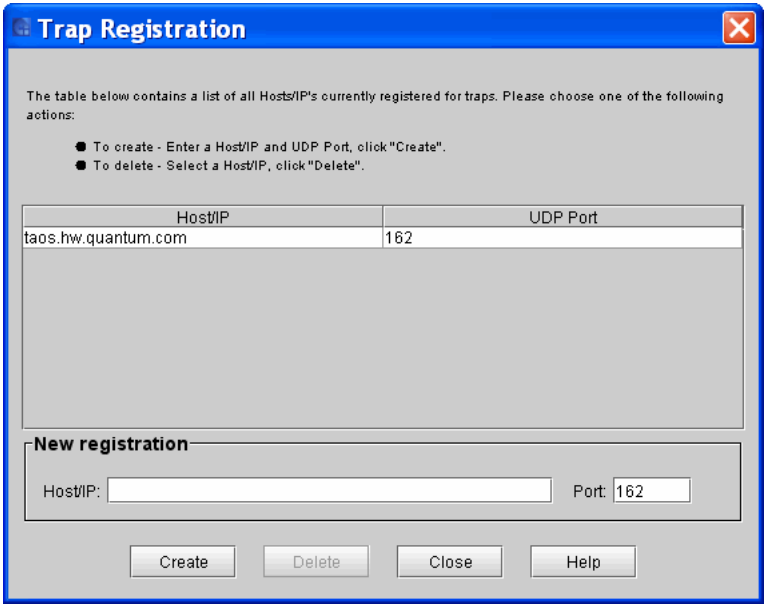
Because the library ignores all SNMP SET operations, external management applications cannot register themselves to receive SNMP traps from the library. The **Trap Registration** dialog box enables you to manually register external applications.

Registering an Application

1 Log on as an administrator.

2 Make sure that you are viewing the physical library. From the **View** menu, click the name of the physical library.

3 Click **Setup > Notifications > Trap Registration**. The **Trap Registration** dialog box appears.



4 In the **Host/IP** text box, type the iPv4 or iPv6 address or host name of the host client running of the external application.

5 In the **Port** text box, type the number of the User Datagram Protocol (UDP) port that you want to associate with the IP address or host name.

6 Click **Create**.

The host application's IP address or name and UDP port number appear in the table to indicate that the application is registered to receive SNMP traps from the library.

Removing an Application's Trap Registration

1. Log on as an administrator.
2. Make sure that you are viewing the physical library. From the **View** menu, click the name of the physical library.
3. Click **Setup > Notifications > Trap Registration**. The **Trap Registration** dialog box appears.
4. Click the IP address of the application for which you want to remove trap registration to highlight it.
5. Click **Delete**.

Configuring Library Security

You can change the library's security settings, including enabling or disabling network services, enabling or disabling remote access to the library, setting up firewall access for server callbacks to remote clients, and enabling or disabling SNMP or SMI-S access. You can configure the library's security while viewing either the physical library or a partition.

Note: Changing security configuration settings using the remote client might cause a loss of connectivity. If this happens, use the local touch panel to reset the security configuration settings and restore remote connectivity.

Accessing the Security Configuration Dialog Box

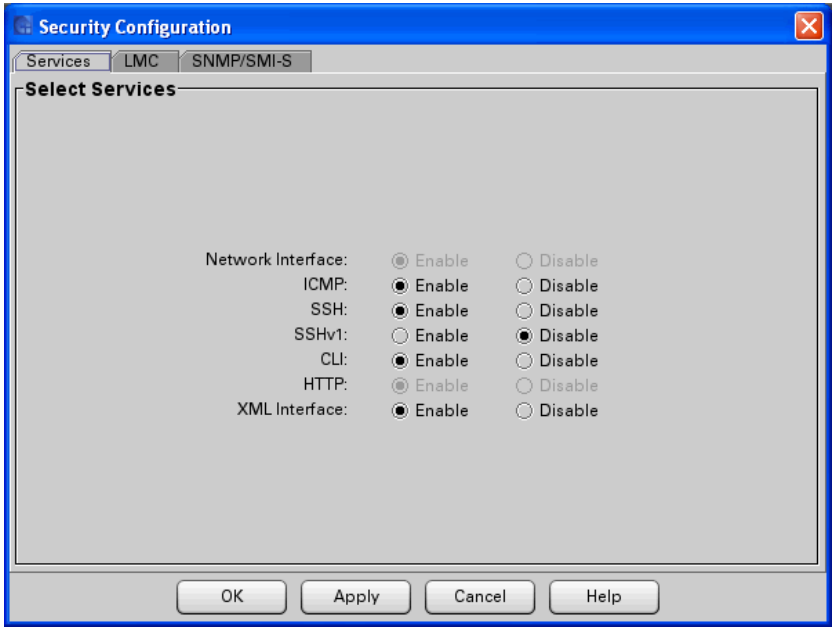
The **Security Configuration** dialog box enables you to restrict external users and various remote services from accessing the library through the Ethernet port on the MCB.

1. Log on as an admin user.
2. Click **Setup > Security**. The **Security Configuration** dialog box appears with the **Services** tab displayed.

Configuring Access for Network Services

The **Services** tab on the **Security Configuration** dialog box enables you to entirely prevent all external access to the library or allow access according to other security settings on the **Security Configuration** dialog box. It also enables you to allow or prevent access by SSH, SSHv1, and to allow or prevent external attempts to discover the library by pinging it.

1 Click the **Services** tab on the **Security Configuration** dialog box.



2 You can change the security settings for any of the following items:

- **Network Interface** — To entirely prevent all external access to the library through the MCB Ethernet port, regardless of other settings on the **Security Configuration** dialog box, select **Disable**. To allow external access to the library in accordance with other security settings on the **Security Configuration** dialog box, select **Enable**. (The **Network Interface** option is unavailable when accessing the LMC remotely.)
- **ICMP** — To prevent external attempts to discover the library by pinging it (by means of Internet Control Message Protocol [ICMP] Echo packets), select **Disable**. Using this setting can prevent denial-of-service (DoS) attacks, which can flood the

library with pings and cause loss of network connectivity and services.

- **SSH** — To prevent Secure Shell access to the library, select **Disable**. To allow SSH to access the library, select **Enable**.
- **SSHv1** — To prevent Secure Shell version 1 protocol from running on the library, select **Disable**. To allow SSHv1 to run on the library, select **Enable.** SSHv1 is enabled by default. If you choose to disable SSHv1, only SSHv2 will connect to the library.
- **CLI** — To access the library using a command line interface, select **Enable**. For more information, see Chapter 14, Using the Command Line Interface.

  Note: Access is gained via SSH. Therefore, to use the CLI to access the library, you must also enable SSH (see above).

- **HTTP** — To prevent access to the library using the Web browser client, select Disable. If you choose to disable HTTP, access to the library is limited to the library's operator panel or the LMC application. To permit access to the library GUI using a Web browser client, select Enable. (The **HTTP** option is unavailable when accessing the LMC remotely.)
- **XML Interface** — If Quantum Vision software is monitoring the library, you need to enable the XML interface so Vision can get the information it needs. In order to select **XML Interface**, the **HTTP** option must also be enabled.

If Dynamic Host Configuration Protocol (DHCP) is enabled for your library on the **Network Configuration** dialog box (**Setup > Network Configuration**), you also should enable ICMP. This ensures that the DHCP server can determine whether the IP address that is assigned to the MCB is still valid. (ICMP is enabled by default.)

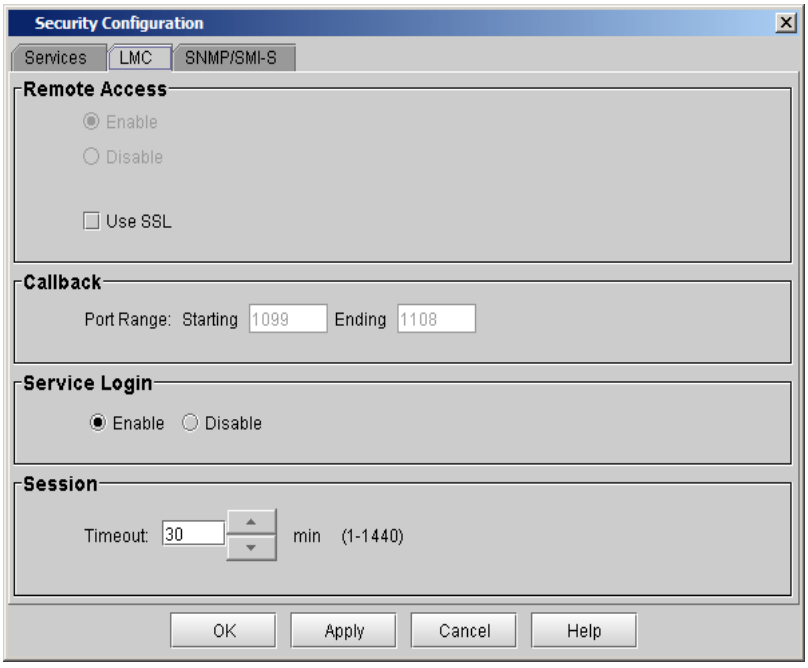
3 If you want to apply the changes, but you do not want to close the dialog box, click **Apply**. Otherwise, click **OK** to apply the changes and close the dialog box.

Configuring Access for Remote LMC Clients

You can use the **LMC** tab on the **Security Configuration** dialog box to configure the following options:

- To allow or prevent remote LMC client access to the library
- To set up firewall access for server callbacks to remote clients
- To enable or disable service login
- To set up the length of time before a session timeout

1 Click the **LMC** tab on the **Security Configuration** dialog box.



2 Change the security settings for any of the following items:

- **Remote Access** — To prevent all remote LMC clients from accessing the library, select **Disable**. To allow them to access the library, select **Enable**.
- Select **Use SSL** to enable secure communication between the LMC client and the library.

  Note: Enabling SSL can impact the network performance of remote operations (for example, downloading new library software).

- **Callback Port Range** — To configure firewall access for server callbacks to remote clients, type the first port number of a

range of ports that you want to be used for callbacks in the **Starting** text box, and then type the last port number in the **Ending** text box. Valid port ranges must fit within the range 1024 to 65535. Remote client service ports must be within the range of ports specified here. Otherwise, callbacks fail because the library's firewall blocks outbound packets designated for out-of-range ports.

- **Service Login** — To allow service login, select **Enable**. To prevent service login, select **Disable**. The Admin user can enable or disable the service user login on both the front panel access and the remote client access.

  Note: The default service login through the service port is still available for use. For security purposes, the service port can be physically locked down by locking the back door of the Scalar i6000.

- **Session** — To configure the length of the session's timeout, type or use the arrow buttons to specify the length of a session before it times out. Valid session timeouts are 1 – 1440 minutes (1 minute to 24 hours). The default is 30 minutes.

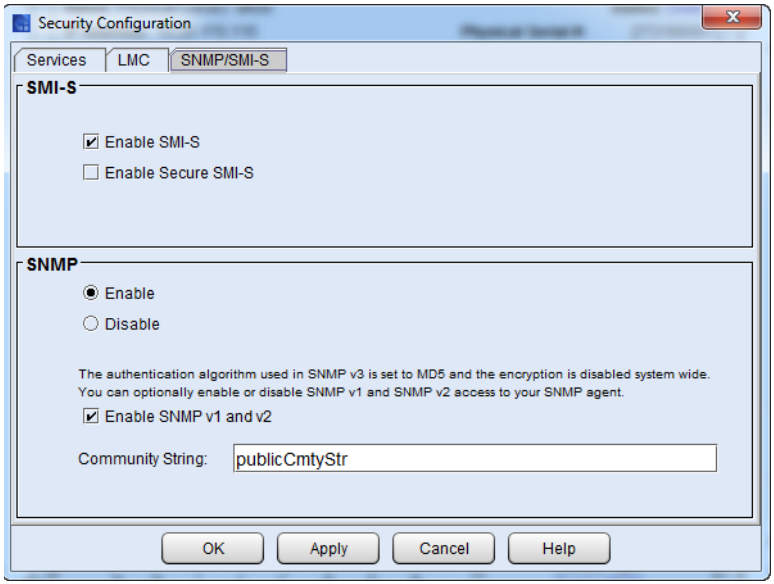
  Note: The Service login timeout is set to 4 hrs and cannot be modified.

3 If you want to apply the changes, but you do not want to close the dialog box, click **Apply**. Otherwise, click **OK** to apply the changes and close the dialog box.

Configuring Access for SNMP and SMI-S

The **SNMP/SMI-S** tab on the **Security Configuration** dialog box allows you to enable or prevent SNMP or SMI-S traffic across the MCB Ethernet port.

1 Click the **SNMP/SMI-S** tab on the **Security Configuration** dialog box.



2 You can change the security settings for any of the following items:

- **SMI-S** — To allow SMI-S traffic (port 5988), select the **Enable SMI-S** check box. To allow encryption of SMI-S traffic (SSL, port 5989), select the **Enable Secure SMI-S** check box.

  Note: Port 427 is used for Service Location Protocol (SLP), which is used along with the Common Information Model (CIM) server.

- **SNMP** — To prevent all SNMP traffic across the MCB Ethernet port, select **Disable**. To allow SNMP Get operations, select **Enable**.

  If SNMP traffic is allowed, then SNMP v3 is always available. If you want to permit less secure SNMP access, select **Enable SNMP v1 and v2**. If you decide you do not want to use SNMP v1 and v2, clear the **Enable SNMP v1 and v2** check box.

You can also change the community string from the default.

The library ignores all remotely issued SNMP SET operations under any circumstance, which means that external applications cannot register themselves to receive SNMP traps from the library. However, the **Trap Registration** dialog box (**Setup > Notifications > Trap Registration**) enables you to perform this registration yourself by entering the necessary IP and port information. For more information about the **Trap Registration** dialog box, see Registering SNMP Traps on page 223.

3 If you want to apply the changes, but you do not want to close the dialog box, click **Apply**. Otherwise, click **OK** to apply the changes and close the dialog box.

Using LDAP

Lightweight Directory Access Protocol (LDAP) is the industry standard Internet protocol that provides centralized user account management. The library supports LDAP Directory servers based on Microsoft Active Directory and Novell eDirectory. For information on how to configure library LDAP settings, see Configuring LDAP on page 232.

You can configure the Lightweight Directory Access Protocol (LDAP) settings any time after the initial library configuration. Once you enable and configure LDAP, you can view your current LDAP settings using the LDAP menu.

Note: Active Directory no longer requires Windows Services for Unix 2.5.

LDAP Server Guidelines

Enabling LDAP allows existing user accounts residing on an LDAP server to be integrated into the library's current user account management subsystem. User account information is centralized and shared by different applications, simplifying user account management tasks. For more information about local user accounts, see Creating Local User Accounts on page 468.

The remote client and operator panel do not allow you to create, modify, or delete user account information on an LDAP server. This must be done by the directory service provider.

User and Group Access

For LDAP accounts with user privileges, access to library partitions is determined by group assignment on the LDAP server. Groups must be created on the LDAP server with names that correspond to the library partition names. User and library groups must reside in or below the group context. Users without administrator privileges must be members of both the user group defined in the LDAP server interface AND part of a group with an identical name as the partition(s) on the library (RDN [Relative Distinguished Name] only) in order to have access to the corresponding partitions on the library. LDAP accounts with administrator privileges have access to all partitions and administrative functions and do not need to be assigned to partition-related groups on the LDAP server.

Note: Usernames and group objects must be in LDAP Distinguished Names formats.

OpenLDAP 2.4

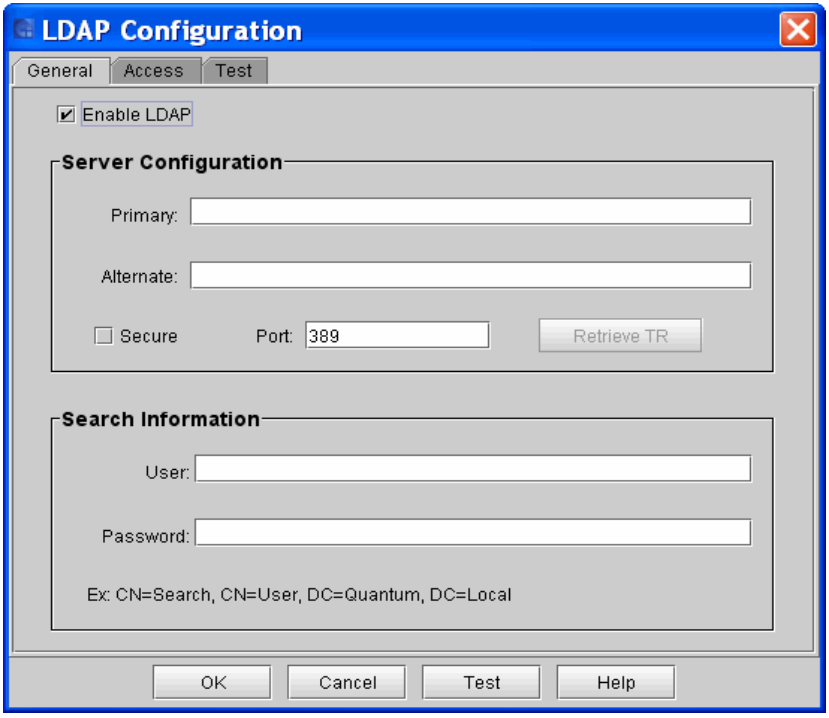
You must install and run OpenLDAP 2.4 or later. The supported Objects in OpenLDAP 2.4 and later are of type “Person” or derived objects, and the group Objects must be of type “GroupOfNames.”

OpenLDAP must be compiled with Overlay Support and requires the installation of “memberOf” overlay. More information can be found in the man pages of OpenLDAP with the “man slapo-member of” command.

Configuring LDAP

You can configure the Lightweight Directory Access Protocol (LDAP) settings any time after the initial library configuration.

1 From the LMC, select **Setup > User Configuration > LDAP**. The **LDAP Configuration** dialog box displays with the **General** tab displayed.



2 In the **General** tab, configure the following items:

- **Enable LDAP**:
  - To enable LDAP, select **Enable LDAP**.
  - To disable LDAP, clear the **Enable LDAP** check box.

  Note: If you disable LDAP, single sign-on functionality will not be available on the library.

- **Server Configuration** section:
  - **Primary:** You must provide a primary IP address or DNS name.
  - **Alternate**: An alternate IP address or DNS name is optional.
  - **Secure**: Use this check box to enable the setup options to access a secure LDAP server, which can be done using any port except 389. The default secure port is 636. If you enable this option, you must retrieve the trusted root

certificate from the LDAP servers. If you use secure LDAP, both LDAP servers specified above MUST use the same trusted root.

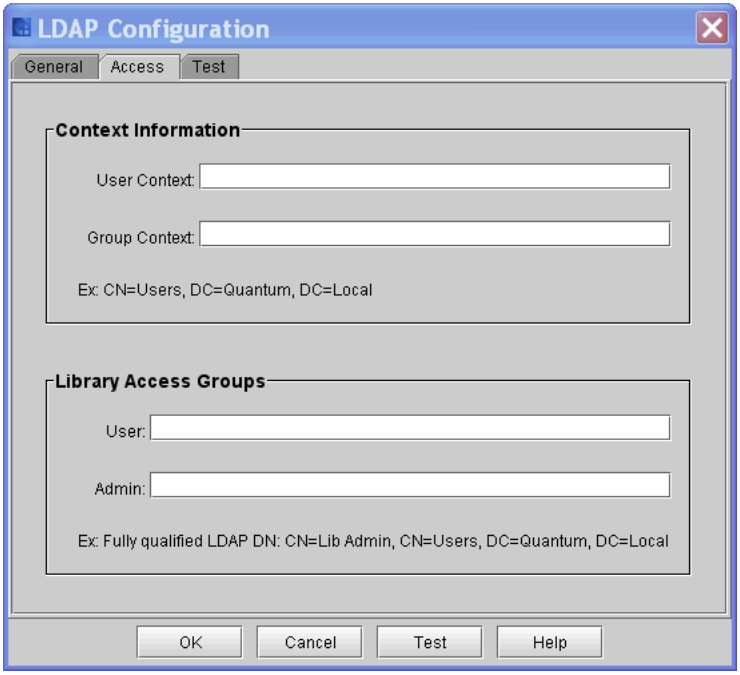
- **Port:** Enter the appropriate port in this field.
- **Retrieve TR:** Use this function to retrieve the trusted root certificate from the primary LDAP server. An MD5 and SHA1 hash is shown to verify the LDAP's server identity.

Note: The first time you use **Retrieve TR**, the process can take 5 to 10 minutes. To connect to a secure LDAP server, you must complete the retrieval process.

Note: This button is only enabled if the **Secure** check box is selected. Some directory servers (for example, Novell eDirectory™) are secure only by default.

- **Search Information** section:
  - Administrative user rights are not required, but the user must have the right to search for all needed user names in the LDAP directory.

3 Click the **Access** tab. Use this tab to configure LDAP authentication.



- **Context Information** section:
  - **User Context**: The User Context is a fully qualified LDAP DN and is used as the base to search for the login users. You can search for a user in the context specified and all contexts below it.
  - **Group Context**: Use this field to search and discover what groups a users is a member of. Only groups which are in the group context or below are considered for library access.
- **Library Access Groups** section:
  - **User**: The group associated with the library. A user that belongs to the library user access group is granted user level permission to access the library. For a user to manage a partition, that user must also be a member of a user group with the same name as the library partition in question.
  - **Admin**: The group associated with the library administrator, equivalent to the local administrative user privilege level. Any member of this group has administrative privileges.

Note: Non-admin library users also need to be members of the groups that match the partition names for which they are granted access. These group names do not need to be specifically listed anywhere in the LDAP setup on the library. When user logins are validated during login, their group memberships for partition access are validated automatically.

4 Test the LDAP configuration.

If you have administrative rights, you can use the Test functionality to simulate an LDAP login for a specific user and quickly discover what access rights the user has and to what partitions the user has access.

Note: If help from support is needed, it is important to run this test. More information is logged using the **Test** option than using the normal login.

Note: The search filter for LDAP is
"(&(|(objectclass=User)(objectclass=person)(objectClass=posixAccount)(objectclass=inetOrgPerson))(|(cn=%USER%)(uid=%USER%)(sAMAccountName=%USER%)))

This means that the objects the LDAP authentication looks for are:
- User
- Person
- posixAccount
- inetOrgPerson

where the
- cn or
- uid or
- sAMAccountName

attributes match the actual username.

To test the LDAP configuration, do the following:

a Click the **Test** tab.

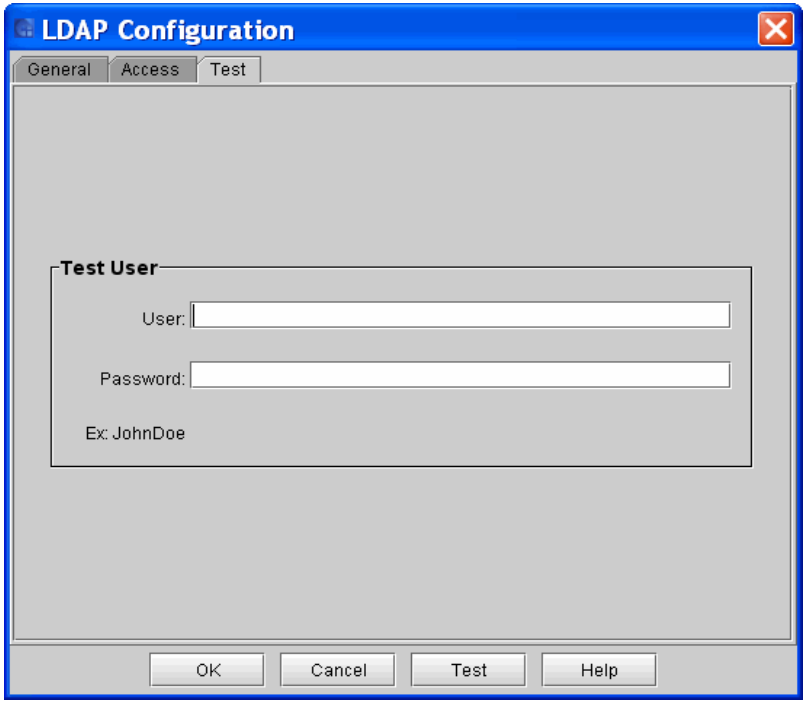
b Fill in the **Test User** section:

- **User**: Type the appropriate user name.
- **Password**: Type the user password.

c After you have entered all the LDAP configurations you wish, click **Test** to verify the LDAP connection.

A message box displays indicating the success or failure of the LDAP connection.

- If the connection failed, the error message contains information that you can use to resolve the issue. Click **OK** to return to the LDAP Configuration dialog box.
- If the connection succeeded, click **OK**.



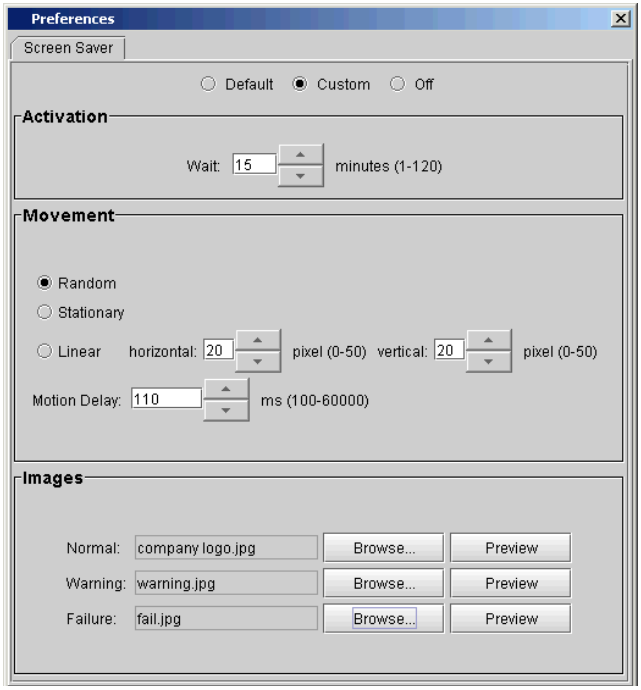
5 To accept and save the library configuration, in the LDAP Configuration dialog box, click **OK**.

Configuring Screen Saver Preferences

Use the **Screen Saver** preferences tab to customize the images that display on the LMC screen when the library is not in use. The screen saver starts automatically if the library is idle for a specified amount of time.

Note: Screen saver preferences can only be configured remotely, not using the touch panel.

1 From the menu bar, click **Setup > System Settings > Preferences**. The **Preferences** dialog box appears with the **Screen Saver** tab displayed.



2 Do one of the following:

- Select **Default** to use the default Quantum screen saver with standard settings.

- Select **Custom** to change screen saver settings such as activation, movement, or images.
- Select **Off** to disable the screen saver. (The current settings are cleared.)

If you selected **Custom**, go to Step 3. Otherwise, go to Step 6.

3 Under **Activation**, enter a value in the **Wait** box to specify how much idle time must pass before the screen saver is activated.

The activation wait time can be 1 – 120 minutes.

4 Under **Movement**, specify the position and the motion of the screen saver image on the screen.

- Select **Random** to display the screen saver image in a variety of positions.
- Select **Stationary** to display a static screen saver image that does not move.
- Select **Linear** to display the screen saver image as a floating image.
- Enter values in the **horizontal** and **vertical** boxes to specify the movement of the screen saver image in pixels.
- Enter a value in the **Motion Delay** box to specify the movement speed of the screen saver image.

5 Under **Images**, specify the image files to display for normal functions, warning notices, and failure notices. You must select image files for all three functions.

- To specify an image file, click **Browse**. Select the image file and then click **Open**. The image file must be in GIF, JPEG, or PNG format, and cannot be larger than 1 MB. In addition, image resolution is limited to 600 x 800 pixels.
- Click **Preview** to preview an image file.

6 Click **OK** to save the settings and close the **Preferences** dialog box.

Or click **Apply** to save the settings without closing the **Preferences** dialog box.

7 Because you made system configuration changes, you are prompted to save the configuration changes. For more information, see Saving and Restoring Library Configuration on page 587.

Working With Data Path Conditioning

The Scalar i6000 provides an automatic means of verifying, monitoring, and protecting data path integrity between hosts and library drives. This feature is referred to as data path conditioning. Using this feature, administrators can proactively detect and resolve data path problems before they affect backup, restore, and other data transfer operations. Data path conditioning ensures that data transmissions are optimized and reliable, resulting in improved system availability.

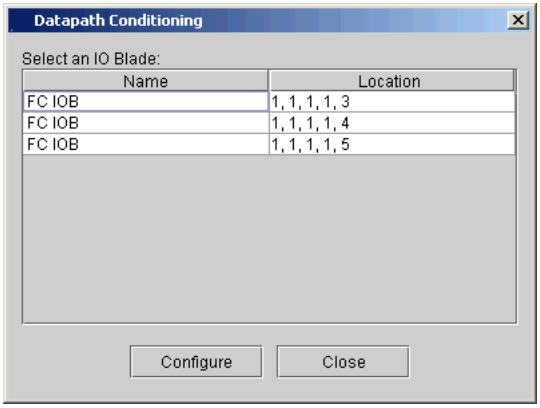
The FC I/O blade manages data path conditioning along the path between itself and the library drives. Data path monitoring automatically occurs at regular, configurable intervals. The I/O blade generates a RAS ticket if monitoring tests fail for two intervals. This indicates either loss of connectivity or drive failure. The FC I/O blades include the data path conditioning feature, and administrators can configure it using the LMC.

Configuring Datapath Conditioning

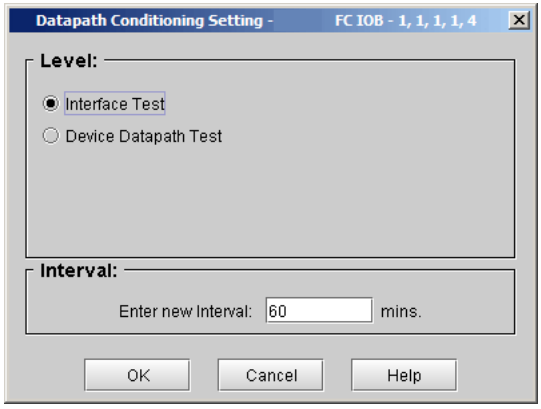
For the library, target-side data path monitoring is performed automatically and proactively. The **Datapath Conditioning** dialog box allows you to set the level at which the data path is monitored between an I/O blade and the drive(s) connected to it. You also can set the time interval between monitoring checks (up to 48 hours).

Note: I/O blades must be present to access the **Datapath Conditioning** dialog box.

1. Log on as an administrator.
2. Make sure that you are viewing the physical library. From the **View** menu, click the name of the physical library.
3. Click **Setup > Blades > Connectivity > Datapath Conditioning**. The **Datapath Conditioning** dialog box appears, showing all the I/O blades found in the library. Each blade is identified by name and by geographic location.



4 Click a blade to highlight it, and then click **Configure**. The **Datapath Conditioning Setting** dialog box appears.



5 In the **Level** area, select the appropriate level. The default level is **Interface Test**. To enable data path monitoring tickets, set the level to **Device Datapath Test**.

The following table describes the functionality for each data path monitoring level.

Level Name	Functionality Description
Interface Test	Performs tests to verify that Fibre Channel controllers on I/O blades are responsive to commands.
Device Datapath Test	Performs tests at the Interface Test level, and also performs a device inquiry on each target device.

6 In the **Enter new Interval** text box, type the amount of time that should elapse between automatic monitoring checks. The interval can range from 1 to 2,880 minutes (48 hours). The default interval is 60 minutes.

Note: The data path from I/O blade to the drive must experience problems for two period intervals before a problem is detected and a ticket is generated.

7 To save your configuration and return to the **Datapath Conditioning** dialog box, click **OK**.

About the Configuration Record

The configuration record contains details about the library's configuration and can be sent to a specified e-mail address or saved as a.txt file.

Information in the configuration record includes:

- Product information — Product name and version, MCB and RCU versions, serial number, and modules/drives/partitions configuration
- License information — License descriptions, quantities, and installation dates
- Network information — Hostname, DHCP status, IP address, and IP, Netmask, and Gateway addresses
- Partition information — Serial numbers, online/offline statuses, and numbers of slots, drives, and I/E slots
- Drive information, for each drive — Location, partition, SCSI element address, online/offline status, vendor, model, serial number, logical serial number, firmware version, drive type, and interface type:
  - SCSI tape drives — SCSI ID
  - Fibre Channel (FC) tape drives — World Wide Name (WWN) and loop ID, speed, and connection type

Note: If the FC tape drive is attached to an FC I/O blade, the WWN indicates the WWN of the I/O blade, not the tape drive.

- I/O blade information — Blade type, location, firmware version, serial number, WWN, and CC LUN

Before you can e-mail the configuration record, the library e-mail account must be configured. For information on configuring the library e-mail account, see Configuring E-mail on page 177.

For instructions on how to e-mail or save the configuration record, see Mailing or Saving the Configuration Record on page 540.

Setting Aisle Lights

Aisle lights are optional on each module, and are mounted to the roof of each module to illuminate the inside of the library.

To set the duration for aisle lighting:

1. From the main console, select **Setup > System Settings > Aisle Lights**. The **Aisle Light Settings** dialog box appears.
2. Select a duration for the light to illuminate: **30 minutes, 1 hour**, or **Always Off.**
3. Click **OK**.

Note: Regardless of the selected setting, the aisle lights will turn off automatically during all inventory and teach operations. At the completion of these events the lights are automatically turned back on if they were on prior to these operations.

Note: For the time limited settings, if the lights were on before the operation, the timer starts over when the lights are automatically turned on.

Note: For time limited aisle light settings, user interaction, such as using the touch panel or opening an I/E station or aisle door, causes the timer to reset. The lights will automatically turn on if they are not already.

Note: The default setting is **Always Off.**

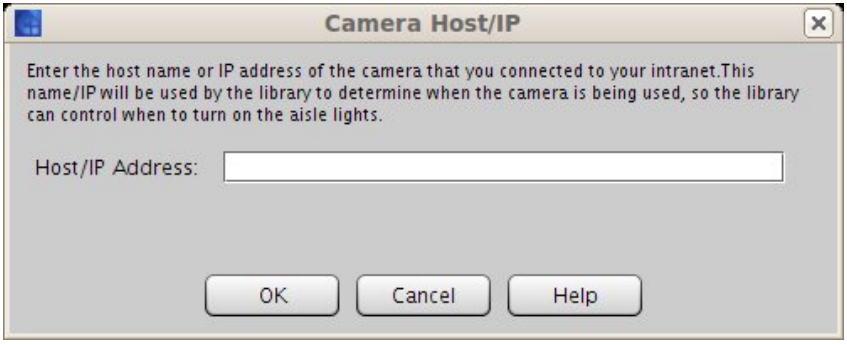
Configuring a Webcam For Your Library

If desired, you can install a webcam in your library to monitor activity.

As of version 10.2, if you install a webcam in your library, the library aisle lights turn on when the webcam is operating and then turn off when it is stopped. In order to enable the library to control when the aisle lights should be switched on and off in synchronization with webcam usage, you must enter the webcam's IP address.

To enter the webcam's IP address:

1. From the main console, select **Setup > System Settings > Camera Host/IP**. The **Camera Host/IP** dialog box appears.



2. Specify the host name or IP address of the webcam that's connected to your intranet.
3. Click **OK**.

Note: As always, the aisle lights will continue to turn off automatically during all inventory and teach operations. At the completion of these events the lights are automatically turned back on if they were on prior to these operations. For the time-limited settings, if the lights were on before the operation, the timer starts over when the lights are automatically turned on. So even if the webcam is off, the aisle lights will turn on during these operations.

Additional Information

For more information about purchasing a webcam for your library, contact your Quantum sales representative.

For webcam installation instructions, refer to the *Scalar i6000 Installation Guide*.

After you install the webcam, you can learn about its operation by referring to the documentation that came with the webcam, or by downloading the user's guide from www.axis.com.

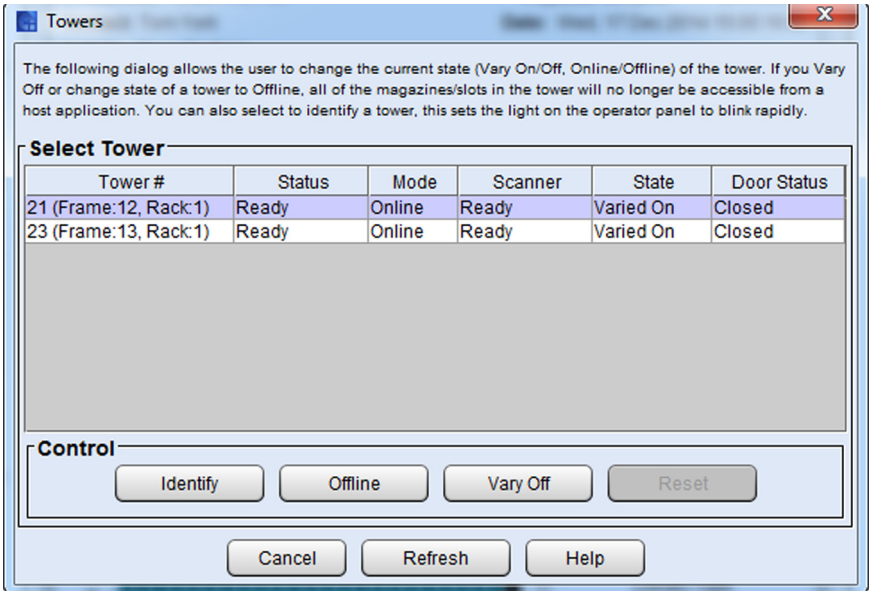
Note: If the webcam timestamp is inaccurate, this may indicate that the battery needs to be replaced. Refer to the webcam documentation for instructions to replace the battery.

Working with Towers

New to the i6000 library are high-density expansion modules (HDEM) or towers. These modules have larger storage capacities making them ideal for libraries where space is an issue.

If your library has a tower installed, you can manage, monitor and maintain it.

1 From the **Tools** menu, select **Towers**. The **Towers** dialog box displays.



The **Towers** dialog box displays all the towers currently installed in the library and gives details about them, including:

- **Tower #** — The index of the tower in the library.

  Note: The **Tower #** column shows the physical addressing of the tower (i.e. Frame 2, Rack 1) but also the index number of the tower(s) in the library. Libraries with multiple towers will see them listed in the **Tower #** column as only odd numbers, 1, 3, 5, etc. This is to accommodate future tower expansion.

- **Status** — If the tower is available.
- **Mode** — If the tower is online or offline. When a user sets the tower to Offline mode, the tower will not be accessible to a host but can be used for UI operations, such as move media.
- **Scanner** — Status of the barcode scanner:
  - **Unknown** - scanner is present but not working properly
  - **Not Present** - scanner is not installed
  - **Removed** - scanner has been taken out of the tower
  - **Failed** - scanner is not working properly

- **Ready** - scanner is installed and working properly

- **State** — Whether the tower is varied on or off. Varying Off a tower allows a user to open the rear access door to perform any necessary tower access or maintenance. If a tower is not Varied Off before the rear access door is opened, the tower will automatically go to a Varied Off state and the library will issue a ticket. When a user Varies Off a tower it will no longer be accessible to a host or UI operations.
- **Door Status** - Whether the rear access door is open or closed.

2 In the **Control** section of the **Towers** dialog box, you can click the following buttons:

- **Identify** — This identifies the tower by setting the **Tower Enable** button to blink a pattern for a minute before returning it to its original state. For more details on the blinking patterns for the Tower, see Interpreting HDEM Tower Enable Button Blinking Pattern on page 105.
- **Offline/Online** — Takes the tower offline or online depending on what is displayed in the **Mode** column.
- **Vary Off/On** — Varies the tower either on or off depending what is displayed in the **State** column.
- **Reset** — Resets the HDC in the selected tower. The selected tower must be **Varied Off**.
- **Cancel** — Closes the **Towers** dialog box.
- **Refresh** — Refreshes the Towers dialog so it displays the most current information.
- **Help** — Displays the i6000 online help page referencing the tower.

Chapter 4
Active Vault

The Active Vault feature allows you to keep tape cartridges vaulted within a physical library, rather than having to move them to other onsite or offsite locations. These cartridges are stored in an "Active Vault" partition that is not managed by a host and contains no tape drives. You can configure policies on standard partitions to redirect SSCI host initiated tape cartridge export MOVE operations directly to an Active Vault partition, or you can configure a plug-in to query an external application where the export move operation is intended for an Active Vault partition. Additionally, Active Vault partitions can be enabled for EDLM policies that provide for regularly timed media scan operations.

This chapter covers:

About Active Vault

- The Active Vault feature requires an Active Vault license (see Enabling Licenses on page 115).
- You can move tapes between Active Vault partitions and standard partitions via the library user interface without exporting and importing the tapes (for more information, see Moving Media Between Active Vault or AMP and Standard Partitions on page 690).

Note: Manual movement between library managed partitions and standard partitions will require inventory reconciliation with the backup application managing the standard partition. SCSI Unit Attention 6/2800 and 6/2801 inform host applications of the need to refresh element status.

- Active Vault partitions are library managed partitions. They are not accessible to hosts.
- Active Vault partitions are composed of unlicensed slots. If the size of the Active Vault partition exceeds the number of available unlicensed slots, then the partition will be composed of both unlicensed and licensed slots, or use all licensed slots.
- Active Vault partitions may configure I/E station slots.
- Active Vault partitions do not contain drives.
- You may have multiple Active Vault partitions. However, the total number of standard and library managed partitions cannot exceed the maximum of 16 partitions.
- Library managed Active Vault partitions can be configured with EDLM policies (see Chapter 9, Extended Data Lifecycle Management).

Configure Active Vault

Active Vault policies are configured on standard partitions. The policies intercept host commands that export tape cartridges to library

managed Active Vault partitions. Configuring Active Vault involves the following:

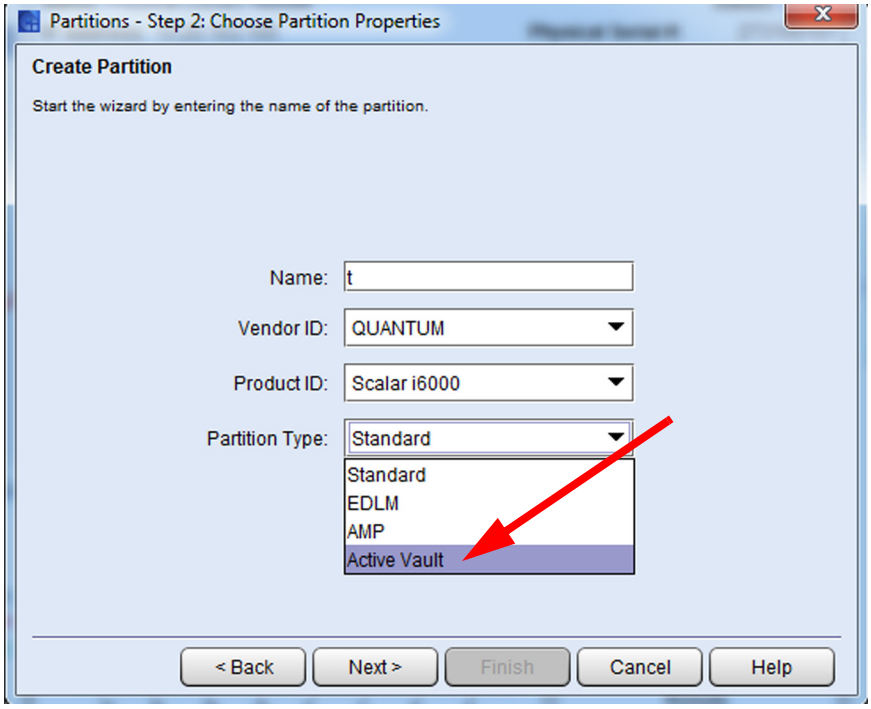
- Create Active Vault Partitions on page 251
- Configure Access to External Applications on page 252 (optional)
- Configure Active Vault Policies on Partitions on page 252
- View Active Vault Partition Policies on page 256

Note: Manual movement between library managed partitions and standard partitions will require inventory reconciliation with the backup application managing the standard partition. SCSI Unit Authentication G/2800 and G/2801 is for host applications with the need to refresh element status.

Create Active Vault Partitions

Create one or more Active Vault partitions as follows:

1. Make sure you are viewing the physical library. From the **View** menu, select the name of the physical library.
2. Make sure the Active Vault license is installed on the library (see Enabling Licenses on page 115).
3. Use Expert Mode to create one or more library managed Active Vault partitions. Follow the instructions in Using Expert Mode on page 131. When you get to the screen named **Partitions - Step 2: Choose Partition Properties**, select **Library Managed (Vault)** from the **Partition Type** drop-down menu.



Configure Access to External Applications

This is optional. You only need to do it if you want to use the library to determine if the external application has a vault name that matches the name of an active vault partition in the library.

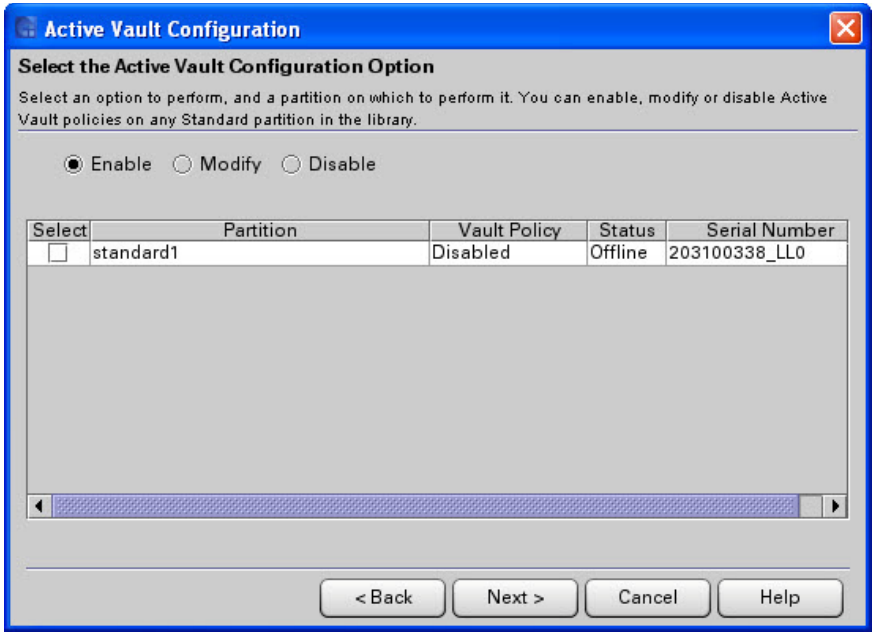
If you want to use an external application to direct media to Active Vault partitions you first need to configure the library for external application access. Follow the steps in Chapter 11, Configuring Access to StorNext, and then return here. You will then be able to select external application policies in the next step.

Configure Active Vault Policies on Partitions

You can only configure an Active Vault Policy on standard partitions (not library managed partitions). This policy redirects SCSI host initiated tape cartridge export MOVE operations to an Active Vault.

1 Click **Setup > Partitions > Policies > Active Vault Configuration**. The **Active Vault Configuration Wizard** appears.

2 Click **Next**. The **Select the Active Vault Configuration Option** screen appears.

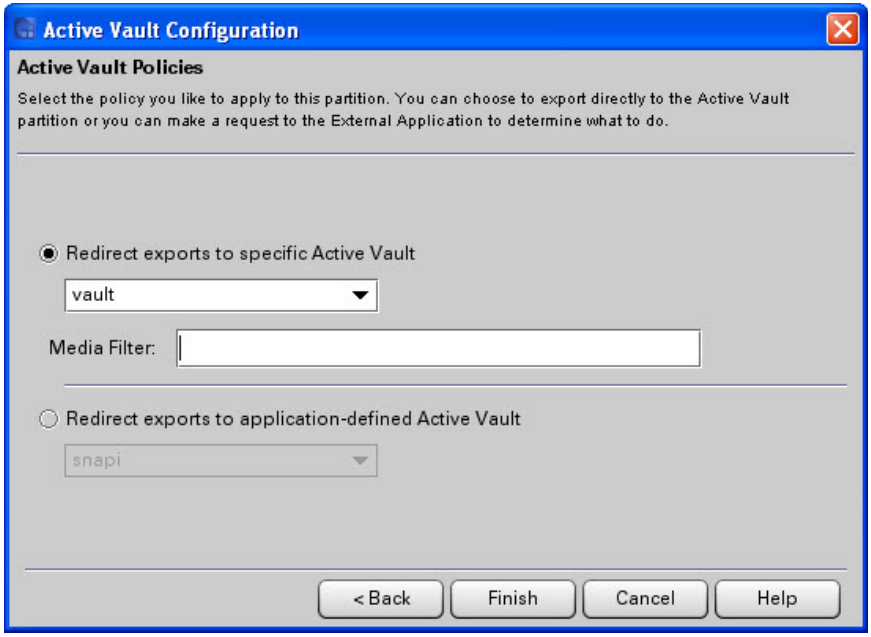


3 Create, modify, or remove policies on a standard partition by doing one of the following:

To...	Do this...
Enable Active Vault policy	1 Select **Enable**. 2 Select a partition from the table that has Active Vault policies disabled. 3 Proceed to Step 4.
Modify existing Active Vault policy	1 Select **Modify**. 2 Select a partition from the table that has Active Vault policies enabled. 3 Proceed to Step 4.

To...	Do this...
Disable Active Vault policy	1 Select **Disable**. 2 Select a partition from the table that has Active Vault policies enabled. 3 Click **Finish**. A confirmation dialog box appears asking you to confirm you want to disable the Active Vault policies on the partition. 4 Click **Yes** to confirm. A "success" dialog box appears. 5 Click **OK** to close the dialog box. Process is complete.

4 Click **Next**. The **Active Vault Policies** screen appears.



5 Choose one of these redirect options:

Policy	Description
Redirect exports to specific Active Vault.	If you select this option, you must select an Active Vault partition from the drop-down list. All host-initiated export requests to move tapes from this partition will redirect the tapes to the specified Active Vault partition instead of the I/E station. If desired, you can specify which media to move by typing a value in the **Filter Media** field. For example, entering a value of ***123L4** will cause all media with barcodes ending with 123L4 to be vaulted. Entering a value of **123*** will cause all media with barcode starting with 123 to be vaulted. **Note:** Only host-initiated export operations will be redirected to the Active Vault. UI-initiated export operations will still move tape cartridges to an I/E element.
Redirect exports to application-defined Active Vault.	If you select this option, you must select an external application plug-in from the drop-down list. When a host-initiated export operation occurs, the library queries the selected external application for the name of the vault that may be associated with the export operation. If the name of the application-tracked vault matches the name of one of the Active Vault partitions in the library, the export request is re-directed to that Active Vault partition. If the name of the application-tracked vault does not match the name of an Active Vault partition in the library, the export request will be directed to the I/E element as specified by the host command. **Note:** Only host-initiated export operations will be redirected to the Active Vault. UI-initiated export operations will still move tape cartridges to an I/E element.

6 Click **Finish**. A confirmation dialog appears.

7 Click **OK** to close the dialog.

View Active Vault Partition Policies

To review the policies you configured, you can go back through the Wizard, or you can click **Monitor > Partitions > Policies**. See Monitoring Partition Policies on page 534 for more information.

Chapter 5
Advanced Reporting

Advanced Reporting is a licensed features that gives you access to the following reports:

- Drive Utilization Report (see Viewing the Drive Resource Utilization Reports on page 596)
- Media Integrity (see Viewing Tape Alerts and Generating Media Integrity Analysis Reports on page 59)
- Media Security Notifications (see Setting Up Media Security Notifications on page 186 and Viewing the Media Security Events Report on page 188)
- Media Usage (see Media Usage Report on page 258).
- Advanced Reporting Options (see Setting Up Advanced Reporting Options on page 602

The Advanced Reporting reports can be found under the **Tools > Reports** menu along with other library reports that do not require the Advanced Reporting license.

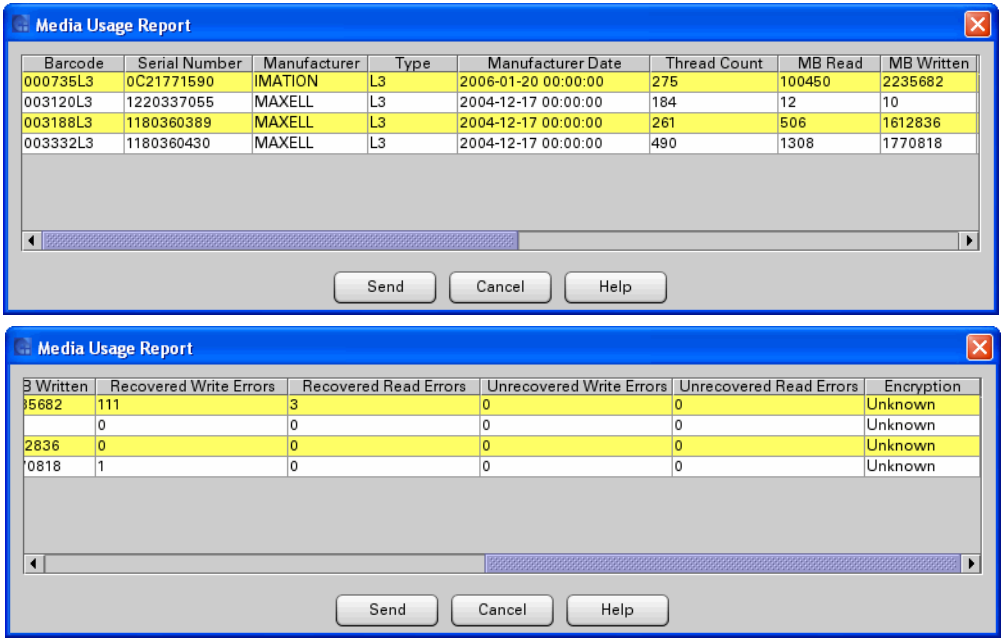
In addition, Advanced Reporting feature allows you to schedule certain library reports to be automatically generated and e-mailed to designated recipients (**Tools > Reports > Reporting Options**). See Setting Up Advanced Reporting Options on page 602.

Media Usage Report

The Media Usage Report collects information on all media that have ever been in the library, including media that is no longer in the library. Lifetime media usage metrics are associated with the cartridge and are kept on the embedded chip. The report reflects what the drive reports from the media chip whenever the media is unloaded, and lists any associated errors.

When the log reaches maximum size, old information is deleted as new information is added.

1. Log on as an administrator.
2. From the main menu, select **Tools > Reports > Media > Usage**. The **Media Usage Report** dialog box is displayed.



The report provides the following information:

Field	Description
Barcode	Media cartridge barcode label.
Serial Number	Media cartridge serial number.
Manufacturer	Media cartridge manufacturer.
Type	Media type (L1, L2, L3 L4, L5, L6, LR, LS, LT, LU, LV, LW)
Manufacturer Date	Media cartridge manufacturing date (format: YYYYMMDD)
Thread Count	Number of times the tape has been mounted and threaded on the drive
MB Read	Cartridge lifetime MB read.
MB Written	Cartridge lifetime MB written.
Recovered Write Errors	Errors in writing data where an attempt to re-write the data was successful.
Recovered Read Errors	Errors in reading data where an attempt to re-write the data was successful.
Unrecovered Write Errors	Errors where all re-write attempts failed and the data could not be successfully written to the tape
Unrecovered Read Errors	Errors where all re-read attempts failed and the data could not be successfully read from the tape
Encryption	Cartridge Encryption Status (**U**=Unknown, **E**=Encrypted, **N**=Not Encrypted)

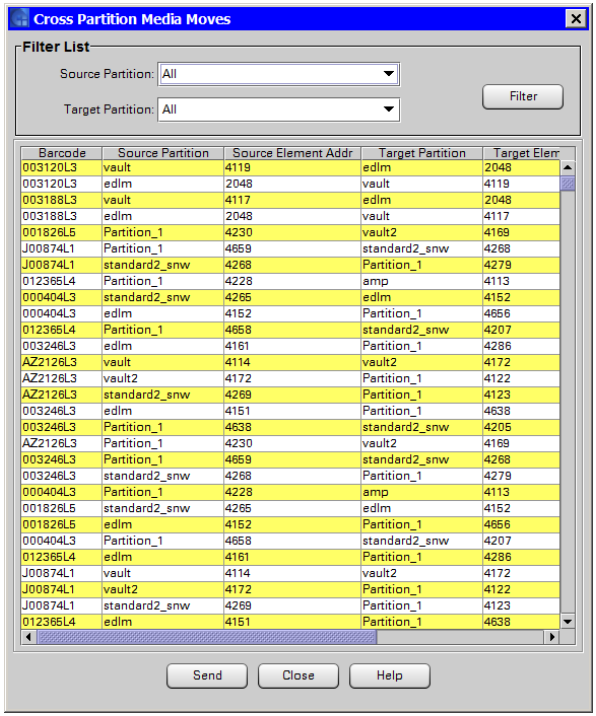
3 To send the report to your e-mail, click **Send**.

Viewing Cross-Partition Media Moves

The library creates a report for media moved across partitions which you can view, save or e-mail.

To view cross-partition media moves

1. Log on as an administrator.
2. Click **Tools > Reports/Media/Moves**. The **Cross Partition Media Moves** report appears.



3. If desired, filter the report output by selecting a single source partition and/or a single target partition from the **Source Partition** and **Target Partition** fields respectively. Click **Filter** to apply your selections and update the report.

The Cross Partition Media Moves report provides the following information pertaining to media moves across partitions:

Field	Description
Barcode	The barcode label number for the tape cartridge moved across partitions
Source Partition	The partition in which the moved tape cartridge originally resided
Source Element Addr.	The element address in the source partition
Target Partition	The target partition to which the tape cartridge was moved
Target Element Addr.	The element address in the target partition
Date	The date on which the tape cartridge move occurred

4 Click **Send** to display the **Print/Save/Email** dialog box.

5 Do one of the following:

- Click **Email** and specify an e-mail recipient for the report. Click **OK**.
- Click **Save** and navigate to the location where you want to save the report. Click **OK**.
- Click **Print** to print the report. Click **OK**.
- Click **Cancel** to return to the report screen

6 When you are finished with the report, click **Close**.

Chapter 6
Automated Media Pool

The Automated Media Pool (AMP) feature allows you to pool media, such as scratch tapes, within a library managed partition to facilitate selective tape cartridge assignments from the media pool to standard partitions without the need for operator intervention to physically load/import additional tape cartridges into standard partitions. Instead of requiring physical import operations to each partition, the Automated Media Pool can contain a number of tape cartridges that can be moved or assigned to a partition via a user-interface-initiated media move or magazine assignment selection at any time.

In addition, the AMP feature allows for the creation of standard partition AMP extensions such that a standard partition gets created with a specified number of actual and accessible storage elements as well as logical, inaccessible element extensions. As a standard partition requires additional accessible storage elements, logical elements can be associated with physical magazines from the AMP such that the logical element extension becomes an actual physical storage element that can now report an accessible status to a host.

Benefits include:

- You can easily move and reassign tapes from the AMP to standard partitions and from standard partitions to the AMP. This allows you to adjust the amount of media within a partition as needed without performing import/export operations (for more information, see Moving Media Between Active Vault or AMP and Standard Partitions on page 690).

- The AMP can provide a “staging area” for scratch tapes and tapes that are no longer needed for backup. When a tape is needed by a partition, it can be moved from the AMP instead of having to be physically imported into the library partition.
- The number of partition accessible storage units can be expanded or reduced as needed without having to reconfigure the library, partition or host application.
- .
- Tapes can be auto-imported from an AMP partition to standard partitions based on filters set up to associate tapes with standard partitions by barcode range.
- Tapes can be auto-exported to an AMP partition via policies to redirect standard partition export MOVE requests.

Note: Manual movement between library managed partitions and standard partitions will require inventory reconciliation with the backup application managing the standard partition. SCSI Unit Attention 6/2800 and 6/2801 inform host applications of the need to refresh element status.

This chapter includes:

Requirements for Automated Media Pool

- The AMP feature requires a Partition license (see Enabling Licenses on page 115).
- Multiple automated media pool partitions can exist. Since they are library managed partitions, an AMP exists solely within the library and is not accessible to hosts.
- You may have multiple AMP partitions. However, the total number of standard and library managed partitions cannot exceed the maximum of 16 partitions.
- All storage slots in the AMP partition must be licensed (via COD).
- AMP partitions do not contain drives.

Configure Automated Media Pool

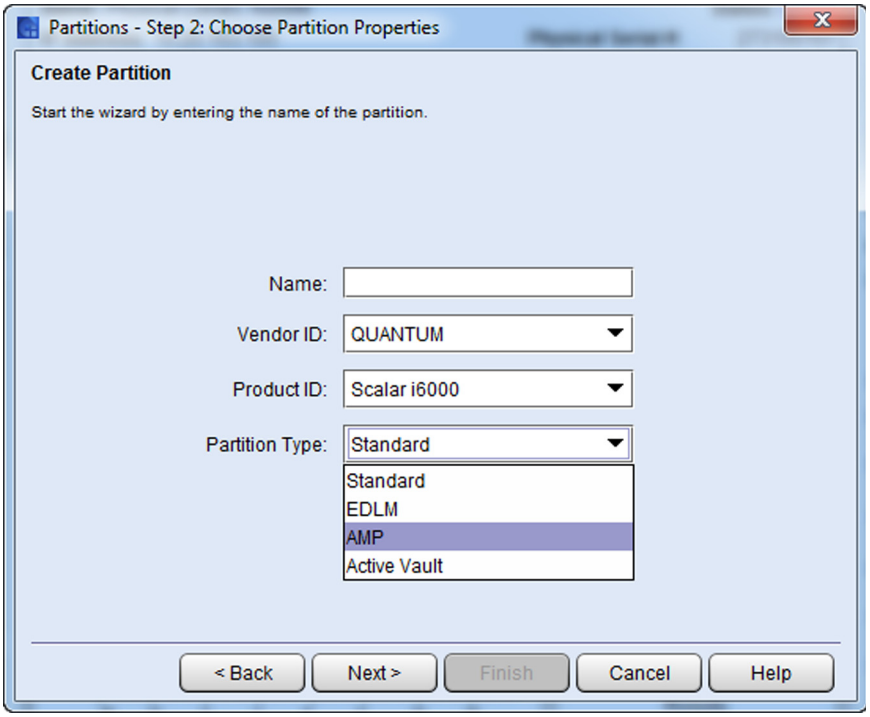
To configure an AMP, you need to set up one or more AMP partitions from which to draw media and optional magazine assignments. If you want to use magazine assignments, you must also configure magazine extensions in one or more standard partitions.

- Create an AMP Partition on page 265
- Create Magazine Extensions in Standard Partitions on page 266
- Configure AMP Import Policies on page 267
- Configure AMP Auto Export Policies on page 267

Create an AMP Partition

1 Use Expert Mode to create one or more AMP library managed partitions. Follow the instructions in Using Expert Mode on page 131.

When you get to the screen named **Partitions - Step 2: Choose Partition Properties**, select **AMP** from the **Partition Type** drop-down menu.



Create Magazine Extensions in Standard Partitions

Magazine extensions are logical storage slot extensions of a standard partition. You need at least one AMP partition to take advantage of actually assigning storage element extensions, so you must create magazine extensions in one or more standard partitions. You can use magazines from an AMP partition to provide additional storage slots as needed.

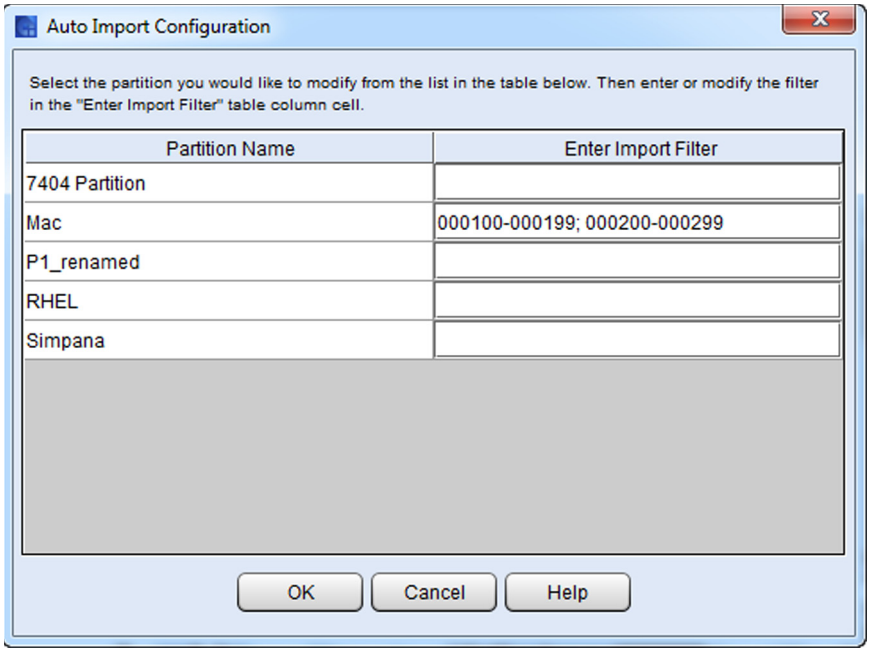
If the standard partition you want to use with the AMP partition doesn't have extensions defined, you must modify the standard partition (see Modifying Partitions on page 137).

Note: You can only create magazine extensions in standard partitions (not library managed partitions).

Configure AMP Import Policies

You can only configure import AMP policies on standard partitions (not library managed partitions).

1 Click **Setup > Partitions > Policies > Auto Import Configuration**. The **Auto Import Configuration** dialog appears.



2 For a specific partition, enter a range of barcode numbers in the **Enter Import Filter** field. Multiple filters can be listed but must be separated by a semi-colon.

3 Click **OK**.

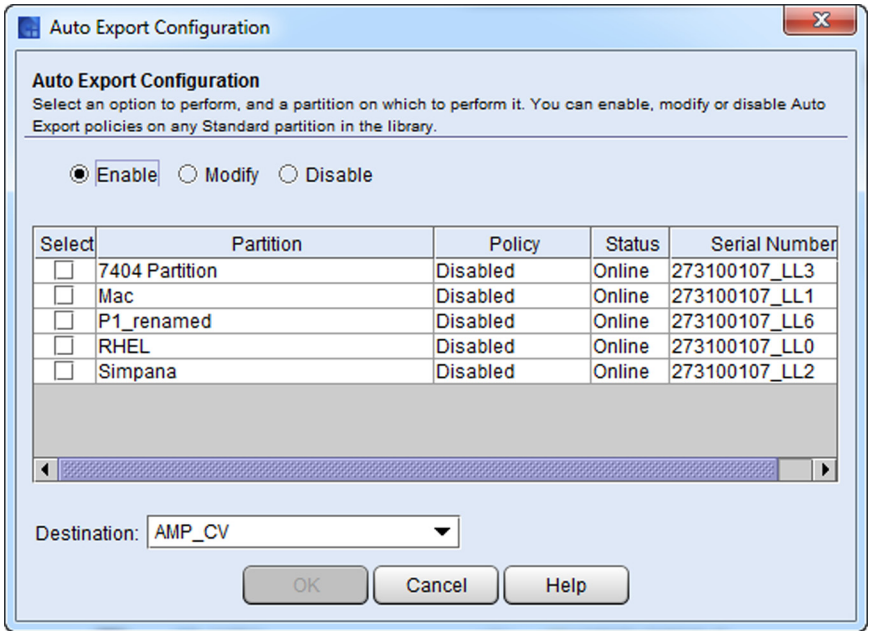
Note: Import filters will be applied to the barcode label only. The filters will not consider any media ID (e.g. L4, L5, etc) on the barcode.

Configure AMP Auto Export Policies

You can only configure export AMP policies on standard partitions (not library managed partitions). However, this export function cannot be performed from the user interface. Instead, any SCSI MOVE commands performed on the standard partition to an assigned I/E elements will

have the media redirected to the designated AMP partition. See Step 5 on page 254 in Chapter 4, Active Vault for redirect options.

1 Click **Setup > Partitions > Policies > Auto Export Configuration**. The **Auto Export Configuration** dialog appears.



2 Select the partition for which you want to enable, modify or disable the policy by clicking the checkbox in the **Select** column.

3 From the **Destination** drop-down menu, select the AMP partition to which you want the tapes exported.

4 Click **OK**.

Use an Automated Media Pool

An AMP has two functions:

- Assign Storage Magazines to/from the AMP on page 269 — Assigns storage elements from the AMP to a standard partition, or from a

standard partition to the AMP. This allows you to control access to partition storage elements without requiring partition reconfiguration for host applications.

- Move Media to/from the AMP on page 271 — Physically moves media from the AMP to a standard partition, or from a standard partition to the AMP. The media then belongs to the partition into which it was moved.

Assign Storage Magazines to/from the AMP

If a standard partition has used all of its physical slots and needs more storage elements, you can assign more slots from the storage pool in the AMP to the partition's logical element extension address range. The host will then recognize these slots as accessible and begin using them.

Similarly, if a partition no longer needs all of its storage slots, you can assign storage elements (magazines) back to the AMP so that these magazines can be assigned and used by other standard partitions.

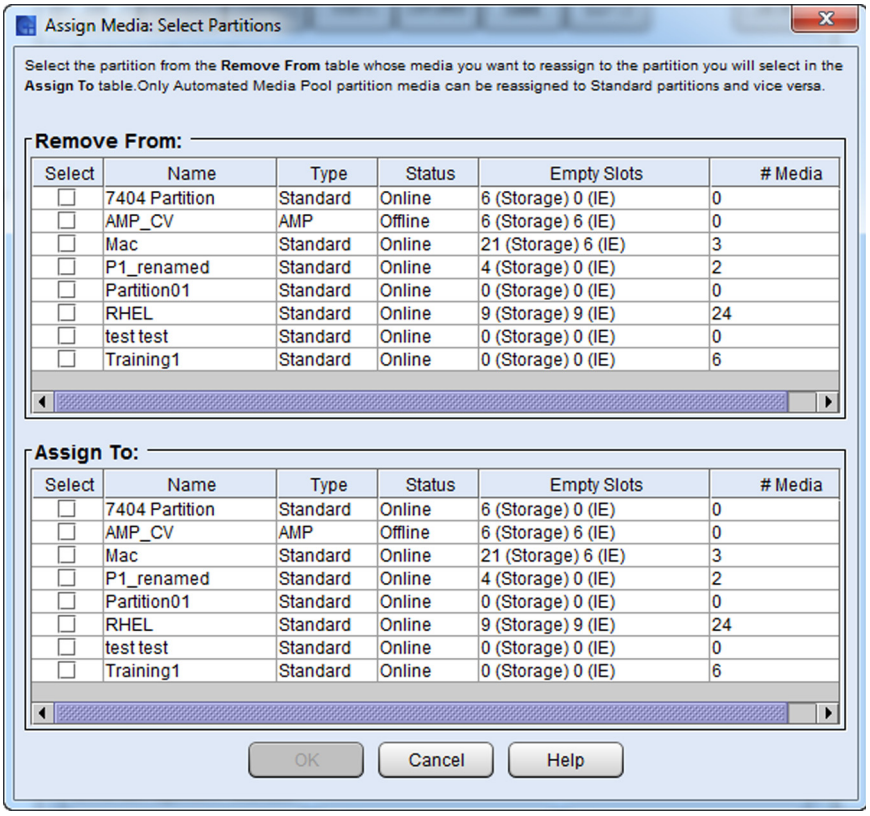
The following rules apply when assigning storage elements:

- The AMP must have slots (at least one magazine) available.
- The number of slots you want to reassign are referenced in magazine increments.
- The standard partition must have sufficient "magazine extensions" configured to allow magazine assignments.
- Magazines can be reassigned whether or not they contain tape cartridges. Any cartridges in the magazines will be reassigned to the new partition along with the magazines, so be careful when reassigning magazines.
- Operations to reassign magazines will not take standard partitions offline since the slots were already configured and known to the host.

To reassign storage:

1. Make sure you are viewing the physical library (from the **View** menu, select the name of the physical library).
2. Make sure that the standard partition has sufficient "magazine extensions" configured (see Create Magazine Extensions in Standard Partitions on page 266.

3 Click **Setup > Partitions > Automated Media Pool > Assign Magazines**. The **Assign Magazines: Select Partitions** screen appears.

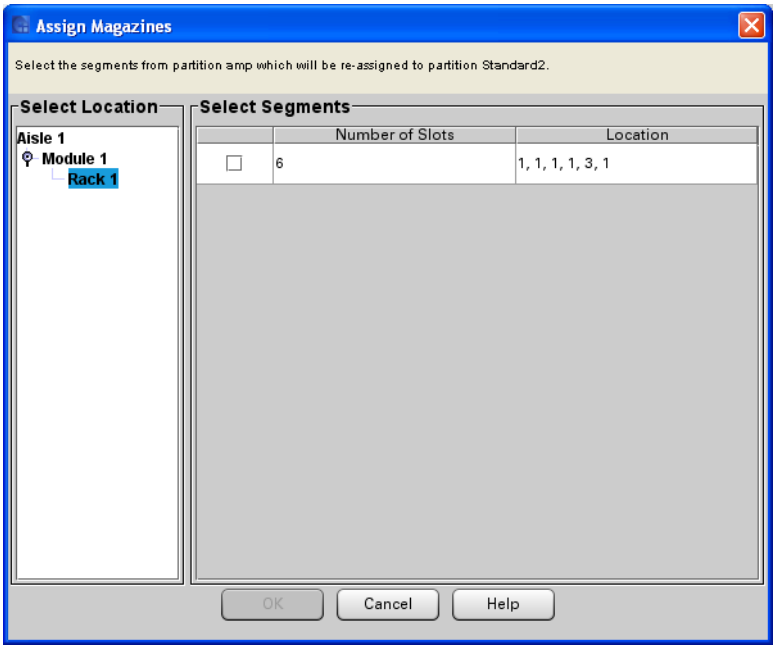


4 Select the partition from which you wish to remove magazines from the **Remove From** list.

5 Select the partition to which you wish to assign magazines from the **Assign To** list.

Note: The Empty Slots column displays both storage and IE slots.

6 Click **OK**. The **Select Segments** screen appears.



7 Select the module(s) and rack(s) from the **Select Location** column.

8 Select the magazine segment(s) from the **Select Segments** column.

9 Click **OK**. The magazines are reassigned.

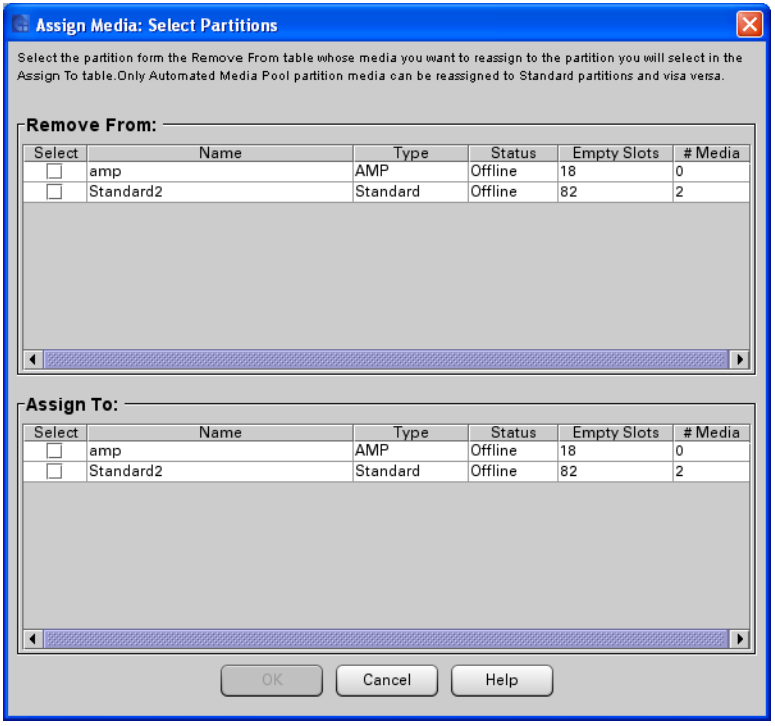
Move Media to/from the AMP

Moving media from an AMP to a standard partition and vice versa physically moves the media into the target partition and reassigns the media to that partition.

Note: You can also accomplish this by following the instructions in Moving Media Between Active Vault or AMP and Standard Partitions on page 690.

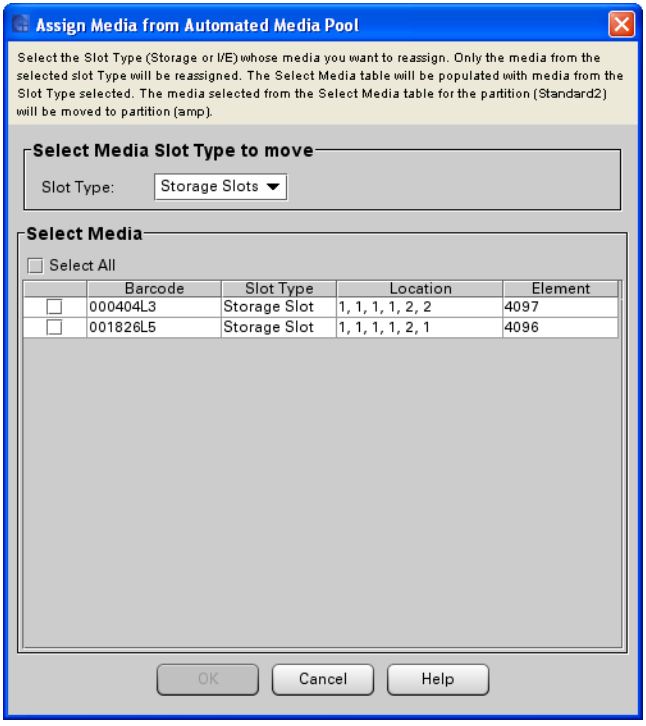
1 Make sure you are viewing the physical library (from the **View** menu, select the name of the physical library).

2 Click **Setup > Partitions > Automated Media Pool > Assign Media**. The **Assign Media: Select Partitions** screen appears.



3 From the **Remove From** section, select a partition from which to move media. From the **Assign To** section, select a partition into which to move media.

4 Click **OK**. The **Assign Media from Automated Media Pool** screen appears.



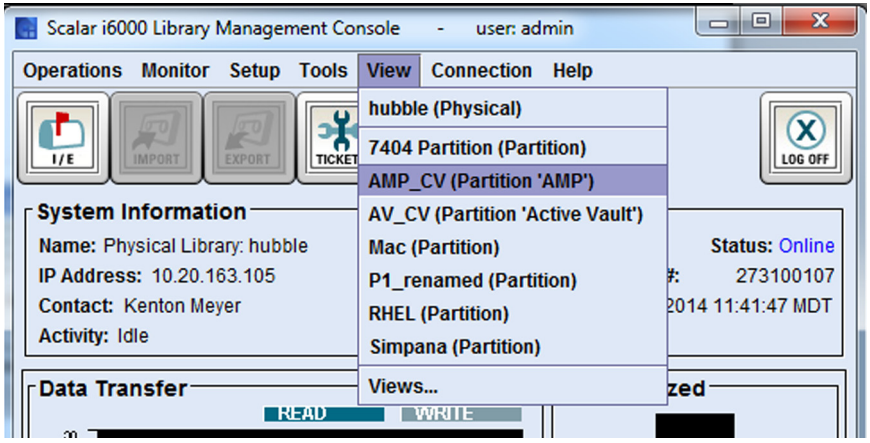
5 From the **Select Media Slot Type to move** drop-down list, select the area from which you want to move the media (Storage Slots or I/E Slots).

6 From the **Select Media** list, select the tape(s) you want to move.

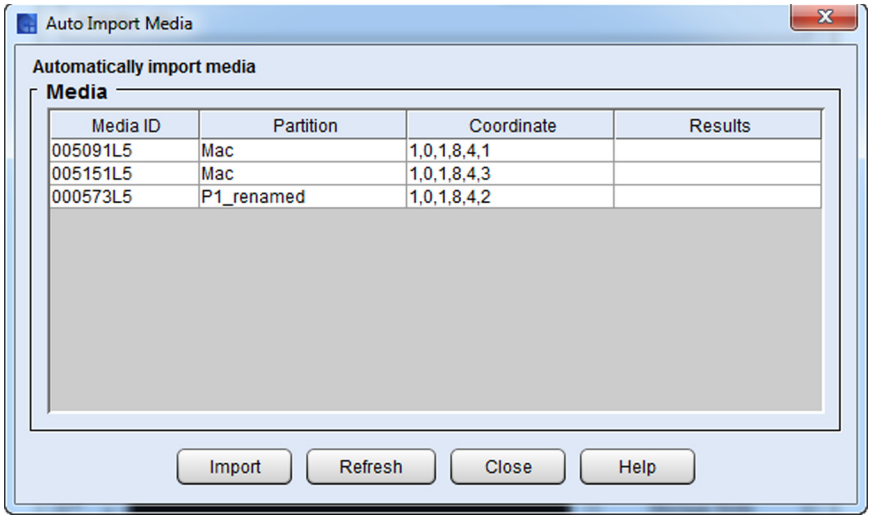
7 Click **OK**.

Auto Import Media

1 From the **View** menu, select the AMP partition from which you want to import tapes.



2 Select **Operations > Auto Import...**The **Auto Import Media** dialog box displays.



3 Click **Import**. The library will begin importing the media to their respective destinations based on the configured barcode filters. When complete, the **Results** column will display the new location, in coordinates, of the media.

4 Click **Refresh** to refresh the **Auto Import Media** dialog box to ensure the media was imported.

5 Click **Close**.

Chapter 7
Capacity on Demand

The library is initially licensed for a default configuration of 100 storage slots.

Capacity on Demand allows you to purchase capacity for your library as needed. As your storage needs change, you can add storage in blocks of 100. Scalar i6000 licensing begins at 100 cartridges and can be increased to as many as 7,146 LTO cartridges (for a single-robot library) or 7,224 LTO cartridges (for a dual-robot library).

Note: Maximum numbers assume only one drive and one 24-slot I/E station in the control module.

Note: Cleaning slots do not count against the libraries available COD account.

To gain the use of additional storage slots, you must purchase a Capacity on Demand license for the desired number of slots.

The library also accommodates the use of unlicensed slots in the following circumstances:

- Your library ships with enough modules to meet your Capacity on Demand needs. If you require additional physical capacity to be physically prepared for non-disruptive future expansion, you can order one or more Unlicensed Expansion Modules.

- You can also use Unlicensed Expansion Modules to accommodate the Active Vault and Extended Data Lifecycle Management (EDLM) features, which do not require the use of licensed slots.

Chapter 8
Encryption Key Management

This chapter covers:

Encryption Key Management Systems

Encryption key management systems generate, protect, store, and manage encryption keys. These keys are used by their respective tape drives to encrypt information being written to tape, and decrypt information being read from tape media.

Encryption Key Management (EKM) is a licensable feature. You must have an EKM license installed on your library in order to use the

Encryption Key Management features described in this chapter. For more information on licensing, see Enabling Licenses on page 115 or Step 1 — Installing the EKM License Key on page 283.

The Scalar i6000 supports four encryption key management systems:

Encryption System	Supported Tape Drives	Supported Media
Quantum Encryption Key Manager (Q-EKM)	IBM LTO-4 Fibre Channel IBM LTO-5 Fibre Channel IBM LTO-6 Fibre Channel	IBM LTO-4, LTO-5 and LTO-6
Scalar Key Manager (SKM)	HP LTO-4 Fibre Channel HP LTO-5 Fibre Channel HP LTO-6 Fibre Channel IBM LTO-5 Fibre Channel IBM LTO-6 Fibre Channel	HP LTO-4, LTO-5 and LTO-6 IBM LTO-5 and LTO-6
RSA Key Manager (RKM)	HP LTO-4 Fibre Channel HP LTO-5 Fibre Channel HP LTO-6 Fibre Channel	HP LTO-4, LTO-5 and LTO-6
KMIP-compliant key management (see KMIP-compliant Encryption Key Management on page 279).	HP LTO-4 Fibre Channel HP LTO-5 Fibre Channel HP LTO-6 Fibre Channel IBM LTO-5 Fibre Channel IBM LTO-6 Fibre Channel	HP LTO-4, LTO-5 and LTO-6 IBM LTO-5 and LTO-6

Note: The library does not support using more than one encryption key management system on a single library.

Encryption on the Scalar i6000 tape library is enabled by partition only. The default setting for encryption-capable drives permits external application-managed encryption support on all encryption-capable tape drives and media within a partition.

You cannot select individual drives for encryption; you must select an entire partition to be encrypted. If you encrypt a partition, all encryption-capable tape drives are enabled for encryption, and all data written to supported media is encrypted. Non encryption-capable tape drives will not be enabled for encryption, and non-supported media will not be encrypted.

You can only configure the encryption settings through the **Setup > Encryption > Partition Configuration** functionality.

KMIP-compliant Encryption Key Management

The Key Management Interoperability Protocol (KMIP) is a specification developed by OASIS®. Its function is to standardize communication between enterprise key management systems and encryption systems. With version i8.2.1, the Scalar i6000 provides a KMIP version 1.0 compliant encryption solution.

KMIP is only supported in certain environments. Contact your Quantum representative for details.

Details about the Scalar i6000 KMIP-compliant implementation include:

- As with other encryption systems supported by the library, in order to use KMIP-compliant encryption systems with the Scalar i6000, you must have an Encryption Key Management license installed on the library.
- A minimum of two KMIP-compliant encryption servers are required for failover purposes. A total of 10 KMIP-compliant encryption servers are allowed, for increased failover capability.

See Encryption Key Management Systems on page 277 for instructions on how to configure KMIP-compliant encryption systems on the library.

FIPS-Certified Encryption Solution

FIPS (Federal Information Processing Standard) 140-2 is a U.S. government standard relating to computer security and encryption.

The Quantum Scalar i6000 now offers a FIPS 140-2 Level 1 certified encryption solution composed of the Scalar Key Manager and HP LTO-5 and LTO-6 Fibre Channel tape drives in a Scalar i6000 library. FIPS mode can be enabled on the HP LTO-5 and LTO-6 tape drives via the library user interface. Once in FIPS mode, all encryption key communication

between the tape drive and the library controller is authenticated and encrypted.

Details about configuring FIPS mode include:

- Library firmware must be at version 630Q or later.
- HP LTO-5 and LTO-6 FC tape drive firmware must be at the latest version qualified with the Scalar i6000 library (see the *Scalar i6000 Release Notes* for qualified firmware levels).
- An Encryption Key Management license must be installed on the library sufficient to cover the tape drive(s) on which you want to enable FIPS mode.
- A Storage Networking license must be installed on the library.

Note: Use of FIPS on a drive does not count against the Storage Networking license drive count. FIPS is not considered a "Storage Networking feature;" however, the SNW license is still required on the library.

- FIPS mode is configured by partition. FIPS partitions must contain only HP LTO-5 or LTO-6 FC tape drives.
- The partition encryption method must be set to **Enable Library Managed** in order to set FIPS mode.
- FIPS mode is disabled by default.
- The library must be connected to Scalar Key Manager (SKM). SKM software must be at version 2.0 or later in order to be FIPS certified. FIPS currently only works with SKM.
- Ethernet connectivity is required for the tape drives on which you want to enable FIPS mode. This means that every HP LTO-5 or LTO-6 FC drive in the partition must be connected to an Ethernet Expansion blade installed in the library.

Caution: If the Ethernet Expansion blade fails and the attached tape drives have FIPS mode enabled, all encryption operations (encrypting, decrypting, key requests) on the attached tape drives will fail. If this happens, contact Quantum Support for a replacement Ethernet Expansion blade as soon as possible.

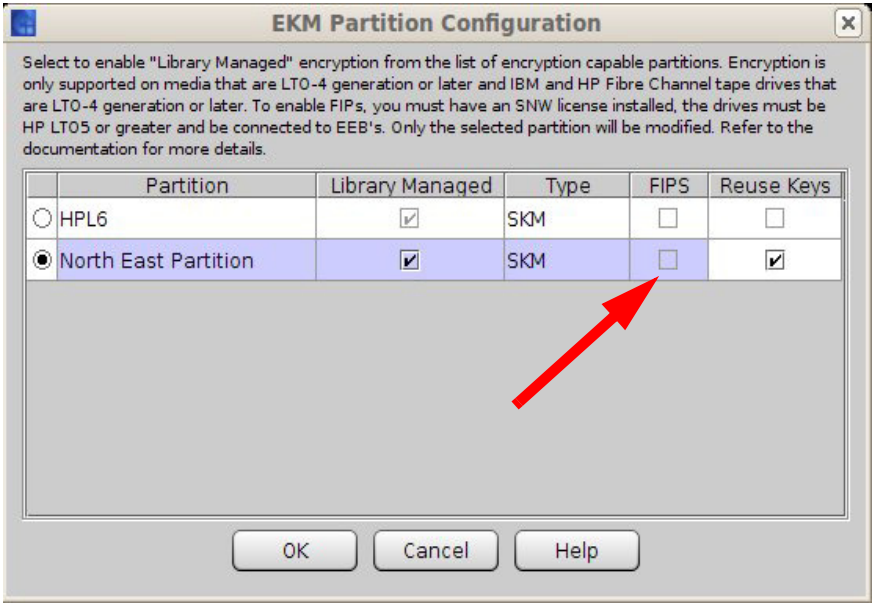
Enabling and Disabling FIPS Mode on HP LTO-5 or LTO-6 Tape Drives

To operate your HP LTO-5 or LTO-6 Fibre Channel tape drives to be compliant with FIPS, you must enable "FIPS mode." FIPS mode is enabled by partition. You enable FIPS mode on a partition, which enables FIPS mode on all of the tape drives in the partition.

To change FIPS mode for a partition, do the following:

1. Log on as an administrator.
2. Make sure you are viewing the physical library (from the **View** menu, select the name of the physical library).
3. Select **Setup > Encryption > Partition Configuration**. The **EKM Partition Configuration** dialog box displays (see Figure 36).
4. Change the Encryption Method of a partition to **Enable Library Managed**.
5. Select the **FIPS** check box to enable FIPS mode for the partition. Clear the **FIPS** check box to disable FIPS mode for the partition.
6. Click **OK**.

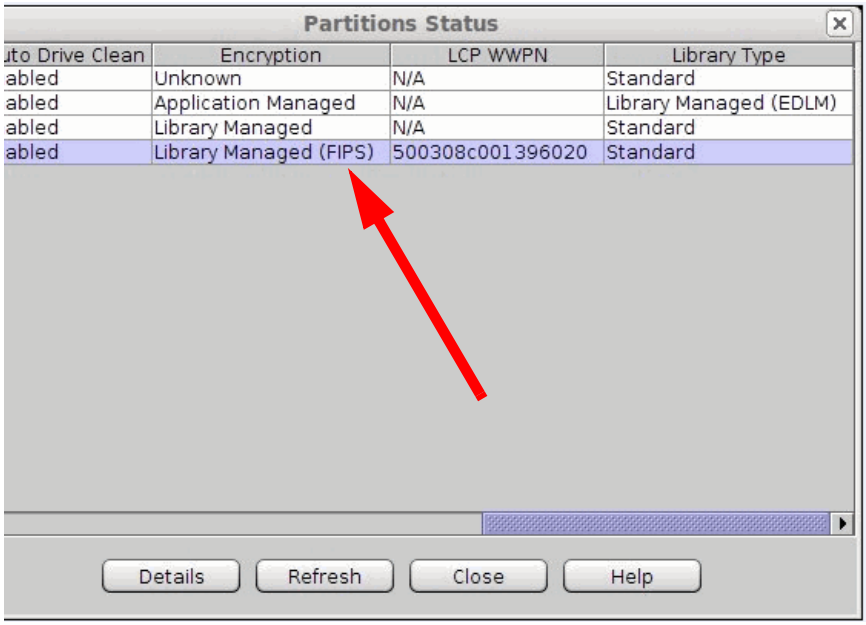
Figure 36 Enabling FIPS Mode



Viewing FIPS Status on the Library

To view FIPS status on partitions, do either of the following:

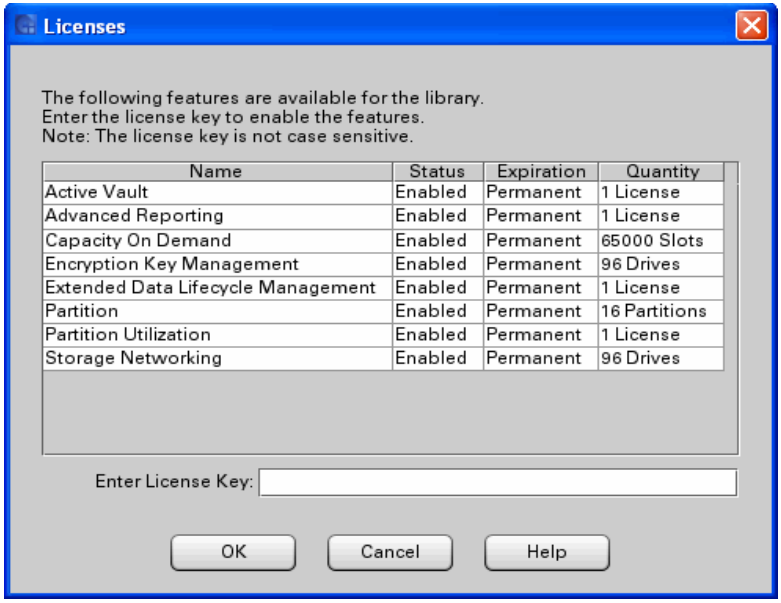
- The Partition Configuration dialog box **(Setup > Encryption > Partition Configuration)** shows which partitions are enabled for FIPS. All tape drives in FIPS partitions are enabled. See Figure 36 on page 281.
- The Partitions Status report (**Monitor > Partitions > Status**) lists FIPS in the Encryption column if FIPS is configured on the partition.



Setting up EKM on the Scalar i6000

Step 1 — Installing the EKM License Key

1 Click **Setup > Licenses**. The Licenses dialog box appears.



This dialog box lists the licensed features for your library, plus Status, Expiration, and Quantity. **Quantity** refers to the number drives licensed to use this feature.

2 In the **Enter License Key** box, type the appropriate license key.

- License keys are not case sensitive and are all-inclusive. For example, J2BGL-22622-52C22 can be entered as j2bgl-22622-52c22.
- If you are using the library's touch screen, enter the library key from the lowercase keyboard, which gives you access to the dash (-) character.
- If you cannot locate the license keys shipped with the library, you can obtain them by contacting technical support or, if you are an end user, by contacting your inside sales representative.

3 Click **OK**.

Step 2 — Preparing Partitions for Library-managed Encryption

1. If not already installed, install tape drives that are supported by the encryption system you are using (see Supported Tape Drives on page 278).
2. Ensure that the partition you are configuring for library-managed encryption contains only tape drives that are supported by the encryption system you are using.
3. On the tape drives, install the latest version of firmware that is qualified for the library firmware installed on your library. Refer to the library release notes for the correct version of tape drive firmware.

Step 3 — Installing TLS Communication Certificates on the Library

Transport Layer Security (TLS) communication certificates are unique certificates that must be installed on the library in order for the library to communicate securely with attached EKM servers.

Take one the following actions, according to what encryption System you are using.

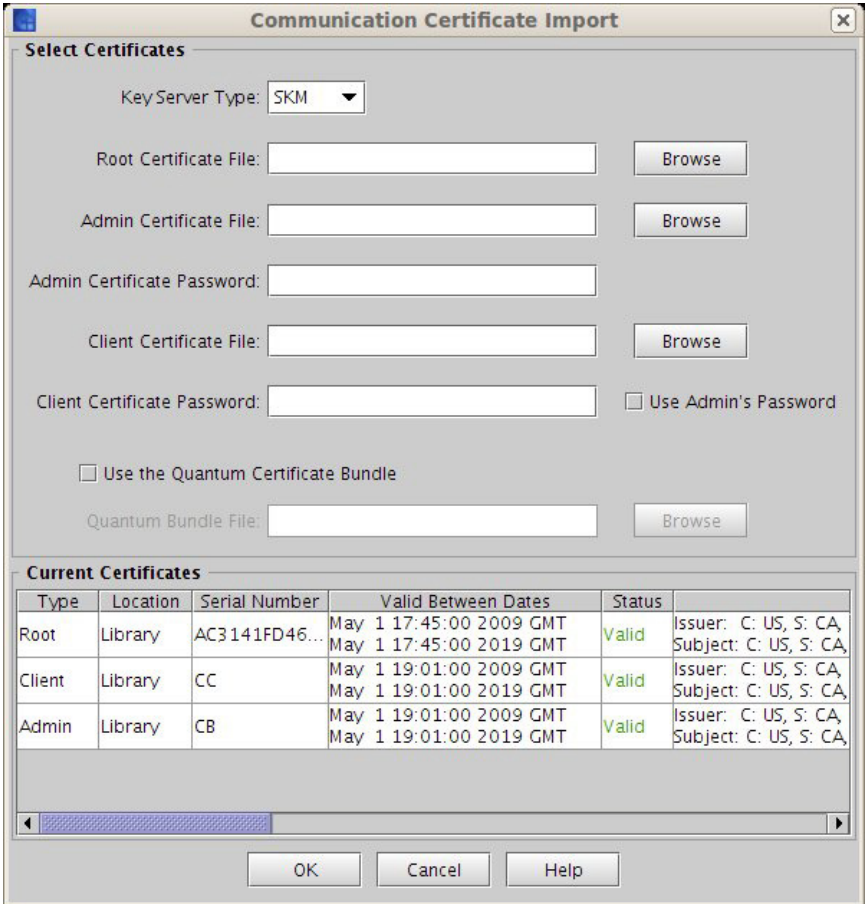
Encryption System	Action
Quantum Encryption Key Manager (Q-EKM) or Tivoli Key Lifecycle Manager (TKLM) or Secure Key Lifecycle Manager (SKLM)	Only one TLS certificate (the Root certificate) is required. Libraries with code versions 600A.GS23201 and higher generate a self-signed certificate when first booting up, and regenerate the certificate if it expires. You do not need to take any action unless you want to install your own Root certificate to supersede the existing certificate. If want to install your own certificate, then follow the instructions in Installing User-Provided Certificates on page 289.

Encryption System	Action
Scalar Key Manager (SKM)	TLS certificates may already be pre-loaded on the library. **1** Check to see if certificates are loaded. See Checking for Current Certificates on page 286. **Note:** If certificates have already been pre-loaded by Quantum, you can replace them by installing your own certificates, if desired. **2** If needed, install certificates following the appropriate set of instructions: • Installing SKM Library TLS Certificates from Quantum CD on page 287, or • Installing User-Provided Certificates on page 289.
RSA Key Manager (RKM)	TLS certificates will be provided by your RSA RKM server administrator. Install certificates per Installing User-Provided Certificates on page 289.
KMIP-compliant key management	TLS certificates will be provided by your KMIP server administrator. Install certificates per Installing User-Provided Certificates on page 289.

Checking for Current Certificates

Follow the steps below to see what certificates are already loaded on your library.

1 From the Tools menu, select **EKM Management > Import Communication Certificates.** The **Communication Certificate Import** dialog box appears.



Note: The **Current Certificates** section of the screen lists the certificates currently loaded on the library. If you install new certificates, they will overwrite the current certificates.

2 Confirm which certificates are appropriate for your installation.

3 Install certificates if needed, following the instructions in the following table for your encryption system.

Encryption System	Action
Q-EKM or TKLM/ SKLM	If you wish to install your own Root certificate to supersede the existing self-generated certificate on the library, follow the instructions in Installing User-Provided Certificates on page 289.
SKM	For **SKM**, you can either: • Install from the Quantum certificate bundle on CD. Refer to Installing SKM Library TLS Certificates from Quantum CD on page 287. • Install your own certificates. Refer to Installing User-Provided Certificates on page 289.
RKM	You must use certificates provided by the RSA RKM server administrator. Refer to Installing User-Provided Certificates on page 289.
KMIP-compliant key management	You must use certificates provided by the KMIP server administrator. Refer to Installing User-Provided Certificates on page 289.

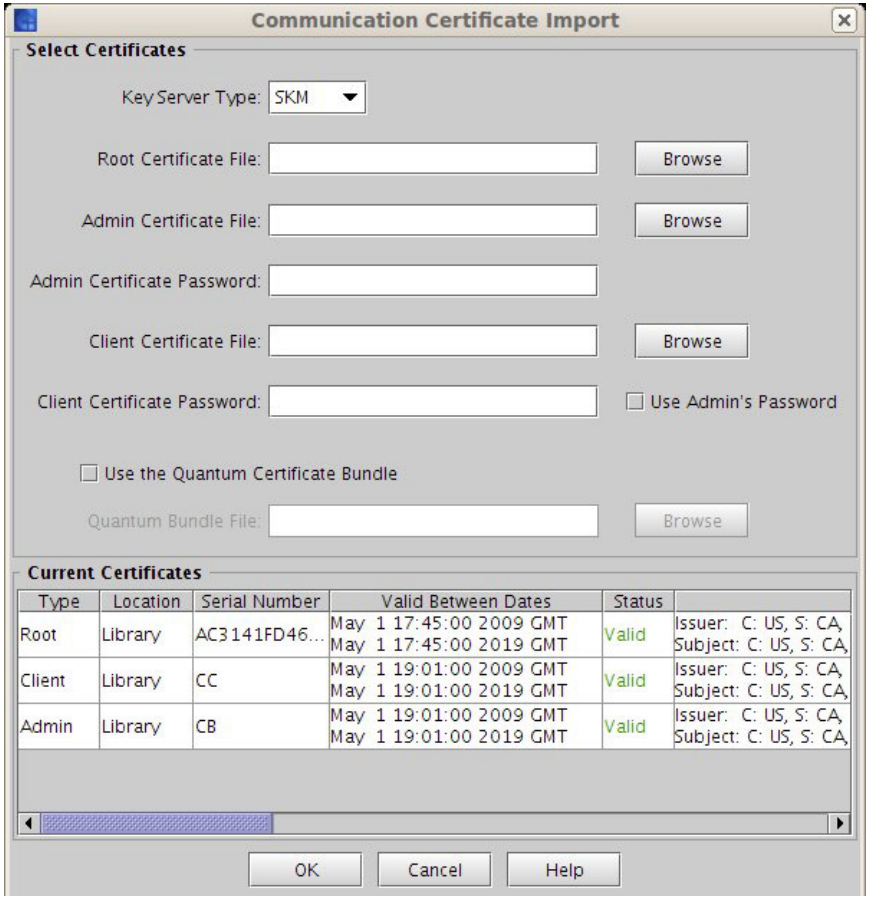
Installing SKM Library TLS Certificates from Quantum CD

Note: The Quantum certificate bundle can be used only with SKM. Quantum TLS certificates for use with SKM may already be pre-loaded on your library. Check if these exist before adding new TLS certificates for SKM. Refer to Checking for Current Certificates on page 286.

1 Insert the CD into the CD ROM drive of your computer.

2 Either copy the file to a known location on your computer or use the CD as the location from which you will retrieve the file.

3 From the **Tools** menu, select **EKM Management > Import Communication Certificates**. The **Communication Certificate Import** dialog box appears.



4 In the **Select Certificates** section, select **SKM** from the **Key Server Type** drop-down list.

5 Select the **Use Quantum Certificate Bundle** check box, and then click **Browse** to locate the Quantum Bundle File.

Note: If you have installed certificates, they are listed in the Current Certificates section.

6 Click **OK**.

Note: Whenever the Compact Flash (CF) is replaced, SKM certificates must be reinstalled.

Installing User-Provided Certificates

Follow these instructions to install your own TLS certificates, or when installing TLS certificates for RKM or KMIP. When providing your own certificates, it is assumed you understand the concepts of PKI and can access the tools or third-party resources needed to generate or obtain certificates.

Note: If you are using SKM, you must be running SKM 1.1 or higher on your SKM servers in order to install your own TLS certificates.

Note: If you are using RSA or KMIP, your server provider will provide TLS communication certificates.

You need to provide the following certificates:

Encryption System	Certificates Required
Q-EKM or TKLM/ SKLM	• Root Certificate (also called the CA certificate, or Certificate Authority Certificate)
SKM	• Root Certificate (also called the CA certificate, or Certificate Authority Certificate) • Client Certificate • Admin Certificate
RKM	• Root Certificate (also called the CA certificate, or Certificate Authority Certificate) • Client Certificate
KMIP-compliant key management	• Root Certificate (also called the CA certificate, or Certificate Authority Certificate) • Client Certificate

These files must be in the proper format, as follows. If any of the following requirements is not met, none of the certificates will be imported.

- The Root Certificate must be 2048 bits.
- The Root Certificate must be in PEM format.

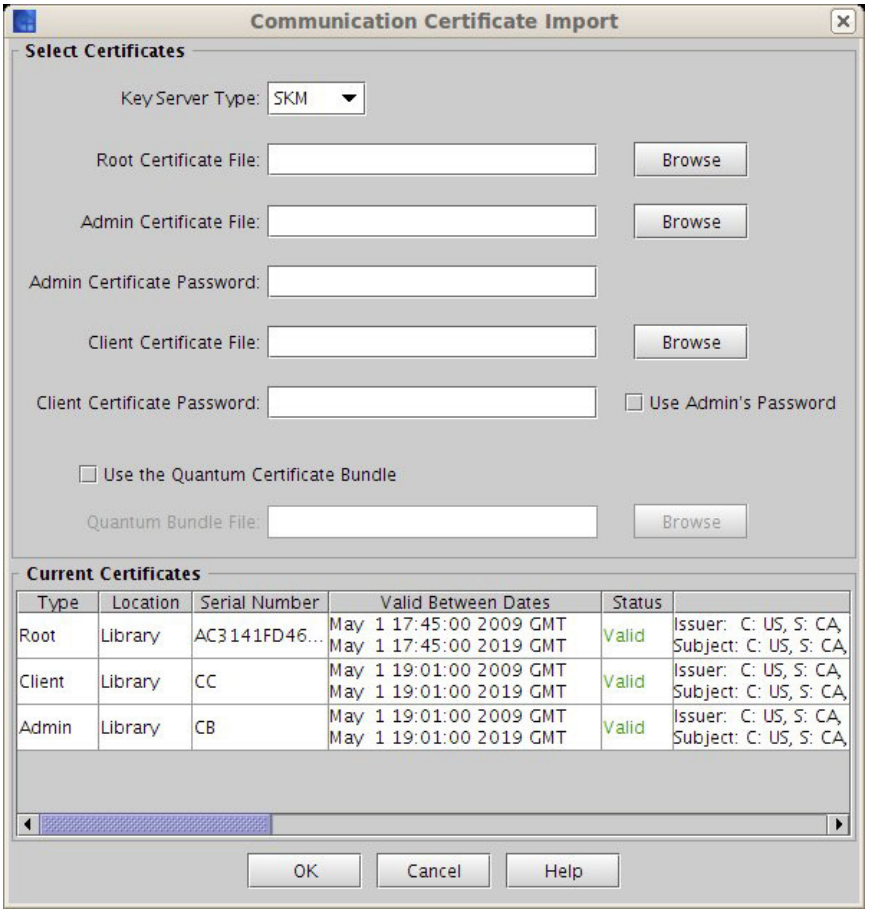
- The Admin and Client certificates must be in pkcs12 (.p12) format, with a separate certificate and private key contained in each.

  Note: The .p12 format combines the public/private key pair files in .pem file format and password protects access to such .pem certificate files.

- The Admin and Client certificates must be 1024 bits.
- The Admin and Client certificates must be signed by the Root Certificate.
- Certificates must have the Organization name (O) set in their Issuer and Subject info.
- The Admin certificate must have its Organizational Unit name (OU) set as "akm_admin" in its Subject Info. (Only applies to SKM).
- The same Root Certificate must be installed on the encryption key servers and the library.
- All the certificates must have a valid validity period according to the date and time settings on the encryption key server.

Follow the steps below to install your own certificates.

1. Place the certificate files in an accessible location on your computer.
2. From the **Tools** menu, select **EKM Management > Import Communication Certificates.** The **Communication Certificate Import** dialog box appears.



3 In the **Select Certificates** section, select the appropriate Key Server Type from the drop-down list.

Depending on your selection, certain fields are enabled.

4 Take the following actions, depending on which Key Server Type you selected:

For Q-EKM or TKLM/SKLM

- Click **Browse** to retrieve the **Root Certificate File**.

For SKM

- Click **Browse** to retrieve the **Root Certificate File**.
- Click **Browse** to retrieve the **Admin Certificate File.**

- In the **Admin Certificate Password** field, type the password used when you generated the certificate files.
- Click **Browse** to retrieve the **Client Certificate File**.
- In the **Client Certificate Password** field, type the password used when you generated the certificate files.
- If you used the same password for the client and admin certificates, you can select the **Use Admin's Password** check box.

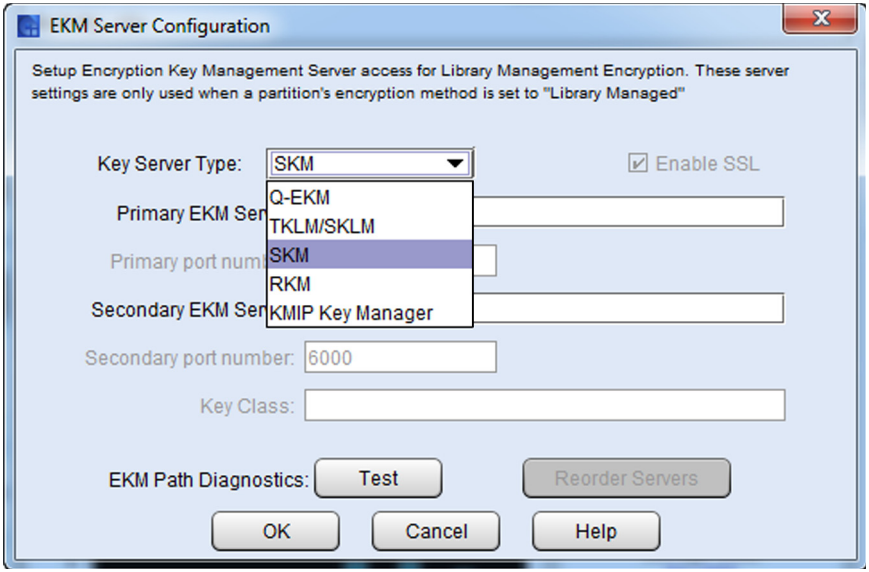
For RKM or KMIP-compliant key managers

- Click **Browse** to retrieve the **Root Certificate File**.
- Click **Browse** to retrieve the **Client Certificate File**.
- In the **Client Certificate Password** field, type the password used when generating the certificate files.

5 Click **OK**.

Step 4 — Configuring the EKM Server

1 From the menu bar, click **Setup** > **Encryption** > **Server Configuration**. The **EKM Server Configuration** dialog box appears.



2 From the **Key Server Type** drop-down list, select the server type.

3 Fill in the rest of the fields as described in the sections below for each server type: Q-EKM on page 293, TKLM/SKLM on page 294, SKM on page 294, RKM on page 295, or KMIP Key Manager on page 296 of this document.

For primary and secondary servers, you can enter the following:

- IPv4 address
- IPv6 address — if IPv6 is configured
- DNS name — if DNS is configured on the LMC (**Setup > Network Configuration > DNS Configuration**)

Q-EKM

a **Enable SSL -** Select the check box if SSL communications should be enabled between the library and encryption server(s).

b **Primary EKM Server** - Type the IP address or DNS name of the primary Q-EKM server.

c **Primary port number** - If SSL is enabled, the default port number is 443. If SSL is not enabled, the default port number is 3801. You can change the port number on the library, but, if you do, you must also change the port number on the key server to match or Q-EKM will not work properly. See the *Quantum Encryption Key Manager User's Guide* for information on setting the port number on the Q-EKM key server.

d **Secondary EKM Server** - Type the IP address or DNS name of the optional secondary Q-EKM server.

Note: If you do not plan to use a secondary server, you may type a zero IP address, 0.0.0.0, into the Secondary EKM Server text box, or you may leave this text box blank.

---

e **Secondary port number** - If SSL is enabled, the default port number is 443. If SSL is not enabled, the default port number is 3801.

Note: If you are using a secondary key server, then the port numbers for both the primary and secondary key servers must be set to the same value. If they are not, synchronization and failover will not occur.

---

f **Key Class** - This field is not applicable for Q-EKM.

g **EKM Path Diagnostics** - Not supported for Q-EKM. The **Test** button is disabled.

TKLM/SKLM

a **Enable SSL** - Check the box if SSL communications should be enabled between the library and encryption server(s).

b **Primary EKM Server** -Type the IP address or DNS name of the primary TKLM/SKLM server.

c **Primary port number** - If SSL is enabled, the default port number is 443. If SSL is not enabled, the default port number is 3801. You can change the port number on the library, but, if you do, you must also change the port number on the key server to match or TKLM/SKLM will not work properly.

d **Secondary EKM Server** - Type the IP address or DNS name of the optional secondary TKLM/SKLM server. If you do not plan to use a secondary server, you may type a zero IP address, 0.0.0.0, into the Secondary EKM Server text box, or you may leave this text box blank.

e **Secondary port number** - If SSL is enabled, the default port number is 443. If SSL is not enabled, the default port number is 3801. If you are using a secondary key server, then the port numbers for both the primary and secondary key servers must be set to the same value. If they are not, synchronization and failover will not occur.

f **Key Class** - This field is not applicable for TKLM/SKLM.

g **EKM Path Diagnostics** - This Test button not supported, and therefore disabled.

SKM

a **Enable SSL** - Check box is checked automatically and field is disabled.

b **Primary EKM Server** - Type the IP address or DNS name of the primary SKM server.

c **Primary port number** - Field is disabled, and port number defaults to 6000 automatically.

d **Secondary EKM Server** - Type the IP address or DNS name of the secondary SKM server.

e **Secondary port number** - Field is disabled, and port number defaults to 6000 automatically.

f **Key Class** - This field is not applicable for SKM.

g **EKM Path Diagnostics** - To test the configuration, click **Test**.

The **Path Diagnostic Results** dialog box appears. For more information on EKM Path Diagnostics, see Using EKM Path Diagnostics on page 302.

RKM

a **Enable SSL** - Check box is checked automatically and the field is disabled.

b **Primary EKM Server** - Type the IP address or DNS name of the primary RKM server.

c **Primary port number** - Accept the default or type the applicable port number. The default port number is 443.

Note: The port number must match the port number on the primary RKM key server.

---

d **Secondary EKM Server** - The secondary EKM server is not supported, therefore this field is disabled.

e **Secondary port number** - A secondary port number is not supported; therefore, this field is disabled.

f **Key Class** - Type the key class that was used during the RKM server configuration process.
The key class that was created on your RSA RKM server will be provided by the RKM server administrator.

g **EKM Path Diagnostics** - To test the configuration, click **Test.**

The Path Diagnostic Results dialog box appears. For more information on EKM Path Diagnostics, see Using EKM Path Diagnostics on page 302.

KMIP Key Manager

Note: KMIP Key Manager requires at least two (2) servers and can have up to ten (10) servers for increased failover capacity. Assign your key servers on this screen in the order in which you want failover to occur.

For an initial key request, the library tries server #1 (the primary server) first. If server #1 is not available to perform a key request, the library tries server #2. If server #2 is not available, the library will try server #3, and so on, in order.

Once the library identifies a server that can perform the request, this server remains the active server until it fails a key request or the library is rebooted. At that point, the library starts over and uses server #1 for key requests.

a **Enable SSL** - Check box is checked automatically and the field is disabled.

b **Server 1** - Type the IP address or DNS name of the primary KMIP key manager server.

c **Port for Server 1** - Type the applicable port number. The port number must match the configured port number on the primary KMIP key manager server. A typical port number used for communication between the KMIP key manager server and the library is port **9003**.

d **Server 2** - Type the IP address or DNS name of the secondary KMIP key manager server.

e **Port for Server 2** - Type the applicable port number. The port number must match the configured port number on the secondary KMIP key manager server. A typical port number used for communication between the KMIP key manager server and the library is port **9003**.

f Repeat Step d and Step e for up to eight additional KMIP key manager servers, in the order in which you would like failover to occur. The port number listed in each **Port** field must match the port number used on that KMIP key manager server.

g **Key Class** - This field is not applicable.

h **EKM Path Diagnostics** - To test the configuration, click **Test.**

The **Path Diagnostic Results** dialog box appears. For more information on EKM Path Diagnostics, see Using EKM Path Diagnostics on page 302.

i **Reorder Servers** - After you have configured at least two KMIP servers, you have the option of clicking the Reorder Servers button to change the order in which servers are used. If failover occurs, the servers will be used in the new order specified.

4 Click **Close**.

5 Click **OK**. An **Operation in Progress** dialog box appears, indicating the settings are being modified. Upon successful completion, the system returns to the main console.

Note: If using SKM, key generation begins in the background. Key generation can take one hour or more. Once SKM encryption keys have been generated, make sure to back up both SKM servers before using any encryption keys. Refer to the *Scalar Key Manager User's Guide.*

6 Ensure all ports corresponding to the EKM servers are open on your firewall to allow the library to connect to the servers. For SKM, ports 80, 6000, and 6001 must be open.

Step 5 — Configuring Partitions for Library-managed Encryption

Encryption on the Scalar i6000 library is enabled by partition only. You cannot select individual drives for encryption; you must select an entire partition for encryption. Only partitions that are encryption-capable are displayed on the configuration screen.

Use the Partition Configuration dialog box to change the encryption method used by a partition. You can modify only one partition at a time.

Encryption Methods, Details, and Restrictions

The following encryption methods are available on the library:

- **Application Managed** (default)— Allows your host application to provide encryption support on all encryption-capable tape drives and media within the partition. This is the default setting if the partition contains encryption-capable tape drives. If you select this option, the library will not communicate with the key server on this partition. If you want an application to manage encryption, you must specifically configure the application to do so. The library will

not participate in performing encryption. See your host documentation for further details.

- **Library Managed** — Select checkbox to enable. Permits library managed encryption support via a connected key manager server—either Quantum Encryption Key Manager (Q-EKM), Scalar Key Manager (SKM), RSA Key Manager (RKM), Tivoli Key Lifecycle Manager (TKLM), Secure Key Lifecycle Manager(SKLM) or KMIP-compliant key server—for all tape drives and encryption-capable media assigned to the partition.

  Details and restrictions for using library managed encryption include:

  - You must have an EKM license installed on the library (Step 1 — Installing the EKM License Key on page 283) before you can select this option. Ensure the EKM license contains the appropriate quantity of drives to match or exceed what is currently installed in the library.
  - Your encryption key servers must be installed, operational, and configured on the library (**Setup > Encryption > Server Configuration**), before you can enable a partition for library managed encryption (**Setup > Encryption > Partition Configuration**).
  - Only HP LTO-4, LTO-5, and LTO-6 and IBM LTO-4, LTO-5 and LTO-6 tape cartridges will be encrypted in library managed encryption partitions, unless they contain unencrypted data already, and data is appended. The partition may contain LTO-2 and LTO-3 tape cartridges, but they will not be encrypted.
  - Encrypted data will never be appended to unencrypted data on tape, and unencrypted data will never be appended to encrypted data on tape.
  - For data to be encrypted via library managed encryption, the media must be blank or have been written to using library managed encryption at the first write operation at the beginning of tape (BOT). If the media was previously written in a non-encrypted format, all data subsequently written to it will continue to be non-encrypted.
  - Data stored on tape cartridges will not be encrypted with more than one encryption key.
  - **Q-EKM** supports encryption for data cartridges using IBM LTO-4, LTO-5, or IBM LTO-6 Fibre Channel tape drives. If you are

using Q-EKM and want to enable library managed encryption for a partition, all of the tape drives in that partition must be IBM LTO-4, LTO-5, and/or IBM LTO-6 Fibre Channel tape drives.

Generating Encryption Keys for Q-EKM: Encryption keys are generated during the Q-EKM installation and configuration process.

- **SKM** supports encryption for data cartridges using HP LTO-4, LTO-5, and LTO-6 as well as IBM LTO-5 and LTO-6 Fibre Channel drives. If you are using SKM and want to enable library managed encryption for a partition, all of the tape drives in that partition must be either HP LTO-4, LTO-5, and/or LTO-6 or IBM LTO-5 and/or LTO-6 Fibre Channel tape drives.

  Generating Encryption Keys for SKM: The library automatically generates keys as soon as you configure the SKM server. Note that you cannot change a partition to library managed encryption until after key generation is complete.

  Caution: Once encryption keys have been generated, make sure to back up both SKM servers before using any encryption keys. Refer to the *Scalar Key Manager User's Guide*.

- **RKM** supports encryption for data cartridges using HP LTO-4, LTO-5, or HP LTO-6 Fibre Channel drives. If you are using RKM and want to enable library managed encryption for a partition, all of the tape drives in that partition must be HP LTO-4, LTO-5, and/or HP LTO-6 Fibre Channel tape drives.

  Generating Encryption Keys for RKM: Encryption keys are generated during the RKM installation and configuration process.

- **TKLM/SKLM** supports encryption for data cartridges using IBM LTO-4, LTO-5, or IBM LTO-6 Fibre Channel tape drives. If you are using TKLM/SKLM and want to enable library managed encryption for a partition, all of the tape drives in that partition must be IBM LTO-4, LTO-5, and/or IBM LTO-6 Fibre Channel tape drives.

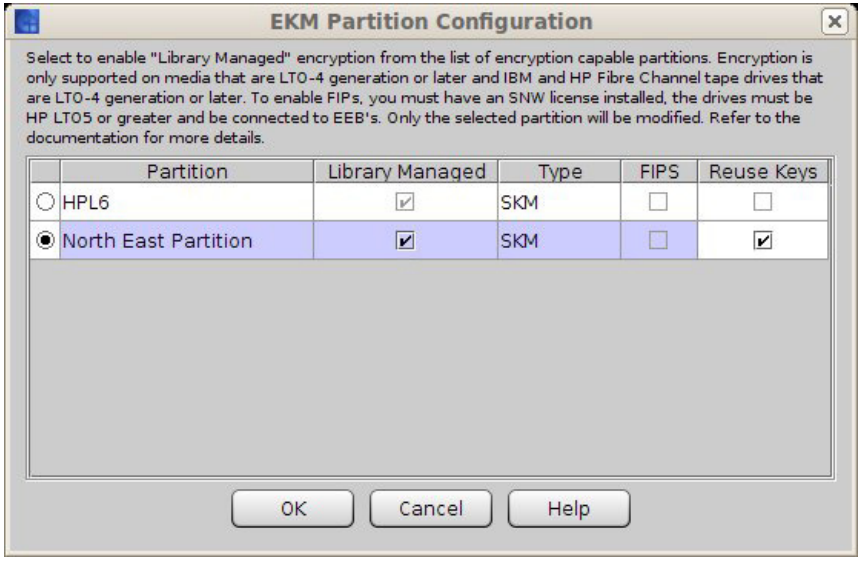
- **Generating Encryption Keys for TKLM/SKLM:** Encryption keys are generated during the TKLM/SKLM installation and configuration process.

- **KMIP-compliant key management (SafeNet)** supports encryption for data cartridges using HP LTO-4, LTO-5, or LTO-6 as well as IBM LTO-5 or LTO-6 Fibre Channel drives. If you are using KMIP-compliant key servers and want to enable library managed encryption for a partition, all of the tape drives in that partition must be either HP LTO-4, LTO-5, and/or LTO-6 or IBM LTO-5 and/or LTO-6 Fibre Channel tape drives.

  Generating Encryption Keys for KMIP-compliant key servers: Encryption keys are generated one at a time, as needed, upon request.

Changing the Encryption Method

1. If you are not already viewing the physical library, click **View** and select the name of the physical library.
2. Click **Setup > Encryption > Partition Configuration**. The **EKM Partition Configuration** dialog box appears. Each partition's current encryption method is listed under Encryption Method.



3. If you want to change a partition's encryption method, make sure that the tape drives in that partition do not have cartridges loaded. If there are cartridges in the tape drives, you cannot change the encryption method.
4. Select the partition whose encryption method you want to change.

5 Change the encryption method by selecting from the **Encryption Method** drop-down list:

Encryption Method	Description
Allow Application Managed	This is the default setting if you have encryption-capable tape drives in the partition. This option should remain selected ***unless*** you are connecting the library to an external EKM server. This option allows an external backup application to provide encryption support to all encryption-capable tape drives and media within the partition. **Note:** If you want an application to manage encryption, you must specifically configure the application to do so.
Enable Library Managed	Enables encryption support via connected EKM servers to the partition. Choose this option for SKM, Q-EKM, RKM, TKLM, SKLMor SafeNet key servers.

Note: When you change a partition from Enable Library Managed to Allow Application Managed, any encrypted data that was written to the tapes while the partition was configured for library managed encryption can no longer be read, until you change the partition back to Enable Library Managed.

6 To enable FIPS mode on all tape drives in the partition, click the FIPS check box.

Note: There are specific requirements for FIPS. See FIPS-Certified Encryption Solution on page 279 for details.

7 Click the **Reuse Keys** check box if you want the partition to reuse encryption keys.

Note: IBM drives do not support the key reuse feature.

8 Click **OK**. The dialog box is closed and you are returned to the main console.

If the partition encryption settings were not successfully configured, follow the screen instructions to resolve any issues.

Step 6 — Saving the Library Configuration

When you are finished configuring the library, save the library configuration (**Tools > Save/Restore)**.

Using EKM Path Diagnostics

EKM Path Diagnostics is a series of short tests performed by the library to determine whether the EKM servers are connected and operating properly.

Note: This feature is not available for Q-EKM.

You can perform EKM Path Diagnostics tests manually at any time, or automatically in the background at regular intervals:

- **Manual** — You can perform manual EKM Path Diagnostics at any time by clicking the **Test** button on the EKM server setup screen (**Setup > Encryption > Server Configuration**).
- **Background** — You can configure the library to automatically perform background EKM Path Diagnostics tests at regularly scheduled intervals and notify you via RAS tickets if any problems arise. To do this, go to **Setup > System Settings > Physical Library**. Under **EKM Path Diagnostics**, select the **Enable** check box.

  Note: This feature is enabled by default. You can disable it for SKM but you cannot disable it for RKM or KMIP key managers. Unless directed by Quantum Support to disable this feature, the background EKM Path Diagnostics should always be enabled so the library can monitor SKM server status and report issues as soon as they arise.

The tests performed are:

- **Ping** — Verifies the Ethernet communication between the library and the key servers.
- **Path** — Verifies that SKM/RKM/KMIP services are running on the key servers.
- **Config** — Verifies that the key servers are capable of serving encryption keys.

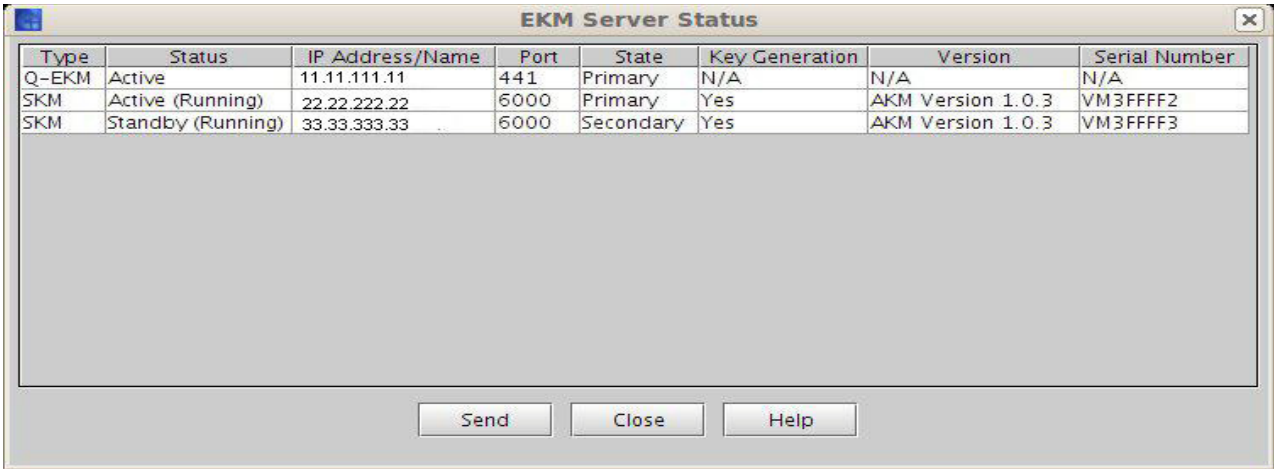
Troubleshooting EKM Path Diagnostics Problems

If this occurs...	Do this...
The Ping test fails	Either the referenced server is not running, or the server address may not have been entered correctly.
The Ping test passes, but the Path test fails	Check the key server to make sure all required services are running. Also, there may be an issue with the communication certificates required for exchanging keys.
The Ping and Path tests pass, but the Config test fails	One of the following may have occurred: • For RKM, the key class entered in the Encryption Server Configuration screen does not match the one set up on the server. • For SKM, a database inconsistency has been detected. Contact Quantum Support.

Monitoring EKM Server Status

You can monitor all configured EKM servers using the EKM Server Status dialog box.

1. From the **View** menu, select the name of the physical library or partition that communicates with the EKM servers you want to monitor.
2. On the menu bar, click **Monitor** > **EKM Servers**. The **EKM Server Status** dialog box appears.



For each server, the EKM Server Status dialog box displays the following information:

Element	Description
Type	The encryption server type (Q-EKM, SKM, RKM, or KMIP)

Status	The current status of the server: **Note:** "Active" status indicates that this server will receive the next key request. **Q-EKM** — Active, Standby or Not Configured **SKM** — Active Running, Standby Running or Down, or Not Configured **RKM** — Active Running or Down, Standby Running or Down, or Not Configured **KMIP** — Active Running or Down, Standby Running or Down, or Not Configured
IP Address/Name	The IP address or host name of the server
Port	The server port number: **Q-EKM** — Default 3801 for non-SSL and 443 for SSL **SKM** — 6000 (fixed) **RKM** — Default 443 **KMIP** — No default
State	**Q-EKM, SKM, RKM** — Whether the server is Primary or Secondary. **KMIP** — Order of failover. Server 1 is primary, Server 2 is secondary, and so on.
Key Generation	Applies to SKM only: **Yes** — encryption key generation in progress. **No** —encryption key generation not in progress.
Version	Applies to SKM only: Software version number
Serial Number	Applies to SKM only: Server serial number

You can mail, save, or print status information by using the **Send** button.

Using Q-EKM

Note: For Q-EKM to work properly, you must upgrade both your library and tape drive firmware to the latest released versions. For instructions on performing the firmware upgrades, see Updating Library Software on page 564 and Updating Drive Firmware on page 578.

Using Q-EKM to Manage Encryption

Q-EKM is an optional, licensed Java software program that generates, protects, stores, and manages the encryption keys. These keys are used by the LTO-4 or greater tape drives to encrypt the information being written to tape media and read from tape media. Policy control and keys pass through the library-to-drive interface; therefore encryption is transparent. Q-EKM was designed to generate and communicate encryption keys for LTO-4 or greater drives in Quantum libraries across the customer's environment.

If you choose to purchase and use the licensed Q-EKM application, you must supply a server on which to install EKM. Professional Q-EKM integration must be performed by Quantum or Quantum authorized service personnel. For more information, contact the Quantum Technical Assistance Center at www.quantum.com/support.

Note: Prior to configuring Q-EKM on the Scalar i6000 library, Quantum recommends installing and configuring the Q-EKM server or servers first.

For more information about installing and configuring the Q-EKM server and Q-EKM best practices, see the *Quantum Encryption Key Manager User's Guide* (6-01847-xx).

Q-EKM on the Scalar i6000 library supports encrypting LTO-4 or higher tape media using IBM LTO-4 or higher Fibre Channel drives only. All IBM LTO-4 or higher FC drives are encryption-capable, but to use the Q-EKM software application, you must purchase an Encryption Key Management license and provide a server or servers on which to install Q-EKM. Q-EKM does not currently support encryption on other tape

drive types or manufacturer brands, even if they are assigned to a partition selected for encryption.

Note: You must be running Q-EKM version 2.0 (or higher) to support IBM LTO-5 or LTO-6 tape drives.

The encryption keys pass through the library, so that encryption is “transparent” to the applications. If you purchase Q-EKM, Quantum's Service department will schedule an appointment to install the application onto your server(s).

Using SKM

If you purchase SKM, you will receive the software application, two servers (optional beginning with SKM 1.1), and installation and configuration instructions. This chapter describes how to configure your encryption key management (EKM) solution (Q-EKM or SKM) on the library.

SKM Management

Sharing Encrypted Tape Cartridges

If you are using SKM, you can use the library to facilitate sharing encrypted tapes with other companies and individuals who also use SKM for managing encryption keys.

Each SKM server provides a unique encryption key for each tape cartridge that is encrypted. To read an encrypted tape in a library that is attached to a SKM server that is different than the one that originally provided the encryption key, the encryption key from the originating (i.e., source) SKM server needs to be shared with the receiving (i.e., destination) SKM server.

The key (or list of keys, if there is more than one tape) is exported from the source SKM server to a file, which is sent to the destination recipient. Each key contained in the file is encrypted using the public key of the destination SKM server. The destination SKM server provides its public key to the source SKM server as part of an Encryption Key Certificate, which the source SKM server uses to wrap (encrypt) the

encryption keys for transport. Upon arrival, the file containing the wrapped encryption keys can only be unwrapped by the corresponding private key, which resides on the destination SKM server and is never shared.

The process is as follows:

1. The destination administrator exports the Encryption Key Certificate that belongs to the destination SKM server. The Encryption Certificate is saved as a file to a location specified by the administrator on a computer (see Exporting Encryption Certificates on page 309).
2. The destination administrator e-mails the Encryption Key Certificate file to the source administrator.
3. The source administrator saves the Encryption Key Certificate file to a location on a computer, and then imports the Encryption Key Certificate onto the source SKM server (see Importing Encryption Certificates on page 308).
4. The source administrator exports the Encryption Keys, assigning the same Encryption Key Certificate noted above to wrap the keys. The file containing the wrapped encryption keys is saved to a location on a computer specified by the source administrator. See Exporting Encryption Keys on page 311.
5. The source administrator e-mails the file containing the wrapped encryption keys to the destination administrator.
6. The destination administrator saves the file containing the wrapped encryption keys to a location on a computer, and then imports the keys onto the destination SKM server (see Importing Encryption Keys).
7. The destination library can now read the encrypted tapes.

Importing Encryption Certificates

The encryption certificate contains a public key that is used to wrap (encrypt) encryption keys prior to transporting them to another SKM server. When sharing tape cartridges, or when performing a backup in the event of SKM server failure, you need to import the encryption key certificate of the destination SKM server.

Note: This function is available to users with administrator-level privileges and only applies to SKM servers. Both SKM servers must be connected and operational in order to import encryption key certificates.

Before starting this process, read and follow the sequence of steps outlined in Sharing Encrypted Tape Cartridges on page 307.

1. Receive the encryption key certificate file from the destination SKM server administrator and save it to a known location on your computer.
2. From the **Tools** menu, select **EKM Management > Encryption Certificate > Import**. The **SKM Encryption Certificate Import** dialog box appears.

.

3. Click **Browse** to locate the saved encryption key certificate file.
4. Highlight the file and click **Open**.
5. Click **OK** to import the certificate onto your SKM server. The dialog box closes and you are returned to the main console.

Exporting Encryption Certificates

Before you can receive encryption keys from another SKM server, you must first send your native encryption key certificate to that server. You can use the Export functionality to export the native certificate to a file that can be imported into another SKM server. The public key contained

in the certificate will be used to wrap (encrypt) the encryption keys to protect them during transport to you.

NOTE: This function is available to users with Administrator-level privileges and only applies to SKM servers. Both SKM servers must be connected and operational in order to export encryption key certificates.

To export an encryption key certificate:

1. Before starting this process, read and follow the sequence of steps outlined in Sharing Encrypted Tape Cartridges on page 307.
2. From the Tools menu, select **EKM Management > Encryption Certificate > Export.** The **SKM Certificate Export** dialog box appears.

3. Click **Browse** to locate the saved encryption key certificate file.
4. Highlight the file and click **Open**.
5. Click **OK** to export the file. The dialog box closes and you are returned to the main console.

Importing Encryption Keys

Each SKM server provides a unique encryption key for each tape cartridge that is encrypted. In order to read tapes encrypted by a different (i.e., source) SKM server, you need to import the encryption keys used to encrypt those tapes onto your SKM server.

You may also use this function to import a backup of your own SKM server encryption keys in case of a catastrophic SKM server failure.

Note: This function is available to users with Administrator-level privileges and only applies to SKM servers. Both SKM servers must be connected and operational in order to export encryption key certificates.

1. Before starting this process, read and follow the sequence of steps outlined in Sharing Encrypted Tape Cartridges on page 307.
2. Receive the file of encryption keys from the source SKM server and save it in a known location on your computer.
3. From the **Tools** menu, select **EKM Management > Encryption Key > Import**.
4. Click **Browse** to locate the saved file of encryption keys.
5. Highlight the file and click **Open**.
6. Click **OK** to import the keys onto your SKM server.

   After a successful import, a message is displayed recommending you backup your encryption keys to protect against a catastrophic EKM server failure. Consult your EKM server documentation for details on how to perform an EKM backup.

   The dialog box closes and you are returned to the main console.

Exporting Encryption Keys

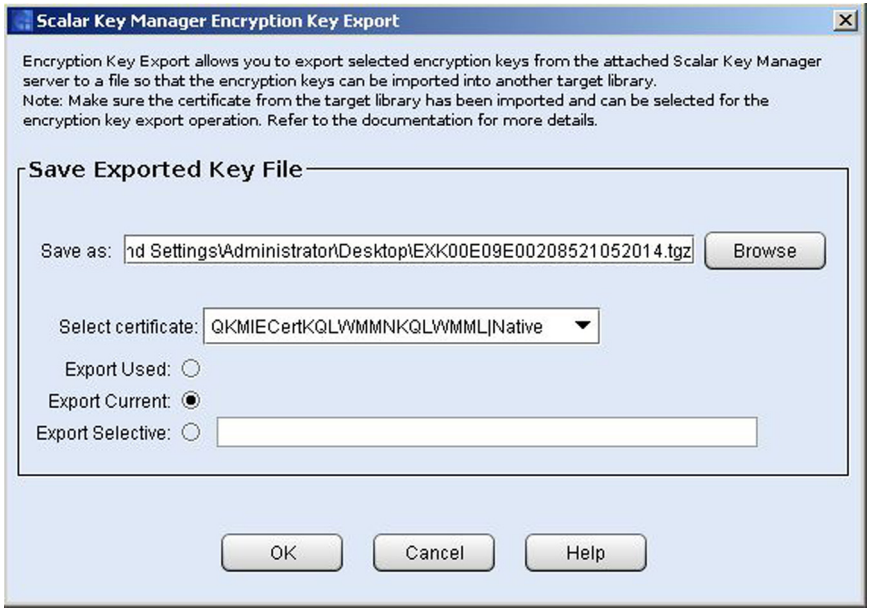
Each SKM server provides a unique encryption key for each tape cartridge that is encrypted. In order for another (i.e., destination) SKM server to read tapes encrypted by your SKM server, you need to export the encryption keys used to encrypt those tapes and send them to the destination server.

You may also use this function to create a backup of your SKM server encryption keys in case of a catastrophic SKM server failure.

Note: This function is available to users with Administrator-level privileges and only applies to SKM servers. Both SKM servers must be connected and operational in order to export encryption key certificates.

1. Before starting this process, read and follow the sequence of steps outlined in Sharing Encrypted Tape Cartridges on page 307.

2 From the **Tools** menu, select **EKM Management > Encryption Key > Export**. The **Scalar Key Manager Encryption Key Export** screen appears.



3 In **Save As** field, click **Browse** to save the encryption key file to a location on your computer.

4 In the **Select Certificate** drop-down list, assign the encryption key certificate with which you will "wrap" the keys.

The drop-down list contains all of the encryption key certificates that you have ever imported onto your SKM server (indicated by the word "imported" in the list).

The list also contains the native encryption key certificate for your SKM servers, indicated with the word "Native" in the name.

If destination server is:

- **Someone else's SKM server** — The destination administrator should have sent you the encryption key certificate previously and you should have imported it onto your SKM server (see Importing Encryption Certificates on page 308). It should appear on the list for you to select.
- **Your SKM server** — If you are sending your encryption key certificate to someone else to use to wrap encryption keys,

select your “native” certificate. You might also need to export your “native” certificate for disaster recovery in the event that one of your SKM servers failed and you needed to re-import all of your keys onto a new SKM server.

5 Select which SKM encryption keys to export from the following options:

- **Export Used** — Exports all the keys that have ever been used to encrypt tape cartridges on the library.
- **Export Current** — Exports only keys for tape cartridges currently present in the library.
- **Export Selective** — Exports the keys that are associated with a string of characters that you type into the text box. Each key is associated with its encrypted tape cartridge, identified by the tape cartridge barcode. You can type in all or part of a tape cartridge barcode, and any keys that are associated with that string will be exported. This is helpful if you only want to export a single key associated with a particular tape cartridge.

6 Click **OK**.

Each key is wrapped (encrypted) using the destination public key contained on the selected destination encryption certificate. All the selected keys are saved to a single file.

Retrieving SKM Server Logs

The SKM Server Logs contain information on activity that has occurred on the SKM servers. You can save the logs to a location on a computer, or e-mail the logs to a recipient. The logs downloaded from the servers are stored in the form of tar files.

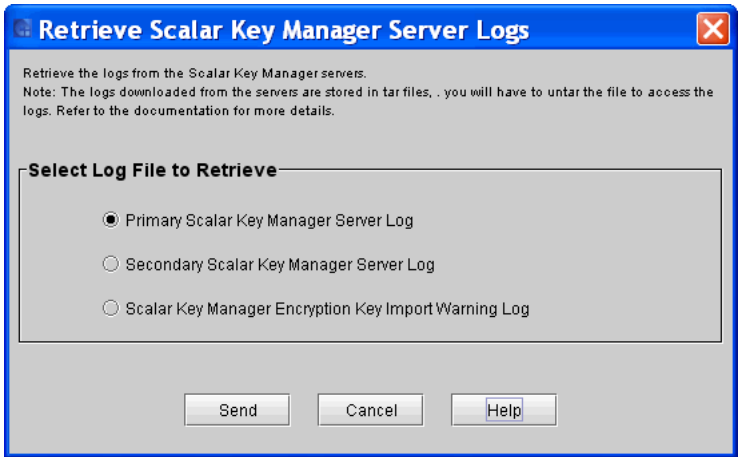
To access the file, you will have to untar the file first.

To retrieve these logs, you must have Library Managed Encryption licensed on the library and be running a SKM server or servers.

Note: This function is available to users with administrator-level privileges only.

---

1 From the **Tools** menu, select **EKM Management > Retrieve SKM Logs**.



2 Select which log you want to retrieve. If a server is down or not connected, you will not be able to select it.

- Primary SKM Server Logs
- Secondary SKM Server Logs
- SKM Encryption Key Import Warning Log

  Contains a list of keys that failed import. If you have only partial success when importing a file of encryption keys (meaning, some keys import successfully but some keys do not), the library generates an "import warning" message as well as a RAS ticket that directs you to view this log to see which keys did not get imported. This log is only available if you are running SKM and have encryption key management licensed on the library. When the log file reaches its maximum size, the oldest information is replaced as new information is added.

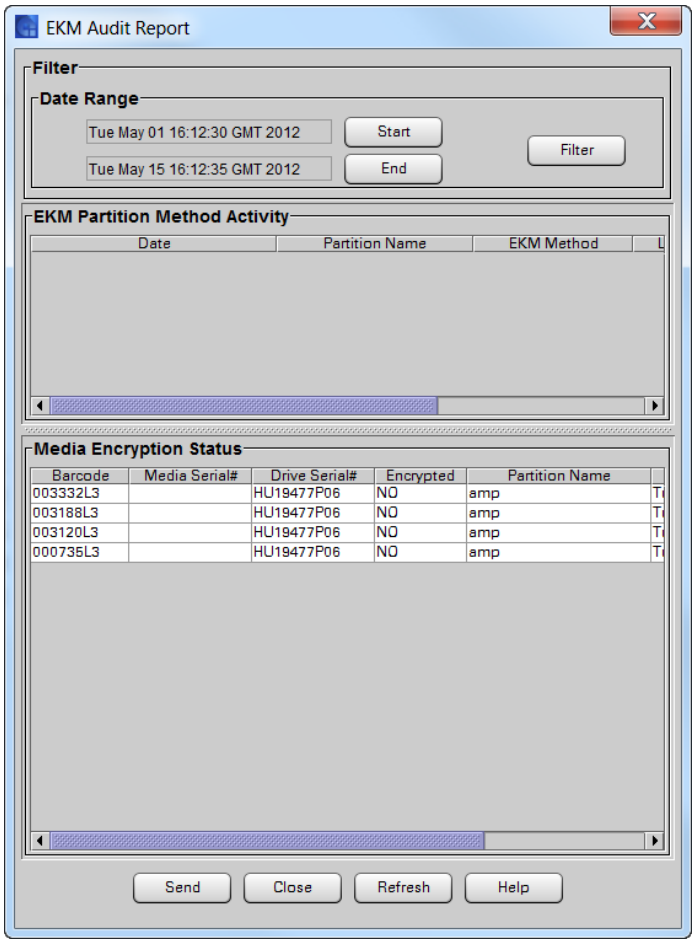
3 Click **Send** to save, e-mail, or print the information. The **Email**, **Save**, or **Print** dialog box appears.

Generating EKM Audit Reports

The EKM Audit Report option allows you to view or print library information, encryption method activity and media encryption status. If desired, you can save, print or email the generated information.

Note: This function is available to users with administrator-level privileges only.

1 From the **Tools** menu, select **EKM Management > EKM Audit Report**. The **EKM Audit Report** screen appears.



2 If desired, click the **Start** and **End** buttons in the **Date Range** section to specify starting and ending dates for the report. Click **Filter** to apply your entries.

3 Click **Send** to save, e-mail, or print the information. The **Email**, **Save**, or **Print** dialog box appears.

4 When you save or email the report, a zip file containing the following three files is created:

- encryptionMethodChanges.csv
- mediaEncryptionStatus.csv
- libraryInfo.txt

These three files contain the same information that is displayed on the **EKM Audit Report** screen.

5 Click **Close** when you are finished with the EKM Audit Report.

Chapter 9
Extended Data Lifecycle Management

Extended Data Lifecycle Management (EDLM) provides data protection and integrity checking by scanning your tape cartridges, providing results, and allowing StorNext Storage Manager to migrate data off of bad or suspect tapes. EDLM allows you to run manual scans on any tape cartridge in the library at any time, and performs automatic scans according to schedules and policies that you set up.

To use EDLM, you set up an EDLM library managed partition into which tapes are moved for scanning. Scanning takes place using "EDLM scanning drives." You can use EDLM for manual scans at any time and also set up automatic scanning policies.

EDLM is typically used to check the health of data on cartridges in long-term retention (archive or disaster recovery) that are no longer used in normal operations. (Conversely, health information for active cartridges is presented in the Media Integrity and Media Usage reports, which are part of the Advanced Reporting feature.).

This section covers the following topics:

About EDLM

- The EDLM feature requires an Extended Data Lifecycle Management license (see Enabling Licenses on page 115). One license covers the entire library.
- EDLM expands upon and replaces the Media Data Integrity Analysis (MeDIA) feature previously used on the library. The MeDIA feature only included manual media scans. If you previously installed a Media Data Integrity License on the library, you will notice that the name of the license changes to Extended Data Lifecycle Management when you upgrade to version 612Q or later code, and the additional features of EDLM are added. The *Scalar i6000 User's Guide* section "Running MeDIA Test Reports" will be replaced by Running Manual EDLM Tests on page 332 and Viewing EDLM Test Sessions and Report Details on page 338.
- One library managed partition is required for the media scans. This library managed partition is accessible only by a library administrator. It is not presented to any other applications. The library managed partition is assigned its own dedicated resources and EDLM scanning is executed in the background with no impact to normal tape operations. Cartridges are moved into the EDLM library managed partition and scanned using EDLM-scanning drives residing in the EDLM library managed partition. After being scanned, cartridges are returned to their original locations. See Step 1: Creating the EDLM Library Managed Partition on page 320.
- Automatic media scanning policies are configured by partition. Each partition can have its own unique set of media scanning and action policies. See Step 3: Configuring EDLM Policies on Partitions on page 322.

- You can also scan cartridges manually at any time. See Running Manual EDLM Tests on page 332.
- You need Administrator privileges to use EDLM.
- All types of tape cartridges (data, cleaning, diagnostic, and firmware update tapes) can be scanned manually. However, only data cartridges can be scanned automatically.
- Media scan requests are performed as they are received. If there are not enough drives to scan all requests concurrently, the scans are queued based on the priority you select (high, medium, low). Manual scans can be initiated to scan immediately, superseding previously queued scans. Queued tests are reported as "Not Completed" in the test report (see Viewing EDLM Test Sessions and Report Details on page 338).
- You may optionally use StorNext Storage Manager to trigger media scans and automatically copy data off of suspect or failed tapes. To use StorNext you must separately install an API client plug-in. See Step 2: Configuring Access to StorNext on page 322.
- If a cartridge is being scanned and the host initiates a move request, the scan is aborted and the library performs the host-requested move. The scan is not rescheduled, but the cartridge will be scanned at the next scheduled time according to the policy. The EDLM report indicates the interruption or cancellation. This ensures that normal operations are not affected by EDLM scanning.
- You can move tapes between EDLM library managed partitions and standard partitions via the library user interface without exporting and importing the tapes (for more information, see Moving Media Between Active Vault or AMP and Standard Partitions on page 690).

Note: Manual movement between library managed partitions and standard partitions will require inventory reconciliation with the backup application managing the standard partition.

- EDLM drives and blades must be separate from other blades in the library.

Configuring EDLM

Step 1: Creating the EDLM Library Managed Partition

The EDLM library managed partition is a dedicated partition that you set up in the library for scanning media with EDLM. This partition exists solely for media scanning purposes and is not accessible to hosts or other applications. Tape cartridges are moved into the EDLM library managed partition and scanned using the tape drives residing in the EDLM library managed partition. When the scan is complete, the cartridges are returned to their original partitions.

Details about the EDLM library managed partition include:

- There can be only one EDLM library managed partition in the library.
- All tape drives in the EDLM library managed partition must be "EDLM-scanning drives" (not standard tape drives) which must be purchased from Quantum. Previously purchased "MeDIA drives" are the same thing and are now known as "EDLM-scanning drives." These EDLM-scanning drives are HP LTO-4, LTO-5 or HP LTO-6 Fibre Channel tape drives. You can have LTO-4, LTO-5 and LTO-6 EDLM-scanning drives in the EDLM library managed partition.
- The EDLM library managed partition can support any number of EDLM-scanning drives (within the normal support of the physical library).
- All of the EDLM scanning drives in the EDLM library managed partition can be connected to either a 7404 Fibre Channel I/O blade or an Ethernet Expansion Blade (EEB). The FC I/O blade must not be connected to a host, nor may it be shared with drives located in another partition. Each FC I/O blade supports up to 4 tape drives while an EEB supports up to 6 tape drives. You can use multiple FC blades and EEBs to support the EDLM-scanning drives.
- Tape drives in the EDLM library managed partition will only be used for EDLM scanning purposes.
- The EDLM library managed partition is composed of unlicensed slots. If the size of the EDLM partition exceeds the number of unlicensed slots, then the partition will be composed of both unlicensed and licensed slots, or all licensed slots.
- The normal library tape drive cleaning policies apply to the tape drives in the library managed partition.

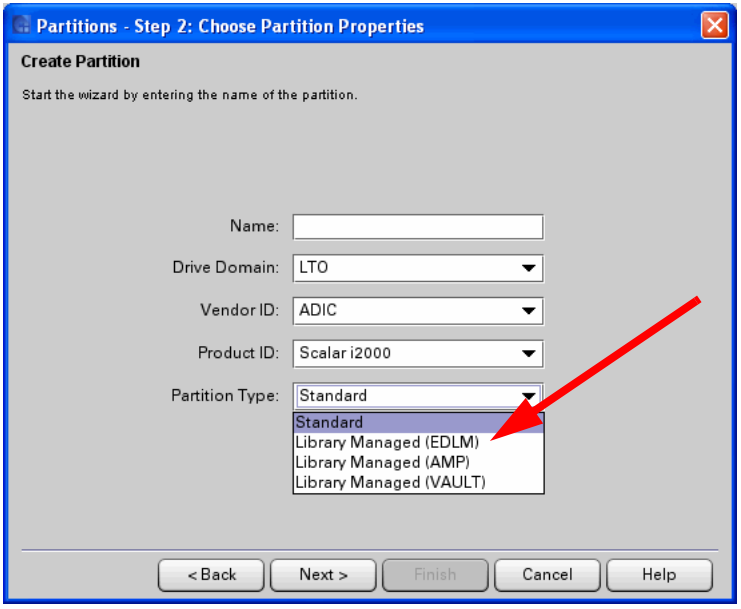
- You can set up EDLM scanning policies on the EDLM library managed partition.

To create the EDLM library managed partition, do the following:

1. Install EDLM-scanning drives in the library.
2. Connect each EDLM-scanning drive to one of the four initiator ports in a dedicated 7404 Fibre Channel I/O blade. Make sure that this Fibre Channel I/O blade is not be connected to a host, and that it only has EDLM-scanning drives connected to it. If you have more than four EDLM-scanning drives, you will need to use more than one dedicated Fibre Channel I/O blade.
3. Log on as an administrator.
4. From the **View** menu, select the physical library.
5. Install the Extended Data Lifecycle Management license on the library.

   Note: If you already have the MeDIA license installed, it will automatically become the Extended Data Lifecycle Management license.

6. Use Expert Mode to create the EDLM library managed partition. Follow the instructions in Using Expert Mode on page 131. When you get to the screen named **Partitions - Step 2: Choose Partition Properties**, select **Library Managed (EDLM)** from the **Partition Type** drop-down menu.



Step 2: Configuring Access to StorNext

This step is optional. If StorNext Storage Manager is managing your partition, you can use StorNext with EDLM to automatically copy data off of bad or suspect tapes or to trigger media scans.

In order to use StorNext for these purposes, you first need to configure the library for StorNext access. Follow the steps in Chapter 11, Configuring Access to StorNext, and then return here. You will then be able to select StorNext policies in the next step.

Step 3: Configuring EDLM Policies on Partitions

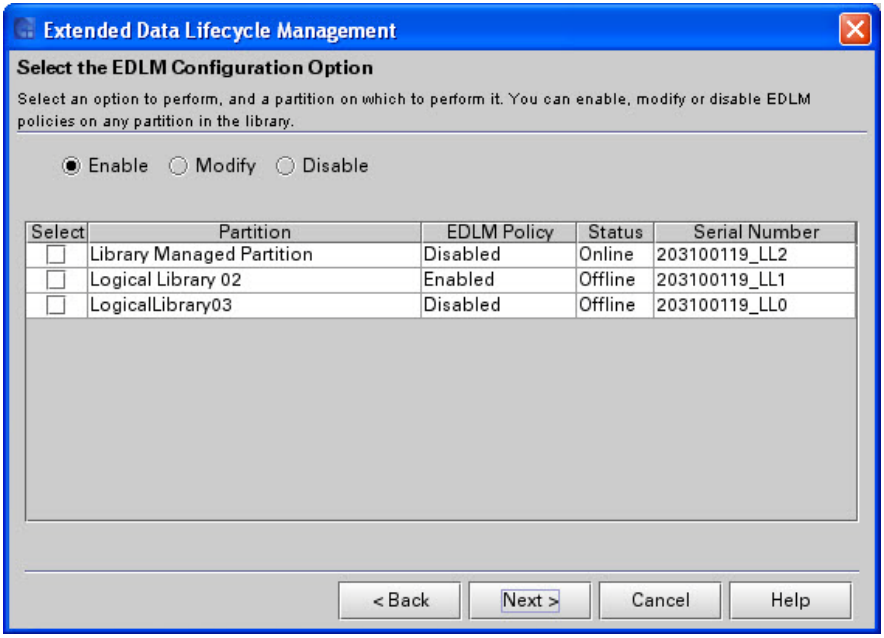
Automatic scanning and other EDLM policies are enabled by partition. You can set up EDLM policies on as many standard and Active Vault partitions as you want, as well as an EDLM library managed partition. (Some policies are not available on the EDLM and other library managed partitions; namely, those that require external access to a host application.) You can configure the following types of policies:

Media Scan Candidate Policies	Specifies when to perform automatic scans on media in the partition. See Step 5 on page 326.
Media Scan Type Policies	Specifies which type of automatic scans to perform (quick, normal, or full). See Step 7 on page 329.
Media Scan Results Action Policies	Specifies what actions to take on suspect or failed media. These policies apply to all media in the partition, whether they were scanned manually or automatically. See Step 11 on page 331.

This section describes how to create, modify, and remove EDLM policies on partitions.

Note: Cartridges that are not capable of being read by at least one of the tape drives in the EDLM library managed partition are excluded from all scans. (For example, if the EDLM library managed partition contains only LTO-5 tape drives, then LTO-1 and LTO-2 cartridges will not be scanned.)

1. Select **Setup > Partitions > Policies > EDLM Configuration**. The Extended Data Life Management Configuration Wizard appears.
2. Click **Next**. The **Select the EDLM Configuration Option** screen appears. All of the library's partitions are displayed in a table. The **EDLM Policy** column indicates whether EDLM policies are enabled or disabled on the partition.



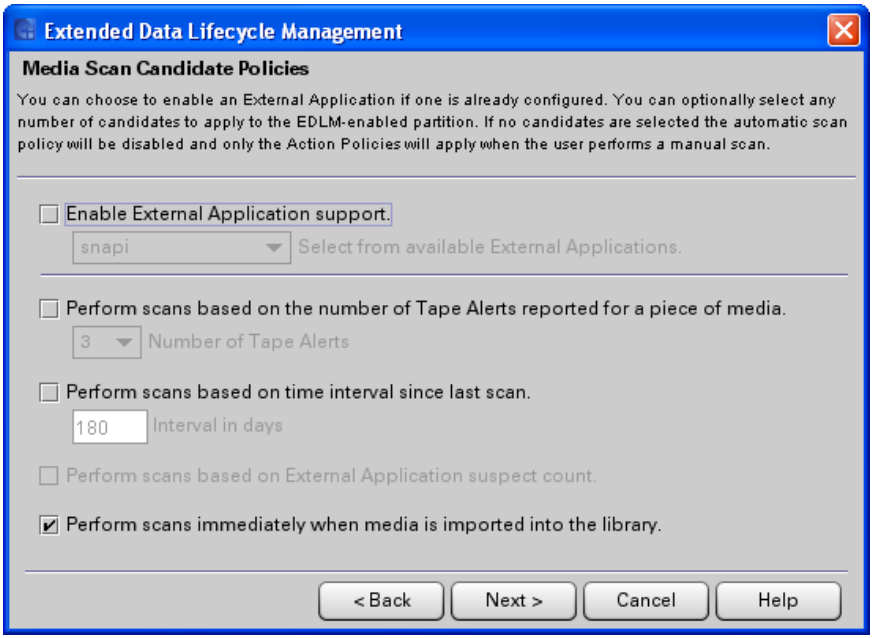
3 Create, modify, or remove policies on a partition by doing one of the following:

To...	Do this...
Enable EDLM policies on a partition	**1** Select the **Enable** radio button. **2** Select the check box of a partition in the table that has EDLM policies disabled. **3** Proceed to Step 4.
Modify existing EDLM policies on a partition	**1** Select the **Modify** radio button. **2** Select the check box of a partition in the table that has EDLM policies enabled. **3** Proceed to Step 4.

To...	Do this...
Disable EDLM policies on a partition	**1** Select the **Disable** radio button. **2** Select the check box of a partition in the table that has EDLM policies enabled. **3** Click **Finish**. A confirmation dialog box appears asking you to confirm you want to disable the EDLM policies on the partition. **4** Click **Yes** to confirm. A "success" dialog box appears. **5** Click **OK** to close the dialog box. Process is complete.

4 Click **Next**. The **EDLM Media Scan Candidate Policies** screen appears.

Note: Depending on the type of partition you are setting policies for, some of the choices shown below may not appear. For example, library managed partitions cannot be configured for external application support.



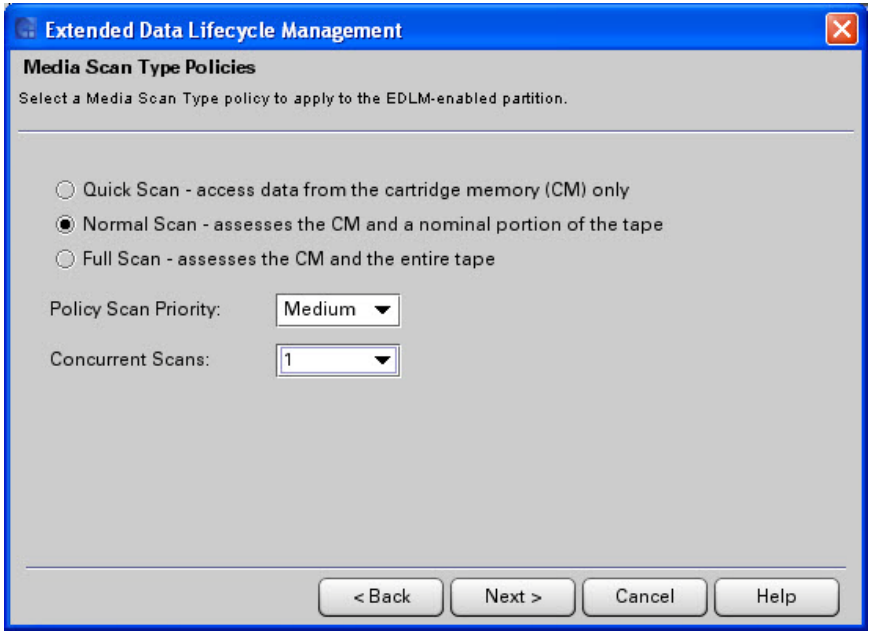
5 Select as many media scan candidate policies as you wish. The policies apply to all tape cartridges in the partition. Depending on your library and partition configuration, some of the options listed below may not be available.

Note: You may select zero scan candidate policies by clearing all of the check boxes. This means no automatic scans will be performed on this partition. You might wish to do this to temporarily halt automatic scans on media in the partition but keep your policy drop-down list selections intact so that you can re-enable them later. You can still perform manual scans on tapes residing in the partition, and media scan action results policies (Step 11 on page 331) will remain in effect.

Media Scan Candidate Policy	Description
Enable External Application support	Allows you to use a supported external application to perform corrective action and trigger media scans. Once you enable this policy, you will be able to configure the following options: • Perform scans based on External Application suspect count. on page 328 • Request Media Copy by External Application on page 332 In order to select this policy, access to an external application must be configured (see Step 2: Configuring Access to StorNext on page 322). Choose the desired external application from the drop-down list. This policy is disabled by default. This policy is not available on library managed partitions.
Perform scans based on the number of Tape Alerts reported for a piece of media.	Scans a tape if the number of Tape Alerts reported for that cartridge exceeds the specified value. From the drop-down list, select the number of Tape Alerts. The Tape Alerts included in the count are: • **01h (1)** – Read Warning • **03h (3)** – Hard Error • **04h (4)** – Media • **05h (5)** – Read Failure • **06h (6)** – Write Failure • **12h (18)** – Tape Directory Corrupted on Load • **33h (51)** – Tape Directory Invalid on Unload • **34h (52)** – Tape System Area Write Error • **35h (53)** – Tape System Area Read Error • **37h (55)** – Loading Failure • **3Bh (59)** – WORM Medium Integrity Check Failed This policy is disabled by default. The default number of Tape Alerts is 3. This policy is not available on the library managed partitions.

Media Scan Candidate Policy	Description
Perform scans based on time interval since last scan.	Scans a tape if the time interval since the last scan was performed has been exceeded. In the text box, type a time interval (in days) after which a scan will be performed. **Note:** When deciding on the interval, consider the number of tapes to be scanned in the entire library, as well as the type of scan to be performed. Full scans can take more than 2 hours on full tapes. Over-scheduling can cause delays or tapes not to be scanned as intended. This policy is disabled by default. The default interval is 180 days. To change the interval, type a new value in the interval text box.
Perform scans based on External Application suspect count.	A suspect count is a means by which an external application determines when to stop writing data to tape. If you select this policy, a tape will be queued for EDLM testing when its suspect count threshold is reached. If the EDLM test indicates the tape is good, you can reset the suspect count on the external application and continue to use the tape. For more information on suspect counts and resetting suspect counts, refer to your external application's documentation. This policy is disabled by default. You can only select this policy if **Enable External Application support** is also selected (see Enable External Application support on page 327), and if the external application supports suspect counts.
Perform scans immediately when media is imported into the library.	Scans a tape cartridge as soon as it is imported into the partition.

6 Click **Next**. The **EDLM Media Scan Type Policies** screen appears.



7 Select a media scan type policy.

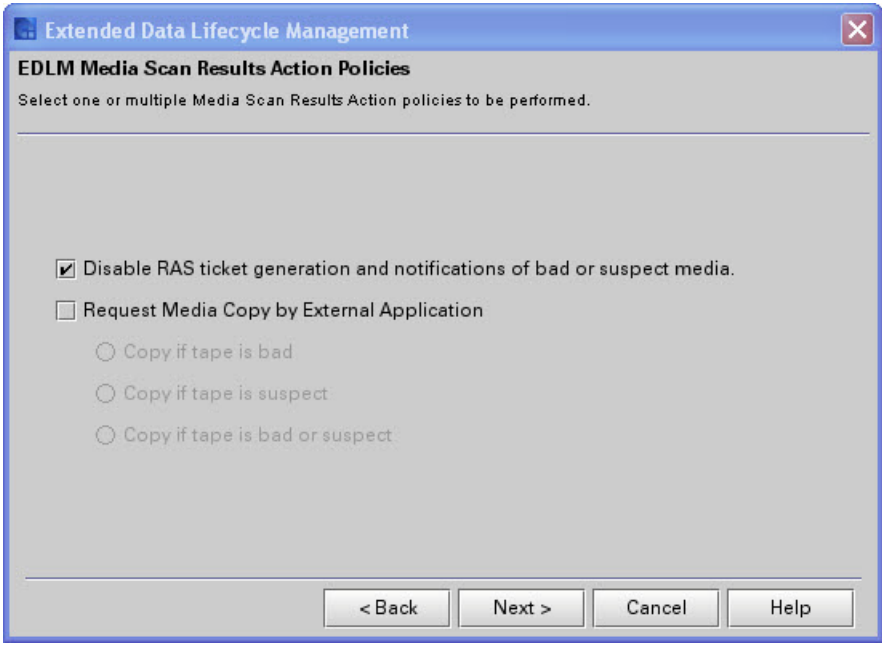
Note: When deciding on a scan type policy, consider how the tapes are being used. Depending on the number of EDLM drives and the scan type policy you choose, scans can take a very long time to complete, and may overlap the next scheduled scan.

Media Scan Type Policy	Description
Quick Scan	Does not scan the tape. Evaluates data from the cartridge memory (CM) only. A quick scan takes less than one minute per tape. **Examples of when to use a quick scan:** • When you first import previously used scratch tapes into the library. • When you import data cartridges that have been used in other backup and archival environments and need to do a quick check to determine whether the tape cartridge is nearing end of life, at end of life, or may have had issues reading or writing.
Normal Scan (default)	Evaluates the cartridge memory (CM) and scans selected portions of the tape, focusing on areas most likely to indicate problems. A normal scan can take 20 minutes per tape. **Examples of when to use a normal scan:** • For tapes in frequent use within the library, with scanning triggered by drive-reported media Tape Alert events. • For tapes in frequent use within the library, with scanning being performed at regular time intervals.
Full Scan	Evaluates the cartridge memory (CM) and scans the entire tape. A full scan can take more than 2 hours on a full tape. **Example of when to use a full scan:** • When tape cartridges are accessed infrequently and are used primarily for on-site or off-site long-term data retention. • When tape cartridges with valuable data are introduced into the library and the state and condition of the tapes are unknown.

8 Select a scan priority from the **Policy Scan Priority** drop-down list (Low, Medium, or High). The default is medium. The priority is used to queue scans when there are too many to be performed concurrently.

9 Select the maximum number of concurrent scans allowed from the **Concurrent Scans** drop-down list. The maximum allowed (default) is the number of scanning drives in the EDLM partition.

10 Click **Next**. The EDLM Media Scan Results Action Policies screen appears.



11 Select one or more of the following media scan results action policies to be performed when media is bad or suspect.

Note: These action policies apply to all tapes scanned in this partition, whether they are scanned manually or automatically.

Media Scan Results Action Policy	Description
Disable RAS ticket generation and notifications of bad or suspect media.	Select this option if you do not wish to receive RAS tickets and e-mail notifications of bad or suspect media. RAS ticket generation is disabled by default.

Media Scan Results Action Policy	Description
Request Media Copy by External Application • Copy if tape is bad (default) • Copy if tape is suspect • Copy if tape is bad or suspect	Automatically requests a supported external application to copy all data from a bad and/or suspect tape to another tape. Once you enable this policy, you can select whether to copy bad tapes, suspect tapes, or both. A RAS ticket will be generated for each request to copy data indicating whether the request succeeds or fails. You can only select this option if a supported external application is enabled for use with EDLM on this partition (see Enable External Application support on page 327). In order for this policy to work, the partition must contain at least two tape drives (one for the bad/suspect tape from which you are copying data and one for the good tape to which you are copying data).

12 Click **Next**. The **EDLM Configuration Summary** screen appears.The screen displays all of your choices.

13 Click **Finish** to apply your settings, or use the **Back** button to make changes. A "success" dialog box appears.

14 Click **OK** to close the dialog box.

Step 4: Viewing EDLM Partition Policies

To review the policies you configured, you can go back through the Wizard, or you can click **Monitor > Partitions > Policies**. See Monitoring Partition Policies on page 534 for more information.

Running Manual EDLM Tests

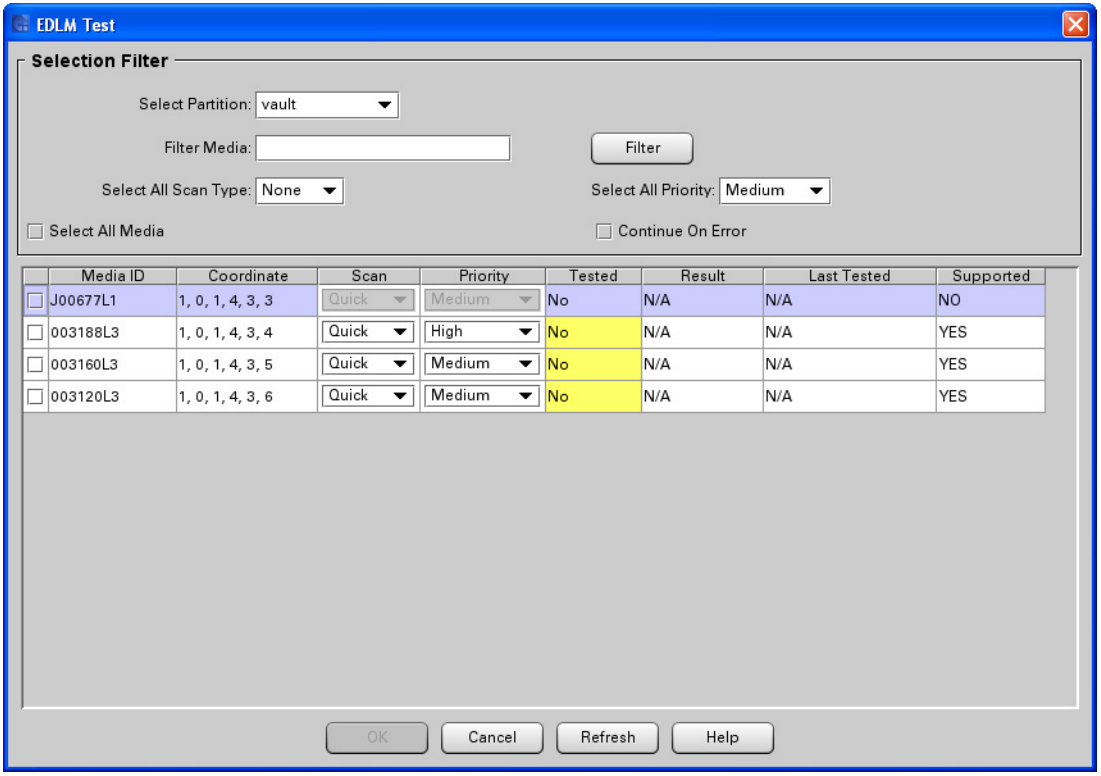
You may wish to evaluate media outside of the EDLM automatic scanning policies. You can manually scan tape cartridges in the library at any time. Manual EDLM scans can be run on any tape in the library, as long the following conditions are met:

- An EDLM license must be installed on the library.

- The EDLM library managed partition must be configured on the library (see Step 1: Creating the EDLM Library Managed Partition on page 320).
- The cartridge you want to scan must be capable of being read by a tape drive in the EDLM library managed partition.
- The cartridge can be located in any partition, including the EDLM library managed partition.
- The cartridge must be located in a storage slot, not in a drive or I/E station.

To run a manual EDLM test, do the following:

1. Log on as an administrator.
2. From the **View** menu, select the physical library or a partition on which EDLM policies are enabled.
3. From the main menu, select **Tools > EDLM > Test Selection**. The EDLM Test screen appears.



The media selection table contains the following information:

Item	Description
Media ID	The media barcode.
Coordinate	Where the cartridge is located within the library.
Scan	Scan type, described in Step 7 on page 336.
Priority	The order in which scans are performed, described in Step 9 on page 337.

Item	Description
Tested	Indicates whether the media has already been tested (Yes/No), or if the media is currently part of a test session that has not yet completed (Pending; cell is highlighted in yellow).
Last Tested	The date the media was last tested.
Test Result	The last test result for the media. Test results include the following: • **Good** — The tape is good. • **Bad** — The tape is bad. • **Suspect** — The tape is possibly unreliable or defective. • **Untested** — The tape could not be fully scanned, for various reasons, including: incompatible or unknown media type; tape could not be loaded; tape is encrypted but the data encryption key could not be obtained; drive not communicating with I/O blade, test was stopped. **Note:** Untested media do not initiate RAS tickets or EDLM media action policies (such as copying data from a bad or suspect tape). • **Not Completed** — The test has not completed yet.
Supported	Indicates whether the media is a supported media type (Yes/No) (meaning, it can be read by at least one of the drives in the EDLM library managed partition). For example, an LTO-1 tape cannot be read by an LTO-4 drive. Unsupported media cannot be selected for testing.

4 From the **Select Partition** drop-down list, select the partition that contains the media you want to test.

5 To filter the displayed list of media, in the **Filter Media** field, type the desired Media ID (barcode label), or a portion of a Media ID, and click **Filter**. If you choose not to filter the list, skip this step.

6 From the media table, select the check box for each tape you want to scan. To select all media listed, select the **Select All Media** check box.

Note: You can sort the media list by **Media ID**, **Coordinate**, **Tested**, and **Result** by clicking the column header. An arrow appears in the column header indicating whether the column is sorted in ascending or descending order. Click the column header again to toggle between ascending and descending order.

Note: You cannot select unsupported media.

7 For each selected tape, choose a scan type from the drop-down list in the **Scan** column. To select the same type of scan for all selected tapes, choose a scan type from the **Select All Scan Type** drop-down list. The scan types are described in the following table.

Note: When deciding on the type of test to run, consider how the tapes are being used. Depending on the number of EDLM drives and the test type you choose, scans can take a very long time to complete.

Type of Scan	Description
Quick	Does not scan the tape. Evaluates data from the cartridge memory (CM) only. A quick scan takes less than one minute per tape. **Examples of when to use a quick scan:** • When you first import previously used scratch tapes into the library. • When you import data cartridges that have been used in other backup and archival environments and need to do a quick check to determine whether the tape cartridge is nearing end of life, at end of life, or may have had issues reading or writing.
Normal (default)	Evaluates the cartridge memory (CM) and scans selected portions of the tape, focusing on areas most likely to indicate problems. A normal scan can take 20 minutes per tape. **Examples of when to use a normal scan:** • For tapes in frequent use within the library, with scanning triggered by drive-reported media Tape Alert events. • For tapes in frequent use within the library, with scanning being performed at regular time intervals.

Type of Scan	Description
Full	Evaluates the cartridge memory (CM) and scans the entire tape. A full scan can take more than 2 hours on a full tape. **Example of when to use a full scan:** • When tape cartridges are accessed infrequently and are used primarily for on-site or off-site long-term data retention. • When tape cartridges with valuable data are introduced into the library and the state and condition of the tapes are unknown.

8 If desired, select the **Continue On Error** check box. You can select this check box for a **Normal Scan** or **Full Scan**. If this option is selected, the test scans the tape even if the cartridge memory (CM) test fails. If this check box is not selected, the test will not scan the tape if the CM test fails.

9 For each selected tape, choose a priority from the drop-down list in the **Priority** column. To select the same priority for all selected tapes, choose a priority from the **Select All Priority** drop-down list. The scans are queued along with all other queued EDLM scans in order of priority. The priority types are described in the following table.

Priority	Description
Immediate	Scanned immediately. If an EDLM scanning drive is busy scanning tapes in a queue, it finishes scanning the current tape and then scans the “immediate” tape before accepting another tape from the queue. If you select multiple drives with “immediate” priority, they will all be scanned before tapes with lower priorities are scanned.
High	Placed in the queue behind existing queued tapes with “high” priority.
Medium	Placed in the queue behind existing queued tapes with “medium” priority.
Low	Placed in the queue behind existing queued tapes with “low” priority.

10 Click **OK** to start the scan. The message **EDLM Tests have started successfully...** appears.

11 Click **OK** to close the message.

12 To retrieve results, go to **Tools > EDLM Tests > Test Results**. See Viewing EDLM Test Sessions and Report Details on page 338.

Viewing EDLM Test Sessions and Report Details

You can view the status of all your EDLM test sessions, including sessions that are queued but not started yet, in the EDLM Test Sessions List screen. You can stop, pause, resume, or delete test sessions. See Working with the EDLM Test Sessions List on page 338.

Each entry in the EDLM Test Sessions List screen presents an overview of a single EDLM test session. A test session includes all tapes in the library that were scheduled to be scanned at a particular point in time. Thus, a test session can include multiple tapes from different partitions.

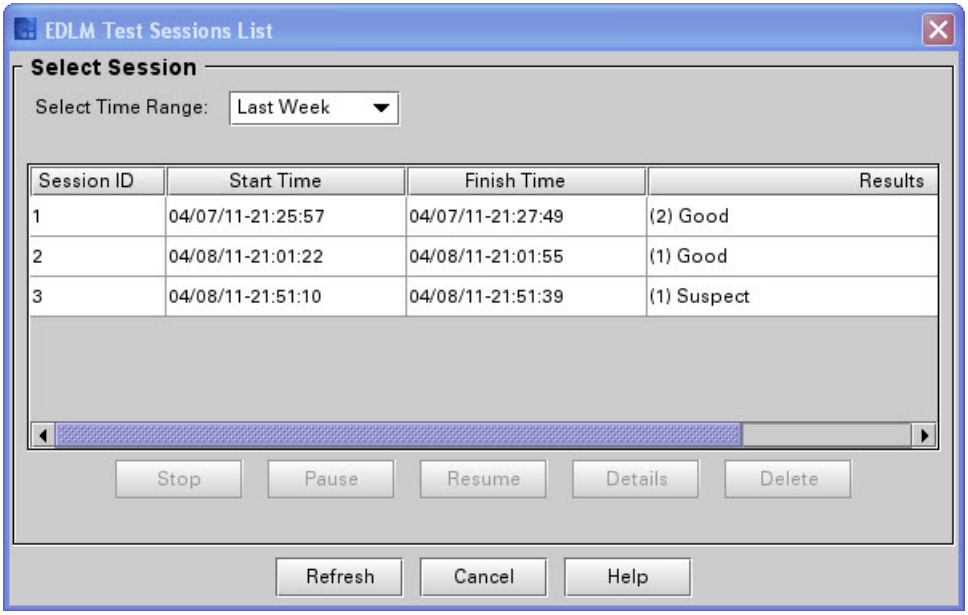
- **Example 1:** You select 10 tapes on which to perform a manual scan. The test session includes 10 tapes.
- **Example 2:** Partition A has an automatic scan policy to scan tapes on import. You import a tape. Meanwhile, Partition B has an automatic scan policy to scan every 180 days. Ten tapes in that partition have reached the 180-day mark at the same time that you import the tape into Partition A. Because these automatic scans occur at the same time, the test session includes all 11 tapes from both partitions.

Within each test session, you view details about each tape that was scanned (see Viewing EDLM Session Report Details on page 341).

Working with the EDLM Test Sessions List

To view the status of EDLM test sessions (both automatic and manual), do the following:

1 From the menu, select **Tools > EDLM > Test Results**. The **EDLM Test Sessions List** dialog box appears.



The **EDLM Test Sessions List** displays the set of media tests that have run based on the time range selected. Each row in the table presents an overview of a single EDLM test session.

You can sort the list by clicking any of the column headers. An arrow appears in the column header indicating whether the column is sorted in ascending or descending order. Click the column header again to toggle between ascending and descending order.

Table 31 displays the following information about the test sessions:

Table 31 EDLM Test Sessions

Item	Description
Session ID	The session identifier, a unique number assigned to each test session that was run.
Start Time	The date and time the test session was started.
Finish Time	The date and time the test session completed. If the test session has not yet completed, "In Progress" displays. If the test session was paused, "Paused" displays.
Results	A summary of results for all media tested in the session. The reported values include the number of tapes scanned (in parentheses) for each result obtained. **Note:** To view results for individual tapes in the session, click a test session row to highlight it, and then click the **Details** button. Results are the following: • **Good** — The tape is good. • **Bad** — The tape is bad. • **Suspect** — The tape is possibly unreliable or defective. • **Untested** — The tape could not be fully scanned, for various reasons, including: incompatible or unknown media type; tape could not be loaded; tape is encrypted but the data encryption key could not be obtained; drive not communicating with I/O blade, test was stopped. **Note:** Untested media do not initiate RAS tickets or EDLM media action policies (such as copying data from a bad or suspect tape). • **Not Completed** — The test has not completed yet.

2 In the **Select Time Range** field, select the range of time for test sessions that you want displayed. The time range is based on the start time of the test session. Choose one of the following:

- **Last Week** — Test sessions that were run in the last seven days.
- **Last Month** — Test sessions that were run in the last month.
- **Last 3 Months** — Test sessions that were run in the last three months.

- **Last 6 Months** — Test sessions that were run in the last six months.
- **All** — Includes all test sessions that were run on the library. The storage limit is 50,000 media scans. When the limit is reached, old scan results are deleted as new scan results are added.

3 To work with a session, click the test session row to highlight it, and then click your desired option:

Option	Description
Stop	Stops a currently running test session. Once stopped, you cannot restart the test. Any test results collected so far are listed. Tapes that did not complete testing as a result of being stopped show a test result of Untested.
Pause	Pauses a currently running test session. The tape that is being tested stays in the scanning drive. Tapes in the test session that have not been tested yet will remain queued.
Resume	Resumes a paused test session. Queued tapes are mounted and scanned.
Details	Displays the test report for the selected test session in a new window. See Viewing EDLM Session Report Details on page 341.
Delete	Deletes the selected test session from the list. Once deleted, you cannot retrieve the information again.
Refresh	Refreshes the test session list so that the latest information about the tests is displayed.

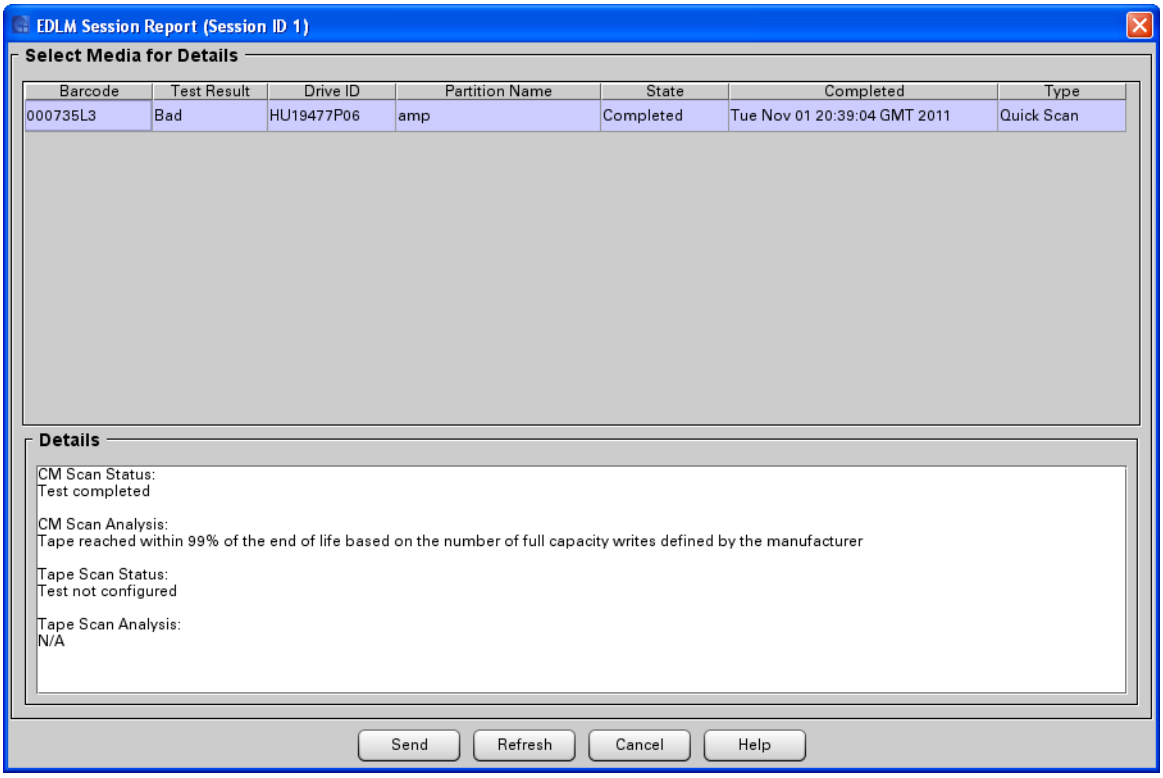
Viewing EDLM Session Report Details

To view details about a specific EDLM test session, do the following:

1 From the EDLM Test Sessions List (**Tools > EDLM > Test Results**), click on a row to highlight it, and then click the **Details** button. The test results display in a new window called EDLM Session Report

(Session ID X), where X is the session ID displayed in the EDLM Test Sessions List.

You can sort the list by clicking any of the column headers. An arrow appears in the column header indicating whether the column is sorted in ascending or descending order. Click the column header again to toggle between ascending and descending order.



The **Select Media for Details** section of the screen lists each tape in the test session. The following information is reported:

Item	Description
Barcode	The media barcode identifier.
Test Result	The test result displays as one of the following: • **Good** — The tape is good. • **Bad** — The tape is bad. • **Suspect** — The tape is possibly unreliable or defective. • **Untested** — The tape could not be fully scanned, for various reasons, including: incompatible or unknown media type; tape could not be loaded; tape is encrypted but the data encryption key could not be obtained; drive not communicating with I/O blade, test was stopped. **Note:** Untested media do not initiate RAS tickets or EDLM media action policies (such as copying data from a bad or suspect tape). • **Not Completed** — Test has not completed yet.
Drive ID	The serial number of the tape drive that tested the tape.
State	The current test status: Pending, In Progress, Completed, Stopped or Paused.
Completed	The date and time the test completed.
Type	The type of test that was run: Quick Scan, Normal Scan or Full Scan.

2 To view test details for a specific tape, click on a row in the **Select Media for Details** section to highlight it. Details about the test display in the Details section below. The following details display:

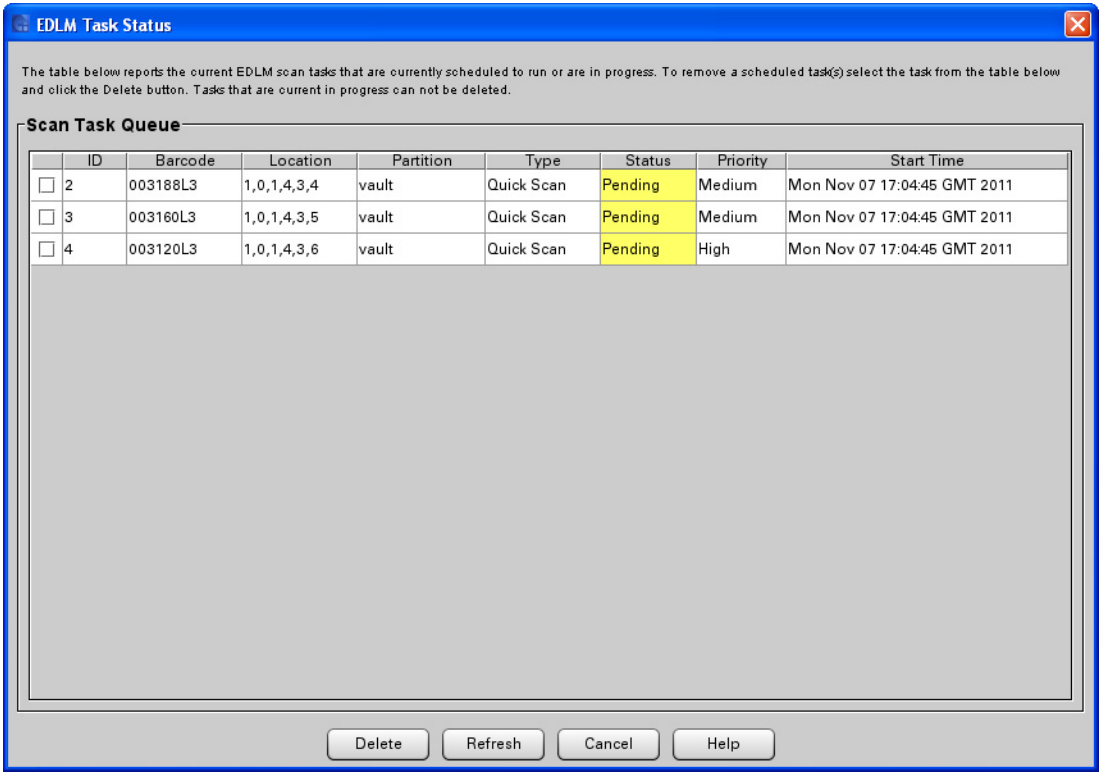
Item	Description
CM Scan Status	One of the following: • Test completed — Test is finished; however, the result may not be "good." You can also get this if the test was stopped. • Test paused. • Test pending. • Test in progress. • Test not run — Media was removed from library before it could be tested, or there were no drives available to test the media.
CM Scan Analysis	Summary of the cartridge memory scan (either "good" or an explanation of the result).
Tape Scan Status	One of the following: • Test completed — Test is finished; however, the result may not be "good." • Test paused. • Test pending. • Test in progress. • Test not run — Media was removed from library before it could be tested, or there were no drives available to test the media. • Test not configured — You requested a Quick Scan only so the tape was not scanned.
Tape Scan Analysis	Summary of the tape scan (either "good" or an explanation of the result).

3 To send a copy of the test session report via e-mail, click **Send**. To update the dialog with the current status, click **Refresh**.

Viewing the EDLM Queue

To see what EDLM scans are currently in the queue:

1 Select **Tools > EDLM > Status**. The **EDLM Task Status** screen opens. The screen lists each tape, its barcode, location, partition, scan type, test status (pending or in progress), priority, and start time. You can sort the list by **ID** or **Start Time** by clicking the column headers.



2 To refresh the list, click **Refresh**.

3 To delete a scan from the queue, select its check box and click **Delete**. Scans that are currently in progress cannot be deleted.

4 To close the screen, click **Cancel**.

Diagnosing a Suspect EDLM Drive

It is possible that any tape errors could be the result of a bad EDLM drive. A ticket will be generated indicating a possible bad EDLM drive.

To diagnose a suspect EDLM drive, it is recommended that users either create a ‘known good tape’ or use a tape that has verifiable, accurate data.

If there is no ‘known good tape’ available and users are not confident that a tape is providing accurate data, they can contact Quantum Service and ask if an EDLM Diagnostic Tape is available to test their suspect EDLM drive.

Chapter 10
Path Failover

Path Failover (formerly known as Native Storage Networking (nSNW)) is a licensable feature that allows you to take advantage of control and data path failover, as well as host access configuration features of IBM and HP LTO-5 and higher tape drives, without those drives being connected to a Fibre Channel I/O blade and instead connected to an Ethernet Expansion Blade (EEB)

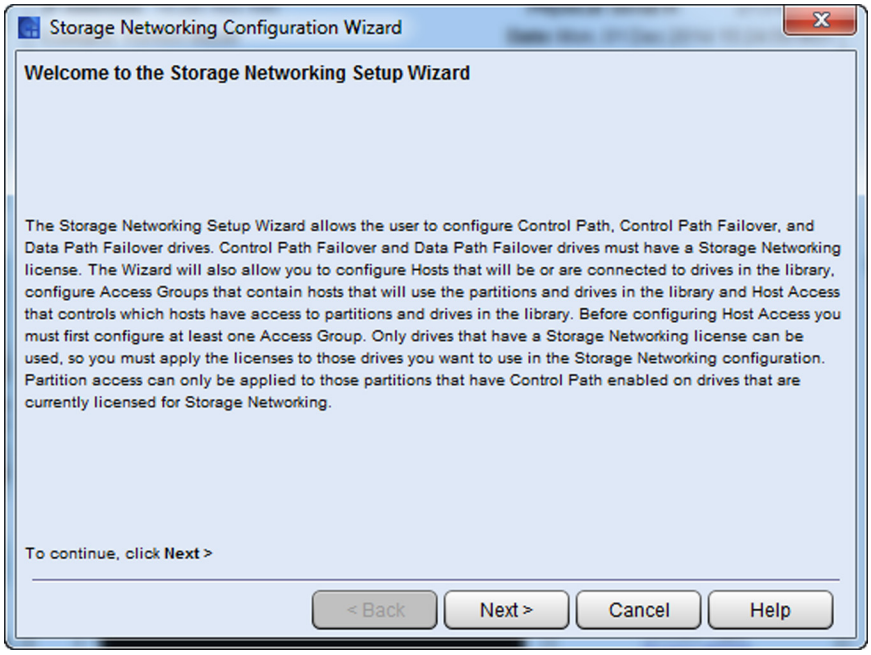
Note: If an SNW license is applied to a drive that has dual ports, both ports will be active. If there is no SNW license, only one of the ports will be active.

This chapter covers:

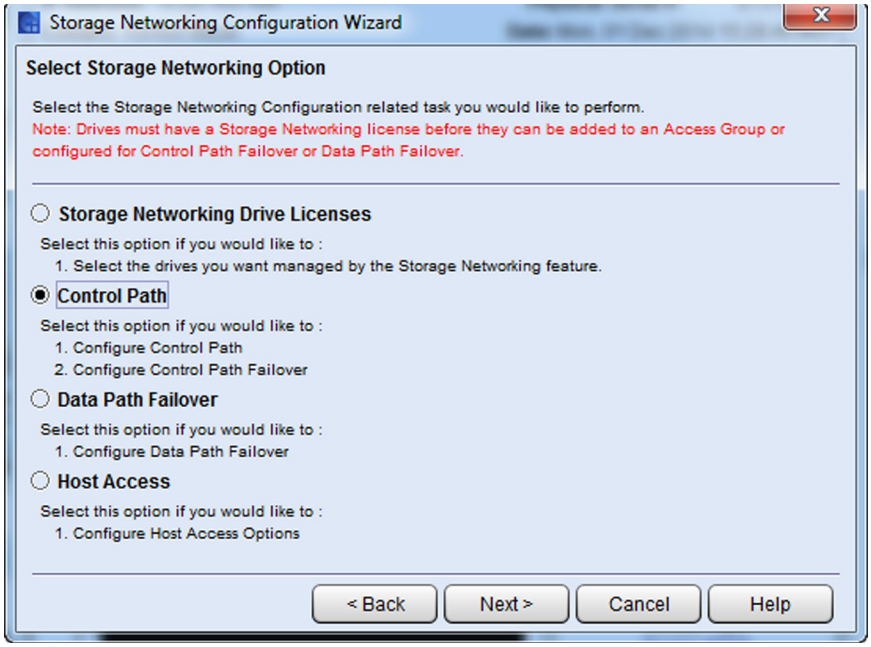
Use the Storage Networking Wizard

The SNW wizard groups all the path failover features together in a single place. To access the SNW wizard:

1 Select **Setup > SNW Wizard**. The **Storage Networking Configuration Wizard** welcome screen appears.



2 Click **Next**. The **Select Storage Networking Option** screen appears.



3 Select an option and click **Next**.

All of the options and their instructions are described in the sections below:

- License Drives for Path Failover on page 349
- Configure Control Path on page 351
- Configuring Data Path Failover on page 366
- Configuring Host Access to Storage Networking Drives and Partitions on page 373

License Drives for Path Failover

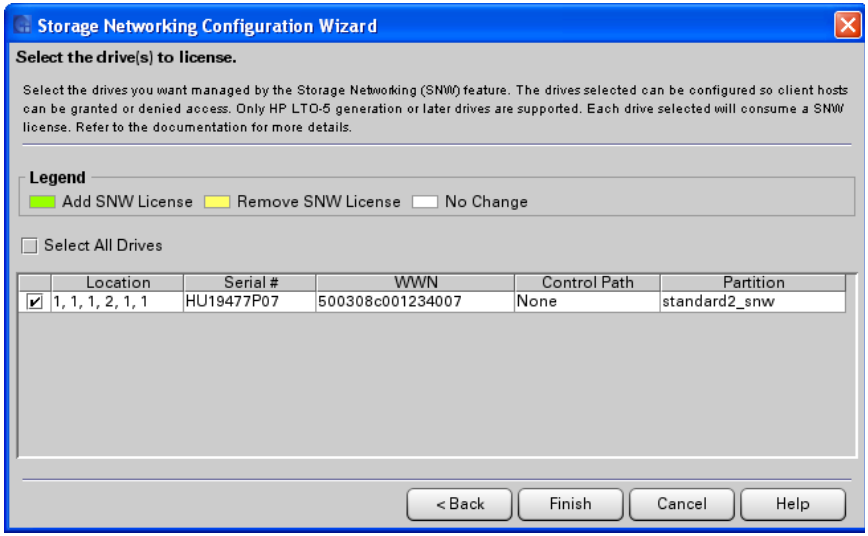
Before you can use a drive for any of the storage networking features, you must assign it to the SNW license. Your SNW license covers a specific number of drives. Any drive you use for an SNW feature consumes one license count. A drive consumes only one license count

even if you use it for multiple SNW features. The type of features available to be configured for SNW include:

- Host Access Control
- Data Path Failover (Basic and Advanced)
- Control Path Failover (Basic and Advanced)
- FIPS

To assign drives to a SNW license:

1. Access the SNW Wizard options screen (select **Setup > SNW Wizard** and click **Next**).
2. From the **Select Storage Networking Options** screen, select **Storage Networking Drive Licenses.**
3. Click **Next**. The **Select the drive(s) to license** screen appears. The screen contains a list of all eligible drives. Drives with their selection boxes checked are currently licensed as SNW drives.



4. Select the check boxes belonging to drives you want to license. Click the **Select All Drives** check box to select all check boxes.
5. Clear the check boxes of drives you no longer want to license. Any changes you make are indicated by colors filling the row.
   - **Green** — indicates you are adding the drive to the SNW count.

- **Yellow** — indicates you are removing the drive from the SNW count.
- **White** — indicates no change.

6 Click **Finish**. If you are adding drives, a dialog warns you that host connectivity may be affected.

7 Click **OK**. A **Success** dialog appears.

8 Click **OK**.

Configure Control Path

There are five types of control path configurations:

Control Path: This configuration options does not require an SNW license and can use any EEB attached IBM or HP LTO drive. For more information, see Configuring Control Paths on page 146.

Multi Control Path: This configuration option requires an SNW license and allows you to assign multiple IBM and/or HP LTO-5 or higher drives as possible control paths.

Basic Control Path Failover (BCPF): This configuration provides support for only HP LTO-5 and LTO-6 path failover licensed drives for basic control path failover. When BCPF is used, one drive is assigned as the primary control path and another drive as the control path failover (secondary) drive. The control path failover drive is used whenever the primary control path drive fails, becomes inoperable, or loses connectivity.

Functionality exists to manually “fail over” and “failback” among the configured control path drives to allow control path and drive diagnostics (see Manual Failover Between Drives on page 358).

Advanced Control Path Failover (ACPF): This configuration provides support for onlyHP LTO-6, path failover licensed drives for advanced control path failover. When ACPF is used, one drive is configured as the primary control path and one or more drives are selected as failover drives.

This configuration requires an Advanced Path Failover (APF) device driver installed on an attached host. This driver will determine and

handle all configured partition control paths, select the active control path and initiate a control path failover operation in the event the currently selected control path fails.

Note: The library issues a ticket when control path failover occurs. In addition, the library monitors the standby port and issues a ticket if the standby port does not report a good Fibre Channel link status.

Advanced Control Path: This configuration provides support for only IBM LTO-5 and LTO-6 drives and requires an SNW license. When Advanced Control Path is used, multiple IBM drives can be designated as control path drives with a device driver installed on an attached host. This driver will determine which drive is used as the primary control path and will choose a new control path drive in the event the primary control path fails.

Multi Control Path

Requirements

To configure drives for multi control path, you need the following:

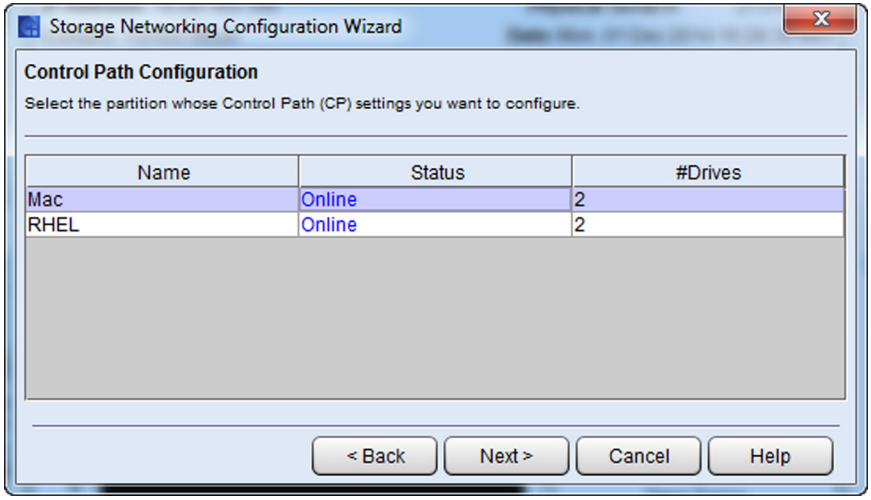
- A Storage Networking (SNW) License must be installed on the library (see Enabling Licenses on page 115).
- All drives must be licensed for SNW (see License Drives for Path Failover on page 349).
- The tape drives must be either IBM and/or HP LTO-5 or higher Fibre Channel drives.
- The tape drives must be connected to an Ethernet Expansion Blade.
- The tape drives must NOT be connected to an FC I/O blade.
- The tape drive topology must be set to Point-to-Point (see Configuring Fibre Channel Drive Speed, Topology, and Loop ID on page 192).

Multi Control Path Configuration

1 Access the appropriate screen in one of two ways:

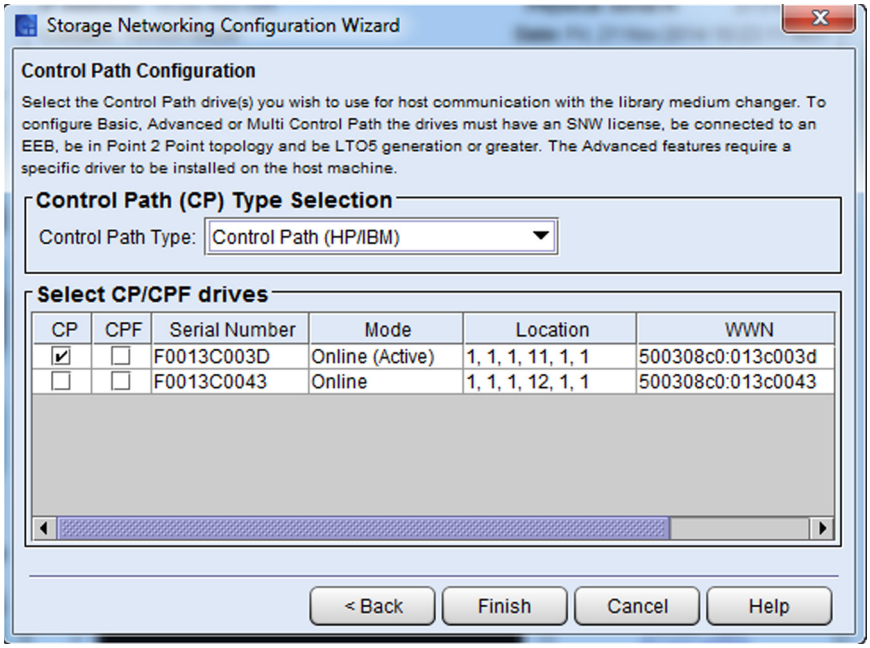
- From the SNW Wizard: Select **Setup > SNW Wizard**. Click **Next**. From the Select Storage Networking Option screen, select **Control Path** and click **Next**.
- Select **Setup > Partitions > Control Path** from the main console.

The **Storage Networking Partitions** dialog box appears, displaying all partitions that contain drives eligible to be a control path.



2 Select the partition whose control path settings you want to configure.

3 Click **Next**. The **Control Path Configuration** dialog box appears.



4 From the **Control Path (CP) Type** drop-down list, select **Multi Control Path (HP/IBM)**.

5 Select the drives you want to be control paths in the **CP** column. You can select all drives listed as long as they have an SNW license.

> **Note:** If you select the checkbox in the CPF column you will receive an error. Failover is not available for the Multi Control Path option.

6 Click **Finish**. An **Operation in Progress** dialog box appears.

Basic Control Path Failover

Requirements

To configure drives for basic control path failover, you need the following:

- A path failover license must be installed on the library (see Enabling Licenses on page 115).

- Both control path failover drives must be licensed for path failover (see License Drives for Path Failover on page 349).
- The tape drives must be HP LTO-5 or LTO-6 Fibre Channel drives.
- The tape drives must be connected to an Ethernet Expansion Blade.
- The tape drives must be connected to the same Fibre Channel switch that supports N-port ID Virtualization (NPIV).
- The tape drives must NOT be connected to an FC I/O blade.
- The tape drive topology must be set to Point-to-Point (see Configuring Fibre Channel Drive Speed, Topology, and Loop ID on page 192).
- Two (2) or more HP LTO-5 or LTO-6 drives must be in the same partition.

Configuration Guidelines

When a logical library partition's media changer control path is configured via a control path drive, the library control path is hosted by the drive's physical FC port and uses the same World Wide Port Name (WWPN) associated with the selected tape drive. While the tape drive (SSC device) responds as LUN 0 at the WWPN, the partition media changer (SMC device) responds as LUN 1 at the WWPN.

For example, consider such a drive configured to host the library control path. A switch could detect the tape drive as LUN 0 with WWPN 500308c0:9e2c3001 and detect the media changer as LUN 1 with WWPN 500308c0:9e2c3001 also via switch port 1:

```
[11:0:0:0]   tape           fc:0x500308c09e2c3001,
0x010100          /dev/st0  /dev/sg2

[11:0:1:1]   mediumx    fc:0x500308c09e2c3001,
0x010101          /dev/sg3
```

If the logical library partition configures two drives for basic library control path failover functionality, then the library control path will be able to fail over to the configured redundant failover drive. In this type of configuration, the library control path is not hosted by a drive's physical FC port, but via a virtual port with a unique WWPN, reporting the SMC device also as LUN 0, not LUN 1.

Virtual port WWPNs are based on the library's WWNN and are identified by the WWPN's last 12 bits. A partition's control path configured via a

virtual port would end in 0x7FF for the first partition, 0x7FE for the second partition, 0x7FD for the third partition and so on. The partition's virtual port is presented by only one of the configured failover drives. If the active path to the media changer fails due to a FC cable issue, a drive failure or even a drive removal, the library control path will switch to the secondary drive and appear to the SAN via the same WWPN.

For example, consider two drives configured for control path failover configured within the first partition. A switch could detect the two tape drives as LUN 0 with WWPNs 500308c0:9e2c3001 and 500308c0:9e2c3005 at switch ports 1 and 2, and detect the media changer also as LUN 0 with WWPN 500308c0:9e2c37ff via switch port 1:

```
[11:0:0:0]   tape           fc:0x500308c09e2c3001,
0x010100          /dev/st0  /dev/sg2

[11:0:1:0]   mediumx    fc:0x500308c09e2c37ff,
0x010101          /dev/sg3

[11:0:2:0]   tape           fc:0x500308c09e2c3004,
0x010200          /dev/st1  /dev/sg4
```

If the drive hosting the library control path fails, or the link from switch port 1 to the hosting drive fails, the control path failover drive would take over and the switch would detect the media changer device no longer on port 1, but port 2:

```
[11:0:1:0]   mediumx    fc:0x500308c09e2c37ff,
0x010201          /dev/sg3

[11:0:2:0]   tape           fc:0x500308c09e2c3004,
0x010200          /dev/st1  /dev/sg
```

Note: When switching a standard control path drive to BCPF functionality, the host needs to be reconfigured to support the new partition WWNN (world wide node name) as well as the WWPN (world wide port name) and LUN mappings.

BCPF Configuration

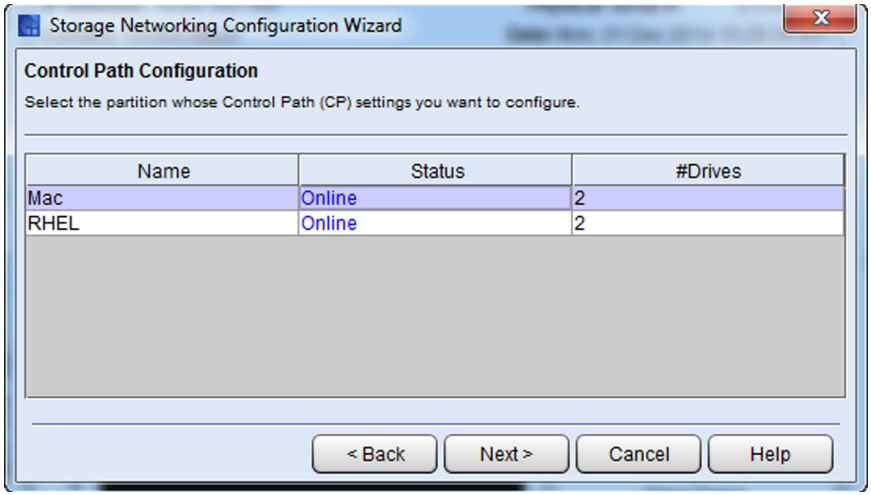
1 Access the appropriate screen in one of two ways:

- From the SNW Wizard: Select **Setup > SNW Wizard**. Click **Next**. From the Select Storage Networking Option screen, select **Control Path** and click **Next**. See Use the Storage Networking

Wizard on page 348.

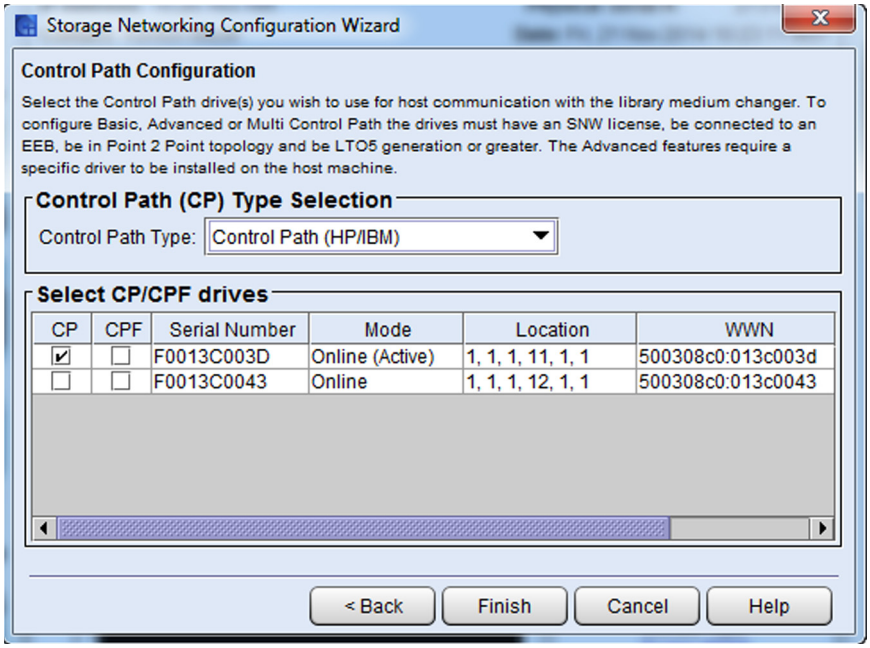
- Select **Setup > Partitions > Control Path** from the main console.

The **Control Path Configuration** dialog box appears, displaying all partitions that contain drives eligible to be a control path.



2 Select the partition whose control path settings you want to configure.

3 Click **OK**. The **Control Path Configuration** dialog box appears.



4 From the **Control Path (CP) Type** drop-down list, select **Basic Control Path Failover (HP)**.

5 Select the primary control path drive from the **CP** column.

6 Select another drive from the **CPF** column. This drive will be the failover drive.

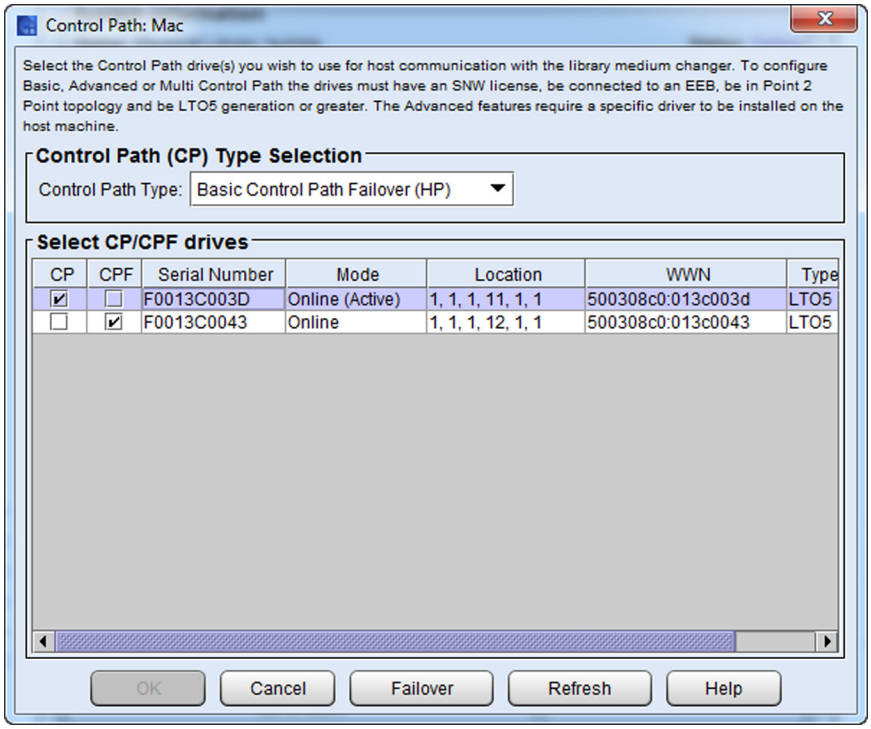
7 Click **Finish**. An **Operation in Progress** dialog box appears.

8 The control path and control path failover drives are configured.

Manual Failover Between Drives

If maintenance needs to be carried out on the currently active control path drive, you can force that drive to fail over to the non-active control path drive.

1 Access the appropriate screen as described above in Step 1 through Step 3 above. The **Control Path** dialog box appears, with the control path drive highlighted, and the control path failover drive checked.



2 Click the **Failover** button.

3 A warning message appears informing that switching the active control path drive could cause temporary loss of communication to the host application.

4 If you still want to perform this operation, click **Yes** to continue. The new active control path drive is configured.

5 Click **OK**.

Advanced Control Path Failover

Requirements

To configure drives for advanced control path failover, you need the following:

- A Storage Networking (SNW) License must be installed on the library (see Enabling Licenses on page 115).

- All control path failover drives must be licensed for SNW (see License Drives for Path Failover on page 349).
- The tape drives must be HP LTO-6 Fibre Channel drives.
- The tape drives must be connected to an Ethernet Expansion blade.
- The tape drives can be connected to the same or different Fibre Channel switch.
- The tape drives must NOT be connected to an FC I/O blade.
- The tape drive topology must be set to Point-to-Point (see Configuring Fibre Channel Drive Speed, Topology, and Loop ID on page 192).
- The APFO driver must be installed on the host(s).

Configuration Guidelines

When a logical library partition's media changer control path is configured via a control path drive, the library control path is hosted by the drive's physical FC port and uses the same World Wide Port Name (WWPN) associated with the selected tape drive. While the tape drive (SSC device) responds as LUN 0 at the WWPN, the partition media changer (SMC device) responds as LUN 1 at the WWPN.

For example, consider such a drive configured to host the library control path. A switch could detect the tape drive as LUN 0 with WWPN 500308c0:9e2c3001 and detect the media changer as LUN 1 with WWPN 500308c0:9e2c3001 also via switch port 1:

```
[11:0:0:0]   tape            fc:0x500308c09e2c3001,
0x010100           /dev/st0  /dev/sg2

[11:0:1:1]   mediumx     fc:0x500308c09e2c3001,
0x010101           /dev/sg3
```

If the logical library partition is configured for advanced control path failover functionality, the managing APF device driver will select a redundant path and request that the library enable the redundant path as the active control path. In this case, the current path is disabled and the new path is enabled, resulting in the existing LUN 1 for the current active path to disappear and a LUN 1 activating the selected redundant device.

Table 32 Example Path List

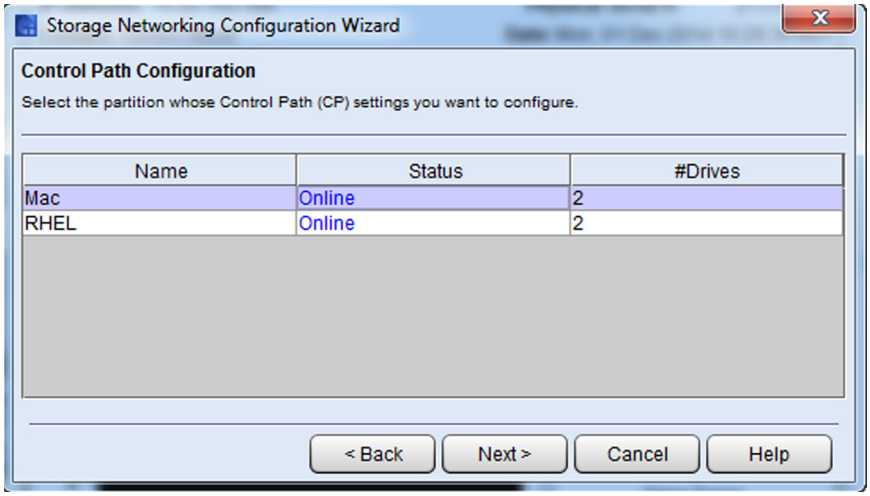
SAN	Addressed Logical Unit	Port	Example SCSI Address	Example Logical Unit Worldwide Identifiers
1	Tape drive 1	A	ID 1 LUN 0	50:01:10:a0:00:00:00:01
1	Library Controller	A	ID 1 LUN 1	50:01:10:a0:00:00:00:02
2	Tape drive 1	B	ID 2 LUN 0	50:01:10:a0:00:00:00:01
2	Library Controller	B	ID 2 LUN 1	50:01:10:a0:00:00:00:02
1	Tape drive 2	A	ID 3 LUN 0	50:01:10:a0:00:00:00:03
1	Library Controller	A	ID 3 LUN 1	50:01:10:a0:00:00:00:02
2	Tape drive 2	B	ID 4 LUN 0	50:01:10:a0:00:00:00:03
2	Library Controller	B	ID 4 LUN 1	50:01:10:a0:00:00:00:02

ACPF Configuration

1 Access the appropriate screen in one of two ways:

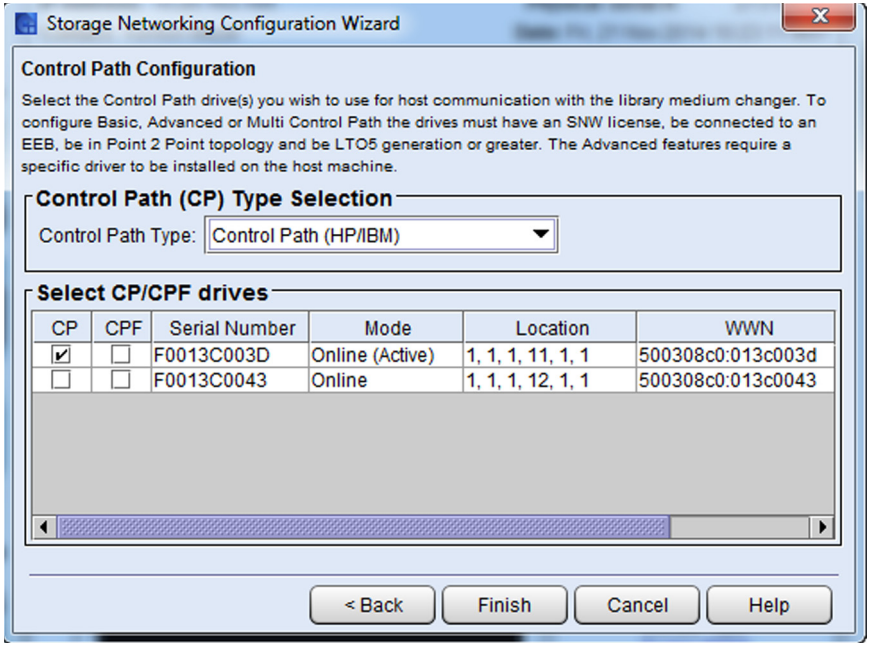
- From the SNW Wizard: Select **Setup > SNW Wizard**. Click **Next**. From the Select Storage Networking Option screen, select **Control Path** and click **Next**. See Use the Storage Networking Wizard on page 348.
- Select **Setup > Partitions > Control Path** from the main console.

The **Control Path Configuration** dialog box appears, displaying all partitions that contain drives eligible to be a control path.



2 Select the partition whose control path settings you want to configure.

3 Click **OK**. The **Control Path** dialog box appears.



4 From the **Control Path (CP) Type** drop-down list, select **Advanced Control Path Failover (HP)**.

5 Select the primary control path drive from the **CP** column.

6 Select one or more drives from the **CPF** column. These drives will be the failover drives.

7 Click **Finish**. An **Operation in Progress** dialog box appears.

8 The control path and control path failover drives are configured.

Advanced Control Path

Requirements

To configure drives for advanced control path, you need the following:

- A Storage Networking (SNW) License must be installed on the library (see Enabling Licenses on page 115).
- All drives must be licensed for SNW (see License Drives for Path Failover on page 349).
- The drives must be IBM LTO-5 or LTO-6 Fibre Channel drives.
- The tape drives must be connected to an Ethernet Expansion Blade.
- The tape drives must NOT be connected to an FC I/O blade.
- The tape drive topology must be set to Point-to-Point (see Configuring Fibre Channel Drive Speed, Topology, and Loop ID on page 192).
- The driver supplied by IBM must be installed on the host(s).

Configuration Guidelines

When a logical library partition's media changer control path is configured via a control path drive, the library control path is hosted by the drive's physical FC port and uses the same World Wide Port Name (WWPN) associated with the selected tape drive. While the tape drive (SSC device) responds as LUN 0 at the WWPN, the partition media changer (SMC device) responds as LUN 1 at the WWPN.

For example, consider such a drive configured to host the library control path. A switch could detect the tape drive as LUN 0 with WWPN 500308c0:9e2c3001 and detect the media changer as LUN 1 with WWPN 500308c0:9e2c3001 also via switch port 1:

```
[11:0:0:0]   tape           fc:0x500308c09e2c3001,
0x010100          /dev/st0  /dev/sg2

[11:0:1:1]   mediumx    fc:0x500308c09e2c3001,
0x010101          /dev/sg3
```

If the logical library partition is configured for advanced control path failover functionality, the managing APF device driver will select a redundant path and request that the library enable the redundant path as the active control path. In this case, the current path is disabled and the new path is enabled, resulting in the existing LUN 1 for the current active path to disappear and a LUN 1 activating the selected redundant device.

Table 33 Example Path List

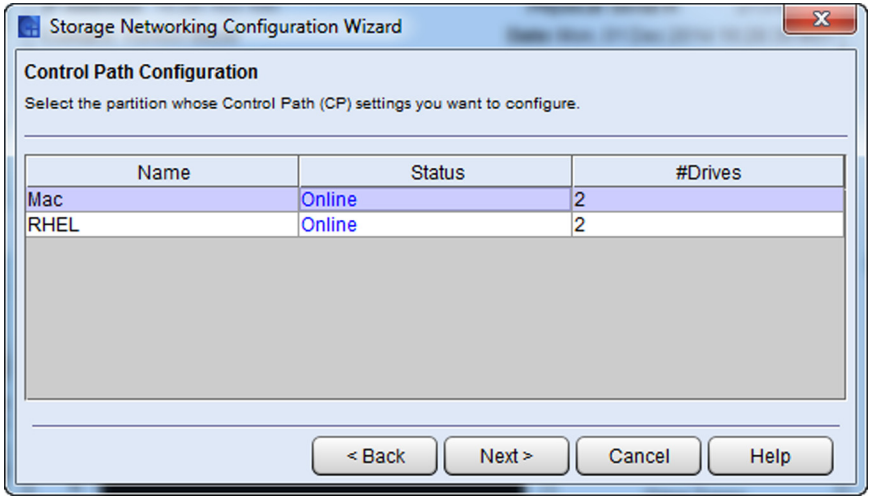
SAN	Addressed Logical Unit	Port	Example SCSI Address	Example Logical Unit Worldwide Identifiers
1	Tape drive 1	A	ID 1 LUN 0	50:01:10:a0:00:00:00:01
1	Library Controller	A	ID 1 LUN 1	50:01:10:a0:00:00:00:02
2	Tape drive 1	B	ID 2 LUN 0	50:01:10:a0:00:00:00:01
2	Library Controller	B	ID 2 LUN 1	50:01:10:a0:00:00:00:02
1	Tape drive 2	A	ID 3 LUN 0	50:01:10:a0:00:00:00:03
1	Library Controller	A	ID 3 LUN 1	50:01:10:a0:00:00:00:02
2	Tape drive 2	B	ID 4 LUN 0	50:01:10:a0:00:00:00:03
2	Library Controller	B	ID 4 LUN 1	50:01:10:a0:00:00:00:02

Advanced Control Path Configuration

1 Access the appropriate screen in one of two ways:

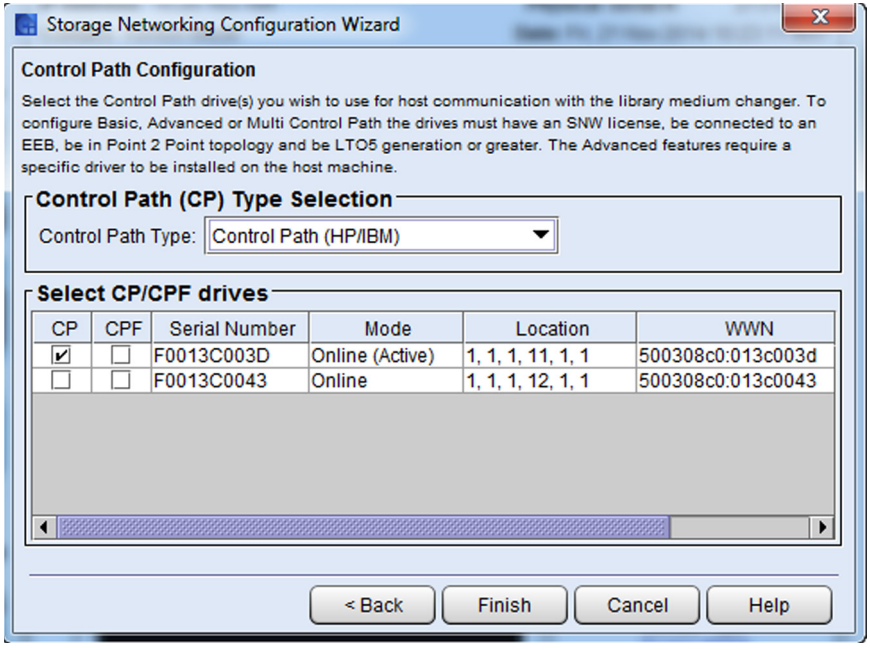
- From the SNW Wizard: Select **Setup > SNW Wizard**. Click **Next**. From the **Select Storage Networking Option** screen, select **Control Path** and click **Next**.
- Select **Setup > Partitions > Control Path** from the main console.

The **Storage Networking Partitions** dialog box appears, displaying all partitions that contain drives eligible to be a control path.



2 Select the partition whose control path settings you want to configure.

3 Click **Next**. The **Control Path Configuration** dialog box appears.



4 From the **Control Path (CP) Type** drop-down list, select **Advanced Control Path (IBM)**.

5 Select the drives you want to be control paths in the **CP** column. You can select all drives listed as long as they have an SNW license.

> **Note:** If you select the checkbox in the CPF column you will receive an error. Failover is not available for the Advanced Control Path option.

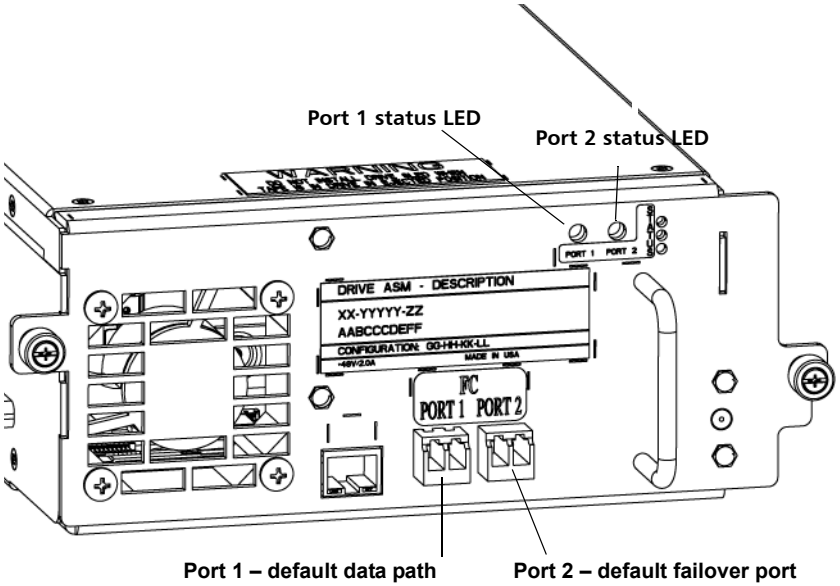
6 Click **Finish**. An **Operation in Progress** dialog box appears.

Configuring Data Path Failover

There are two types of data path failover: basic and advanced.

Basic Data Path Failover (BDPF): Basic Data Path Failover is a feature provided as part of the Storage Networking license and applies to HP LTO-5 and LTO-6 Fibre Channel tape drives only. It provides an alternate data path when a preferred data path fails. If you previously installed a Storage Networking license, you can use this feature once you upgrade library firmware to the appropriate version. Verify firmware version requirements in the *Scalar i6000 Release Notes*.

The HP LTO-5 and higher Fibre Channel tape drives have two Fibre Channel ports. If you enable Data Path Failover on the tape drive, one port is used as the "active port" for data transmission, and the other port stands by for use if the active port fails. If the tape drive loses its Fibre Channel link with the active port, it will automatically "fail over" and use the standby port to continue drive operations.



Note: The library issues a RAS ticket when automatic data path failover occurs. In addition, the library monitors the standby port and issues a RAS ticket if the standby port does not report a good Fibre Channel link status.

The library uses Port 1 for data path transmission unless a failover occurs. Once failover occurs, the library uses Port 2 until failover occurs again or the library is rebooted. Similarly, if a tape drive configured for data path failover is the control path for a partition, the host uses Port 1 for media changer commands unless a failover occurs. Once failover occurs, the host uses Port 2 until failover occurs again or the library is rebooted.

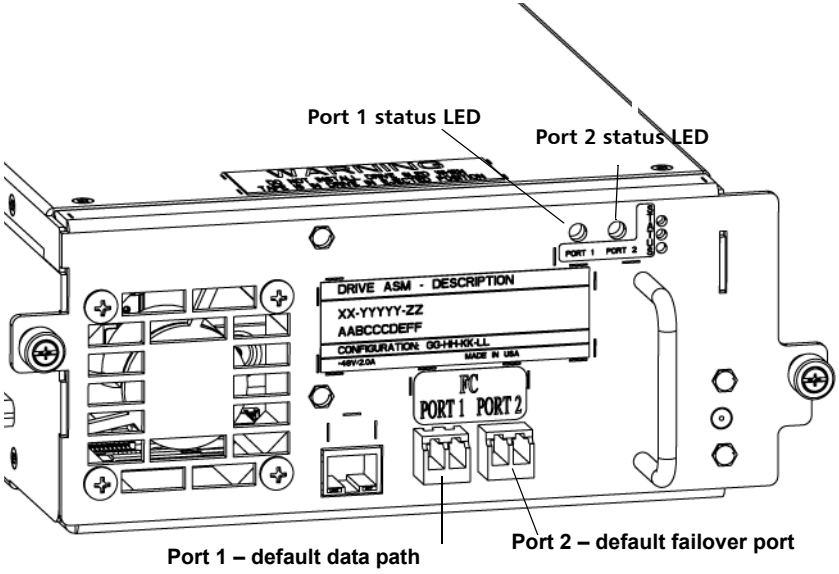
Note: Performing a drive reset operation is another way to make Port 1 the active port again.

A tape drive can be configured for both data path failover and control path failover. If both are configured, the control path will not fail over to another tape drive unless both ports on the control path tape drive fail.

Advanced Data Path Failover (ADPF): Advanced Data Path Failover is a feature provided as part of the Storage Networking license and applies only to HP LTO-6 Fibre Channel tape drives. It provides an alternate data

path when a preferred data path fails. If you previously installed a Storage Networking license, you can use this feature once you upgrade library firmware to the appropriate version. Verify firmware version requirements in the *Scalar i6000 Release Notes*.

The HP LTO-6 Fibre Channel tape drives have two Fibre Channel ports. If you enable Advanced Data Path Failover on the tape drive, both ports are available but the driver chooses one port to be "active" and used for data transmission, while the other port stands by for use if the "active" port fails. If the tape drive loses its Fibre Channel link with the "active" port, it will fail over and use the standby port to continue drive operations.



Note: The library issues a RAS ticket when a data path failover occurs. In addition, the library monitors the standby port and issues a RAS ticket if the standby port does not report a good Fibre Channel link status.

The library utilizes a driver installed on the host to manage path failover. It uses Port 1 for data path transmission unless a failover occurs. Once failover occurs, the driver uses Port 2 until failover occurs again or the library is rebooted. Similarly, if a tape drive configured for advanced data path failover is the control path for a partition, the host uses Port 1

for media changer commands unless a failover occurs. Once failover occurs, the host uses Port 2 until failover occurs again or the library is rebooted.

A tape drive can be configured for both advanced data path failover and advanced control path failover. If both are configured, the control path will not fail over to another tape drive unless both ports on the control path tape drive fail.

Basic Data Path Failover

Requirements

To configure a tape drive for basic data path failover, you need the following:

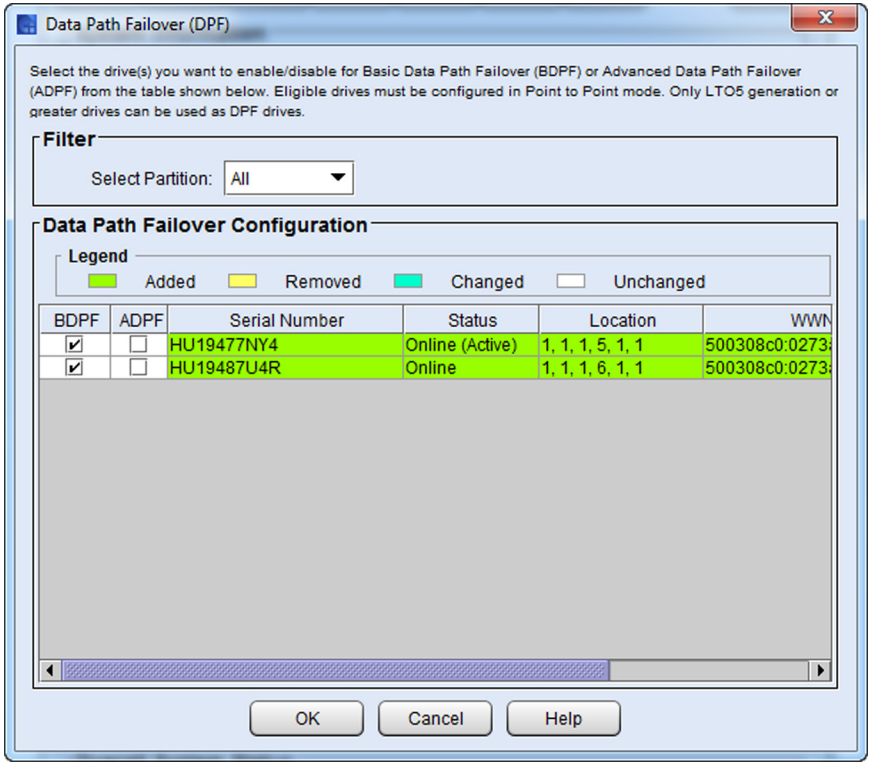
- The library must have a Storage Networking license installed.
- The tape drive to be configured for data path failover must be licensed for storage networking (see License Drives for Path Failover on page 349.
- The tape drive must be an LTO-5 or higher Fibre Channel tape drive.
- The tape drive must be connected to an Ethernet Expansion Blade (EEB) via an Ethernet cable.
- Both tape drive fibre ports MUST be connected to the same FC switch.
- Neither FC port on the drive may be connected to a FC I/O blade.
- The tape drive topology settings must be set to Point to Point (see Configuring Fibre Channel Drive Speed, Topology, and Loop ID on page 192).

Enabling/Disabling BDPF

To enable or disable data path failover functionality:

1. From the main console, select **Setup > Drives > Access > Data Path Failover**. Or, via the SNW Wizard: Select **Setup > SNW Wizard**. Click **Next**. From the options screen, select **Data Path Failover** and click **Next**.

   The **Data Path Failover (DPF)** dialog box appears. Drives with BDPF configured have check marks in the **BDPF** column.



2 In the **BDPF** column, select the drive(s) you want to enable or disable Basic Data Path Failover.

   Your choices are indicated by the following colors:

   - **Green** - Added
   - **Yellow** - Removed
   - **Teal** - Changed
   - **White** - Unchanged

3 Click **OK**. An **Operation in Progress** dialog box appears.

4 When Basic Data Path Failover configuration is complete, click **OK**.

Advanced Data Path Failover (ADPF)

Requirements

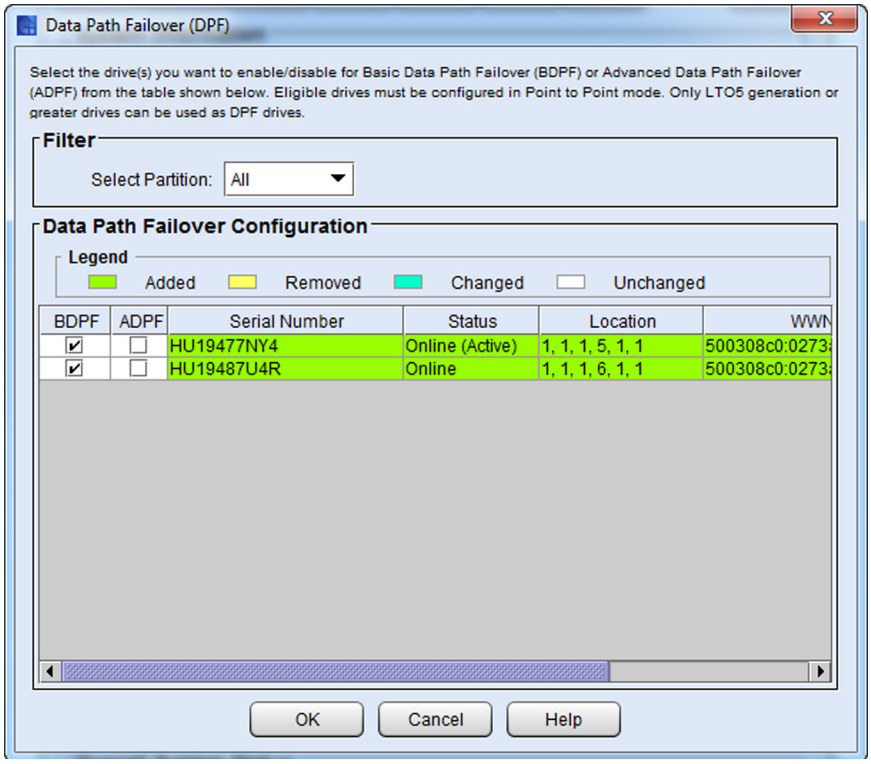
To configure a tape drive for advanced data path failover, you need the following:

- The library must have a Storage Networking license installed.
- The tape drive to be configured for data path failover must be licensed for storage networking (see License Drives for Path Failover on page 349.
- The tape drive must be an LTO-6 Fibre Channel tape drive.
- The tape drive must be connected to an Ethernet Expansion Blade (EEB) via an Ethernet cable.
- Both tape drive fibre ports MUST be connected to the same FC switch.
- Neither FC port on the drive may be connected to a FC I/O blade.
- The tape drive topology settings must be set to Point to Point (see Configuring Fibre Channel Drive Speed, Topology, and Loop ID on page 192).
- APFO driver must be installed on the host(s).

Enabling/Disabling ADPF

To enable or disable advanced data path failover functionality:

1. From the main console, select **Setup > Drives > Access > Data Path Failover**. Or, via the SNW Wizard: Select **Setup > SNW Wizard**.
2. Click **Next**.
3. From the options screen, select **Data Path Failover** and click **Next**. The **Data Path Failover (DPF)** dialog box appears. Drives with ADPF configured have check marks in the **ADPF** column.



4 In the **ADPF** column, click the check box of the drive(s) on which you want to enable or disable Advanced Data Path Failover.

   Your choices are indicated by the following colors:

   - **Green** - Added
   - **Yellow** - Removed
   - **Teal** - Changed
   - **White** - Unchanged

5 Click **OK**. An **Operation in Progress** dialog box appears.

6 When Advanced Data Path Failover configuration is complete, click **OK**.

Note: Unless a drive is configured for control path failover, drives can enable either BDPF or ADPF within the same partition.

Configuring Host Access to Storage Networking Drives and Partitions

The SNW Host Access feature provides a way to limit host access to specific SNW tape drives and partitions via the library interface.

Note: This section describes host access for storage networking drives and partitions only. For information about FC I/O blade LUN mapping, see FC Host on page 194.

This section covers:

Without host access restrictions, all hosts can view all drives connected to the SAN and all partitions to which there is a library control path. Host access gives you the ability to deny/restrict access to specific hosts.

Details about host access include:

- If a control path drive has an SNW license applied to it, it will not be seen by external applications until you create an access group and add the host and partition to the access group.
- Access is granted using “access groups.” An access group is made up of partitions, drives, and hosts. Drives and partitions can be in multiple access groups, but each host can only be in one access group.
- A partition can be assigned to a host access group if its control path is through an SNW-licensed tape drive.
- Drives must be licensed for SNW before they can be added to access groups. Once a drive has been licensed for SNW, it is inaccessible to hosts until they are granted access via the host access feature. See License Drives for Path Failover on page 349.

- Tape drives that are licensed for SNW can only be accessed by hosts that are in the same host access group as the drives.
- Tape drives that are not licensed for SNW can be accessed by any hosts that are zoned to the drives WWPN.
- If the control path and any control path failover tape drives for a partition are licensed for SNW, then only the hosts in the same access group as that partition will be able to send medium changer commands to that partition. Hosts not in the same access group as a partition will not be able to send medium changer commands to that partition. However, hosts that are not in the same access group as a partition do still have access and can send commands to any non-SNW-enabled tape drives in that partition.
- Host access to a partition means the host can issue media changer commands to the partition.
- Host access to a drive means the host can issue SCSI commands to the drive.

Requirements for Host Access

To use host access, you need the following:

- A Storage Networking license on the library (see Enabling Licenses on page 115)
- Drives licensed for Storage Networking (see License Drives for Path Failover on page 349).
- To add a partition to a host access group, the partition must have its control path via a SNW drive (see Configuring an IBM or HP LTO-5 or LTO-6 Drive as the Control Path on page 149).
- Hosts configured (see Configuring Hosts on page 374).
- Host access groups configured (see Viewing All Access Groups on page 407).

Configuring Hosts

All hosts that are zoned or directly connected to the drives are available to be assigned to host access groups. You may wish to modify existing hosts to make their names more “user friendly” for when you add them to access groups. You may wish to delete hosts that are not connected to the SAN. Using the host configuration option, you can do the following:

- Create Host — You can add hosts that are not currently connected to the SAN (i.e., “prep” your library for a future host). These are hosts that you plan to add to the SAN later, but want to pre-configure in host access groups now. If you don’t eventually add the hosts to the SAN, they will not be able to access the drives/partitions you choose. In most cases, you will not need to create hosts in this way.
- Modify Host — You can modify the name, type, port, or WWPN of a visible host. Unmodified hosts that are connected to the drive(s) have no predefined name and are named “Unknown” by default. You may wish to change the name to a more “user friendly” name to distinguish one host from another.
- Delete Host — You can delete hosts that are no longer connected to the SAN. You can only delete hosts whose state is offline (i.e., not connected to the SAN). Any time you delete a host you remove all host mappings configured for that host.

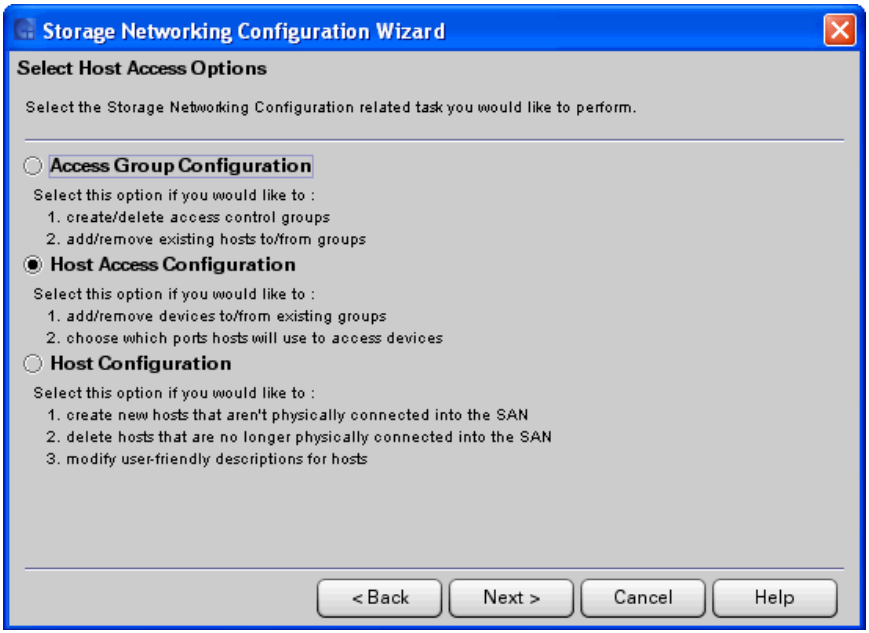
Create Host

To create a host:

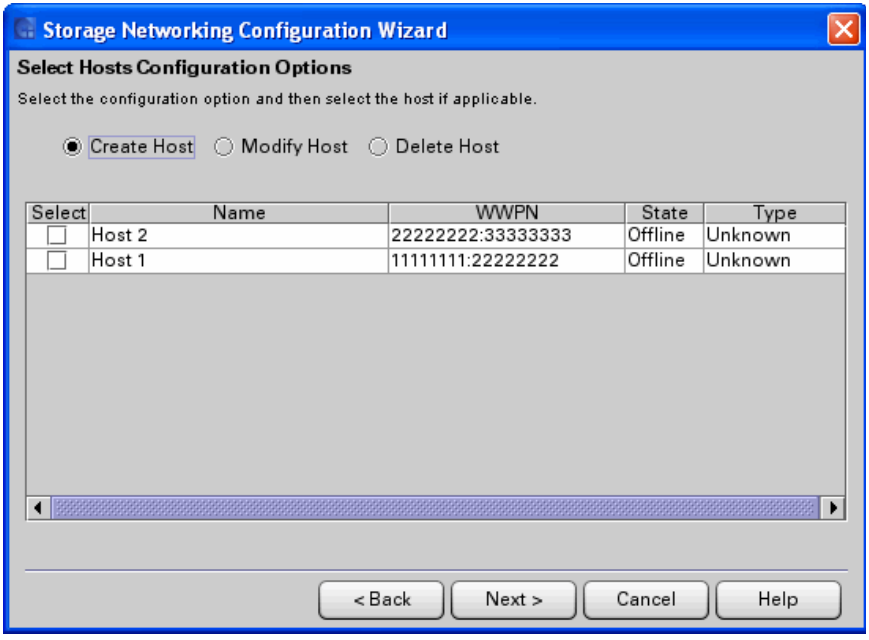
1. Select **Setup > SNW Wizard** to display the SNW Wizard.
2. Click **Next** to display the **Select Storage Networking Option** screen.


Storage Networking Configuration Wizard
Select Storage Networking Option
Select the Storage Networking Configuration related task you would like to perform.
Note: Drives must have a Storage Networking license before they can be added to an Access Group or configured for Control Path Failover or Data Path Failover.
Storage Networking Drive Licenses
Select this option if you would like to :
1. Select the drives you want managed by the Storage Networking feature.
Control Path
Select this option if you would like to :
1. Configure Control Path
2. Configure Control Path Failover
Data Path Failover
Select this option if you would like to :
1. Configure Data Path Failover
Host Access
Select this option if you would like to :
1. Configure Host Access Options
< Back
Next >
Cancel
Help

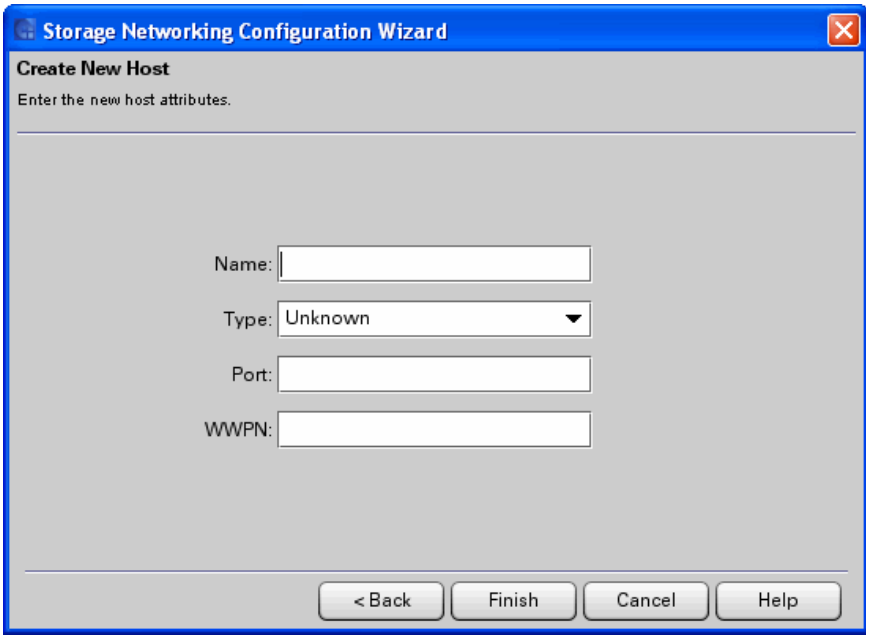
3 Select **Host Access** and click **Next** to display the **Select Host Access Options** screen.



4 Select **Host Configuration** and click **Next** to display the Select Hosts Configuration Options screen.



5 Select **Create Host** and click **Next** to display the **Create New Host** dialog box.



6 Type an appropriate value into the **Name** field.

7 Select the operating system of the host from the **Type** field pull-down menu.

8 Type the port number into the **Port** field.

9 Type the world wide port name into the **WWPN** field.

The string must be 8 hexadecimal numbers, a colon (:), and 8 hexadecimal numbers (########:########).

10 Click **Finish** to create the host.

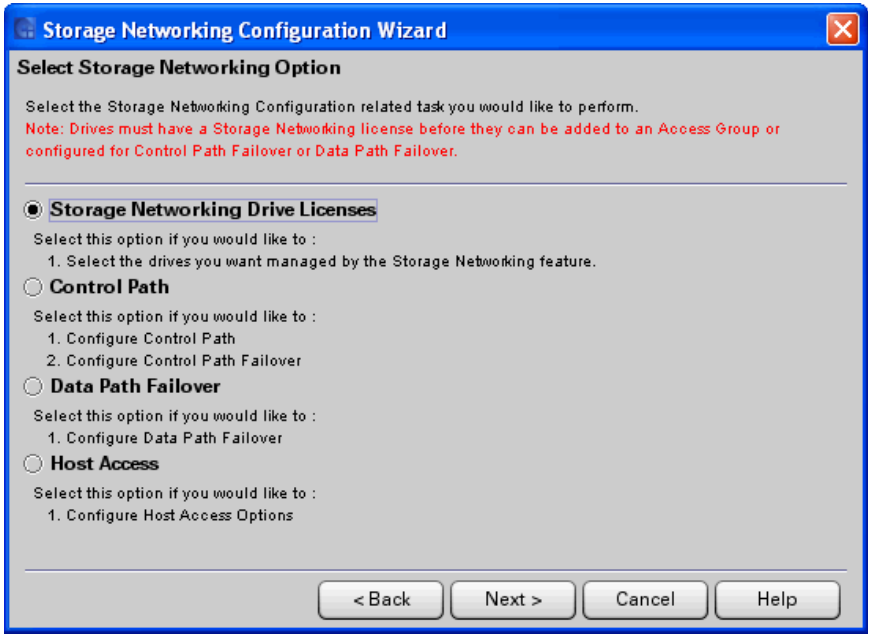
11 Click **OK** in the **The Host was created successfully** dialog box.

Modify Host

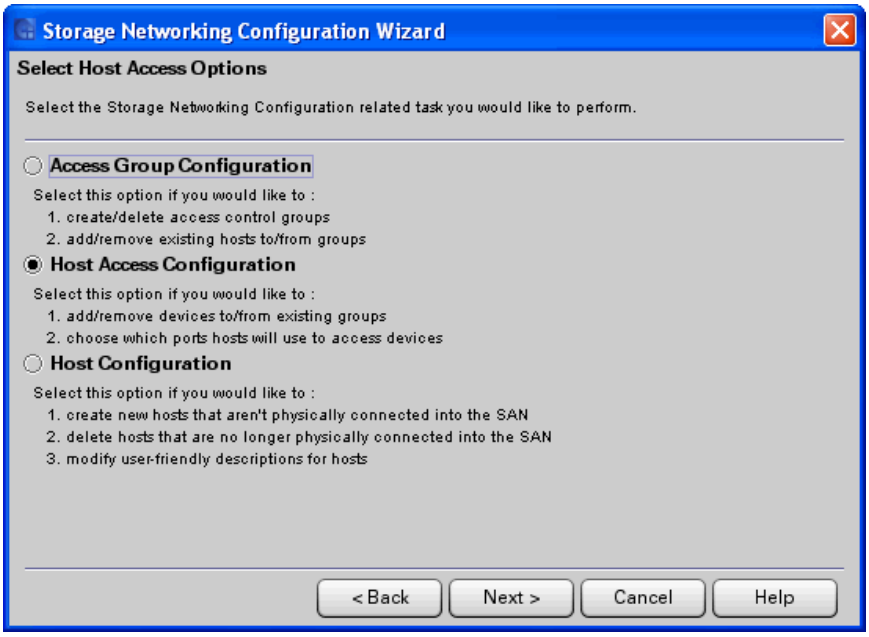
To modify an existing host:

1 Select **Setup > SNW Wizard** to display the **SNW Wizard**.

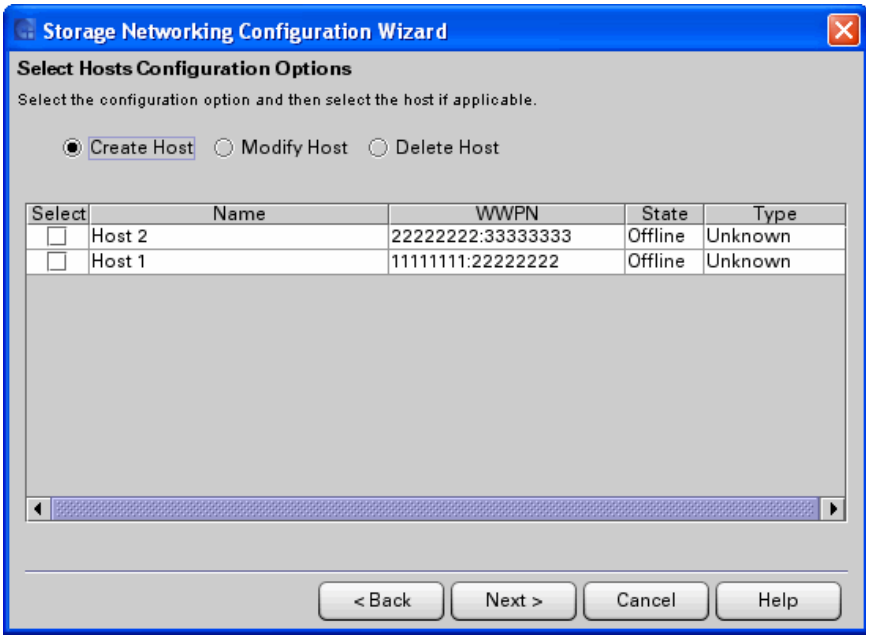
2 Click **Next** to display the **Select Storage Networking Option** screen.



3 Select **Host Access** and click **Next** to display the **Select Host Access Options** screen.



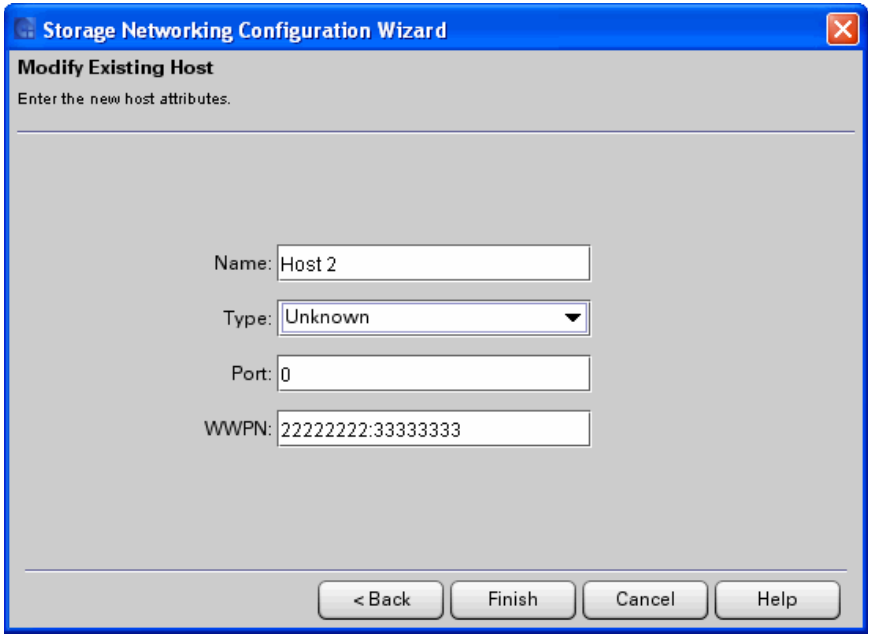
4 Select **Host Configuration** and click **Next** to display the **Select Hosts Configuration Options** screen.



5 Select **Modify Host**.

6 Click the appropriate box in the **Select** column to select the host to modify.

7 Click **Next** to access the **Modify Existing Host** dialog box, which displays current information for the host.



8 Correct the information in the **Name**, **Type**, **Port**, and **WWPN** fields.

9 Click **Finish** to save the modifications.

10 Click **OK** in the The Host was modified successfully dialog box.

Delete Host

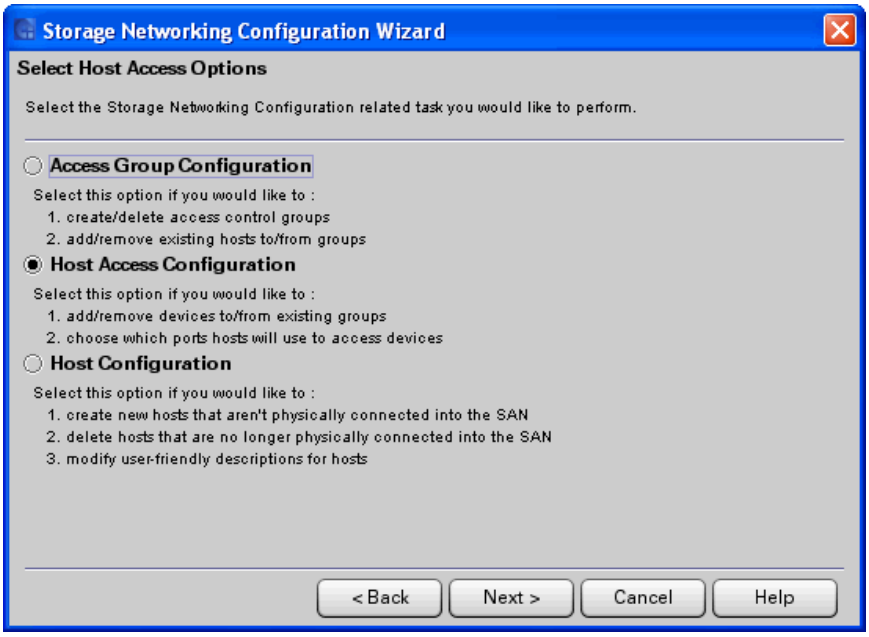
To delete an existing host:

1 Select **Setup > SNW Wizard** to display the SNW Wizard.

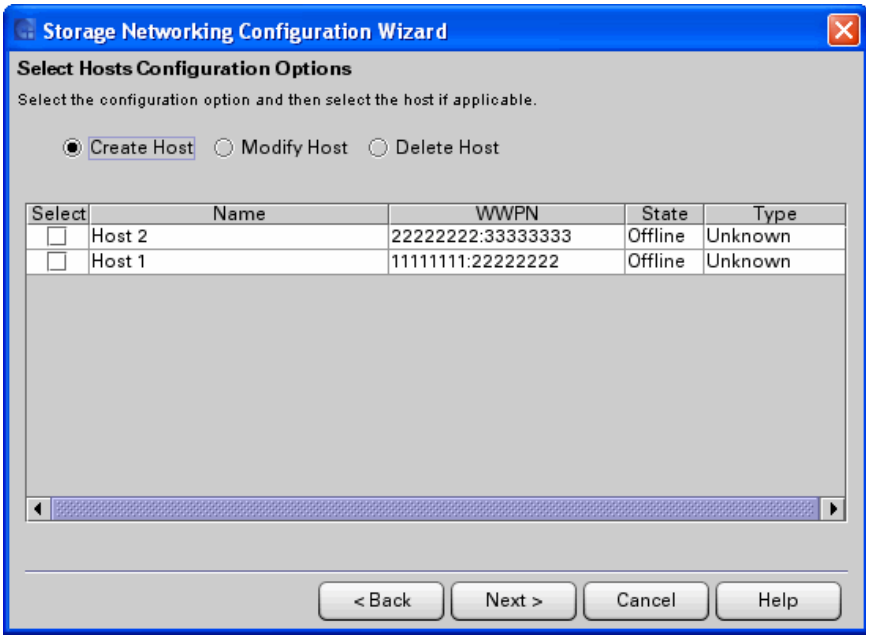
2 Click **Next** to display the **Select Storage Networking Option** screen.


Storage Networking Configuration Wizard
Select Storage Networking Option
Select the Storage Networking Configuration related task you would like to perform.
Note: Drives must have a Storage Networking license before they can be added to an Access Group or configured for Control Path Failover or Data Path Failover.
Storage Networking Drive Licenses
Select this option if you would like to :
1. Select the drives you want managed by the Storage Networking feature.
Control Path
Select this option if you would like to :
1. Configure Control Path
2. Configure Control Path Failover
Data Path Failover
Select this option if you would like to :
1. Configure Data Path Failover
Host Access
Select this option if you would like to :
1. Configure Host Access Options
< Back
Next >
Cancel
Help

3 Select **Host Access** and click **Next** to display the **Select Host Access Options** screen.



4 Select **Host Configuration** and click **Next** to display the **Select Hosts Configuration Options** screen.



5 Select **Delete Host**.

6 Click the appropriate box in the **Select** column to select the host to delete.

7 Click **Finish** to delete the host. A warning message appears letting you know that deleting the host will remove all host mappings configured for the host.

8 Click **Yes** to continue.

9 Click **OK** in the The Host was deleted successfully dialog box.

10 If necessary, click **Cancel** then **Yes** to exit the dialog box.

Creating, Modifying, and Deleting Host Access Groups

If necessary, you can make the following modifications to host access groups:

- Creating Host Access Groups on page 387
- Changing an Access Group Name on page 393

- Deleting a Host Access Group on page 395
- Adding a Host to an Access Group on page 396
- Removing a Host from an Access Group on page 398
- Host Access Configuration – Modifying Drives/Partitions and Viewing Host Access Groups on page 401

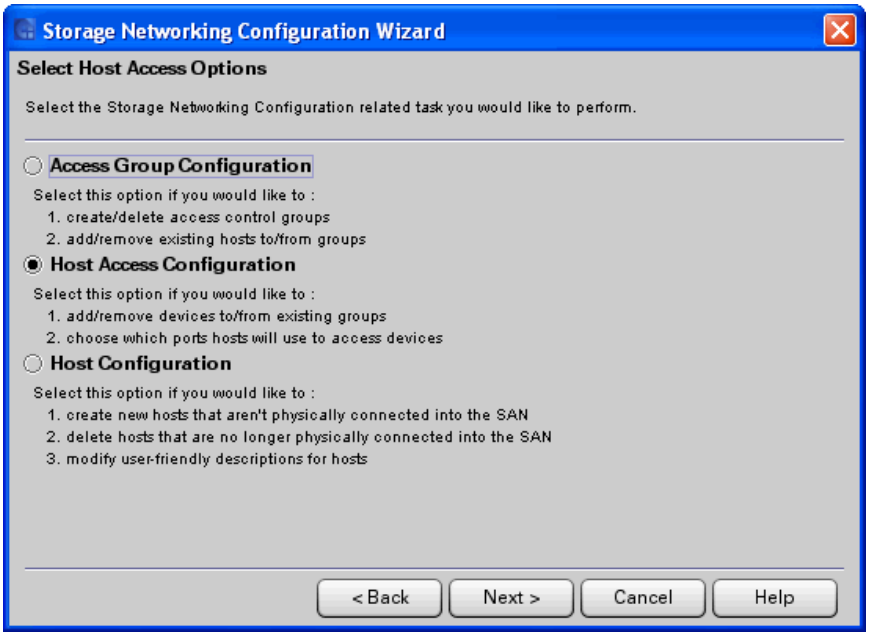
Creating Host Access Groups

A host access group is composed of at least one host and one drive. Each host in the access group can send read/write commands to the drives in the group, and can send move commands to the partitions in the group. A host can only be in one access group. Drives and partitions can be in multiple access groups.

To create host access groups:

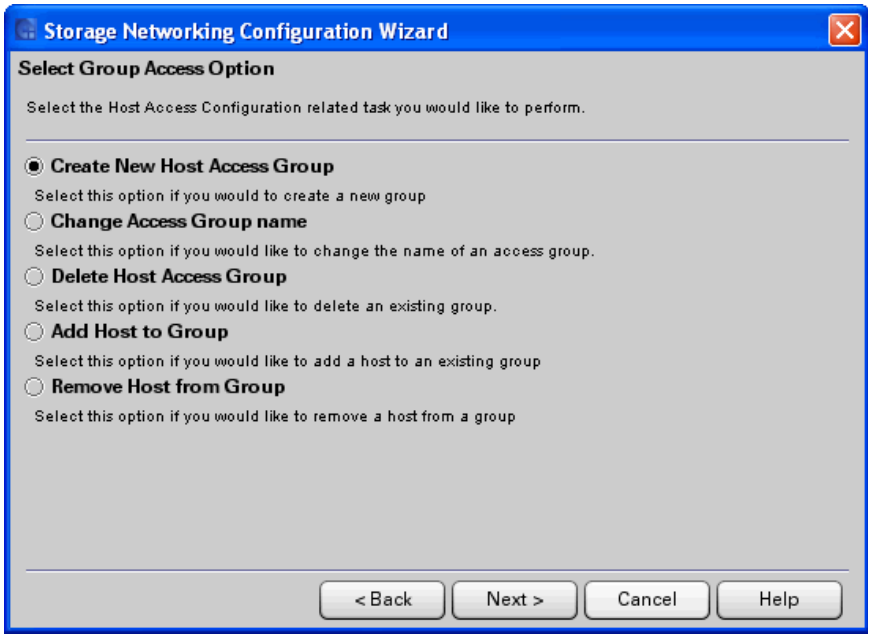
1. Select **Setup > SNW Wizard** to display the SNW Wizard.
2. Click **Next** to display the **Select Storage Networking Option** screen.

3 Select **Host Access** and click **Next** to display the **Select Host Access Options** screen.

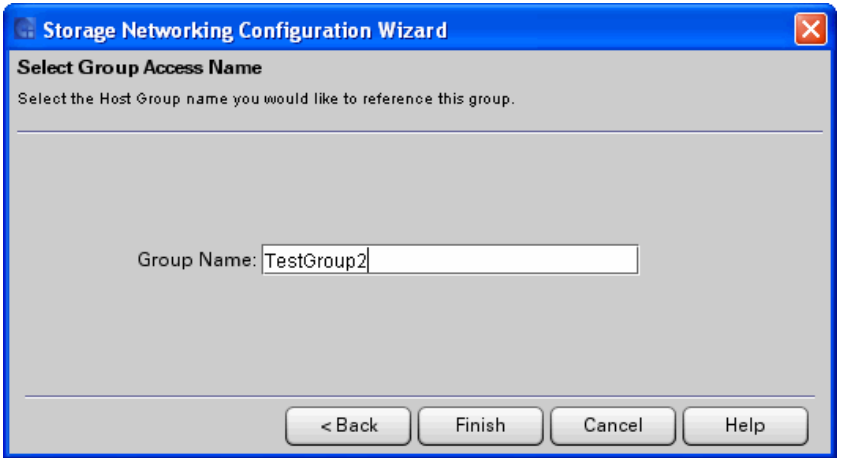


4 Select **Access Group Configuration** and click **Next** to display the **Host Access Group Configuration Wizard**.

5 Click **Next** to display the **Select Group Access Option** screen.



6 Select the **Create New Host Access Group** radio button and click **Next** to display the **Select Group Access Name** dialog box.

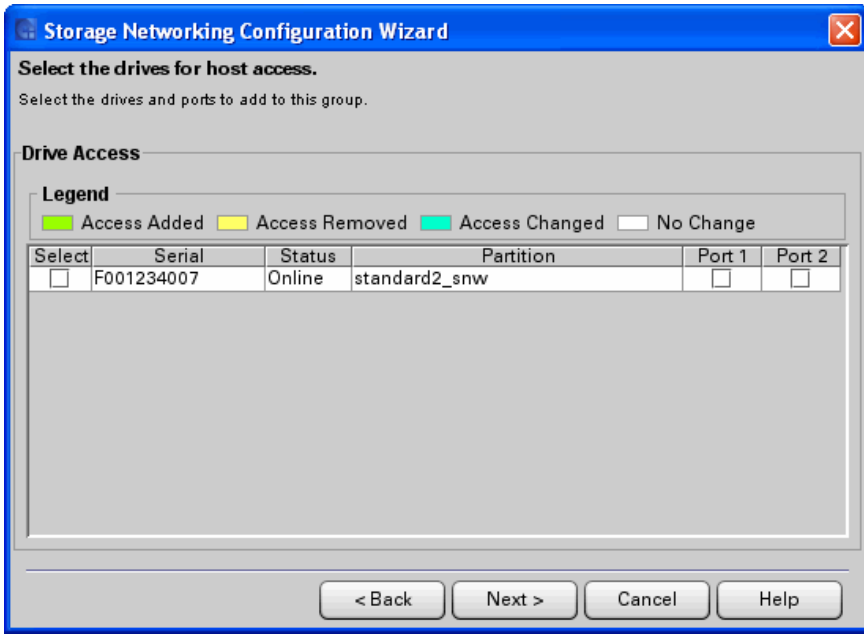


7 Type a name into the **Group Name** field.

8 Click **Next** to display the **Select Group Access Hosts** dialog box. All the hosts visible on the SAN are displayed.

9 Select one or more check boxes in the **Select** column to indicate which host or hosts to include in the access group, or select the **Select All Hosts** check box to include all of the hosts in the group.

10 Click **Next** to display the **Select the drives for host access** dialog box.



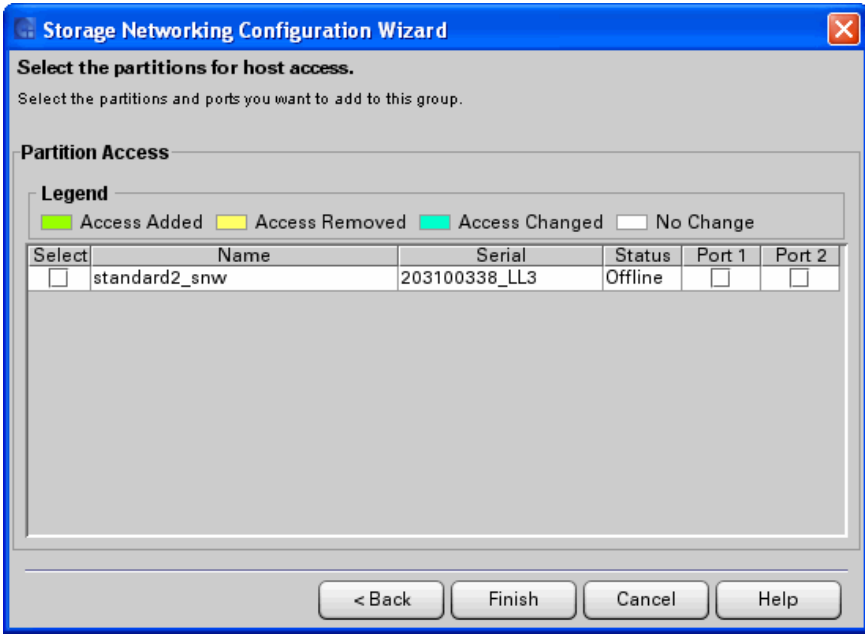
11 To add drives to the host access group, select their check boxes in the **Select** column.

Caution: If control path failover is configured for a partition you are planning to add to this host access group, make sure you assign both the control path drive and the control path failover drive to this host access group. If you do not, then if the control path fails over, you will lose host access to the partition.

12 For each drive selected, make sure to select either Port 1 or Port 2 for processing drive commands (the default is Port 1). Both drive ports are active and have different WWPNs, so the port you choose must be physically connected to a host or switch or the host will not see it. **Exception**: If the drive is configured for Data Path Failover, you should only select Port 1(if the data path fails over to Port 2, the host will still be able to access it because DPF is configured).

13 Click **Next** to display the **Select the partitions for host access** dialog box. In order for a partition to appear on the list, both the following conditions must apply:

- the partition has its control path configured via control path bridging (meaning, the control path is via an HP LTO-5 or LTO-6 drive connected to an Ethernet Expansion blade); and
- the control path drive has an SNW license applied to it.



14 To add partitions to the host access group, select their check boxes in the **Select** column.

For each partition selected, make sure to select either Port 1 or Port 2 for processing host medium changer commands (the default is Port 1). Both drive ports are active and have different WWPNs, so the port you choose must be physically connected to a host or switch or the host will not see it. The port you choose depends on which ports on the control path drive are physically cabled.

15 Click **Finish** to create the new access group.

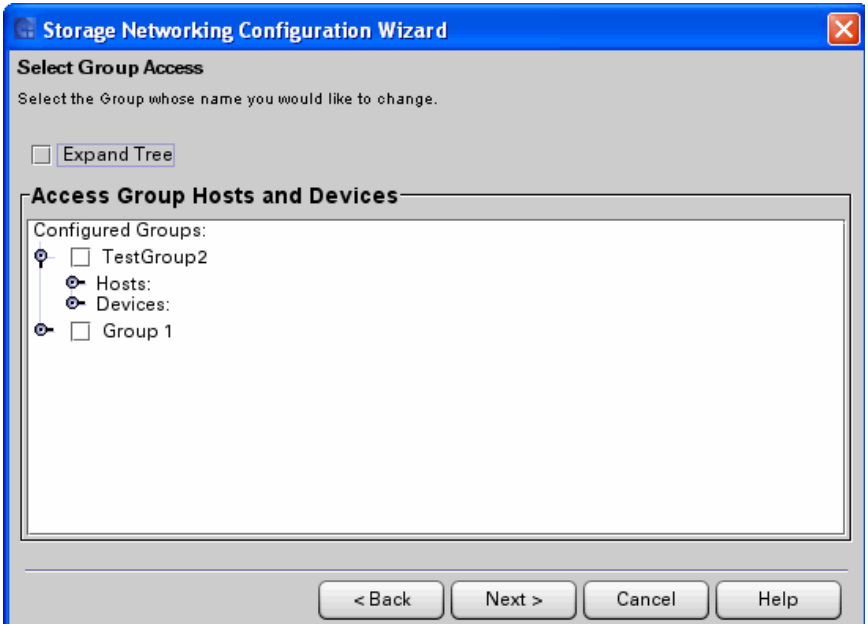
16 Click **OK** in the **The Host Access was updated successfully** dialog box.

Changing an Access Group Name

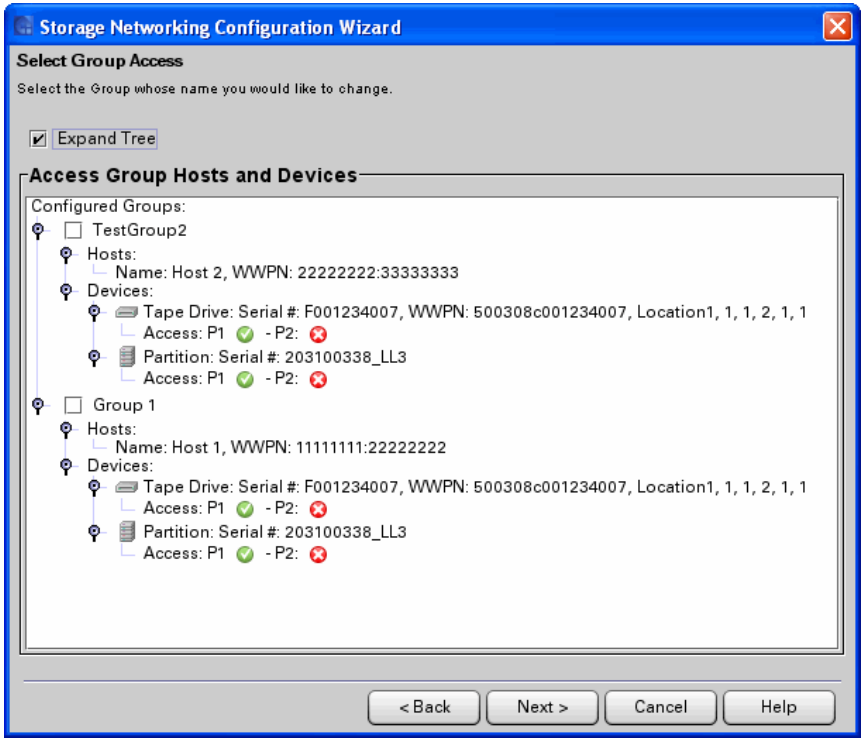
1 Display the **Host Access Group Configuration Wizard** by performing Step 1 through Step 5 of Viewing All Access Groups on page 407.

2 Select the **Change Access Group name** radio button.

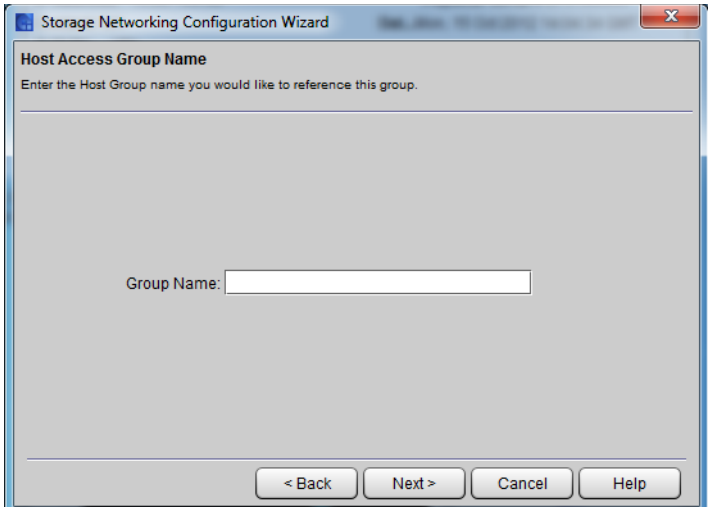
3 Click **Next** to display the **Select Group Access** dialog box.



4 Select the **Expand Tree** check box to list all items in the **Access Group Hosts and Devices** section of the dialog box.



5 Select the box corresponding to the access group whose name you want to change.Click **Next** to display the **Select Group Access Name** dialog box.



6 Type the new name into the **Group Name** field.

7 Click **Finish**.

Deleting a Host Access Group

Caution: When you delete a host access group, all host mappings for this group are deleted.

To delete a host access group:

1 Display the **Host Access Group Configuration Wizard** by performing Step 1 through Step 5 of Viewing All Access Groups on page 407.

2 Select the **Delete Host Access Group** radio button.

3 Click **Next** to display the **Select Group Access** dialog box.

4 Select the **Expand Tree** box to list all items in the **Access Group Hosts and Devices** section of the dialog box.

5 Select the box corresponding to the access group to delete.

6 Click **Finish** to display the **Warning** dialog box.

7 Click **Yes** to delete the access group.

8 Click **OK** in the **The Group Access was deleted successfully** dialog box.

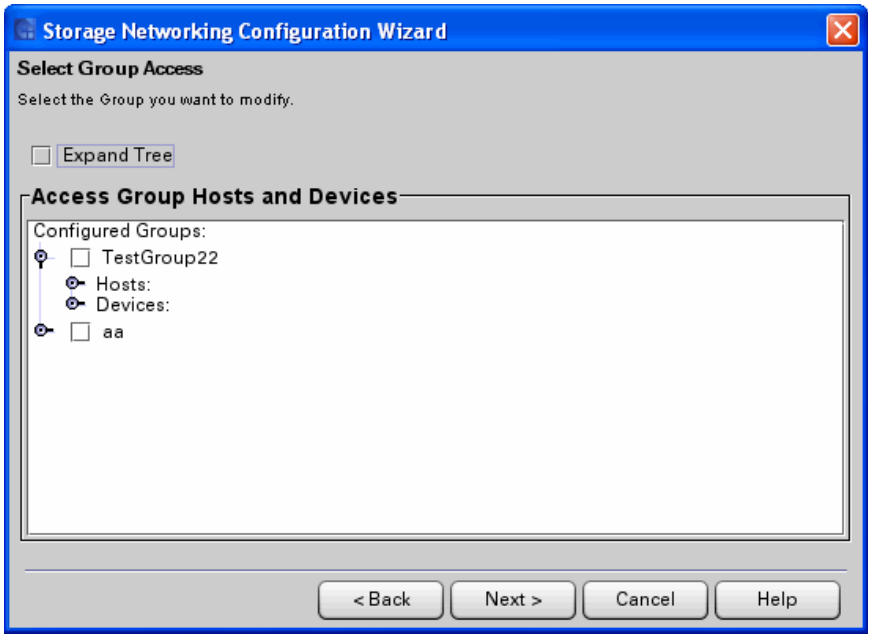
Adding a Host to an Access Group

To add a host or hosts to a host access group:

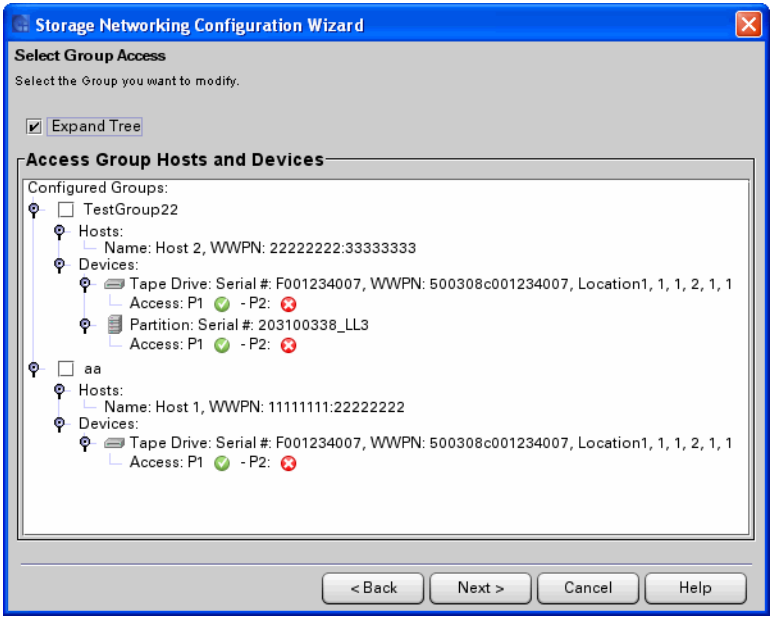
1 Display the **Host Access Group Configuration Wizard** by performing Step 1 through Step 5 of Viewing All Access Groups on page 407.

2 Select the **Add Host to Group** radio button.

3 Click **Next** to display the **Select Group Access** dialog box.

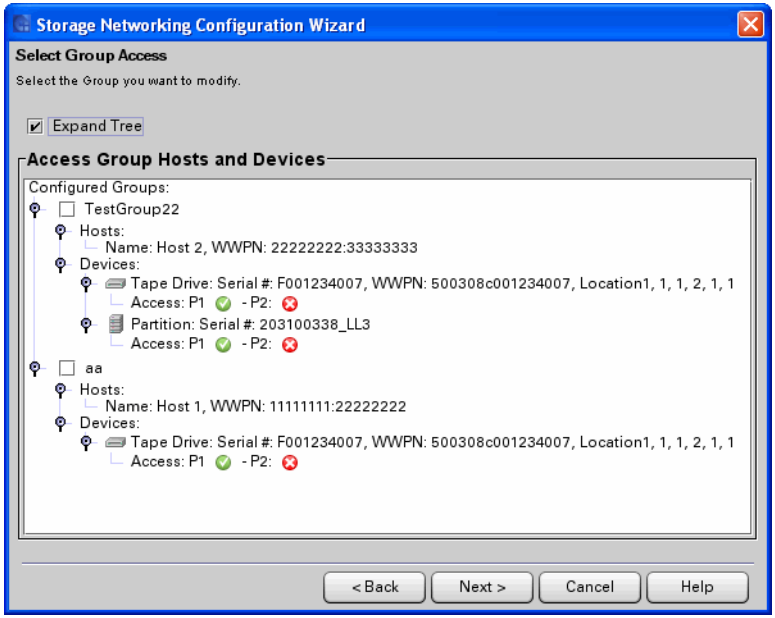


4 Select the **Expand Tree** box to list all items in the **Access Group Hosts and Devices** section of the dialog box.



5 Select the box corresponding to the access group to modify.

6 Click **Next** to display the **Select Group Access Hosts to Add** dialog box.



7 Select the box in the **Select** column to indicate which host or hosts to add to the group, or select the **Select All Hosts** box to add all of the hosts in the group.

8 Click **Finish** to save the modification.

9 Click **OK** in the **The Group Access was updated successfully** dialog box.

Removing a Host from an Access Group

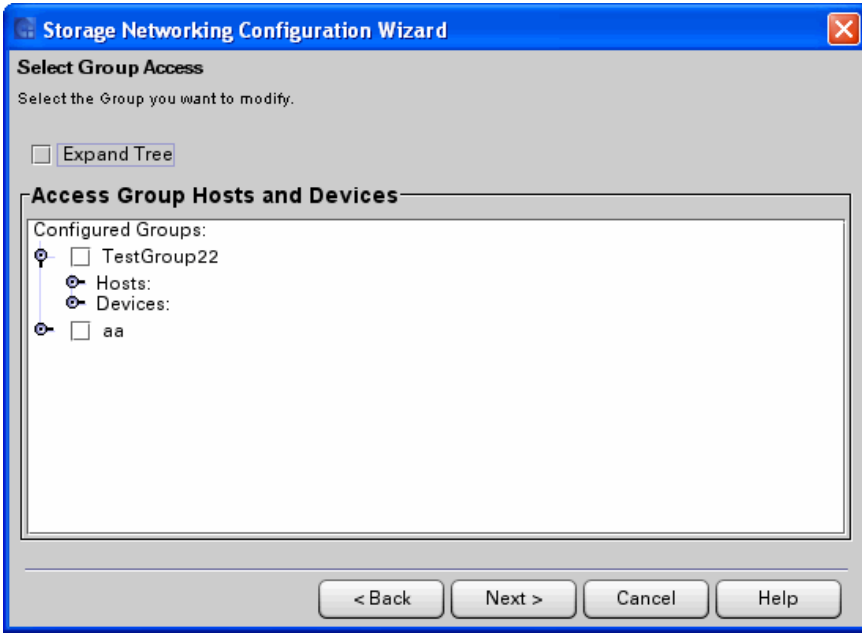
Caution: Deleting a host from an access group will remove all host mappings configured for the host.

To remove a host from a host access group:

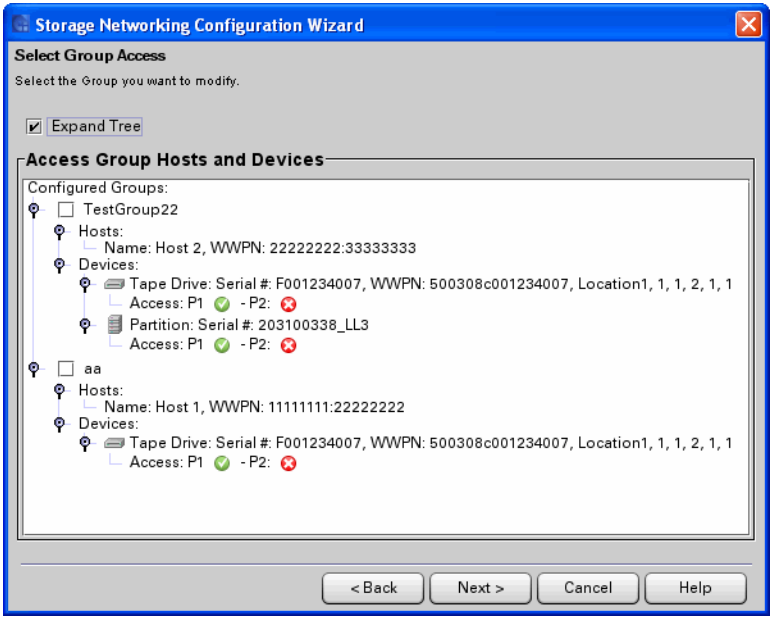
1 Display the **Host Access Group Configuration Wizard** by performing Step 1 through Step 5 of Viewing All Access Groups on page 407.

2 Select the **Remove Host from Group** radio button.

3 Click **Next** to display the **Select Group Access** dialog box.

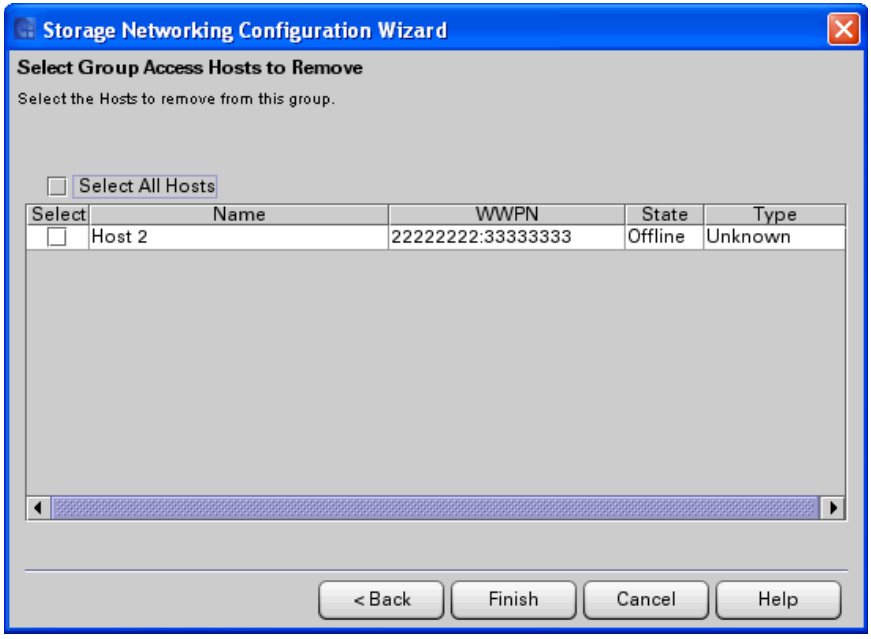


4 Select the **Expand Tree** box to list all items in the **Access Group Hosts and Devices** section of the dialog box.



5 Select the box corresponding to the access group from which to remove a host.

6 Click **Next** to display the **Select Group Access Hosts to Remove** dialog box.



7 Select the box in the **Select** column to indicate which host or hosts to remove from the group, or select the **Select All Hosts** box to remove all of the hosts from the group.

8 Click **Finish** to save the modification.

9 Click **Yes** in the Warning dialog box.

10 Click **OK** in the **The Group Access was updated successfully** dialog box.

Host Access Configuration – Modifying Drives/ Partitions and Viewing Host Access Groups

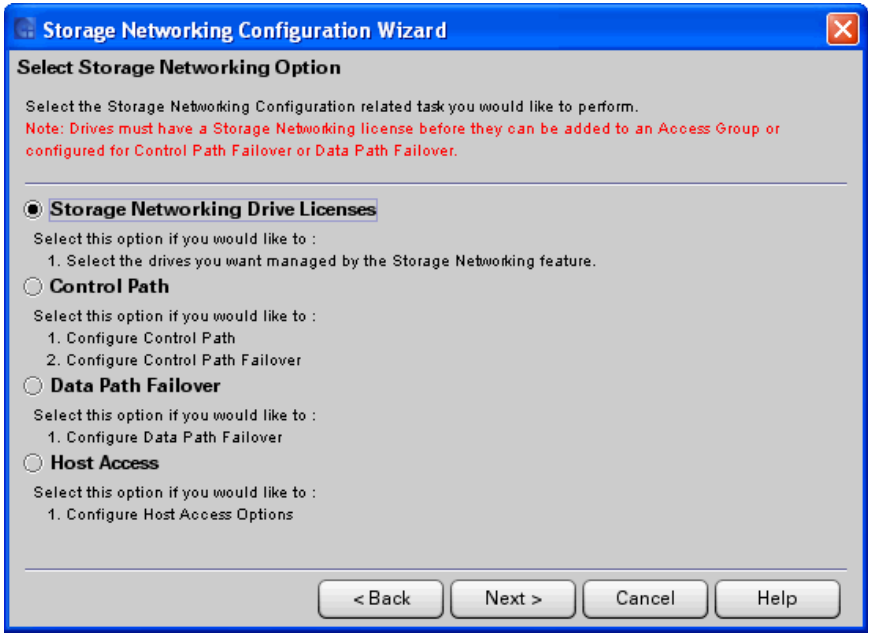
The Host Access Configuration option allow you to do the following:

- Adding and Removing Drives and Partitions to/from Host Access Groups on page 402
- Viewing All Access Groups on page 407

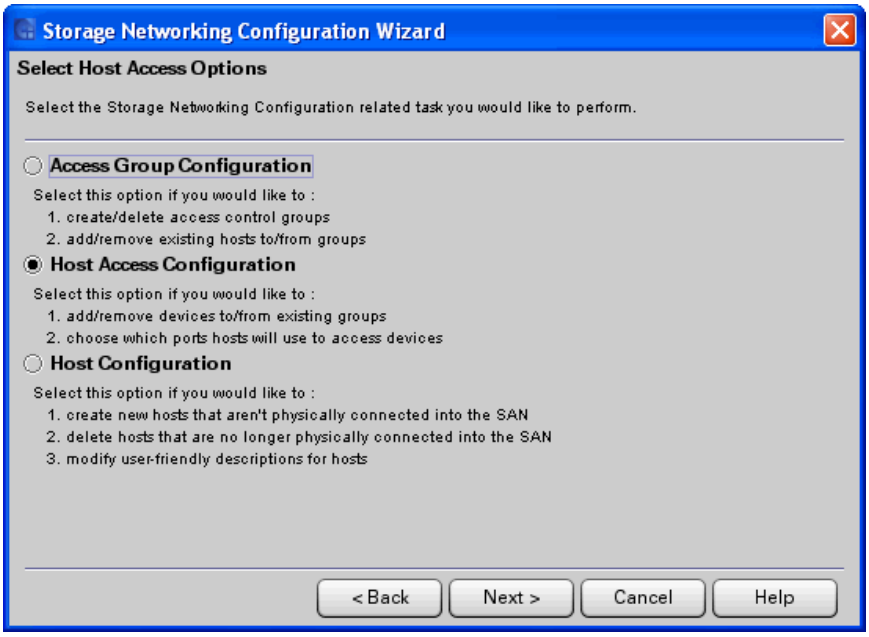
Adding and Removing Drives and Partitions to/from Host Access Groups

To add devices to or remove devices from an existing group, or to select which ports the hosts will use to access devices, use the **Host Access Configuration** option. To do so:

1. Select **Setup > SNW Wizard** to display the SNW Wizard.
2. Click **Next** to display the **Select Storage Networking Option** screen.

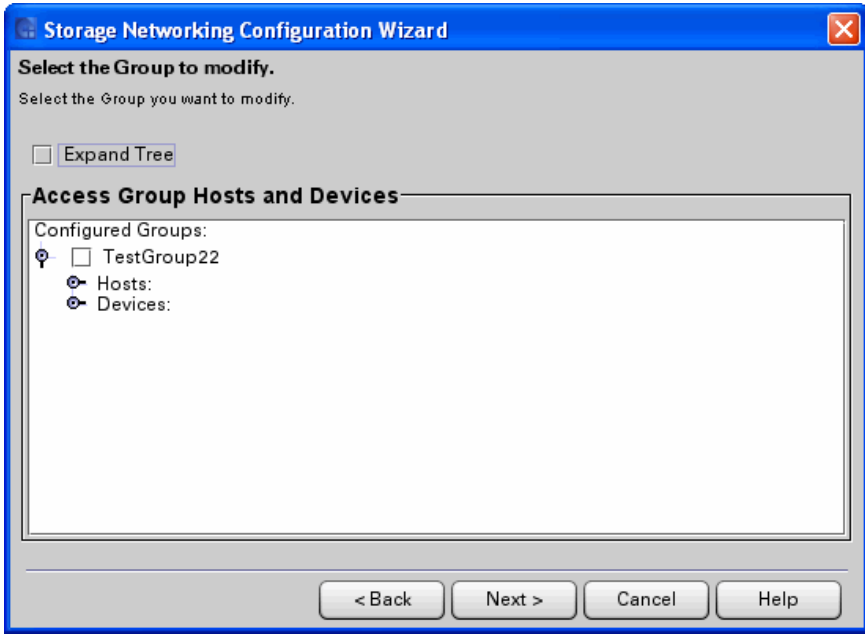


3 Select **Host Access** and click **Next** to display the **Select Host Access Options** screen.

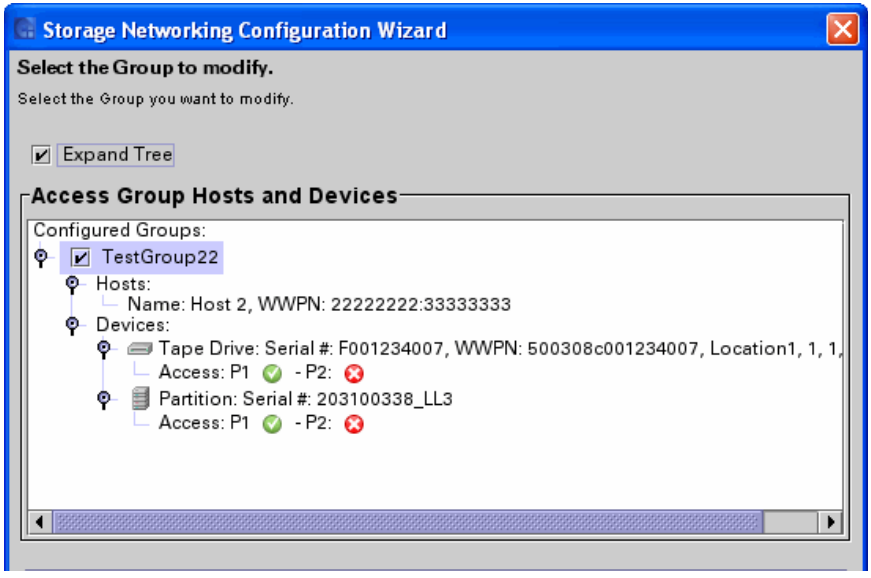


4 Select the **Host Access Configuration** radio button.

5 Click **Next** to display the **Select the Group to modify** screen.

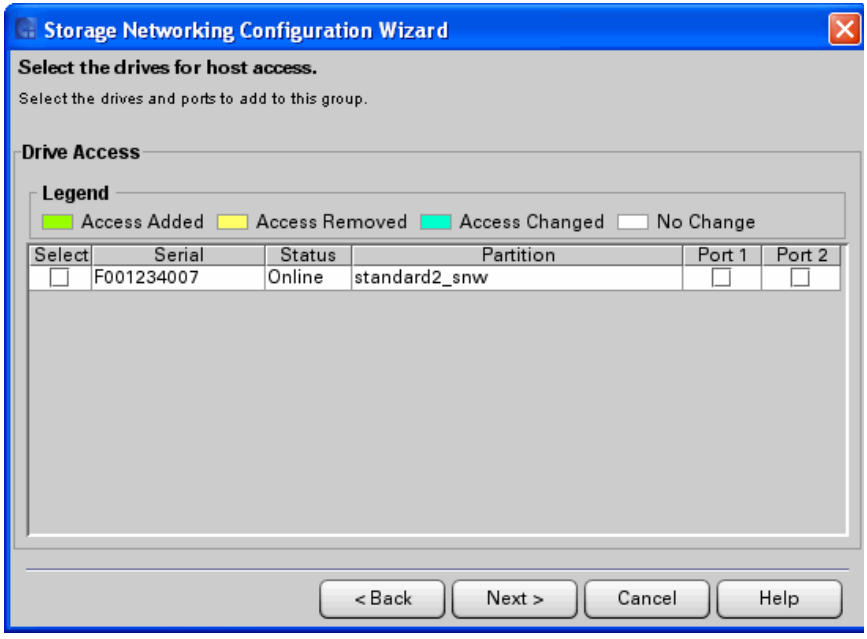


6 Select the **Expand Tree** box to list all items in the **Access Group Hosts and Devices** section of the dialog box.



7 Select the box corresponding to the access group you want to modify.

8 Click **Next** to display the **Select the drives for host access** dialog box which shows the current settings.



9 Select or clear boxes in the **Select** column to indicate which drive or drives to include in the host access group. You do not have to include drives in the host access group.

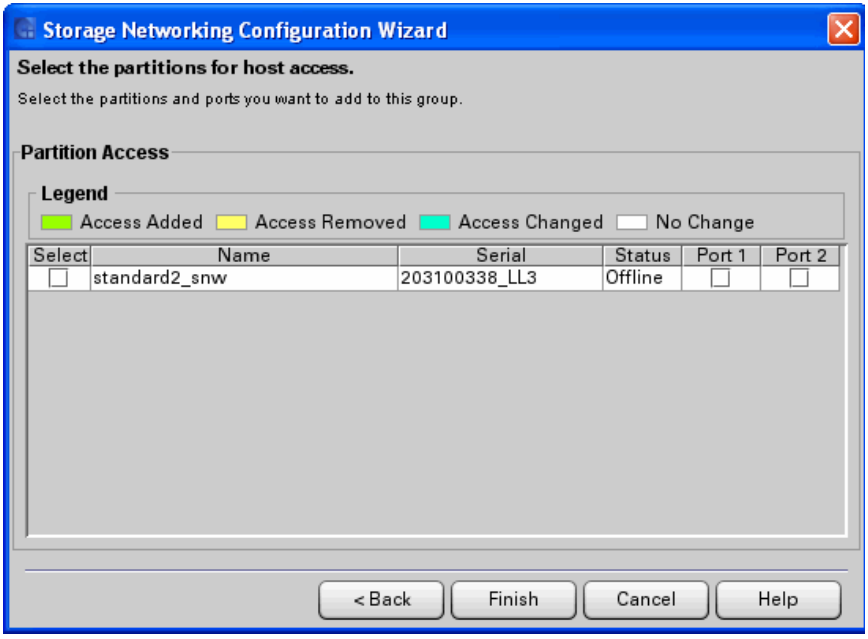
Caution: If control path failover is configured for a partition you are planning to add to this host access group, make sure you assign both the control path drive and the control path failover drive to this host access group. If you do not, then if the control path fails over, you will lose host access to the partition.

10 For each drive selected, make sure to select either Port 1 or Port 2 for processing drive commands (the default is Port 1). Both drive ports are active and have different WWPNs, so the port you choose must be physically connected to a host or switch or the host will not see it. **Exception**: If the drive is configured for Data Path Failover,

you should only select Port 1(if the data path fails over to Port 2, the host will still be able to access it because DPF is configured).

11 Click **Next** to display the **Select the partitions for host access** dialog box. In order for a partition to appear on the list, both the following conditions must apply:

- The partition has its control path configured via control path bridging (meaning, the control path is via an IBM or HP LTO-5 or higher drive connected to an Ethernet Expansion blade); and
- The control path drive has an SNW license applied to it.



12 Select or clear boxes in the **Select** column to indicate which partitions to include in the host access group.

13 For each partition selected, make sure to select either Port 1 or Port 2 for processing host medium changer commands (the default is Port 1). Both drive ports are active and have different WWPNs, so the port you choose must be physically connected to a host or switch or the host will not see it. The port you choose depends on which ports on the control path drive are physically cabled.

14 Click **Finish** to update host access.

15 Click **OK** in the **The Host Access was updated successfully** dialog box.

Viewing All Access Groups

If you want to see all of the access groups you configured:

1 Select **Setup > SNW Wizard** to display the **SNW Wizard**.

2 Click **Next**.

3 Select the **Host Access** radio button and click **Next**.

4 Select the **Host Access Configuration** radio button.

5 Click **Next** to display the **Select the Group to configure** screen.

6 Select the **Expand Tree** box to list all items in the **Access Group Hosts and Devices** section of the dialog box.

7 Click **Cancel** to exit.

8 Click **Yes**.

Chapter 11
Configuring Access to StorNext

Certain licensed features (EDLM and Active Vault) can use an external application to perform partition policies. To configure access to an external application, you must first install an application programming interface (API) client plug-in, and then configure the library to communicate with the external application.

The API client plug-in is a Quantum-provided plug-in that allows the library to communicate with a supported external application (such as StorNext Storage Manager). The API client plug-in must be installed before you can configure library access to the external application.

You can install as many API client plug-ins as necessary.

The same API client plug-in may be used for multiple features.

This chapter covers:

Step 1: Confirming the External Application is Supported

Confirm that the **external application** managing your partition is supported by EDLM.

For a list of supported external applications and their corresponding plug-ins, see the *Scalar i6000 Release Notes*.

Step 2: Installing/ Removing the Scalar i6000 API Client Plug-in

Installing a StorNext API Client Plug-in

Install the plug-in as follows:

Note: If you install an API client plug-in that has the same **Name-Version** of an already installed plug-in but is at a different **Revision**, the newly installed plug-in will replace the existing plug-in. The screen shot in Step 9 on page 412 shows the difference between version and revision.

1. See the release notes for a list of supported API client plug-ins and their corresponding external applications. Currently the library supports only StorNext API (SNAPI) Client Plug-in version 2.0.1.
2. Download the correct API client plug-in bundle as follows:
   a. Go to the following Web site.

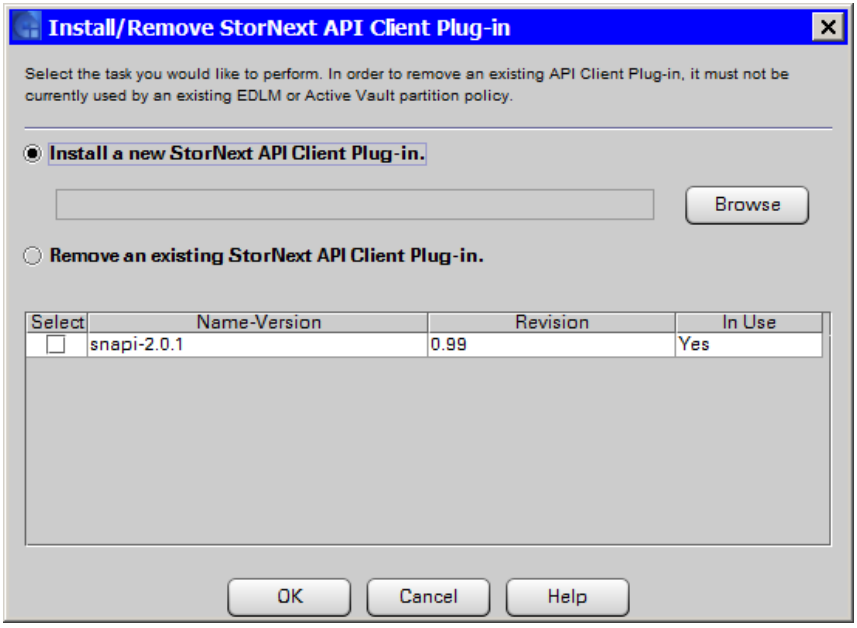
      http://www.quantum.com/ServiceandSupport/SoftwareandDocumentationDownloads/S6K/Index.aspx

   b. Click the **Drivers** tab to view the available plug-ins.

   c. Click the **Download** button for the plug-in you want to install.

   The plug-in bundle is a .zip file containing the following files:

   - Client plug-in
   - End User/Open Source License Agreement
3. Extract the files from the .zip file.
4. Read the End User/Open Source License Agreement. Installation of the plug-in implies acceptance of the license agreement.
5. Select **Tools > Update Software > Plug-in**. The **Install/Remove StorNext API Client Plug-in** screen appears.

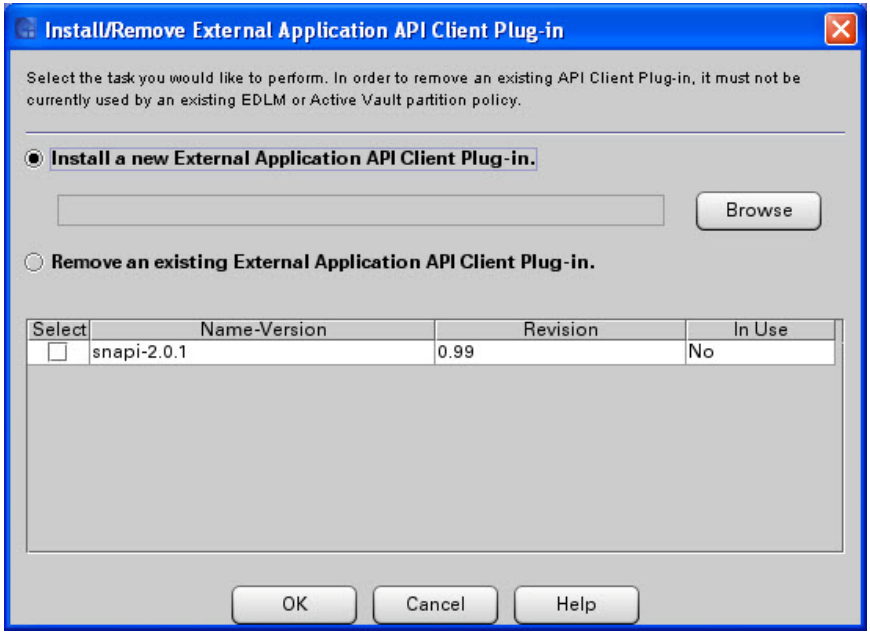


6 Select **Install a new StorNext API Client Plug-in.**

7 Click **Browse** to retrieve the plug-in file.

8 Click **Finish**. The plug-in is installed or removed. A “success” dialog box appears.

9 Click **OK** to close the dialog box. The installed plug-in appears on the Install or Remove StorNext API Client Plug-in screen.



Removing an API Client Plug-in

To remove an installed plug-in, do the following:

Note: To remove an external application API client plug-in, it must not currently be used by an existing EDLM partition policy.

1 Select **Remove an existing External Application API Client Plug-in**.

2 Select the plug-in(s) to remove from the list displayed in the table.

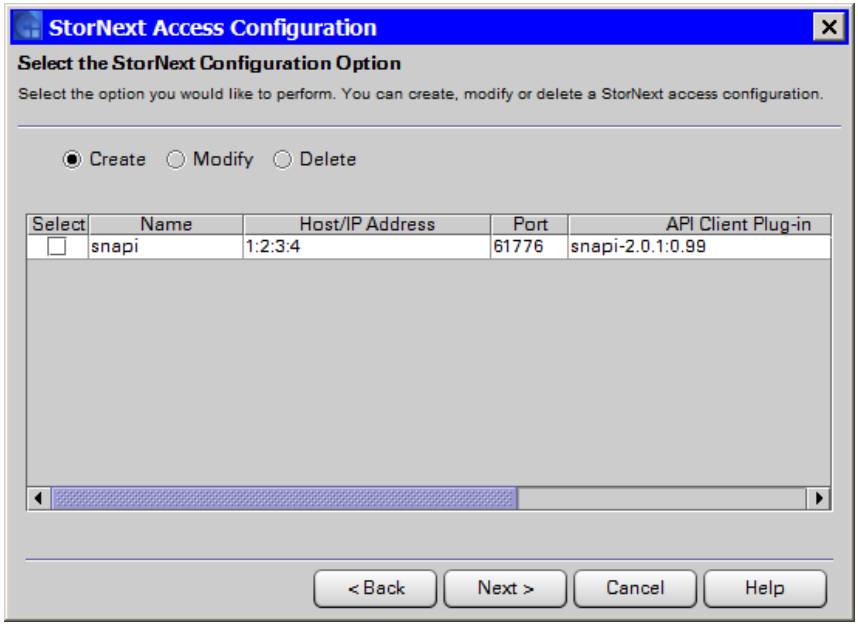
3 Click **Finish**. A confirmation dialog box appears.

4 Click **Yes** to confirm you want to remove the plug-in.

Step 3: Configuring External Access

1 Click **Setup > Partitions > Policies > StorNext Access**. The StorNext Access Configuration Wizard appears.

2 Click **Next**. The **Select the StorNext Configuration Option** screen appears.

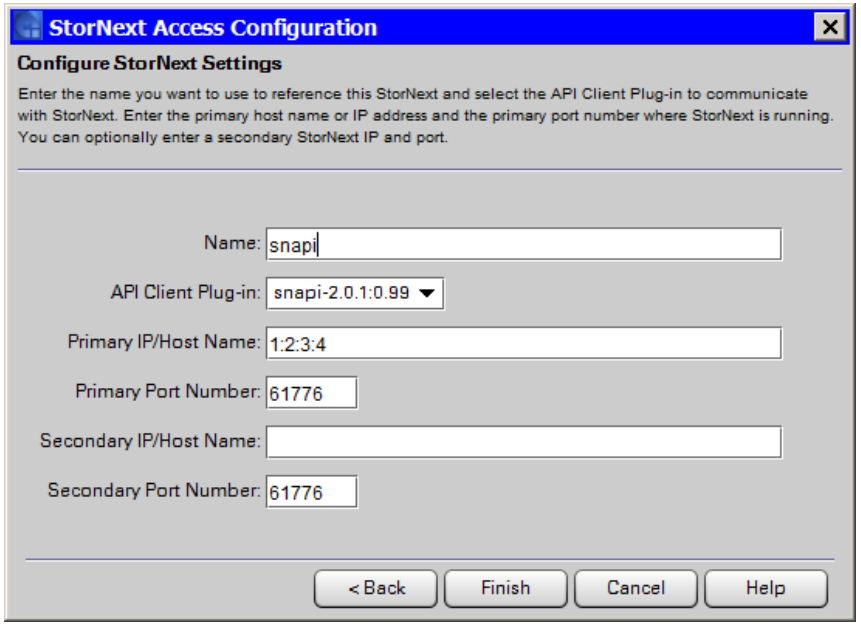


3 Do one of the following:

To...	Do this...
Add a new external application	1 Select **Create**. 2 Click **Next.**
Modify an existing external application	1 Select **Modify.** 2 Select the application you want to modify from the table. 3 Click **Next**.

To...	Do this...
Delete an existing external application	**1** Select **Delete.** **2** Select the application you want to delete from the table. **3** Click **Finish**. A confirmation dialog appears. **4** Click **Yes** to confirm you want to delete the application. **5** Click **OK**. **6** Process is complete.

If you are creating or modifying, the **Configure StorNext Settings** screen appears.



4 If you are creating or modifying, configure the following the fields:

Field	Description
Name	Type a descriptive name you will use to identify the external application.

Field	Description
API Client Plug-in	Select the appropriate API client plug-in from the drop-down list. The list contains the API client plug-ins you installed in Step 2: Installing/Removing the Scalar i6000 API Client Plug-in on page 410.
Application IP/Host Name	Type the IP address or DNS host name (if DNS is configured) of the external application server. **Note:** To use a host name, DNS must be configured on the LMC (**Setup > Network Configuration > DNS Configuration**).
Application Port Number	Accept the default or type an external application host server port number.

5 Click **Finish**. A **success** dialog box appears.

Caution: If you get an error dialog box that says, "Failed to validate the External Application," this may mean that the IP address or host name is incorrect, or the server is not responding or not configured. The library will accept the settings you entered, but you should double-check that all the information is correct and modify it if necessary. If any of the configured information is incorrect, successful communication will not occur.

6 Click **OK** to close the dialog box.

Chapter 12
Partition Utilization Reporting

Partition Utilization reporting allows you to optimize resource assignments among host applications and partitions.

Details about Partition Utilization include:

- Partition Utilization is a licensable feature. A single license applies to the entire library and you can use the feature on as many partitions as you wish.
- The Partition Utilization license overrides your library's current Capacity on Demand (COD) license and Partition license and allows you to use the maximum number of slots and partitions available on the physical library. The library **Licenses** screen (**Setup > Licenses**) will show a Capacity On Demand license with 6500 slots available, and a Partition license with 16 partitions allowed.
- You can have the reports automatically e-mailed to recipients of your choice on a regular basis.
- Partition Utilization reports are not included in library snapshots.
- The report contains the last 12 months of activity.

Viewing the Partition Utilization Report

To view the on-screen Partition Utilization report:

1 If you are not already viewing the physical library, click **View** and select the name of the physical library.

2 Select **Tools > Reports > Partition Utilization**.

Interpreting the Partition Utilization Report

The Partition Utilization report is a single file containing data for the last 12 months. For each month, the report displays a High Water Marks section and a Partition Activity section, which are described below.

To e-mail, save, or print the report, click **Send**.

To automatically send reports to recipients at scheduled intervals, see Scheduling Partition Utilization Reports on page 419.

High Water Marks

The high water mark is the highest number of tape drives, storage slots, or media present in a partition during a given month. The report displays the following high water mark information for each partition:

- **DWM** — Drive high water mark. The highest number of tape drives configured in the partition during the month.
- **SWM** — Storage high water mark. The highest number of storage slots configured in the partition during the month.
- **MWM** — Media high water mark. The highest number of media residing in the partition during the month.
- **PN** — Partition name.

If you pull a report in the middle of a month, the report displays high water mark counts received so far.

If you delete a partition, that partition's high water marks will be reported for the period of time before the partition was deleted.

Partition Activity

Partition activity is defined as creating, modifying, and deleting partitions, as well as physically adding media to and removing media from partitions. This section lists each occurrence of partition activity that took place during the month.

Each entry in this section includes the following information:

- Date and time the activity occurred.
- Partition name.

- Drive count when the activity completed.
- Slot count when the activity completed.
- Media count when the activity completed.
- Type of activity that occurred.

If no activity occurred on a partition during the month, there will be no entry for that partition.

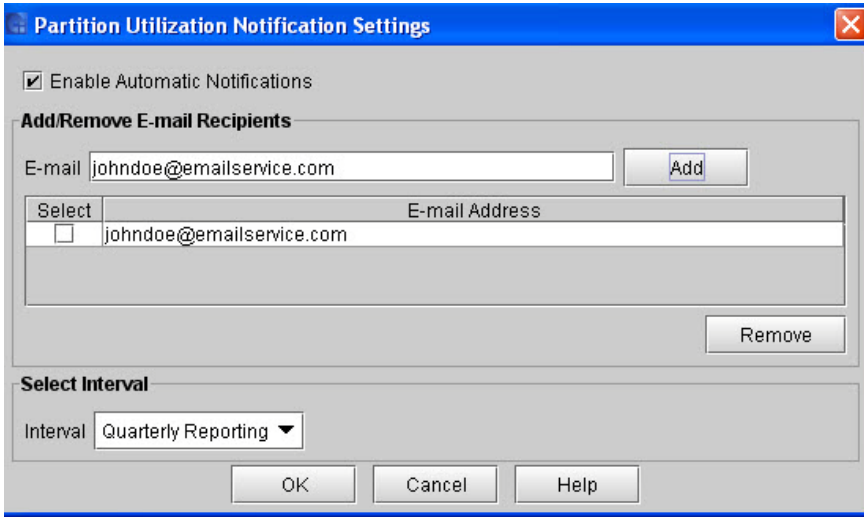
Scheduling Partition Utilization Reports

You can automatically e-mail Partition Utilization reports to recipients at regular intervals as follows.

Note: The Partition Utilization reports are monthly reports. You can send them automatically more or less frequently, but the data are still compiled and reported by month.

Note: Before you can set up the Partition Utilization reports, you must configure e-mail properties on the library. If they are not yet configured, an error message directs you to go to **Setup > Email Configuration** and fill in the required fields.

1 Click **Setup > Notifications > Partition Utilization**. The **Partition Utilization Notification Settings** screen appears.



2 Select the **Enable Automatic Notifications** check box.

3 Enter the proper address into the E-mail field.

4 Click **Add**. The account is added to the **E-mail Address** list.

5 To add more recipients to receive the report, type another recipient e-mail address in the **E-mail** field and click **Add**. Repeat as necessary.

Note: The total number of characters for all recipient e-mail addresses listed in this section cannot exceed 512.

---

6 To delete a recipient, select the check box next to the recipient's e-mail address and click **Remove**.

7 Select how often recipients will receive reports from the **Interval** drop-down list. If Quantum is doing the billing for this library, select **Monthly**.

The interval choices are the following:

- **Daily** — Every day.
- **Weekly** — Every Monday.
- **Monthly** — The first day of every month.

- **Quarterly** — The first day of January, April, July, and October.

8 Click **OK**. Reports will be sent on the scheduled days.

Chapter 13
Running Your Library

This chapter includes the following sections, which explain how to access and operate your library:

- Using the Library Access Feature on page 482
- Using the Library Access Feature on page 482

Logging On and Off

The Library Management Console (LMC) is the library user interface. You can log on and off locally by using the library's touch screen. Or you can log on and off remotely by using a Web browser.

Logging On From the Touch Screen (Local Client)

1 If the **Scalar i6000 Logon** dialog box is not already displayed on the library's touch screen because the screen saver appears, tap the touch screen. The **Scalar i6000 Logon** dialog box appears.

2 In the **Name** text box, type the name of the user or administrator account with which you want to log on. If you want to log on with the default administrator account, type **admin**.

Note: User names and passwords are case-sensitive. Select the **Shift** key to display uppercase letters and special characters. This enables you to type one uppercase letter or special character before the **Scalar i6000 Logon** dialog box returns to displaying lowercase characters. To type more than one uppercase character or special character, select the **Caps** key. The **Caps** key toggles between displaying uppercase and lowercase characters.

Note: Only one administrator at any given time can be logged on to the library.

Note: If you want to log on using the default administrator account (admin), and you do not remember the password, contact Quantum Support to reset the password.

Note: If the date and time have reset to January 1, 1970 or if the year is set to a date earlier than 1970, a warning dialog will display on login.

3 Position the cursor in the text box below the **Name** text box by tapping it, and then type the password for the user or administrator account.

Note: If you are logging on to the library for the first time using the default administrator account (admin), type `password`. After you log on, the library prompts you to change the default admin password. You must enter and confirm a new password. Passwords that are most secure include a combination of letters, numbers, and non-alphanumeric characters. Passwords must be eight or more characters in length. The word “password” is not available for use.

4 After you type a user name and password, select **OK**.

Logging Off From the Touch Screen (Local Client)

1. Select **Operations > Log Off** or select the **Log Off** button on the toolbar. A message appears that asks you whether you are sure that you want to log off.
2. Select **Yes**. The **Scalar i6000 Logon** dialog box appears.

Logging On From a Web Browser (Remote Client)

You can access all features of the LMC from a host computer using a standard Web browser. The host computer must have network access to the library, and you must know the IP address of the library.

Note: If you do not know the IP address of the library, log on to the library using the touch screen. Click **Setup > Network Configuration**, and then write down the value in the **IP Address** field.

Software Requirements

Before logging on from the Web browser, make sure the host computer meets the following software requirements:

- **Web Browser** – Microsoft Internet Explorer 7 or 8; Mozilla Firefox 1.0.6 or higher
- **Java Plug-in** – Java Plug-in 1.4 or higher

For information on downloading the Java Plug-in contact: www.quantum.com/support

Accessing the Library via the Web Browser

After verifying that the host computer meets the software requirements and has network access to the library:

1. On the host computer, point your Web browser to the IP address of the library.

   The first time you access the library, an LMC applet is downloaded to the host computer. Downloading the applet can take several minutes depending on the speed of the network. Once the applet is downloaded, it is stored on the host computer and does not need to be downloaded again.

2 If a security warning appears asking if you are sure you want to run the applet, click **Run** or **Yes**. The **Scalar i6000 Logon** dialog box appears.

3 In the **Name** text box, type the name of the user or administrator account with which you want to log on. If you want to log on with the default administrator account, type `admin`.

Note: User names and passwords are case-sensitive.

Note: Only one administrator at any given time can be logged on to the library.

Note: If you want to log on using the default administrator account (admin), and you do not remember the password, contact technical support to reset the password.

Note: If the date and time have reset to January 1, 1970 or if the year is set to a date earlier than 1970, a warning dialog will display on login.

4 In the **Password** text box, type the password for the user or administrator account.

Note: If you are logging on to the library for the first time using the default administrator account (admin), type `password`. After you log on, the library prompts you to change the default admin password. You must enter and confirm a new password. Passwords that are most secure include a combination of letters, numbers, and non-alphanumeric characters. Passwords must be eight or more characters in length. The word “password” is not available for use.

5 Click **OK**.

Note: After logging on, do not close the Web browser window or use it to navigate to another URL. Doing so will close the LMC applet but might leave the current session active.

Logging Off the Web Browser (Remote Client)

1 Click **Operations > Log Off**, or click the **Log Off** button on the toolbar. A message appears asking if you are sure you want to log off.

2 Click **Yes**. The **Scalar i6000 Logon** dialog box appears.

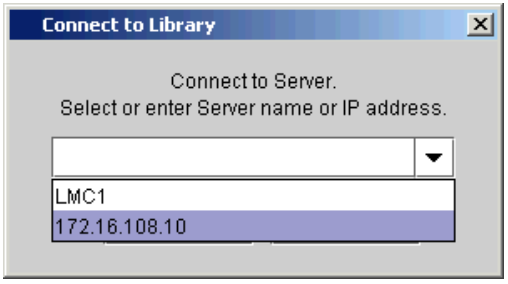
3 To close the LMC applet, click **Cancel**.

Connecting to Multiple Libraries

This feature allows you log in to multiple libraries, and switch from one library console to another without logging off.

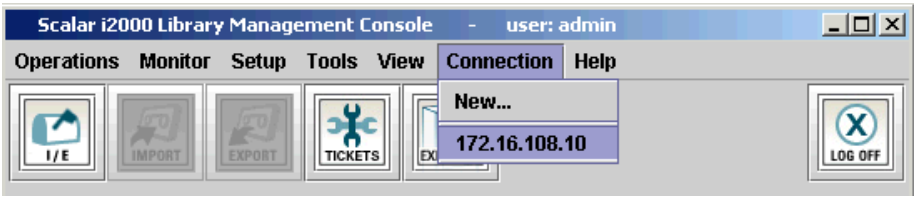
Note: This feature is available only if all libraries are at the same firmware level.

1 From the LMC menu, click **Connection > New**. The **Connect to Library** dialog box appears.



1 Type or select the library server name or library IP address, and click **OK**. You can use either iPv4 or iPv6 addresses.

Once you have connected to additional libraries, you can choose any of those libraries from the **Connection** drop-down list.

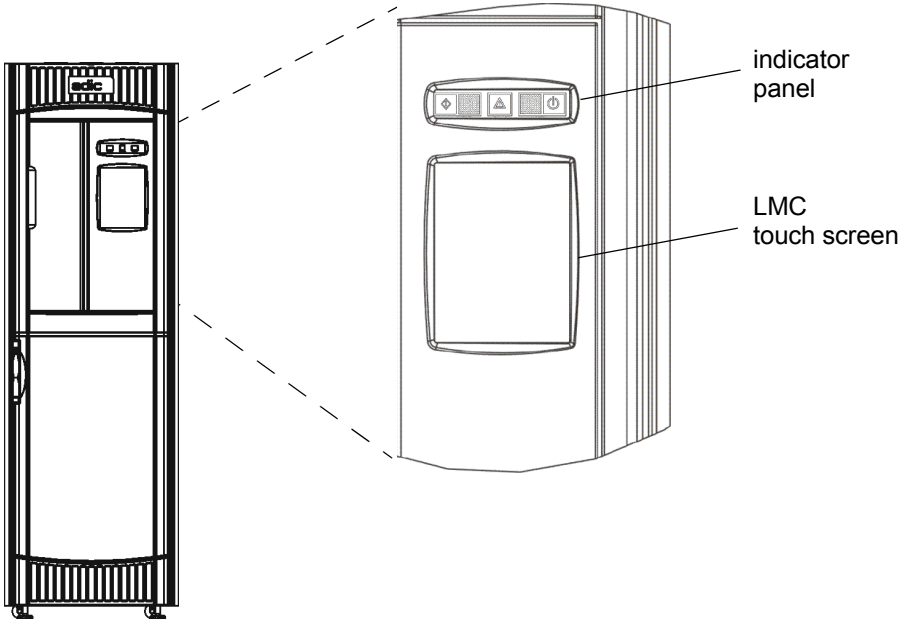


Note: To log off when connected to multiple libraries, first log off from one of the connected libraries. To do this, select the library on the **Connection** menu, click **Operations > Log Off**, and then click **Yes**. When the **Scalar i6000 Logon** dialog box appears, click **Cancel**. You can then repeat this process to log off from additional libraries.

Operator Panel

The operator panel on the library includes an indicator panel and a touch screen, as shown in Figure 37.

Figure 37 Library Op Panel

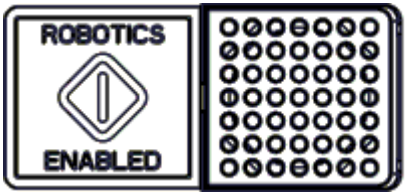


The indicator panel includes a **Robotics Enabled** button with its associated indicator, a **Status** indicator, and a **Power** button with its associated indicator. The Library Management Console (LMC) appears on the touch screen. For more information about indicator panel functions, see Indicator Panel on page 430. For a brief overview of the LMC, see Library Management Console (LMC) on page 432.

Indicator Panel

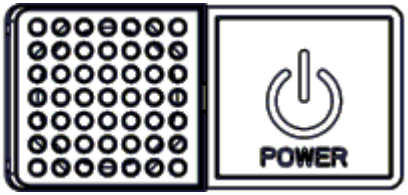
The **Robotics Enabled** indicator and the **Power** indicator each include a button. The **Status** indicator is not a button. These indicators do not report the status of communications with a host.

Note: The enabled state does not mean that robotics are communicating with the host. It means that the robotics are communicating with the library controller.



Robotics Enabled indicator and button

Status indicator



Power button and indicator

The following tables describe the indicators in detail.

Table 34 Robotics Enabled Indicator

Indicator	State and Explanation
Green	**Solid on** — robotics are enabled and ready to process commands or are actively processing commands from the library controller. No attention required. Do not open the access door. **Blinking** — a change of robotics state is pending, either from the enabled state to the not enabled state or from the not enabled state to the enabled state. No attention required. Do not open the access door.
No color	**Solid off** — either robotics are not ready, the doors might be open, or the library might be powered off. Attention required. The operator should close the doors and press the **Robotics Enabled** button to return robotics to the enabled state.

Table 35 Status Indicator

Indicator	State and Explanation
Green	**Solid on** — normal. No attention required.
Amber	**Blinking or solid on** — fault. Attention required. Monitor the system status buttons. To determine whether the library has created any tickets, click **Tools > Tickets**.

Table 36 Power Indicator

Indicator	Operational Status
Green	**Solid on** — power on. No attention required.
No color	**Solid off** — power off. Attention required. To operate the library, you must turn on the power. Press the **Power** button.

Library Management Console (LMC)

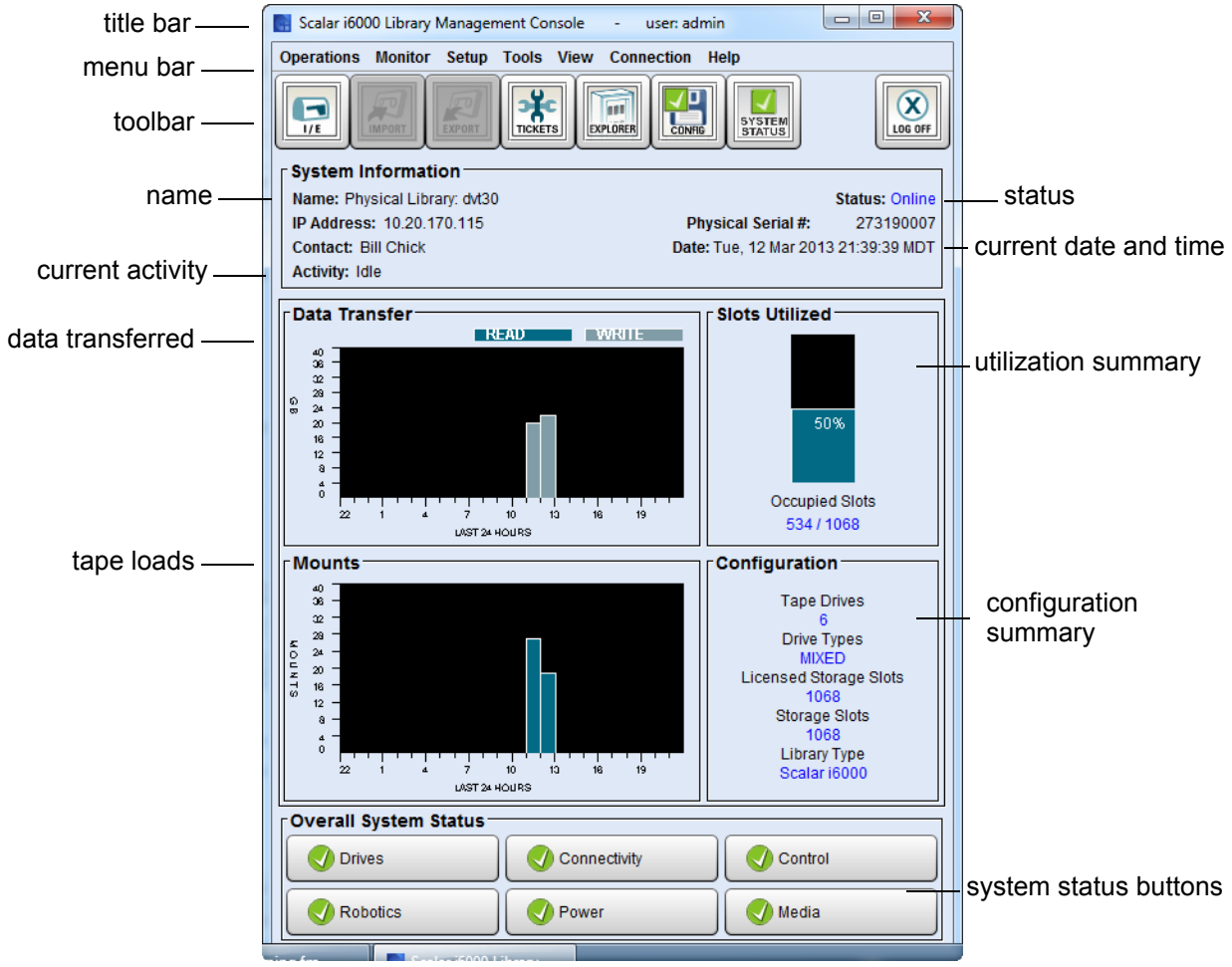
You can view the LMC from either the library's touch screen or a remote computer. If you use the touch screen, you do not need to install the LMC because it is already installed on the library. To access the LMC using a Web browser, see Logging On From a Web Browser (Remote Client) on page 426.

Note: To manage your library from a remote client, you must set up the library's initial network configuration from the touch screen. For more information, see Setting Up the Network Configuration on page 152.

The main LMC display consists of five areas:

- The title bar on the touch screen view of the LMC displays the words "Scalar i6000 Library Management Console." The title bar appears slightly differently on the remote client view of the LMC. Compare Figure 38 to Figure .
- The menu bar provides access to all menu commands used to manage library functions.
- The toolbar displays icons that represent the most commonly run commands.
- The library information panel fills most of the main LMC display, presenting operational data from the current library, whether physical or partition.
- The system status buttons provide current status information for the six subsystems of the physical library.

Figure 38 Library Management Console (LMC)



Menus

The following seven LMC menus organize commands into logical groupings:

- The **Operations** menu consists of commands, such as changing the library's mode of operation, importing and exporting cartridges, loading and unloading drives, moving media, performing inventory, and logging off.

- The **Monitor** menu consists of commands that you can use to obtain status information about various aspects of the library, including system, drives, connectivity, I/E stations, storage slots, media, sensors, and users.
- The **Setup** menu consists of commands that you can use to set up and configure various aspects of the library, including partitions, devices, connectivity, network, physical library, users, notifications, date and time, licenses, e-mail, and SNMP trap registration.
- The **Tools** menu consists of commands that you can use to maintain and troubleshoot the library. These tools enable you to work with RAS tickets, drives, and connectivity. They also enable you to capture snapshots, update software, teach the library, save and restore library configurations, run verification tests, and obtain drive resource utilization reports.
- The **View** menu enables you to select the library (either the physical library or a partition) that you want currently displayed on the main LMC display. Some LMC menu commands require you to be in either a physical library or partition view to run them.
- The **Connection** menu enables you to log on to multiple libraries and switch between consoles for different libraries without logging off.
- The **Help** menu provides you with access to Online Help as well as information about the library, such as copyright information, the product version, firmware version, and build information for various library components (LMC server, LMC client, MCB, CMB, and RCU).

Table 37 on page 435 summarizes all available commands, including required user privilege levels and required library environments (touch screen or remote client). The LMC prompts you to take the library offline or to select either the physical library or a partition if the command you request requires you to change library mode.

System status buttons are located at the bottom of the library information panel. If the touch screen remains unused after a period of time, the library screen saver appears. The color of the screen saver image reflects the status of the library as indicated by the system status buttons. For example, if system status buttons show a mix of green (Good), yellow (Warning or Degraded), and red (Failed) states, the color of the screen saver image will be red.

Table 37 Menu Commands: Privileges and Environments

Menu Command	Privilege Level	Physical Library View	Partition View	Touch Screen	Remote
Operations menu:					
Change Mode	Admin, User[1]	X	X	X[2]	X[3]
Import[4]	Admin, User[1]		X	X	X
Export[4]	Admin, User[1]		X	X	X
Drives[4]	Admin, User[1]		X	X	X
Load[4]	Admin, User[1]		X	X	X
Unload[4]	Admin, User[1]		X	X	X
Move Media	Admin, User[1]		X	X	X
Inventory	Admin, User[1]	X[5]	X[4, 6]	X	X
System Shutdown	Admin	X			
Log Off	Admin, User, Guest	X	X	X	X
Monitor menu:					
System	Admin, User[1]	X	X	X	X
Drives	Admin, User[1]	X	X	X	X
Connectivity	Admin, User[1]	X		X	X
IO Blade	Admin, User[1]	X		X	X

1 Users can use this command only from partitions to which they have privileges. 2 Shutdown is available to administrators only. 3 Affected partition must be offline. 4 Physical library must be offline. 5 Physical library must be online. 6 Feature is configurable from the library's touch screen only, but the configuration is viewable from the touch screen or remote client. 7 Appears on the library's touch screen only. 8 Depending on operation, physical library or relevant partition must be offline. 9 Available only on libraries with I/O blades installed. 11 Guest can view the main LMC display, but cannot obtain more details or perform operations.

Menu Command (Continued)	Privilege Level	Physical Library View	Partition View	Touch Screen	Remote
Fibre Channel	Admin, User[1]	X		X	X
Ethernet Blade	Admin, User	X		X	X
IE Station	Admin, User[1]	X		X	X
Slots	Admin, User[1]	X	X	X	X
Media	Admin, User[1]	X	X	X	X
Sensors	Admin, User[1]	X	X	X	X
E-Mail Configuration Record	Admin, User[1]	X		X	X
Users	Admin, User[1]	X	X	X	X
Partitions...	Admin, User[1]	X	X	X	X
Status	Admin, User[1]	X	X	X	X
Policies	Admin	X	X	X	X
EKM Servers	Admin, User	X	X	X	X

1 Users can use this command only from partitions to which they have privileges. 2 Shutdown is available to administrators only. 3 Affected partition must be offline. 4 Physical library must be offline. 5 Physical library must be online. 6 Feature is configurable from the library's touch screen only, but the configuration is viewable from the touch screen or remote client. 7 Appears on the library's touch screen only. 8 Depending on operation, physical library or relevant partition must be offline. 9 Available only on libraries with I/O blades installed. 11 Guest can view the main LMC display, but cannot obtain more details or perform operations.

Menu Command (Continued)	Privilege Level	Physical Library View	Partition View	Touch Screen	Remote
Setup menu:					
Setup Wizard	Admin	X		X	X
Partitions[5]	Admin	X		X	X
Configure	Admin	X		X	X
Control Path	Admin	X		X	X
Automated Media Pool	Admin	X		X	X
Assign Magazines	Admin	X		X	X
Assign Media	Admin	X		X	X
Policies	Admin	X		X	X
EDLM Configuration					
Active Vault Configuration					
StorNext Access					
Drives	Admin, User[1]	X	X	X	X
SCSI ID's[4]	Admin, User[1]		X	X	X
FC Settings	Admin				
Access	Admin	X		X	X
Data Path Failover	Admin	X		X	X
SNW Wizard	Admin	X		X	X
Blades					

1 Users can use this command only from partitions to which they have privileges. 2 Shutdown is available to administrators only. 3 Affected partition must be offline. 4 Physical library must be offline. 5 Physical library must be online. 6 Feature is configurable from the library's touch screen only, but the configuration is viewable from the touch screen or remote client. 7 Appears on the library's touch screen only. 8 Depending on operation, physical library or relevant partition must be offline. 9 Available only on libraries with I/O blades installed. 11 Guest can view the main LMC display, but cannot obtain more details or perform operations.

Menu Command (Continued)	Privilege Level	Physical Library View	Partition View	Touch Screen	Remote
Access					
Channel Zoning	Admin	X		X	X
FC Host	Admin	X		X	X
LUN Mapping Wizard	Admin	X		X	X
Connectivity	Admin	X		X	X
Port Configuration	Admin	X		X	X
Datapath Conditioning	Admin	X		X	X
FC Host Port Failover	Admin	X		X	X
Network Configuration[7]	Admin	X		X	
IPv4 Configuration	Admin	X		X	X
IPv6 Configuration	Admin	X		X	X
DNS Configuration...	Admin	X		X	X
System Settings	Admin	X		X	X
Physical Library	Admin	X		X	X
Aisle Lights	Admin	X		X	X
Preferences	Admin	X		X	X
Health Check Intervals	Admin	X		X	X
Camera Host/IP...	Admin	X		X	X
User Configuration	Admin	X		X	X

1 Users can use this command only from partitions to which they have privileges. 2 Shutdown is available to administrators only. 3 Affected partition must be offline. 4 Physical library must be offline. 5 Physical library must be online. 6 Feature is configurable from the library's touch screen only, but the configuration is viewable from the touch screen or remote client. 7 Appears on the library's touch screen only. 8 Depending on operation, physical library or relevant partition must be offline. 9 Available only on libraries with I/O blades installed. 11 Guest can view the main LMC display, but cannot obtain more details or perform operations.

Menu Command (Continued)	Privilege Level	Physical Library View	Partition View	Touch Screen	Remote
Local Users	Admin	X		X	X
LDAP	Admin	X		X	X
Notifications	Admin	X		X	X
System Setup	Admin	X		X	X
Media Security	Admin	X		X	X
Partition Utilization	Admin	X		X	X
Trap Registration	Admin	X		X	X
Tickets Filter	Admin	X		X	X
Date and Time	Admin	X		X	X
Licenses	Admin	X		X	X
Email Configuration	Admin	X		X	X
Security[8]	Admin	X		X	
Drive Cleaning	Admin	X		X	X
Encryption	Admin	X		X	X
Server Configuration	Admin	X		X	X
Partition Configuration	Admin	X		X	X

1 Users can use this command only from partitions to which they have privileges. 2 Shutdown is available to administrators only. 3 Affected partition must be offline. 4 Physical library must be offline. 5 Physical library must be online. 6 Feature is configurable from the library's touch screen only, but the configuration is viewable from the touch screen or remote client. 7 Appears on the library's touch screen only. 8 Depending on operation, physical library or relevant partition must be offline. 9 Available only on libraries with I/O blades installed. 11 Guest can view the main LMC display, but cannot obtain more details or perform operations.

Menu Command (Continued)	Privilege Level	Physical Library View	Partition View	Touch Screen	Remote
Tools menu:					
Tickets	Admin	X	X	X	X
Drives[5]	Admin	X		X	X
Connectivity	Admin	X		X	X
Capture Snapshot	Admin	X		X	X
Update Software[9]	Admin	X	X	X	X
Library	Admin	X	X	X	X
Drives	Admin	X	X	X	X
Plug-in	Admin	X	X	X	X
Teach[5]	Admin	X		X	X
Save/Restore[5]	Admin	X		X	X
Verification Tests	Admin	X		X	X
Reports	Admin	X	X	X	X
Reporting Options	Admin	X	X		
Drive Utilization	Admin	X	X		X
Tickets	Admin	X	X		X
LUN Mapping	Admin	X	X		X

1 Users can use this command only from partitions to which they have privileges. 2 Shutdown is available to administrators only. 3 Affected partition must be offline. 4 Physical library must be offline. 5 Physical library must be online. 6 Feature is configurable from the library's touch screen only, but the configuration is viewable from the touch screen or remote client. 7 Appears on the library's touch screen only. 8 Depending on operation, physical library or relevant partition must be offline. 9 Available only on libraries with I/O blades installed. 11 Guest can view the main LMC display, but cannot obtain more details or perform operations.

Menu Command (Continued)	Privilege Level	Physical Library View	Partition View	Touch Screen	Remote
Media	Admin	X	X		X
Integrity Analysis	Admin	X	X		X
Usage	Admin	X	X		X
Security	Admin	X	X		X
Moves	Admin	X	X		X
Library Configuration	Admin	X	X		X
Partition Utilization	Admin	X			X
Library Explorer	Admin, User[1]	X	X	X	X
Command History Log	Admin	X	X	X	X
IE Stations		X			
Partitions Defragmentation		X			
EKM Management	Admin	X	X	X	X
Import Communication Certificates	Admin	X	X	X	X
Encryption Certificate	Admin	X	X	X	X
Import	Admin	X	X	X	X
Export	Admin	X	X	X	X
Encryption Key	Admin	X	X	X	X
Import	Admin	X	X	X	X
Export	Admin	X	X	X	X

1 Users can use this command only from partitions to which they have privileges. 2 Shutdown is available to administrators only. 3 Affected partition must be offline. 4 Physical library must be offline. 5 Physical library must be online. 6 Feature is configurable from the library's touch screen only, but the configuration is viewable from the touch screen or remote client. 7 Appears on the library's touch screen only. 8 Depending on operation, physical library or relevant partition must be offline. 9 Available only on libraries with I/O blades installed. 11 Guest can view the main LMC display, but cannot obtain more details or perform operations.

Menu Command (Continued)	Privilege Level	Physical Library View	Partition View	Touch Screen	Remote
Retrieve SKM Logs	Admin	X	X	X	X
EKM Audit Report	Admin	X	X	X	X
EDLM	Admin	X		X	X
Test Selection	Admin	X		X	X
Test Reports	Admin	X		X	X
Status	Admin	X		X	X
Sift Sort	Admin	X	X	X	X
Export...	Admin	X	X	X	X
Capture Report...	Admin	X	X	X	X
Retrieve MIBs	Admin	X		X	X
Library	Admin	X	X	X	X
Robot State	Admin	X	X	X	X
Towers...	Admin	X	X	X	X
View menu:					
[physical library name] **(Physical)**	Admin, User, Guest[11]	X	X	X	X
[partition name] **(Partition)**	Admin, User, Guest[11]	X	X	X	X
Views...	Admin, User, Guest[11]	X	X	X	X

1 Users can use this command only from partitions to which they have privileges. 2 Shutdown is available to administrators only. 3 Affected partition must be offline. 4 Physical library must be offline. 5 Physical library must be online. 6 Feature is configurable from the library's touch screen only, but the configuration is viewable from the touch screen or remote client. 7 Appears on the library's touch screen only. 8 Depending on operation, physical library or relevant partition must be offline. 9 Available only on libraries with I/O blades installed. 11 Guest can view the main LMC display, but cannot obtain more details or perform operations.

Menu Command (Continued)	Privilege Level	Physical Library View	Partition View	Touch Screen	Remote
Connection menu:					
New	Admin, User, Guest	X			X
[library IP address]	Admin, User, Guest	X			X
Help menu:					
Content	Admin, User	X	X	X	X
About	Admin, User, Guest	X	X	X	X

1 Users can use this command only from partitions to which they have privileges. 2 Shutdown is available to administrators only. 3 Affected partition must be offline. 4 Physical library must be offline. 5 Physical library must be online. 6 Feature is configurable from the library's touch screen only, but the configuration is viewable from the touch screen or remote client. 7 Appears on the library's touch screen only. 8 Depending on operation, physical library or relevant partition must be offline. 9 Available only on libraries with I/O blades installed. 11 Guest can view the main LMC display, but cannot obtain more details or perform operations.

Toolbar

The toolbar consists of icons that represent commonly used commands that also are available on the menus.

The **I/E** button displays a table of the current contents of the I/E station. You also can display the table by clicking **Monitor > IE Station**. For more information, see Monitoring I/E Station Status on page 517.

The **Import** button launches the import of cartridges if the current library is a partition. You also can request an import operation by clicking **Operations > Import**. For more information, see Importing Cartridges Into Partitions on page 683.

The **Export** button launches the export of cartridges if the current library is a partition. You also can request an export operation by clicking **Operations > Export**. For more information, see Exporting Cartridges From Partitions on page 685.

The **Tickets** button displays tickets that the library created when it detected issues within its subsystems. You also can display tickets by clicking **Tools > Tickets**. For more information, see Troubleshooting

Your Library on page 35.

The **Explorer** button provides a graphical presentation of all the drives, cartridges, and slots in the library. The Library Explorer can display all library elements according to physical location in any configuration, from one module to eight modules, and one drive up to the maximum number of 96 drives.

The **Config** button indicates whether you have saved the current library configuration. For more information, see CONFIG Button Alerts on page 589.

The **System Status** button displays a dialog box that has four (4) tabs: Components, Robots, Drives and, if installed, Towers. Each tab indicates the status of the elements and provides a graphical representation of the general status of each area. The button will display a green check mark if all system are online and running normally. It will display a red X if any of the components are offline or failing.

The **Log Off** button logs off the current user after confirming the log off request. You also can log off by clicking **Operations > Log Off**. For more information, see Logging On and Off on page 424.

Reading the Library Information Panel

The library information panel, shown in Figure 39, occupies the central portion of the main LMC display. It provides you with a significant amount of dynamically updated status information.

Figure 39 Library Management Console

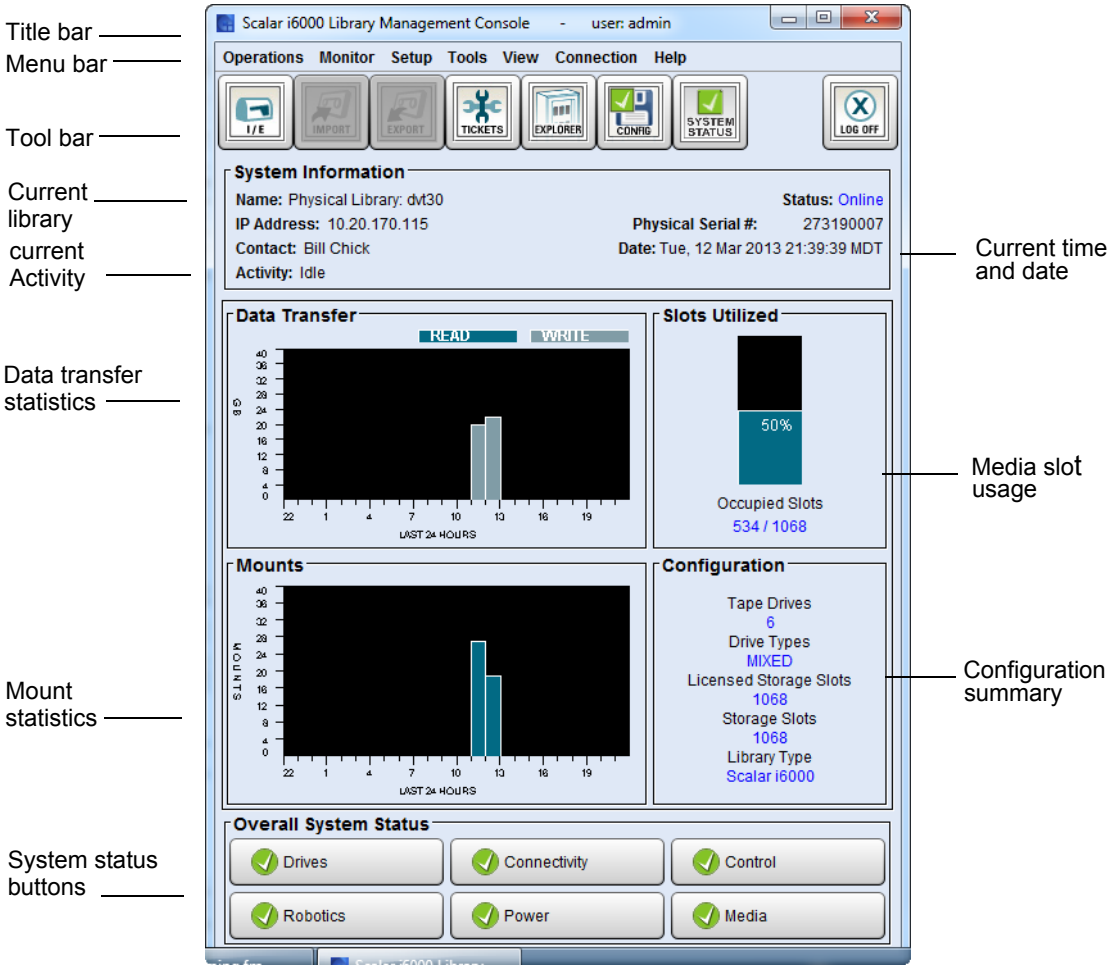


Table 38 describes the areas on the library information panel.

Table 38 Areas on the Library Information Panel

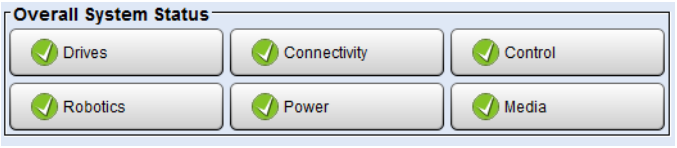
Area	Description
Name	The name of the current library. This is the library that appears with a check mark beside it in the **View** menu. First, the genre of library appears, i.e. physical or partition. Then, after a colon, the name of the library appears.
IP Address	The IP address of the library.
Contact	The name of the customer contact identified in **Setup > Notifications > System Setup**.
Activity	The current activity for the current library.
Status	Online/offline status of the library/partition being viewed.
Physical Serial #	Physical serial number of the library or partition being viewed.
Date	The current date and time. The date that appears reflects user settings, but the system operates according to Greenwich Mean Time (GMT). The displayed time reflects user settings, but the system operates on the GMT zone.
Data Transfer	The bar graph contrasts the amount of data read and written for the past 24 hours. The units being reported appear beside the graph.
Slots Utilized	This graph shows the percentage of occupied media slots in the library or partition, depending on the current view. The number of used media slots appears beneath the graph (occupied slots/total number of storage slots).
Mounts	The bar graph reports mount statistics compiled during the past 24 hours. The library updates this information every five minutes.

Area	Description
Configuration	Configuration summary information is presented textually. Data points reported are: • Number of tape drives • Drive types: AIT, LTO, DLT or—for the physical library only—Mixed • Total number of licensed storage slots (appears only in the physical library view) • Total number of storage slots in the physical library or partition, depending on the current view • Library type • Number of robots (library view only).

System Status Buttons

System status buttons are located in the **Overall System Status** area at the bottom of the LMC (see Figure 40).

Figure 40 System Status Buttons in Good Status



Each button represents a subsystem. Table 45 shows the library subsystems and some of the components that each subsystem represents. Each field replaceable unit (FRU) in the library belongs to one of the subsystems.

Table 39 Subsystems and Their Components

Subsystem	Components
Drives	Drives, such as brick firmware, drive bricks, drive sleds

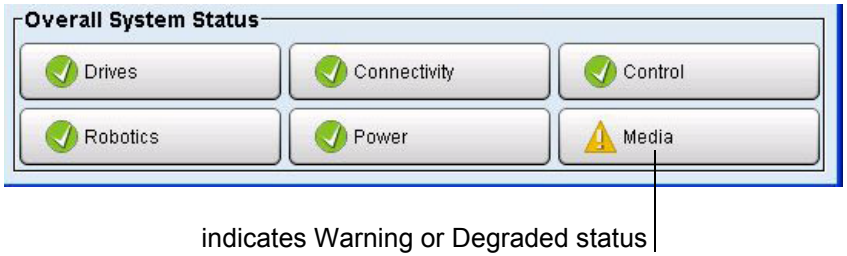
Subsystem	Components
Robotics	Assemblies and processors involved in the movement and handling of library media, such as the IEX board, I/E stations, the pivot and reach assemblies, system barcode labels, doors, filters, the accessor, drive mounts, rails, towers, and carriages
Connectivity	Host connectivity components, such as I/O management units, I/O blades, and the chassis management blade (CMB)
Power	Power supplies and related hardware, such as the power distribution unit (PDU), power chassis, and fuses
Control	Main processor cards and related hardware and software, such as system firmware, the management control blade (MCB), the robotics control unit (RCU), the library motor drive (LMD), and the operator panel
Media	Media components such as cartridges and magazines

Each button displays a status indicator that reveals a Good, Warning, Degraded, or Failed state as follows:

	Good (green)	The library system is in working order; no problems or issues exist.
	Warning *or* Degraded (yellow)	There is a degraded or failed component within this category that requires action, but the overall category still is functioning.
	Failed (flashing red)	A component in this category has failed.

For example, the buttons shown in Figure 40 on page 447 indicate that all subsystems are functioning normally (Good), while those shown in Figure 41 indicate that issues exist in the Media subsystem.

Figure 41 Status Buttons - Drives and Robotics Issues



You can click system status buttons to display additional information about the subsystems. The information that appears depends on the status shown on the button:

- **Good** — Either a message appears informing you that no tickets exist for the subsystem or a list of subsystem tickets appears that are in Closed or Verified states.
- **Warning, Degraded, or Failed** — A list of open tickets for the subsystem appears.

Tickets provide information about issues that the library has detected. For more information, see Using System Status Buttons to Display Ticket Lists on page 45.

Understanding Location Coordinates

This section describes the coordinate addressing system that the library uses to indicate the location of cartridges, drives, and I/O blades in the library.

You can use the **Library Explorer** feature to view a graphical presentation of all the drives, cartridges, and slots in the library. The **Library Explorer** can display all library elements according to physical location in any configuration, from one module to eight modules, and one drive up to the maximum number of 96 drives. For more information on **Library Explorer**, see Using Library Explorer on page 543.

Cartridge Locations

The library uses a coordinate addressing system that indicates the location of cartridges using six coordinates. The coordinates are represented by a comma-separated list.

For example:

1,1,1,1,2,1 = aisle 1, module 1, rack 1, section 1, column 2, row 1

The following list explains each location variable:

- **Aisle** — There is only one aisle in the library. This value is always 1.
- **Module** — There can be up to 12 modules in a Gen 1 single-robotics library (control module plus up to 11 expansion modules. For a Gen 2 single robotics library, there can be up to 12 modules as well. However, these modules can be standard or high-density expansion modules. For a Gen 2 dual-robotics library, there can be up to 17 modules in (left parking module, control module, right parking module, and up to 13 standard or high-density expansion modules).

  Modules are numbered from left to right as you look at the front of the modules The control module is always module 1. In dual-robotics libraries, the left parking module, located to the left of the control module, is module 0.
- **Rack** — There are two rack designations inside each module. These will always be either 1 or 2, with 2 being the inside of the access door.
- **Section** — There are 10 sections in a rack, numbered from top to bottom as you face the rack.
- **Column** — There are four columns in a rack, numbered from left to right as you face the rack. These are numbered between 1 and 4. For an HDEM, there are ten (10) rotating columns.
- **Row** — This is equal to one cartridge slot. The number of rows per section can vary depending on the size of the cartridge. The rows are numbered between 1 and 6 for LTO cartridges.

Note: Tape drives that are installed in rack 1 of a control module or an expansion module replace storage in columns 1 and 2. Because drives are installed from the bottom of the rack to the top, you lose the storage starting in section 10 first. You do not lose the magazine in columns 1 and 2 of section 5.

Note: Column 1 of a single-robotics control module never contains storage. Column 1 of a dual-robotics control module can contain storage.

Note: The cartridges in the 24-slot LTO I/E station are addressed as part of column 3 and are in sections 1 through 4 (top to bottom). When you have an I/E station installed on rack 2, there are no cartridges in columns 3 and 4 of section 5. See Figure 44 on page 453.

Note: In Figure 44 on page 453, the five magazines shown in column 4, sections 6-10 do not exist in a single-robot control module. However, these magazines exist in expansion modules.

Figure 42 shows aisle, module, and rack numbering.

Figure 43 on page 452 shows section, column, and row numbering for rack 1 of a library that contains LTO cartridges.

Figure 44 on page 453 shows the section, column, and row numbering for rack 2 of a library that contains LTO cartridges.

Figure 45 on page 454 shows examples of location coordinates.

Figure 42 Aisle, Module, and Rack Numbering Locations

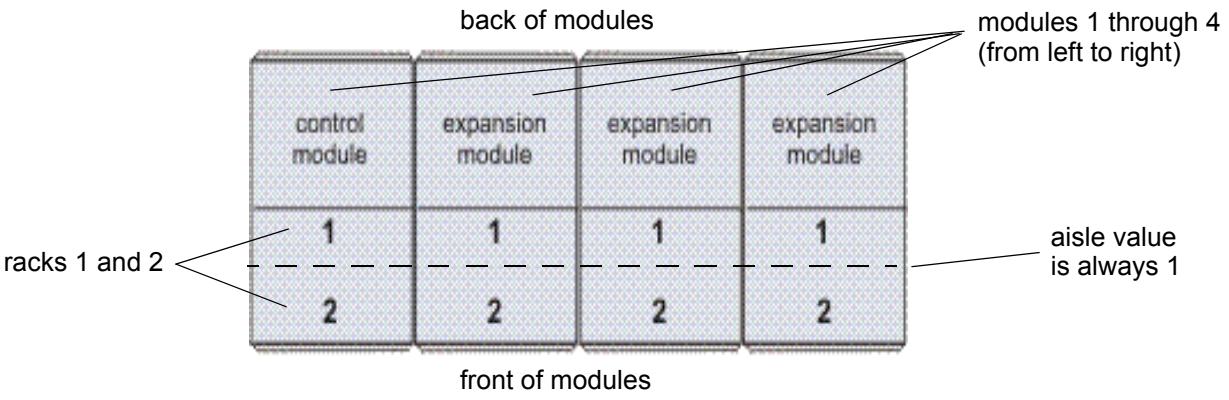


Figure 43 Section, Column, and Row Numbering for Rack 1 - LTO Cartridges

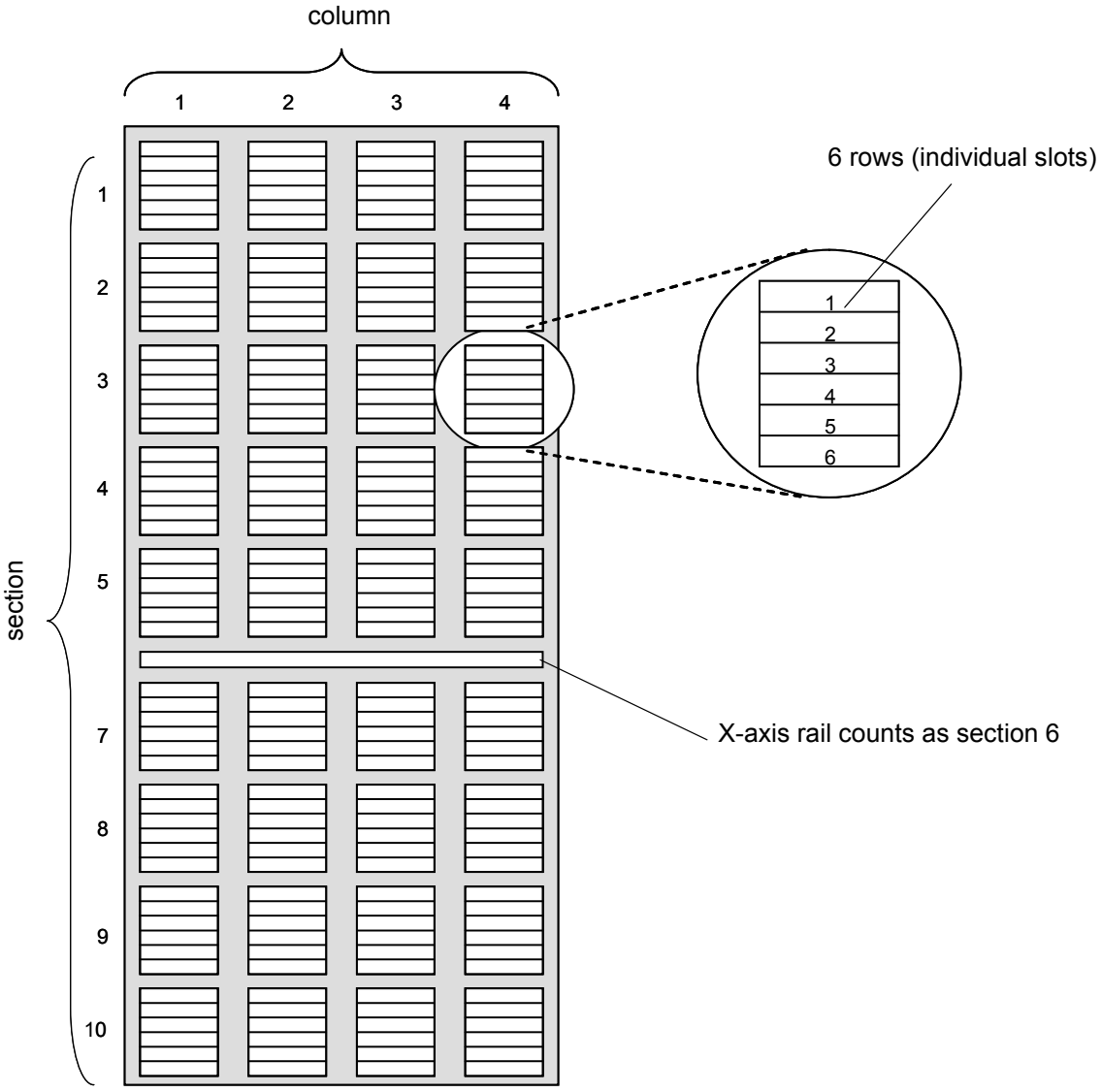


Figure 44 Section, Column, and Row Numbering for Rack 2 - LTO Cartridges

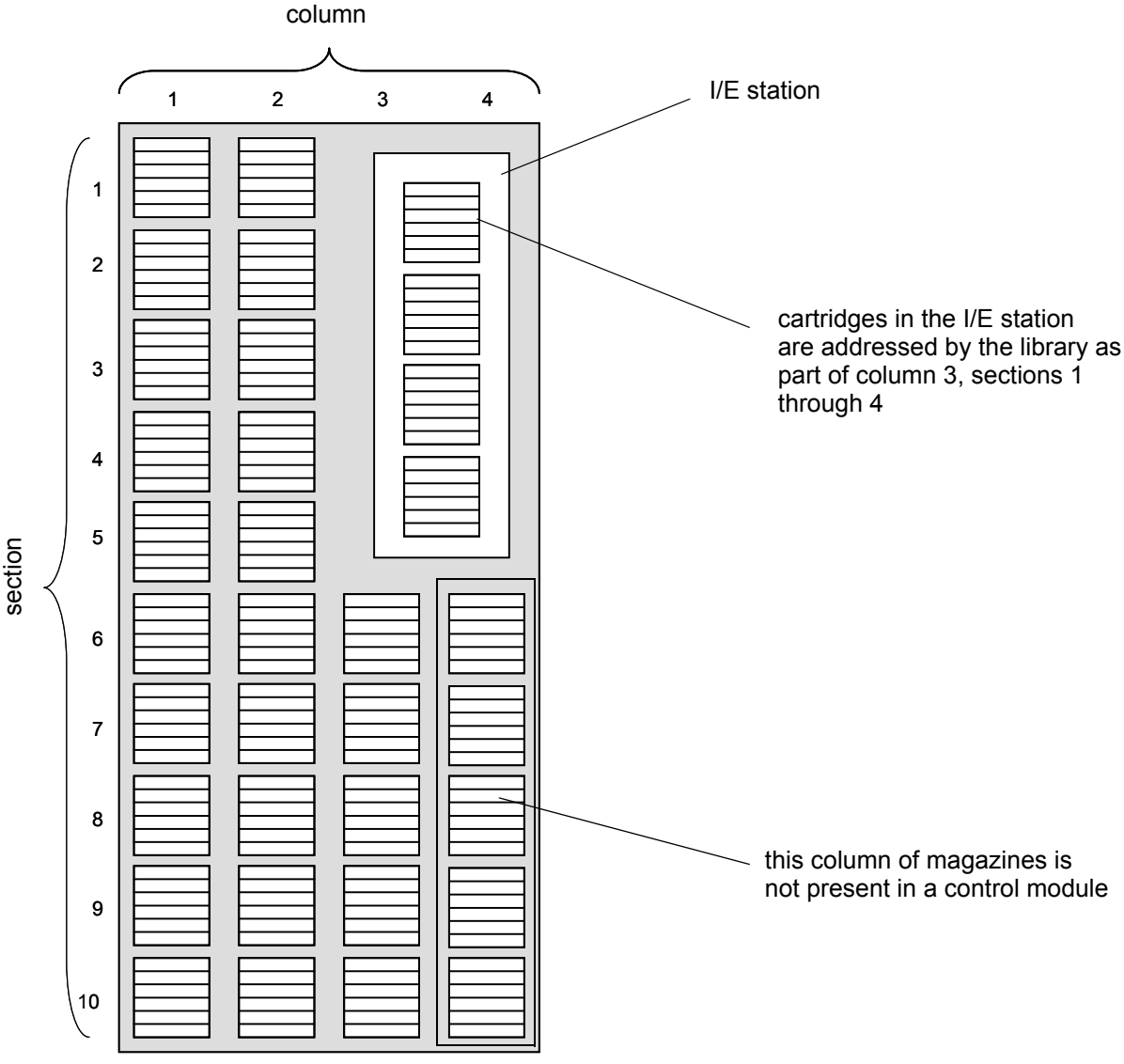
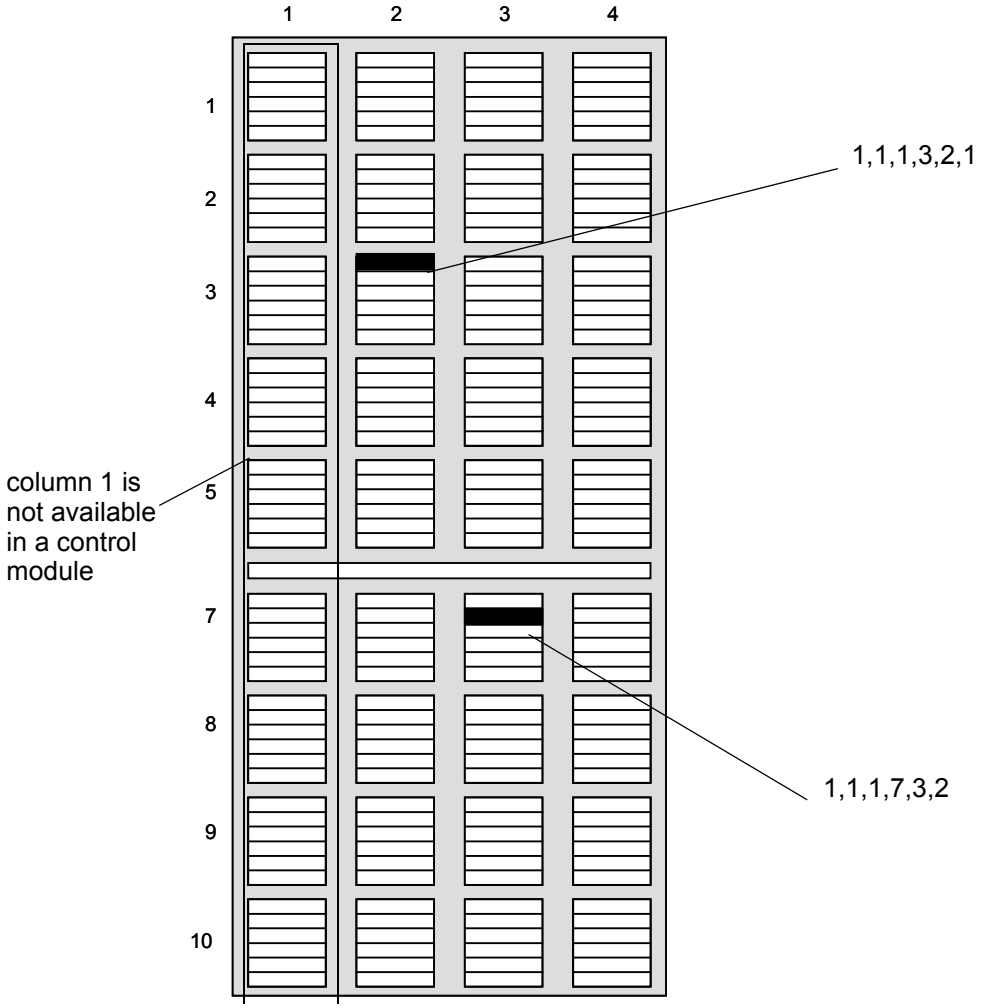


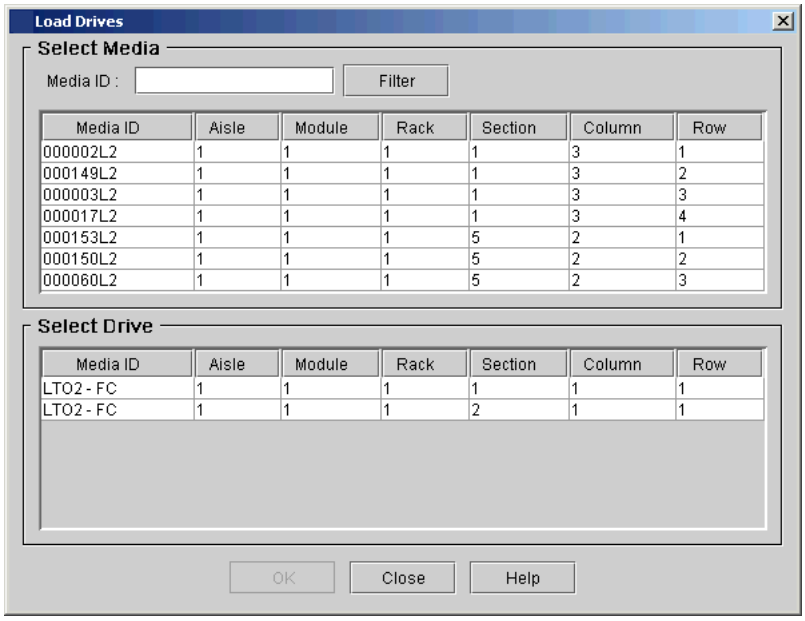
Figure 45 Example - Storage Location Coordinates for Aisle 1, Module 1, and Rack 1

This example assumes that the linear storage is located in aisle 1, module 1, and rack 1. That is why the first three numbers in the coordinate value are 1,1,1. The last three numbers represent the address on the linear storage assembly.



The LMC uses dialog boxes, like the one shown in Figure 46, that enable you to specify cartridge locations. These coordinates are reported in parenthetical format with each element separated by commas. In parenthetical format, the location of cartridge 000002L2, shown in the **Load Drives** dialog box below, is (1,1,1,1,3,1).

Figure 46 Coordinates in Load Drives Dialog Box



Tape Drive Location Coordinates

The location coordinates of a drive is based on the position of the drive in the module and section. The location coordinates are: aisle, module, rack, section, column, and row, defined the same as for other library components (see Cartridge Locations on page 450).

- Tape drives are always in rack 1, column 1, of a particular module. (Columns are numbered from left to right as you face the rack). See Figure 48 on page 458.
- Drives may be installed in any module except high-density expansion modules and the left parking module.
- Because all drives in the library are full-height drives, each drive is in row 1 of the designated section.

- The library can accommodate two drive clusters per rack (an upper and a lower). Each drive cluster contains up to six drives. Drives are numbered from bottom to top. Drive location 1 is in the lowest section of the lower drive cluster. Drive location 12 is the uppermost section of the upper drive cluster.

Table 40 shows the possible drive location coordinate ranges.

Table 40 Possible Drive Location Coordinate

Aisle	Module	Rack	Section	Column	Row
1	1 – 16	1	1 – 12	1	1

Figure 48 on page 458 shows the physical location of drive 9, which is the last drive listed in the **Move Media** dialog box shown in Figure 47 on page 457.

Figure 47 Example - Drive Location Coordinates

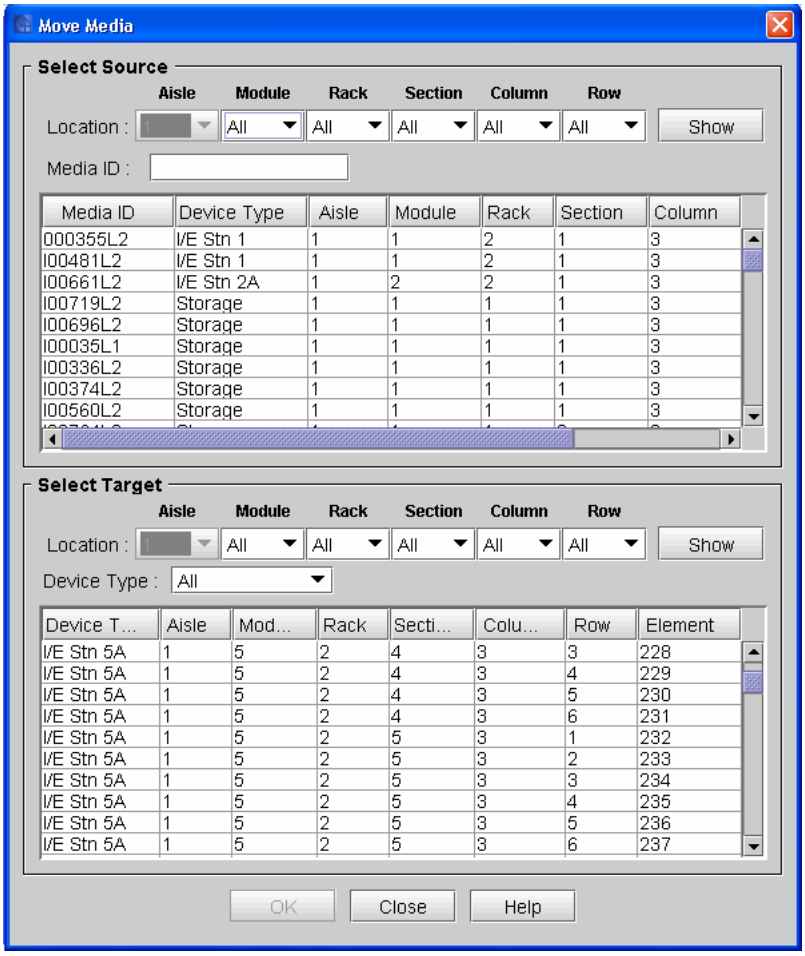
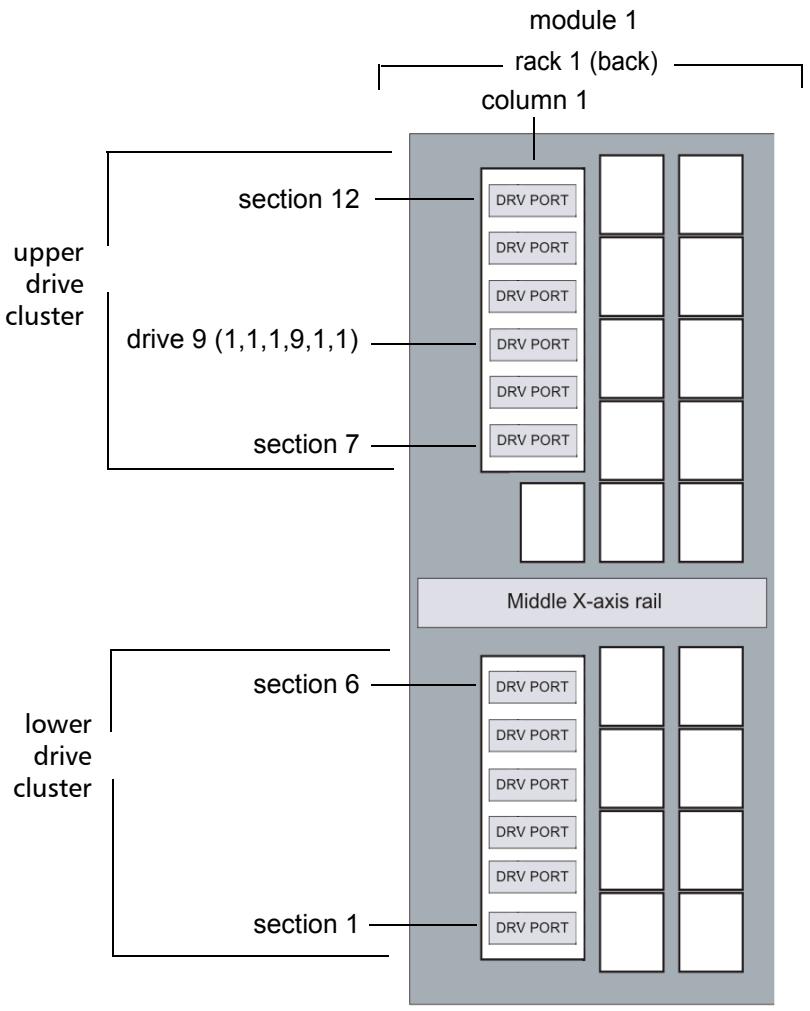


Figure 48 Drive Location Coordinate Numbering and Example in Module 1, Rack 1



I/O Blade Locations

I/O blades are located in the I/O management unit. The LMC displays I/O blade locations in parenthetical format. The location coordinates are aisle, module, rack, cluster, and bay, defined as follows:

- **Aisle, Module, and Rack** — The definitions the same as for other library components (see Cartridge Locations on page 450).
- **Cluster** — Refers to the I/O management unit and is always 1.

- **Bay** — The bays in the I/O management unit as viewed from the rear of the library. There are eight bays in the I/O management unit. Bay 1 is on the lower left and is not populated. Bay 2 always contains the control management blade (CMB). Bays 3 through 6 can contain FC I/O blades and bays 7 and 8 can contains Ethernet Expansion blades. See Figure 49.

Figure 49 I/O Management Unit Bay Numbering

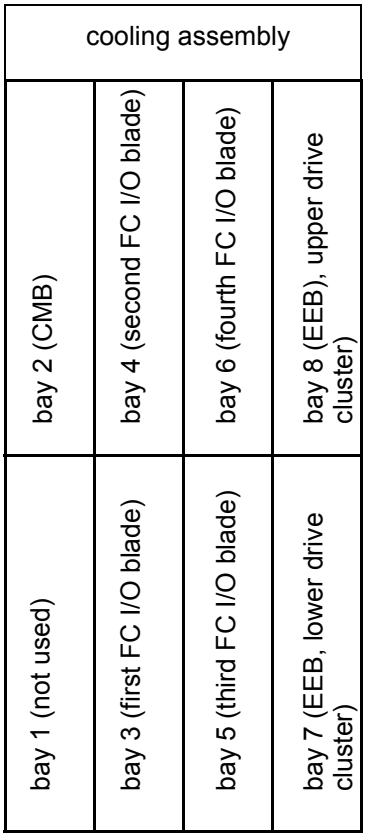


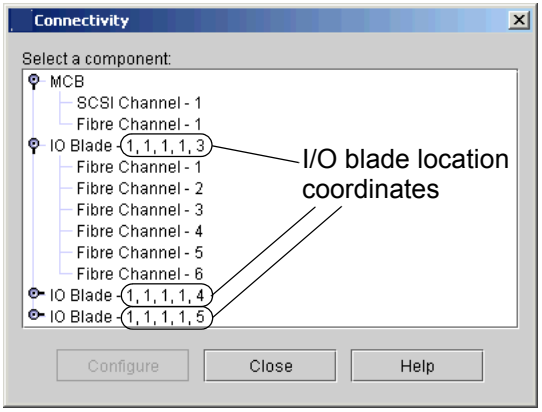
Table 41 lists the range of possible FC I/O blade or EEB location coordinates.

Table 41 FC I/O Blade/EEB Location Coordinates

1	**1-16**	**1**	**1**	**3-8**
Aisle	Module	Rack	Cluster	Bay

Figure 50 shows an example of I/O blade location coordinates. The location for the first I/O blade listed in the **Connectivity** dialog box is reported as (1,1,1,1,3). This I/O blade is located in bay 3 of the left-most module.

Figure 50 Example - I/O Blade Location Coordinates



I/E Station Locations

The location coordinates of an I/E station is based on the position of the module that contains the I/E station. I/E stations are also distinguished by whether they are an I/E stations or a HiCap I/E station.

- Single I/E Station: Designated by stating the module that contains it (see Figure 51 on page 461).
- HiCap I/E Station: Designated by the modules that contains it but since there are two I/E station doors, further designated by an A (left) and B (right) (see Figure 52 on page 462).

Figure 51 I/E Station Location

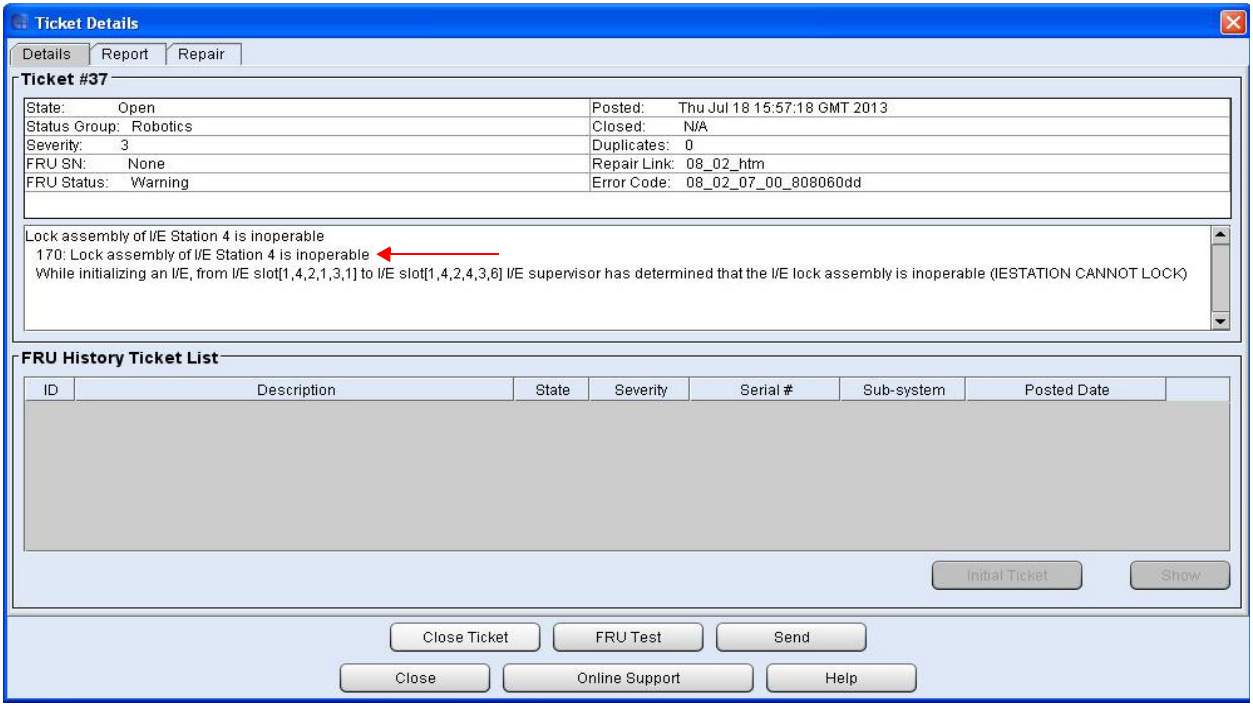
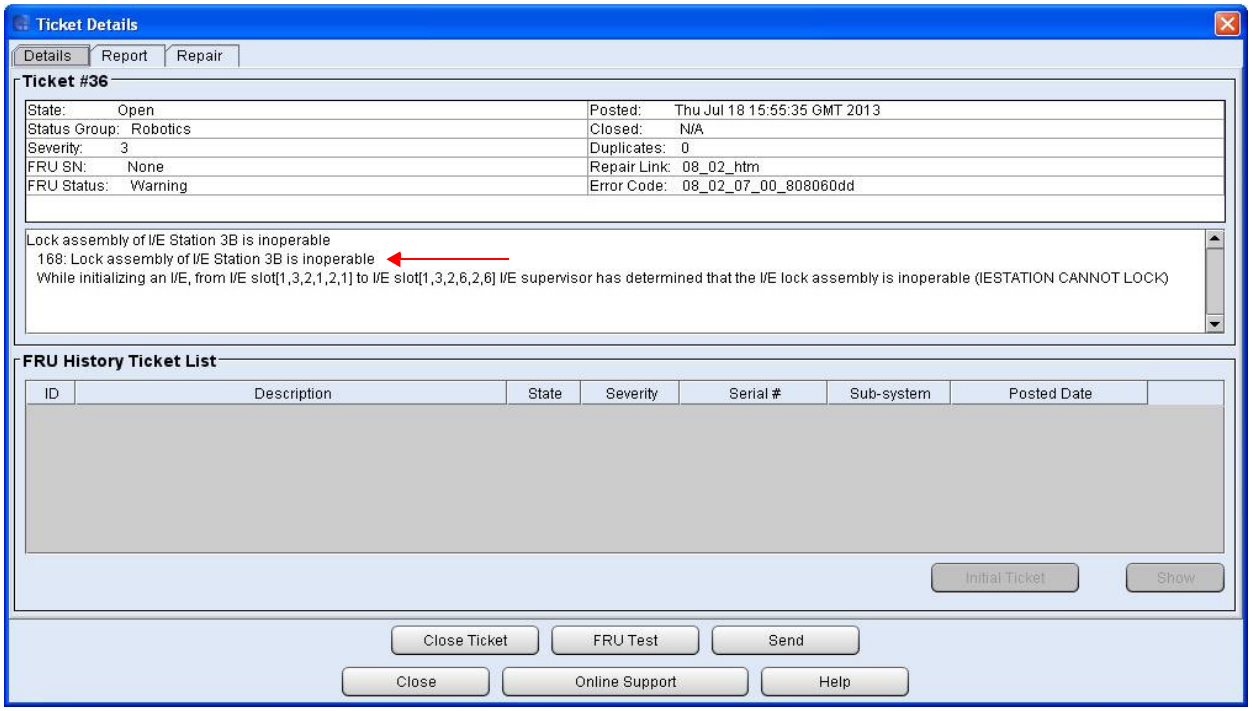


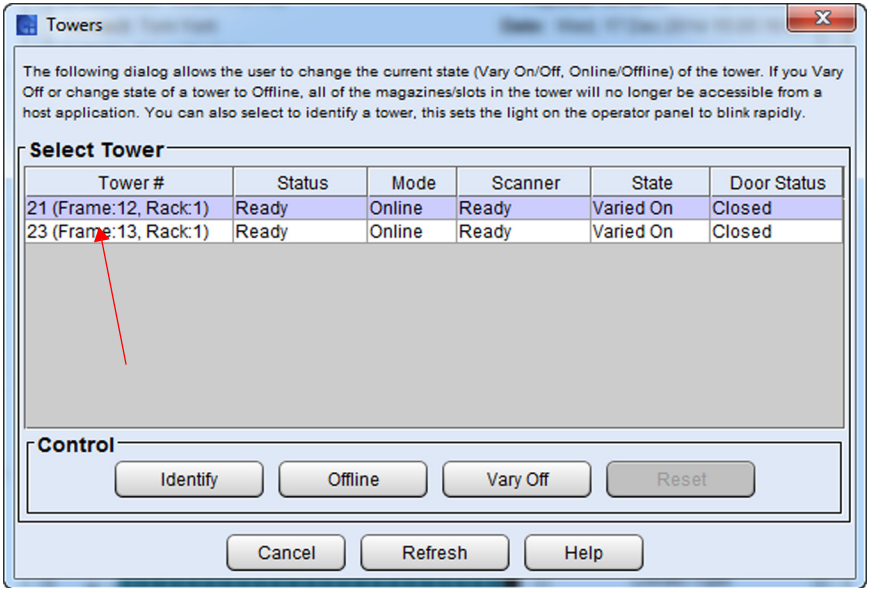
Figure 52 HiCap I/E Station Location



Tower Locations

The location coordinates of a tower is based on the number of towers in the library and it's overall position in the library. The location coordinates are: tower # (module and rack), as indicated in the **Towers** dialog box (see Figure 53 on page 463).

Figure 53 Tower Location Coordinates



Viewing the Library (Physical or Partition)

The **View** menu enables you to view details about the physical library or a specific partition in the library information panel area of the main LMC display. It also provides access to the **Manage Views** dialog box from which you can quickly select between library views (physical or individual partitions) and take the physical library or a partition online or offline.

Note: Before you can begin many of the library operations that this guide describes, you must first set the library view to either the physical library or a partition.

Displaying the Physical Library or a Partition

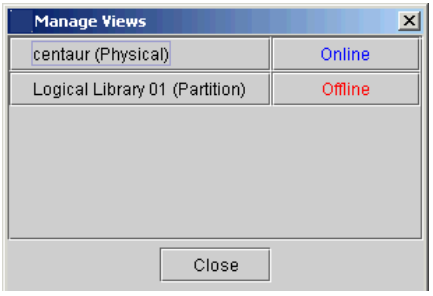
From the **View** menu, click the name of the physical library or a partition. The physical library is listed at the top of the **View** menu. Individual partitions, if they exist, are listed below the physical library.

After you select a library view, the library information panel area of the main LMC display shows status information and statistical details about the physical library or partition.

Managing Library Views

The **Manage Views** dialog box enables you to quickly select between library views (physical or individual partitions) and take the physical library or a partition online or offline. If you are using the LMC from a remote client, you can keep this dialog box in view while you use the LMC to perform other library operations.

1 Click **View** > **Views**. The **Manage Views** dialog box appears with the physical library and any existing partitions listed. It also shows the current online or offline mode of each.



It is recommended that you keep this dialog box displayed to quickly manage library views and change online/offline modes as required by many library operations.

2 To change the library view, click the button with the name of the physical library or partition you want to view.

After you select a library view, the library information panel area of the main LMC display shows status information and statistical details about the physical library or partition.

To take the physical library or a partition online or offline, click the button in the right column that corresponds with the physical library or partition. The **Change Library Mode** dialog box appears.

Note: You do not need to change the current library view to change the online or offline state of the physical library or a partition.

For more information about using this dialog box to change online or offline mode, see Changing the Library's State on page 465.

Changing the Library's State

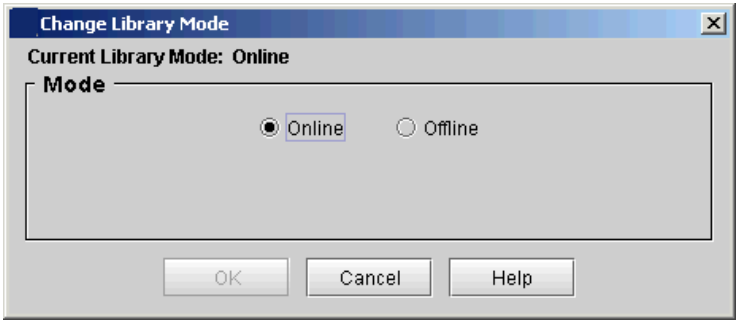
You can take the physical library or any of its partitions online or offline. Some library functions require that the physical library or partitions be in an online or offline state. You also can shut down the physical library from the library's touch screen.

Shutting down the library only prepares it to be powered off. You will use the shutdown procedure in some circumstances to prepare the library for remove and replace procedures. For more information about shutting down the library, see Shutting Down/Rebooting the Library on page 475.

Taking the Physical Library or a Partition Online or Offline

To take the physical library online or offline, change its mode.

1. Make sure that you are viewing the physical library or the partition that you want to take online or offline. From the **View** menu, click the name of the physical library or the appropriate partition.
2. Click **Operations > Change Mode**. The **Change Library Mode** dialog box appears with the current state of the physical library or partition shown.



- You can select the **Online** button to take either the physical library or a partition, depending on the current view, to an online state, which is the normal operating condition. In this mode, the robotics are enabled and all host commands are processed.
- You can select the **Offline** button to take either the physical library or a partition, depending on the current view, to an offline state. If only the physical library is taken offline, the library's partitions will not process robotics commands, even though they are online. If only a partition is taken offline, neither the physical library nor the other partitions are affected.

3 Select either **Online** or **Offline**, and then click **OK**.

4 If you selected **Offline**, a message appears that asks you whether you want to continue. If you are sure that all backup applications are not using the library, click **Yes**.

Online and Offline Functionality

Some library functions require the physical library or partitions to be in a particular state (either online or offline) before they can be performed. If you choose a function that requires the library or partition state to be changed from its current state, you are prompted to do so.

Table 42 on page 467 summarizes the library functions that require the physical library or partitions to be either online or offline.

Table 42 Library Functions Requiring Online or Offline State

Function	Physical Library	Partition
Operations > Import **Operations > Export** **Operations > Drives > Load** **Operations > Drives > Unload** **Operations > Move Media** **Operations > Inventory** (partition view) **Setup > Partitions** (create, modify, or delete)	Online	Offline
Setup > Device > IDs **Tools > Partitions Defragmentation**	—	Offline
Operations > Inventory (physical library view) **Tools > Teach** **Tools > Save/Restore** (restore, revert, or rescue) **Tools > Verification Tests** (start test) **Tools > Update Software** (update or reinstall library software) **Service > Manual Diagnostics**	Offline	—
Tools > Update Software (set up autoleveling or update drive firmware) **Tools > Update Drive Firmware**	(Offline) Current view (library or partition) must be offline	

Working With Local User Accounts

You can set up three levels of user accounts: guest, user, and administrator. Guests see only the main LMC display. Local Users can operate a partition, but cannot run diagnostic tools, which require access to the physical library. Administrators can access the entire physical library and all of its partitions. For a summary of user privileges defined by physical library, partition, and command menu, see Table 37

on page 435.

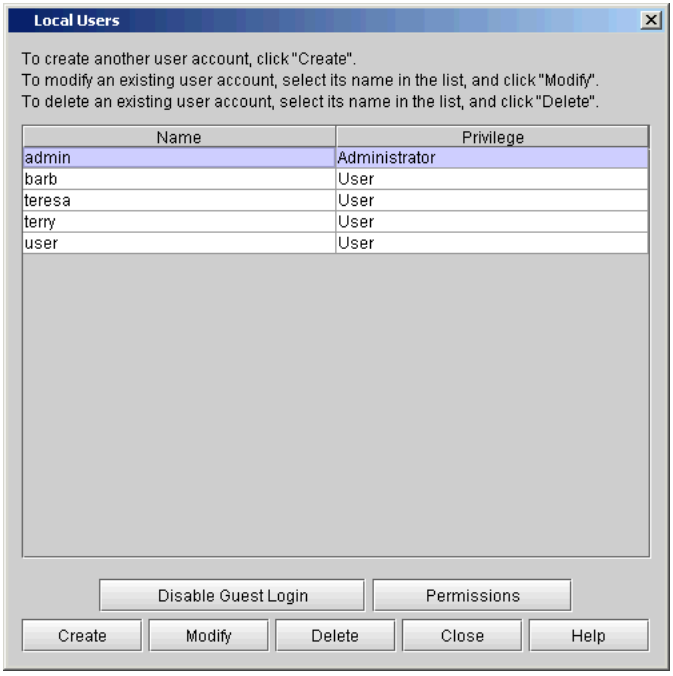
For information on user accounts that reside on a Lightweight Directory Access Protocol (LDAP) server, see Using LDAP on page 231.

Creating Local User Accounts

1 Log on as an administrator.

2 Make sure that you are viewing the physical library. From the **View** menu, click the name of the physical library.

3 Click **Setup > User Configuration > Local Users**. The **Local Users** dialog box appears.

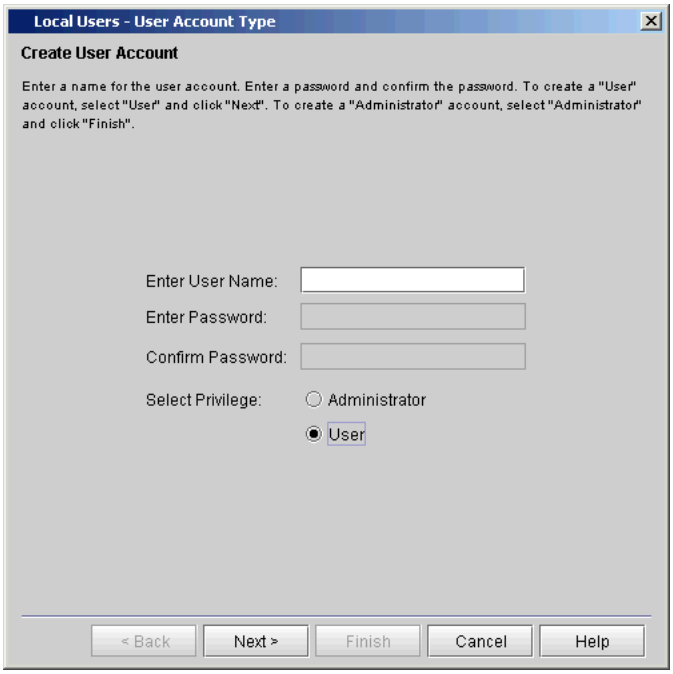


4 To prevent guest login privileges on the library, you must click **Disable Guest Login**. You can toggle between **Disable Guest Login** and **Enable Guest Login**.

Note: For a list of commands that are available to users logging on to the library as a guest, see Table 37 on page 435.

5 To create a user account, click **Create**.

The **Local Users - User Account Type** dialog box appears.



6 In the **Enter User Name** text box, type a user name.

Note: User accounts with the names **guest**, **admin**, and **service** are reserved. You cannot use these names for user accounts.

7 In the **Enter Password** text box, type a password.

Note: Passwords that are most secure include a combination of letters, numbers, and non-alphanumeric characters. Passwords must be eight or more characters in length. The word **password** is not available for use.

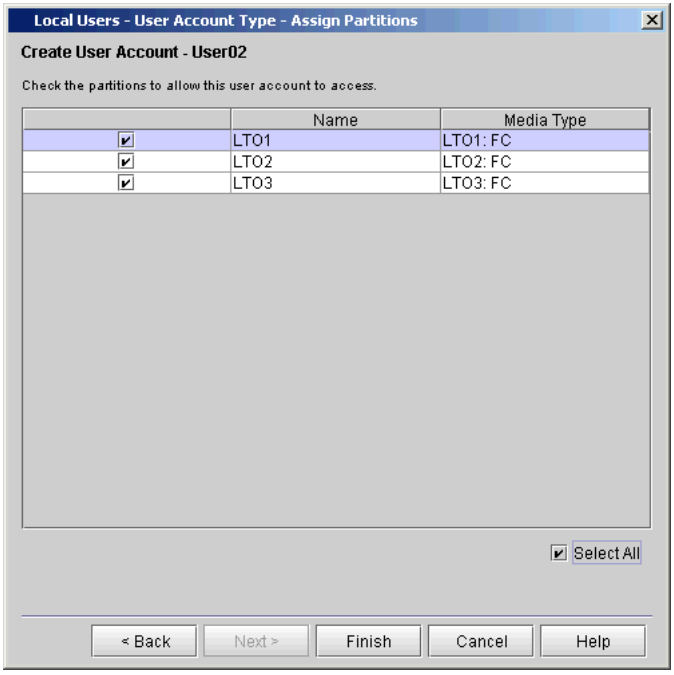
8 In the **Confirm Password** text box, type the password again.

9 For **Select Privilege**, select a privilege level (**Administrator** or **User**).

Note: For a list of commands that are available to administrators and users, see Table 37 on page 435.

10 Perform one of the following tasks:

- If you selected **Administrator**, the **Finish** button becomes available. To register your user account selections, click **Finish**, and then skip the remaining information in this procedure.
- If you selected **User**, click **Next**. The **Local Users - User Account Type - Assign Partitions** dialog box appears.



11 On the **Local Users - User Account Type - Assign Partitions** dialog box, select the check boxes to the left of the libraries to which you want the user to have access, or select the **Select All** check box to give the user access to all listed libraries.

12 To register your user account selections, click **Finish**.

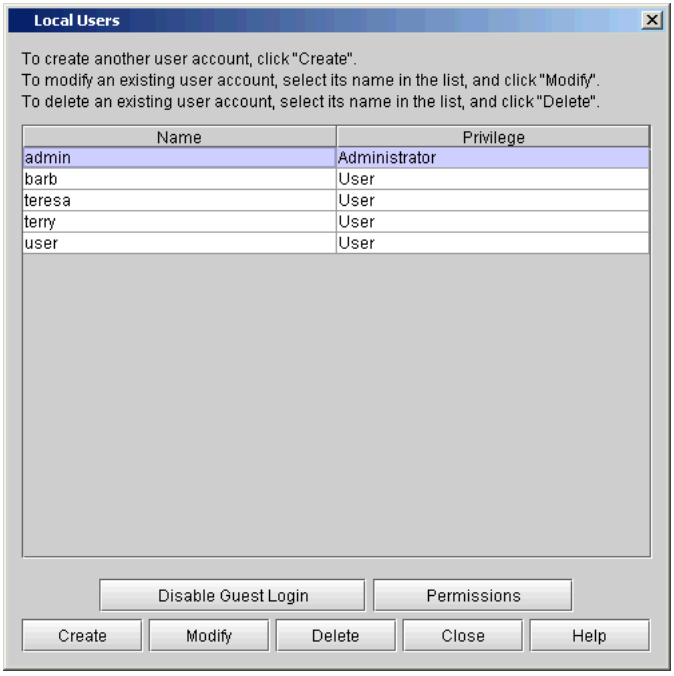
Note: The **Back** button enables you to go back to a previous dialog box and make changes to your selections.

Modifying Local User Accounts

1 Log on as an administrator.

2 Make sure that you are viewing the physical library. From the **View** menu, click the name of the physical library.

3 Click **Setup > User Configuration > Local Users**. The **Local Users** dialog box appears.



Note: If you want to modify guest privileges, you can toggle between **Enable Guest Login** and **Disable Guest Login**. For a list of commands that are available to users logging on to the library as a guest, see Table 37 on page 435.

4 Click the name of the account that you want to modify to highlight it, and then click **Modify**. The following dialog box appears.

5 If you want to change the user account password, type a new password in both the **Enter Password** and **Confirm Password** text boxes. Otherwise, proceed to the next step.

Note: Passwords that are most secure include a combination of letters, numbers, and non-alphanumeric characters. Passwords must be eight or more characters in length. The word "password" is not available for use.

It is recommended that you change all account passwords periodically.

---

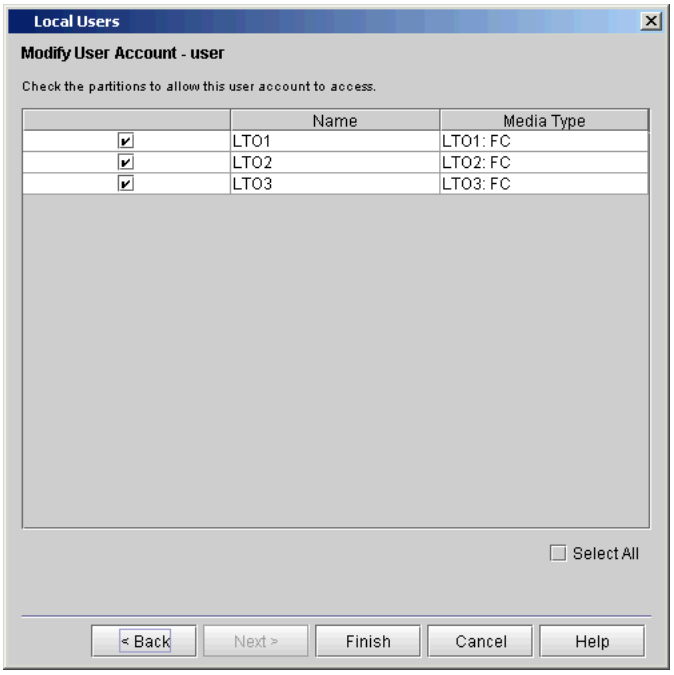
6 If you want to change the privilege level of this user account, select the appropriate privilege level (**Administrator** or **User**). Otherwise, proceed to the next step.

Note: For a list of commands that are available to administrators and users, see Table 37 on page 435.

---

7 Perform one of the following tasks:

- If **Select Privilege** is set to **Administrator**, the **Finish** button is available. To register your user account changes, click **Finish**, and then skip the remaining information in this procedure.
- If **Select Privilege** is set to **User**, click **Next**. The following dialog box appears.



8 On this dialog box, select the check boxes to the left of the libraries to which you want the user to have access, or select the **Select All** check box to give the user access to all listed libraries.

9 To register your user account selections, click **Finish**.

Note: The **Back** button enables you to go back to a previous dialog box and make changes to your selections.

Deleting Local User Accounts

1 Log on as an administrator.

2 Make sure that you are viewing the physical library. From the **View** menu, click the name of the physical library.

3 Click **Setup > User Configuration > Local Users**. The **Local Users** dialog box appears.

4 Click the name of the account that you want to delete to highlight it.

5 Click **Delete**. A message appears that asks you whether you are sure that you want to delete the account.

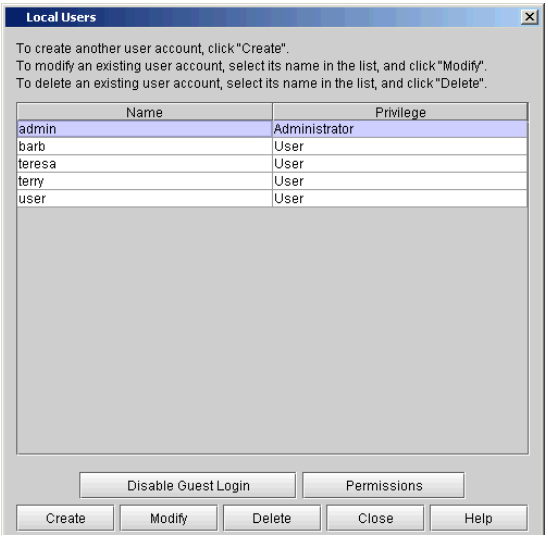
6 Click **Yes**. The library deletes the user account.

Viewing Local User Account Permissions

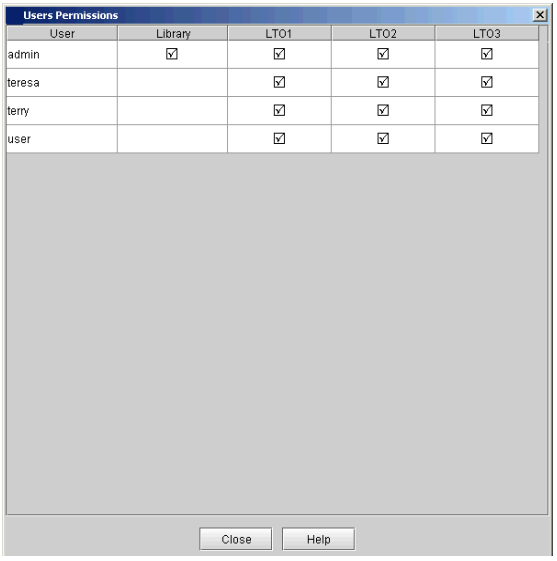
1 Log on as an administrator.

2 Make sure that you are viewing the physical library. From the **View** menu, click the name of the physical library.

3 Click **Setup > User Configuration > Local Users**. The **Local Users** dialog box appears.



4 To view the permissions for all users, click **Permissions**. The **Users Permissions** dialog box appears.



5 Click **Close** to return to the **Local Users** dialog box.

Shutting Down/Rebooting the Library

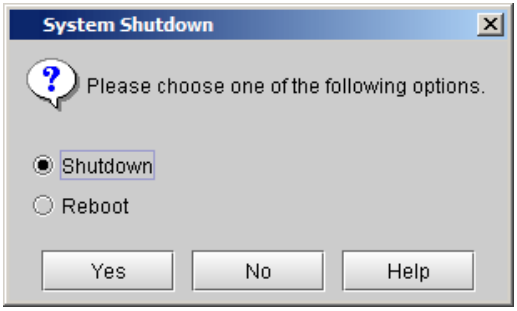
Always perform the shutdown process before you remove power from the library. **Shutdown** prepares the library's operation system and firmware for when you physically turn off power to the library. Shutdown makes sure that the library finishes all active commands received from the host and prevents the processing of any new commands. It also shuts down all partitions.

Reboot shuts down and restarts the library's operating system and firmware. When performing a reboot, the library finishes all active commands received from the host application and does not process any new commands. The library shuts down all partitions and restarts them during the reboot. In addition, if automatic inventory is enabled, the library performs an inventory of cartridges, tape drives, and slots during a reboot. For more information on automatic inventory, see Setting Up Policies for the Physical Library on page 170.

Caution: Before shutting down or rebooting the library, make certain there is no I/O activity on any of the partitions.

1 Make sure that you are viewing the physical library. From the **View** menu, select the name of the physical library.

2 Select **Operations > System Shutdown**. The **System Shutdown** dialog box appears with Shutdown selected as the default.



3 Select **Shutdown** to do a complete shutdown and power off of the library, or select **Reboot** to do a reset of the library without powering off. A message appears that asks you whether you want to continue.

4 If you are sure that all I/O operations are finished, click **OK**.

When the shutdown process completes, the LMC displays a messaging indicating that it is OK to power off the library. The library is now ready to be powered off.

Note: To recover from a library shutdown, you must cycle power on the library (power it off and then power it on). See Powering Off the Library on page 477 and Powering On the Library on page 477.

Powering Off the Library

Caution: Always perform the shutdown procedure before powering off the library. Shutdown prepares the library's operation system and firmware for when you physically turn off power to the library. If you do not perform library shutdown before you power off the library, loss of data could occur. See Shutting Down/Rebooting the Library on page 475.

1. After starting the shutdown process, wait for the LMC to display a messaging indicating that it is OK to power off the library.
2. To turn off power to the library, press the **Power** button on the indicator panel.
3. On the power distribution unit(s), set the circuit breaker switch to the down (O) position.

Powering On the Library

1. Make sure that you wait 15 seconds after powering off the library before you power it on.

   Caution: Waiting 15 seconds is important because the power supply discharges for 10 seconds after you power off the library. If you attempt to power on the library too soon, the power supply will fault.

2. On the power distribution unit(s), set the circuit breaker switch to the up (I) position.
3. To turn on power to the library, press the **Power** button on the indicator panel.

   The library begins to boot up. Within five minutes, the LMC display appears on the library's touch screen. A library with only a few

drives usually will be fully powered on and ready for use within 10 minutes. However, if a library is large with a high number of drives, it can take more than an hour for the library to fully power on, complete its discovery process, and become ready for use. During the power-on process, the **Robotics Enabled** indicator flashes. When the library is fully up and ready to receive commands, the **Robotics Enabled** indicator turns solid green.

Locking/Unlocking the I/E Station

The Scalar i6000 I/E stations have multiple open and close sensors. When you are finished accessing the I/E station, make sure the station door is fully closed.

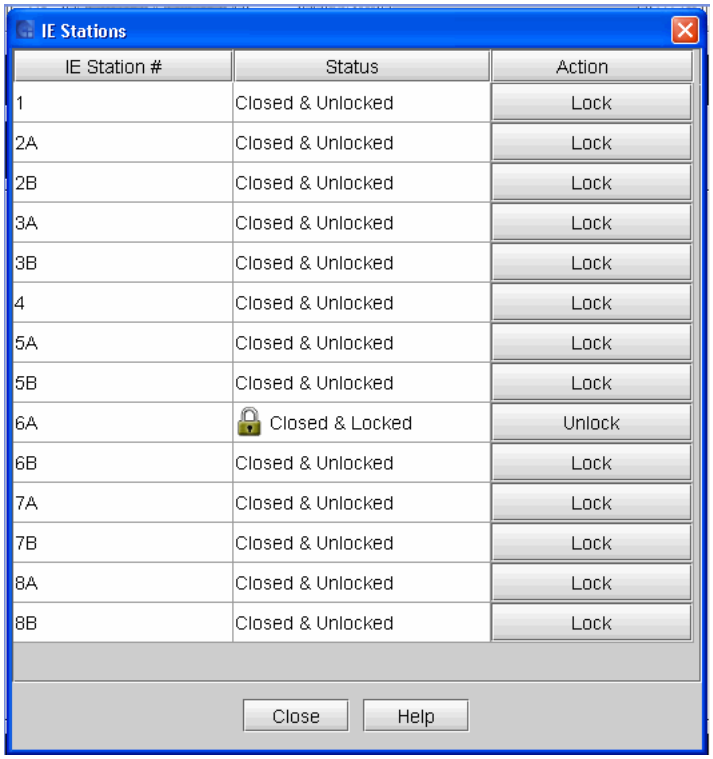
There are two reasons the I/E station door locks:

- The library imports or exports a cartridge from the I/E station door. While the library is attempting to import or export a tape from a given I/E station slot, only the associated I/E station door is locked in the closed position. All other I/E station doors remain accessible. On a Get command from an I/E station slot, the associated I/E station door remains locked until the media has been successfully moved to its destination. This allows the media to be returned to the I/E station slot in the event of a Put error.
- A user has requested that the I/E station door be locked.
- The application software has locked the I/E station as part of the normal tape movement process.

Administrative users can lock or unlock the I/E station doors using an option from the **Tools** menu.

1 Make sure that you are viewing the physical library. From the **View** menu, click the name of the physical library.

2 Click **Tools > I/E Station**. The **I/E Stations** dialog box appears.



Note: The **IE Station #** column lists the I/E station number for each door. All single-door I/E stations are numbered starting with 1at the control module. All double-door I/E stations are numbered with a number and a letter. The number is the module number (1 – 8) and the letter either A (for the left I/E station) or B (for the right I/E station. For example, I/E station number 2A means the left I/E station in module 2.

3 To change the state of the I/E station doors, do one of the following:

- To lock an I/E station door, in the appropriate **Action** column, click **Lock**.
- To unlock an I/E station door, in the appropriate **Action** column, click **Unlock**.

4 To return to the main console, click **Close**.

When Robotics Are Not Ready

When the library robotics are not yet ready to accept commands, aspects of the LMC are still available while other aspects are not. This situation can occur during startup, reboot, or while the library is running. During run time, for example, the robotics will become unavailable if someone opens and closes an access door without then pressing the **Robotics Enabled** button.

Whenever robotics become disabled, a message appears in the **Activity** area on the main LMC display that states, "Warning: The Robotics are not Enabled." Users can log on locally or remotely while the robotics are disabled.

Table 43 on page 480 lists the menu commands that are available when the robotics become disabled either before system discovery can occur or after system discovery has occurred. As the table shows, significantly fewer menu commands are available when the library is started up or rebooted and the robotics become disabled before system discovery occurs.

Note: Menu commands not listed in the table are not available at all when the robotics become disabled, regardless of when the robotics become disabled. Unavailable menu commands are grayed out on the LMC.

Table 43 Menu Commands When Robotics are Disabled

Available Menu Commands When Robotics Become Disabled	After Discovery	Before Discovery
Operations > Change Mode (for shutdown only)	X	X
Operations > Log Off	X	X
Monitor > Drives	X	
Monitor > Connectivity > IO Blade	X	
Monitor > Connectivity > SCSI Channel	X	

Available Menu Commands When Robotics Become Disabled	After Discovery	Before Discovery
Monitor > Connectivity > Fibre Channel	X	
Monitor > IE Station	X	
Monitor > Slot	X	
Monitor > Media	X	
Monitor > Sensors	X	
Monitor > Users	X	
Setup > Setup Wizard	X	
Setup > Partitions	X	
Setup > Device > IDs	X	
Setup > Device > Access > Channel Zoning	X	
Setup > Device > Access > FC Host	X	
Setup > Connectivity > Port Configuration	X	
Setup > Connectivity > Datapath Conditioning	X	
Setup > Connectivity > FC Host Port Failover	X	
Setup > Network Configuration (from library's touch screen only)	X	X
Setup > Physical Library	X	
Setup > Users	X	
Setup > Notification	X	
Setup > Date and Time	X	
Setup > Licenses	X	
Setup > Email Configuration	X	X
Setup > Trap Registration	X	
Setup > Security	X	X
Tools > Tickets	X	X

Available Menu Commands When Robotics Become Disabled	After Discovery	Before Discovery
Tools > Drives	X	
Tools > Connectivity	X	
Tools > Capture Snapshot	X	
Tools > Save/Restore	X	
Tools > Verification Tests	X	X
Tools > Command History Log	X	X
View > [physical library name] (Physical)	X	X
View > [partition name] (Partition)	X	
View > Views	X	X
Help > Index	X	X
Help > About	X	X

Using the Library Access Feature

The Library Access Wizard provides a 10-minute window for you to open the library and perform maintenance activities while reporting a status of “Becoming Ready” to hosts. (If you simply pressed the **Robotics Enabled** button and opened an access door, the library would report “Not Ready” to hosts).

The wizard includes a timer that counts down from 10 minutes. After 10 minutes, the library will go “Not Ready” and hosts will start failing jobs. The 10-minute window includes the time it takes the library to finish the current command, your time working in the library, and time for the library to come ready after you have finished. Since it may take 3 to 4 minutes for the library to come ready, plan your time inside the library to be as short as possible.

Note: The feature is available on the local operator panel only.

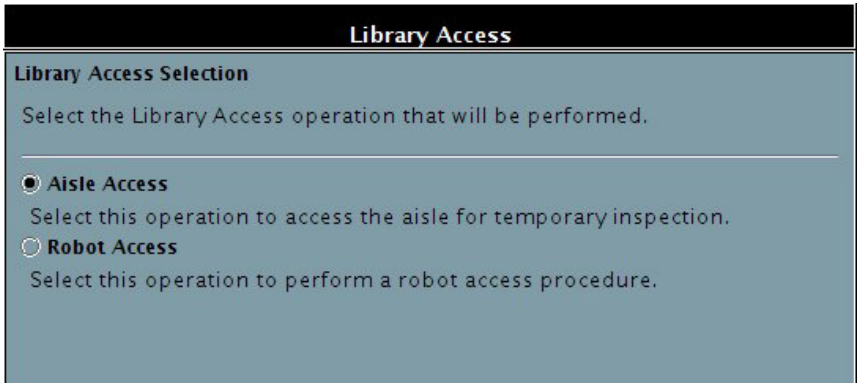
From this wizard, you can do the following two things:

- Aisle Access on page 483 — To gain access for inspection or maintenance.
- Robot Access on page 486 — For replacement or re-installation of a robot.

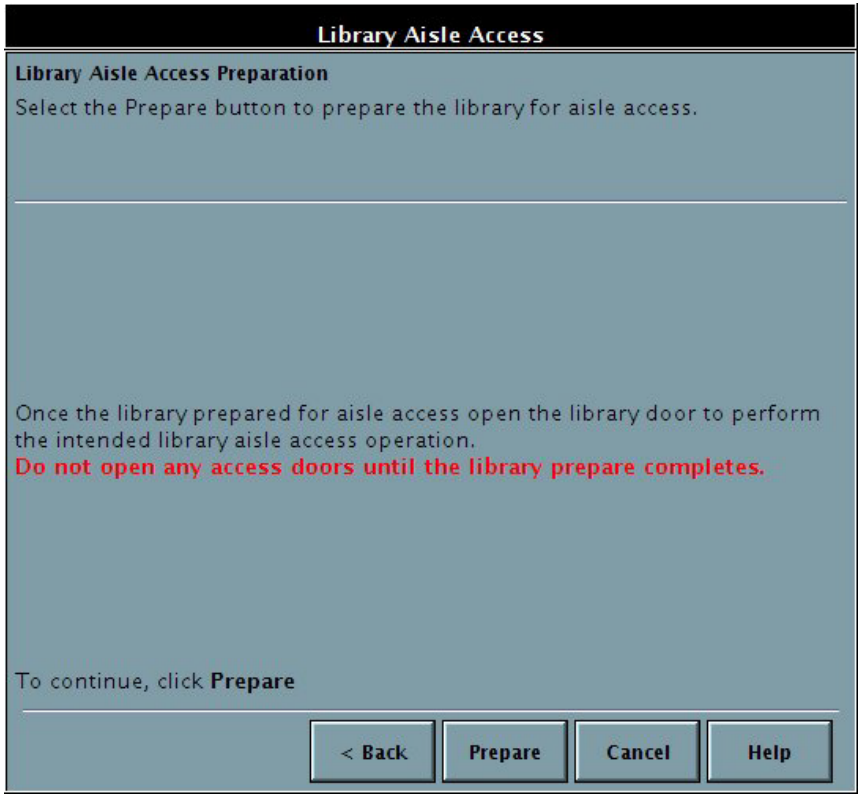
Aisle Access

1 From the local operator panel, select **Tools > Library > Access** to access the wizard.

2 Click **Next** to open the Library Access Selection screen.



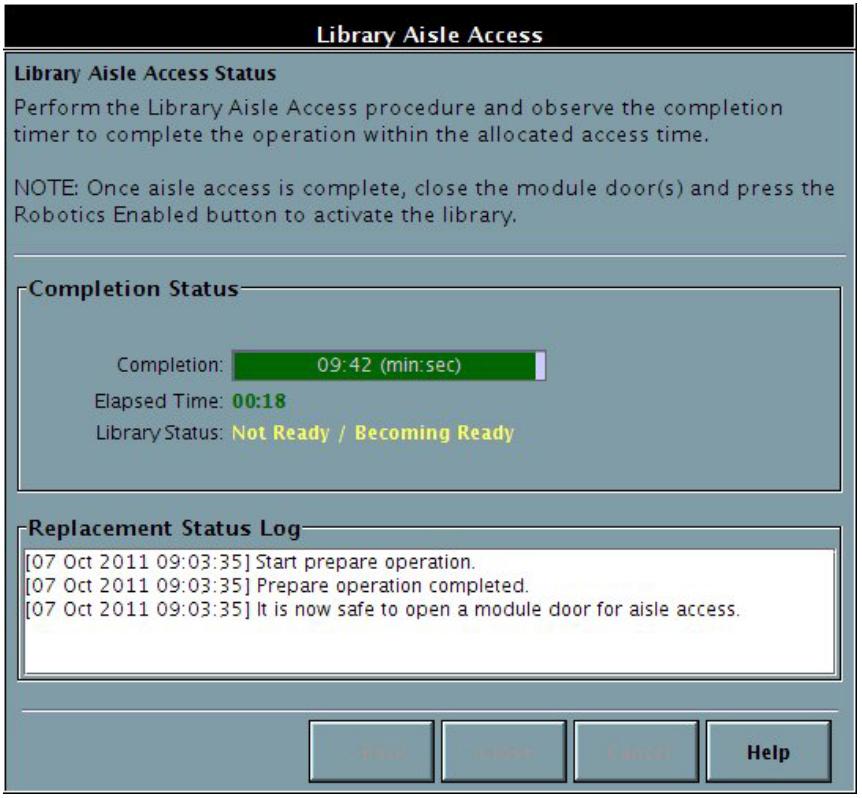
3 Select **Aisle Access** and click **Next** to go to the **Library Aisle Access** screen.



4 Click the **Prepare** button and wait until the screen notifies you that it is safe to open the module door.

The library finishes the current command and begins to report "Becoming Ready" status to hosts. Once this happens, a dialog box appears on the screen stating that it is safe to open the door, and the 10-minute timer starts counting down.

5 Click **OK** to close the dialog box. (The dialog box will close on its own after 15 seconds.)



6 Open a module access door and perform your activity. Try to finish within 6 to 7 minutes.

7 When finished, close the module door and press the **Robotics Enabled** button.

8 Wait for the library to come ready **(Library Status** on the screen says "Ready" and the **Robotics Enabled** button comes on solid).

The timer stops counting down and a **Close** button becomes available. The library is now ready for use.

9 Click **Close**.

Robot Access

Robot removal and installation must be performed by a qualified Service technician only.

Chapter 14
Using the Command Line Interface

Customers as well as Technical Support personnel can access the library using a command line interface (CLI). The CLI is fairly rudimentary and only covers a small portion of the commands available on the library user interface. The CLI is not intended to replace the GUI, but, rather, to be an additional tool that can be used if desired.

This chapter covers:

Note: The CLI uses the term “mail slot” to mean I/E station slot.

Logging on to the CLI

1 Enable CLI on the library:

   a From the LMC, select **Setup > Security**.

   b Under **CLI**, select the **Enable** radio button.

   c Under **SSH**, select the **Enable** radio button.

   Note: Both the **CLI** and **SSH** must be enabled in order to use the command line interface.

   d Click **OK**.

   For more information on library security settings, see Configuring Library Security on page 225.

2 Use SSH to access the CLI.

   Note: When using Putty or Tera Term on Windows, enter the user name and password in boxes.
   When using Linux, log in as: **`ssh admin@library_<ip>`** (where `<ip>` is the IP address of the library).

3 When prompted for the user name, type: **`admin`**.

   Note: The only user name supported on the CLI is **`admin`**.

4 When prompted for the password, type the admin password configured on the library. The main CLI screen appears.

```
Welcome to the XXX Library Command Line Interface.
Type 'help' at the prompt for context-sensitive help.


/>
```

Command Line Interface (CLI) Commands

Navigate through the CLI by typing names of paths or commands. Once you reach an intended path, you can execute a command from that path.The paths can be thought of as a tree with the Initial path as the root.

Initial Path

The initial path is empty, and is displayed as in the following figure.

```
Welcome to the XXX Library Command Line Interface.
Type 'help' at the prompt for context-sensitive help.

/>
```

The initial path is displayed as a '/' character. The path is always followed by a '>' character.

Navigating Paths

The user types in paths, and then presses enter on the keyboard to navigate up and down paths. In the following example, the user typed **`set`**. This action changed the prompt, allowing a different set of commands and paths to become available. The user then typed **`drive`**. The new path is now **`/set/drive`**.

```
Welcome to the XXX Library Command Line Interface.
Type 'help' at the prompt for context-sensitive help.

/> set

/set> drive
/set/drive>
```

Global Commands

Global commands are available in all paths. The global commands are:

Global Command: help

A user invokes this command to get a listing of available paths and commands.

```
Welcome to the XXX Library Command Line Interface.
Type 'help' at the prompt for context-sensitive help.

/> help

Global Commands:
-----------------------------
help - list commands or get help for a specific
command
home - Go to the root level
exit - log out
up   - Go up one level

Paths currently available:
-----------------------------

Commands currently available:
-----------------------------
```

Global Command: home

This command takes the user back to the initial path.

Global Command: exit

This command closes the shell.

Global Command: up

This command moves the customer backwards in the path.

```
Welcome to the XXX Library Command Line Interface.
Type 'help' at the prompt for context-sensitive help.

/set/drive> up
/set>

/set> drive
/set/drive>
```

Path-specific Commands

Path specific commands are available from in a designated path. The user must navigate to the correct path to execute the command or list the entire path and command from the initial prompt.

```
Welcome to the XXX Library Command Line Interface.
Type 'help' at the prompt for context-sensitive help.

/> move
/move> help

Global Commands:
-----------------------------
help - list commands or get help for a specific command
home - Go to the root level
exit - log out
up   - Go up one level

Paths currently available:
-----------------------------
Commands currently available:
-----------------------------
media - Move between drive, slots, and mail slots
within a partition
```

Issuing a Command from the Initial Prompt

```
Welcome to the XXX Library Command Line Interface.
Type 'help' at the prompt for context-sensitive help.

/> move media p1 s10 d1

/set> drive
/set/drive>
```

CLI Command List

The following commands are available. The commands and their usage are described below.

show media

```
show media <partition> [options]
description: Shows media information for storage slots, drives, mail slots, or
all in a particular partition


The partition number is specified using a logical number. Note that using zero
implies the CLI will ignore logical partitions, and return media for the entire
physical library


options: one of the following options is required
    all            - shows media information for all storage slots, drives, and
                     mail slots
    slots  [range] - shows media information for all storage slots or those
                     within a range.
    mail   [range] - shows media information for all mail slots or those within
                     a range.
    drives [range] - shows media information for all drives or those within a
                     range.


The range must be two integers corresponding to the start and end.  Ranges are
1-based.
examples:
media p0 all          -Shows media info for all storage slots, drive, and mail
                       slots for the physical library
media p2 drives       -Shows media info for all drives in partition 2
media p4 slots 1 100  -Shows media info for storage slots 1 through 100
                       in partition 4
```

move media

```
move media <partition> <destination> <source> [force]

description: Moves media between drives, slots, and mail slots within a
partition.


The partition is specified using a number.

of the partition.  For instance:

    Pn - Partition number "n" (range 1..16)


The media locations are specified using a media location type

code and the logical address of the location. For instance:

    Dn - Drive at logical address "n" (range 1..96)

    Mn - Mailslot at logical address "n" (range 1..240)

    Sn - Storage slot at logical address "n" (range 1..9999)


force  - Force the partition to be set offline


examples:

    media p1 S10 D1       - Moves media from storage slot 10 to drive 1

    media p2 D1 M1        - Moves media from drive 1 to mail slot 1

    media p3 M1 S10       - Moves media from mail slot 1 to storage slot 10
```

example of move media with error:

```
/>mov med p1 m1 s1


Partition 'Logical Library 01' must be taken offline prior to performing the
operation.
Changing the partition mode to offline will cause robotics actions against
this partition to fail, please ensure all backup applications are not
currently using this partition.


Enter 'y' to continue or 'n' to skip [default='n']: y
Partition 'Logical Library 01' is going to be taken offline.
Moving '000038L3' from Mailbox slot 1 to Storage slot 1
ERROR: Robot is not ready.
Partition 'Logical Library 01' set back online!
```

show firmware revisions

```
show firmware revisions description: Shows all of the firmware revisions for a
ny valid component.

examples:
    show firmware revisions

/>sho fir rev

Current Firmware Revisions

Tape Library Firmware Revision     : 630Q.GS20601

Tape Drive firmware revisions:
Phys.  Log
  Drive #     Part   Drive Name        Firmware Revision
-----  -----  -----  ----------------  -----------------
1      1      1      Ultrium 5-SCSI    I3FW
2      2      1      Ultrium 5-SCSI    I3FW
3      3      1      Ultrium 5-SCSI    I3FW
.
.
.
94     94     1      Ultrium 5-SCSI    I3FW
95     95     1      Ultrium 5-SCSI    I3FW
96     96     1      Ultrium 5-SCSI    I3FW
```

show library status

```
show library status
description: Shows the current library state and status of each component.
This command should show whether the library is online, offline, or inventorying.  It should also show
whether each drive is loaded or not.
examples:    show library status

/>sho lib stat

Component                 Status   Description
------------------------  -------  ------------------------------------------------------
System Health             Red      Failed

  Control                 Red      Failed; Active events: 1
    Event: 106           Red      Chassis Management Blade(CMB) circuit card at [1,1,1,1,2](CMB ethernet
interface) has failed

  Connectivity            Green    Operational

  Power                   Green    Operational

  Cooling                 Red      Failed; Active events: 5
    Event: 1              Red      Network Chassis fan in [1,8,1,1](CMB fan 1 speed sensor) is in the Low
Warning Range
    Event: 2              Red      Network Chassis fan in [1,1,1,1](CMB fan 1 speed sensor) is in the Low
Warning Range
    Event: 3              Red      Network Chassis fan in [1,7,1,1](CMB fan 1 speed sensor) is in the Low
Critical Range
    Event: 4              Red      Network Chassis fan in [1,4,1,1](CMB fan 1 speed sensor) is in the Low
Critical Range
    Event: 5              Red      Network Chassis fan in [1,3,1,1](CMB fan 1 speed sensor) is in the Low
Critical Range

  Robotics                Yellow   Warning; Active events: 1
    Event: 107            Yellow   Front door switch hardware in Module 1 is open
    Robot# 1              Red      Not Ready; Manual Intervention Required

  Drives                  Green    Operational
    Drive# 1 (P1 D1)      Green    Online; Drive Empty
    Drive# 2 (P1 D2)      Green    Online; Drive Empty
    Drive# 3 (P1 D3)      Green    Online; Drive Empty
    .
    .    .
    Drive# 94 (P1 D94)    Green    Online; Drive Empty
    Drive# 95 (P1 D95)    Green    Online; Drive Empty
    Drive# 96 (P1 D96)    Green    Online; Drive Empty
```

show network information

```
show network info

description: Shows the current library network configuration.

This command should show the library IPv4 and IPv6 configuration, current
addresses, etc.

examples:

    show network information


/>show net info

   - Hostname: dvt20-ms.hw.quantum.com

   - Domain Name: N/A

   - IP versions(s) enabled: IPv4 enabled, IPv6 disabled

   - DHCPv4: disabled

   - IPv4 addr/mask/gtwy: 10.20.171.25 / 255.255.248.0 / 10.20.168.1/>
```

set network ip

```
set network ip

description: Allows the user to set the basic IPv4 static address information.

examples:

    set network ip


/>set net ip 10.0.0.3 255.255.255.0 10.0.0.1

/>
```

show library configuration

```
/>sho lib con

Tape library product ID: Scalar i6000
Tape library serial number: 273190052
Tape library firmware Revision: 630Q.GS20601
Number of frames: 12
Number of Drives (installed/assigned): 96/96
Number of Storage slots (licensed/installed/assigned): 100/4608/102
Number of Mailbox slots (installed/assigned): 24/24
Partitions: Logical Library 01
Active Licenses: Partition (1 units)
                 Capacity On Demand (100 units)
```

show partitions

```
show partitions

description: Prints the partition number and name

examples:
    show partitions

/>sho par

Num   State    Partition Name
----  -------  --------------------------------
P1    Online   LL0
P2    Online   LL1
P3    Online   LL2
P4    Online   LL3
P5    Online   LL4
P6    Online   LL5
P7    Online   LL6
P8    Online   LL7
P9    Online   LL8
P10   Online   LL9
P11   Online   LL10
P12   Online   LL11
P13   Online   LL12
P14   Online   LL13
P15   Online   LL14
P16   Online   LL15
```

set partition online/offline

```
set partition online|offline <partition> [force]

Invalid number of arguments: 0 (1 to 2 expected)

set partition online|offline <partition> [force]
description: Sets the partition state to online or offline for the specified partition.

The partition number is specified using a logical number, and is 1-based.

example:
    online p1
     -Sets partition 1 to online - unless the robot is offline (door open)
    offline p2
     -Shows a prompt about the fact that the host will no longer be able to control the partition.
      and sets the partition offline.
    offline p2 force
     -Forces partition p2 offline.
examples:
  >set partition offline p2
        Partition 'HP LTO5' is going to be taken offline.

        Changing the partition mode to offline will cause robotics actions against this partition to
fail, please ensure all backup applications are not currently using this partition.

        Enter 'y' to continue or 'n' to skip [default='n']:

  />set partition offline p2 force
        Setting logical partition 'HP LTO5' offline!
  />set partition online p1
        Partition p1: 'HP LTO4' is already online.
  />set partition online p2
        Partition 'HP LTO5' is going to be taken back online.
        Changing the partition mode to online will allow robotics actions against this partition to
complete, and inform the backup applications of any changes.
        Enter 'y' to continue or 'n' to skip [default='n']:
```

reboot library

Note: The library performs the same rebooting actions whether you reboot from the CLI or from the GUI.

```
Reboot library

description: Allows the user to reboot the library
controller in a graceful manner


examples:

    reboot library


/>reboot lib


Are you sure you want to reboot the library (Y/N):


:y


Rebooting library controller….
/>
```

Chapter 15
Maintaining Your Library

The library includes advanced system monitoring and alerting mechanisms that inform you of library status and issues. It provides you with status information about various library subsystems and components. It also notifies you of issues it detects and guides you through diagnosing and correcting issues before problems interfere with backups.

This chapter describes commands that you can select from the **Monitor** and **Tools** menus to monitor the library, configure and test drives, work with connectivity, capture snapshots, update library software and drive firmware, run the Teach feature to calibrate and configure the robot, save and restore library configurations, and run tests to verify successful FRU removals and replacements and verify successful library installations and configurations.

Note: The **Tickets** command on the **Tools** menu displays tickets that the library created when it detected issues within its subsystems. For more information about tickets, see Troubleshooting Your Library on page 35.

This chapter consists of the following sections:

Monitoring the Library

The library can provide detailed information about the status of the library and its various components. You also can access statistics about the library and other helpful information, such as library and component serial numbers, port numbers, World Wide Names (WWNs), IDs, and firmware versions.

This section explains how to use **Monitor** menu commands to display status information for the following general areas:

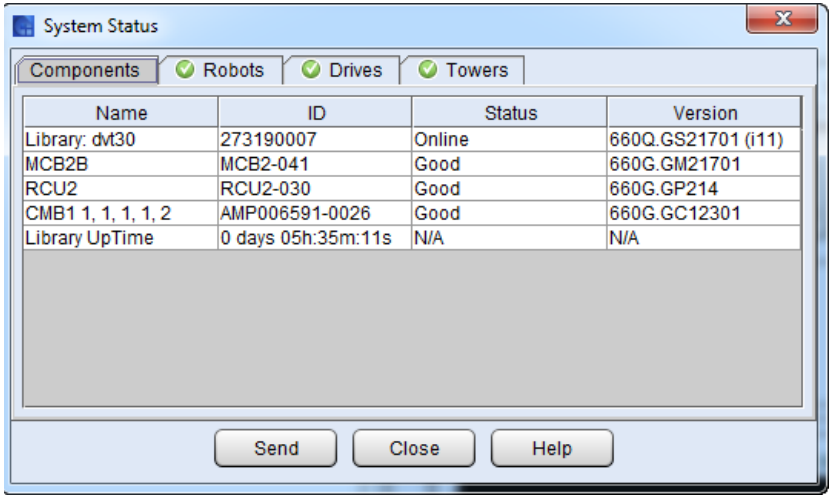
- System

- Drives
- Connectivity
- I/E stations
- Extended I/E Slots
- Slots
- Media
- Sensors
- Email Configuration Record
- Users
- Partitions
- EKM Servers

Monitoring System Status

The **System Status** dialog box displays status information for various library entities (hardware or system metrics). You can perform this procedure while viewing either the physical library or a partition.

1 Click **Monitor > System** or click the **System Status** button. The **System Status** dialog box appears, displaying four (4) tabs, Components Tab, Robots Tab, Drives Tab and, if installed, Towers Tab. These are explained in detail below.



2 From the **System Status** dialog box, you can perform the following tasks:

- Change the sorting of system items in the status list (for example, by item or ID) by clicking the column heading by which you want the system items sorted. Repeatedly clicking a column heading toggles between ascending and descending order.
- Mail, save, or print status information by using the Send button (see Mailing, Saving, and Printing Status Information on page 538).

Components Tab

The **Components** tab displays the following information about the library/partition being viewed:

Name	ID	Status Description	Version
Library/partition	The library/partition serial number	The status of the library (Online or Offline).	Current Firmware Version
MCB version	The MCB serial number	The current status of the MCB (Good, Degraded, or Failed).	Current Firmware Version
RCU version	The RCU serial number	The current status of the RCU (Good, Degraded, or Failed).	Current Firmware Version
CMB version	The CMB serial number	For each CMB that is present, the current status of the CMB (Good, Degraded, or Failed).	Current Firmware Version
Library UpTime	The library serial number	The amount of time that the library has been up (in days, hours, minutes, and seconds).	N/A

Robots Tab

The **Robots** tab displays the following information for each robot in the library:

- **Name** — Left or Right (if only one robot, this will be Left).
- **Status** — Unknown, Good, Not Installed, Initializing, Failed and N/A.

- **State** — Varied On or Varied Off.
- **Serial number** — Robot serial number.
- **Version** — Robot firmware version.
- **Generation** — Hardware generation (Gen 1 or Gen 2).
- **Parked** — Indicates whether robot is in its parking space (Yes or No). If the robot is Gen 1, this will display as N/A.
- **V Motion** — Total number of meters of vertical motion traveled by this robot.
- **H Motion** — Total number of meters of horizontal motion traveled by this robot.
- **Media Moves** — Total number of media move operations performed by this robot.

Drives Tab

The **Drives** tab displays the following information about the library/ partition being viewed:

- **Serial Number** — The serial number of the drive
- **Location** — The coordinates of the drive within the library
- **State** — Whether the drive is varied on or off
- **Partition** — Which partition the drive is assigned to

Towers Tab

The **Towers** tab only displays if a tower (HDEM) is installed in the library and details the following information:

- **Tower #** — The location of the tower in the library
- **Status** — If the tower is available
- **Mode** — If the tower is online or offline
- **Scanner** — If a barcode scanner is installed or not
- **State** — Whether the tower is varied on or off
- **Door Status** - Whether the rear access door is open or closed

Monitoring Drive Status

The **Drive Status** dialog box displays status information for tape drives in the currently selected partition. If you are viewing the physical library, status information for all drives appears. You can perform this procedure while viewing either the physical library or a partition.

1 Click **Monitor > Drives**. The **Drive Status** dialog box appears.

Figure 54 Left view of Drive Status dialog box

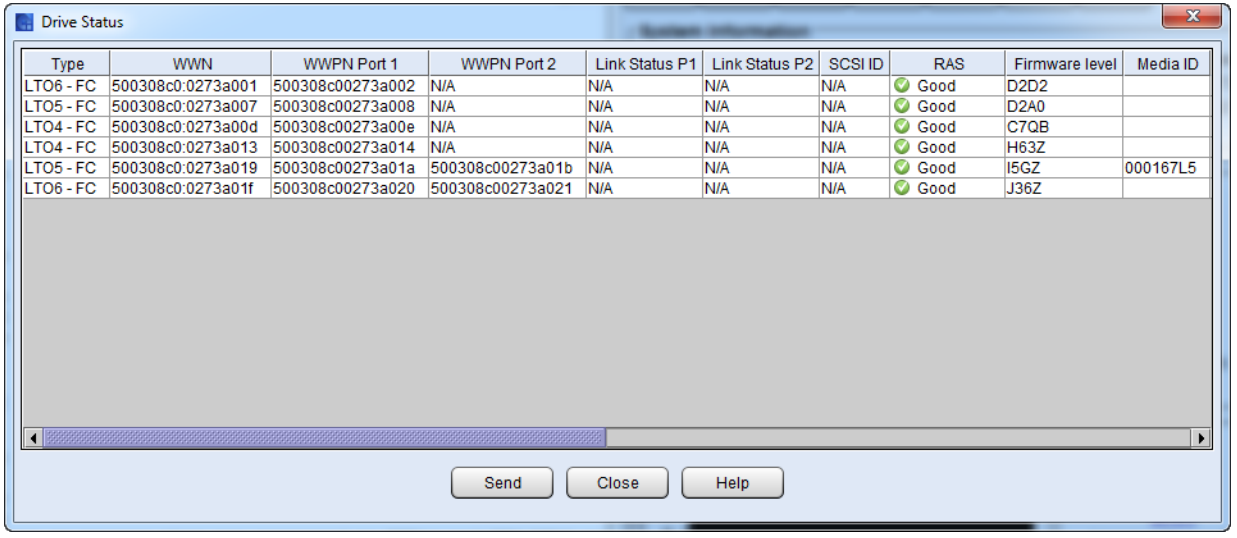
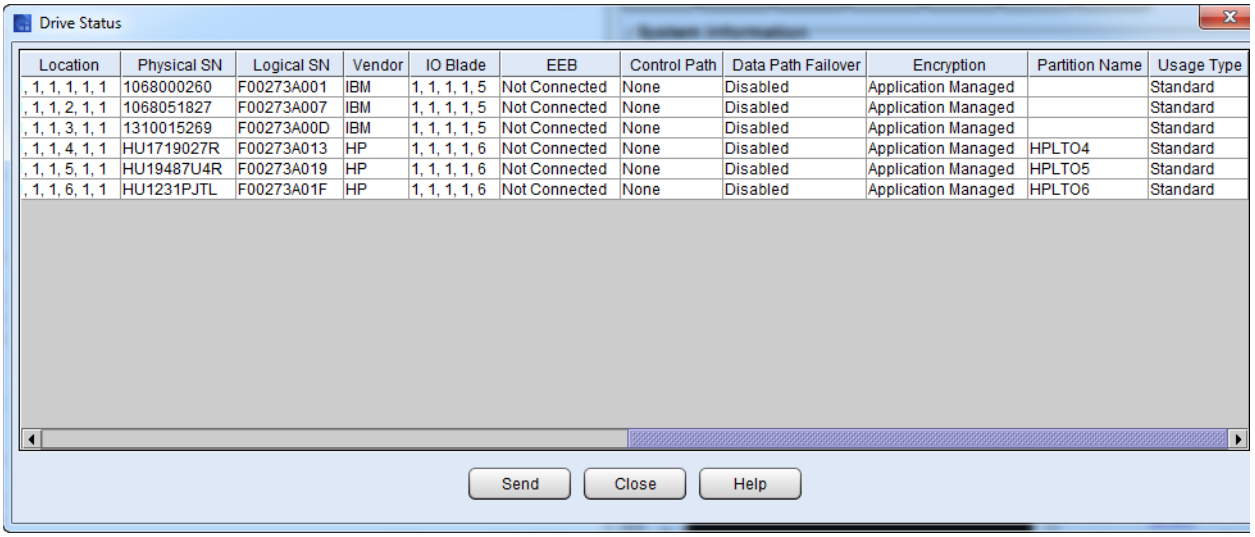


Figure 55 Right view of Drive Status dialog box



The following table describes the elements on the **Drive Status** dialog box.

Element	Description
Type	The type of drive.
WWN	For a Fibre drive only, the World Wide Name of the drive.
WWPN Port 1	For a Fibre Channel drive only, the World Wide Port Name of the drive's port 1.
WWPN Port 2	For a Fibre Channel drive only, the World Wide Port Name of the drive's port 2.
Link Status P1	The status of port 1 on the Fibre Channel drive.
Link Status P2	The status of port 2 on the Fibre Channel drive.
SCSI ID	For a SCSI drive only, the SCSI ID of the drive.
RAS	The status of the drive as reported by the RAS system (for example, Good or Failed).
Firmware level	The firmware level of the drive.
Media ID	The barcode of the loaded cartridge.

Element	Description
Location	The drive coordinate location within the library. For information about location coordinates, see Understanding Location Coordinates on page 449.
Physical SN	The serial number of the particular drive.
Logical SN	The logical serial number that the library assigns to a drive in a specific location. This is not the serial number of the particular drive (see **Physical SN** in this table). If a drive is replaced by another drive in the same library location, the logical serial number remains the same. From the host's perspective, the replacement drive is the same as the original one. If the logical serial number addressing feature is disabled for the library, **Disabled** appears in this field.
Vendor	The name of the drive vendor.
IO Blade	The location of the I/O blade to which the drive is attached. Locations are indicated by means of a coordinate system. For information about location coordinates, see Understanding Location Coordinates on page 449.
EEB	Indicates whether or not the drive is connected to an EEB (Ethernet Expansion blade). Only HP LTO-5 or LTO-6 drives can be connected to an EEB. **Note:** A drive can be connected to either an I/O Blade or an EEB, not both.
Control Path	Reports if a drive is a primary (CP) or a secondary (CPF) drive. The values are Primary, Secondary, or None. It also reports which drive is currently the active drive by displaying "(Active)", example "Primary (Active)"."
Data Path Failover	Indicates whether data path failover is enabled or disabled.
Encryption	Indicates whether or not encryption is set up as Application Managed or Library Managed.
Partition Name	The name of the partition to which the drive is assigned.
Usage Type	Indicates whether the drive is configured as a Standard drive (used for data read/write) or as aEDLM drive (part of a Library Managed partition for testing media integrity). Only LTO-5 or LTO-6 drives can be configured as MeDIA drives.

2 From the **Drive Status** dialog box, you can perform the following tasks:

- Change the sorting of drives in the status list (for example, by type or location) by clicking the column heading by which you want the drives sorted. Repeatedly clicking a column heading toggles between ascending and descending order.
- Mail, save, or print status information by using the **Send** button (see Mailing, Saving, and Printing Status Information on page 538).

Monitoring Connectivity Status

The following dialog boxes display status information about connectivity:

- The **IO Blade Status** dialog box displays information about the I/O blades.

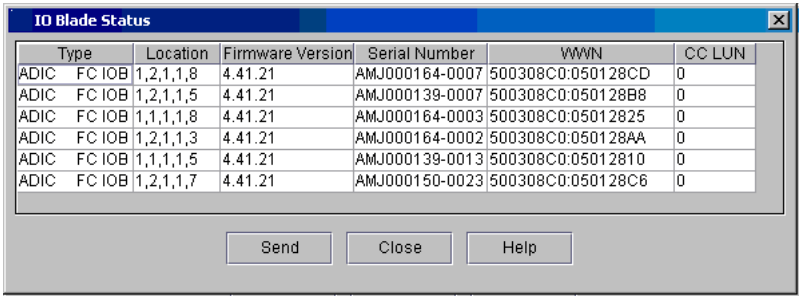
  Note: If the library does not detect at least one chassis management blade (CMB) in the library, the **IO Blade** selection does not appear on the menu.

- The **Fibre Channel Status** dialog box displays information about the FC connections on the MCB and the I/O blades (if any exist).
- The **Ethernet Blade Status** dialog box displays information about the Ethernet Expansion Blade (EEB) connection.

You must perform the following procedures while viewing the physical library.

Viewing I/O Blade Status Information

1. Make sure that you are viewing the physical library. From the **View** menu, click the name of the physical library.
2. Click **Monitor > Connectivity > IO Blade**. The **IO Blade Status** dialog box appears.



See the following table for descriptions of the elements on the **IO Blade Status** dialog box.

Element	Description
Type	The type of I/O blade ("FC IOB" indicates an I/O blade).
Location	The location of the blade (see I/O Blade Locations on page 458).
Firmware Version	The firmware version of the blade.
Serial Number	The serial number of the blade.
WWN	The World Wide Name of the blade.
CC LUN	The Command and Control LUN (typically, the CC LUN is mapped to LUN 0).

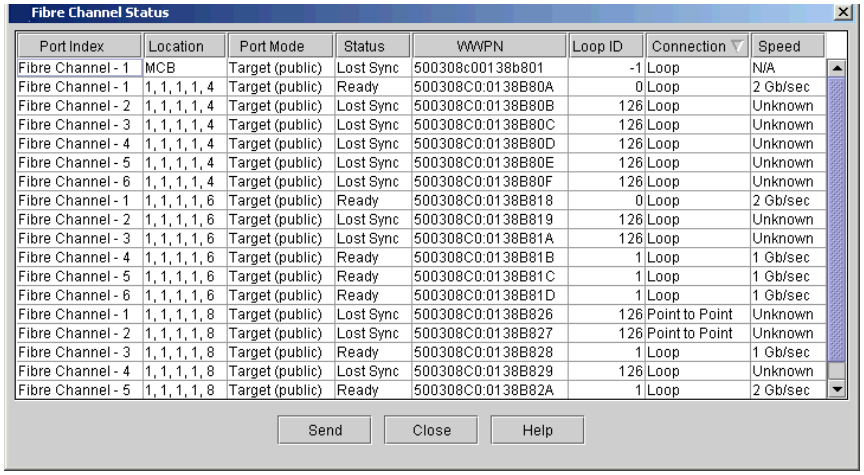
3 From the **IO Blade Status** dialog box, you can perform the following tasks:

- Change the sorting of I/O blades in the status list (for example, by type or location) by clicking the column heading by which you want the I/O blades sorted. Repeatedly clicking a column heading toggles between ascending and descending order.
- Mail, save, or print status information by using the **Send** button (see Mailing, Saving, and Printing Status Information on page 538.

Viewing Fibre Channel Status Information

1 Make sure that you are viewing the physical library. From the **View** menu, click the name of the physical library.

2 Click **Monitor** > **Connectivity** > **Fibre Channel**. The **Fibre Channel Status** dialog box appears.



The following table describes the elements on the **Fibre Channel Status** dialog box.

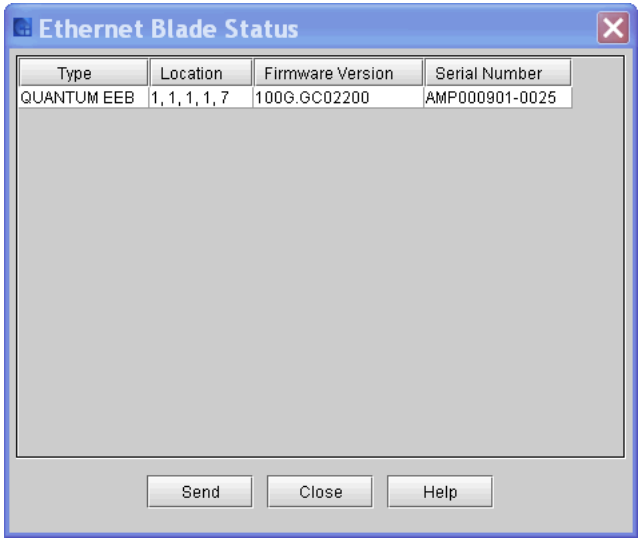
Element	Description
Port Index	The port number.
Location	The location of the port (for example, MCB).
Port Mode	The mode of the port (Target or Initiator).
Status	The status of the Fibre Channel (Operational, Lost Sync).
WWPN	The World Wide Port Name.
Loop ID	For arbitrated loops only, the loop ID. “-1” indicates that **Soft** is selected on the **Fibre Channel Parameters** dialog box (see Port Configuration on page 163).
Connection	The type of connection (Loop, Point to Point, Loop Preferred).
Speed	The speed in gigabits per second (1 Gb/s, 2 Gb/s, 4 Gb/s, or Auto). “Unknown” appears in this field when the Fibre Channel link is not up and ready (“Lost Sync” status).

3 From the **Fibre Channel Status** dialog box, you can perform the following tasks:

- Change the sorting of Fibre Channel connections in the status list (for example, by type or location) by clicking the column heading by which you want the connections sorted. Repeatedly clicking a column heading toggles between ascending and descending order.
- Mail, save, or print status information by using the **Send** button (see Mailing, Saving, and Printing Status Information on page 538).

Viewing Ethernet Blade Status Information

1. Make sure that you are viewing the physical library. From the **View** menu, click the name of the physical library.
2. Click **Monitor** > **Connectivity** > **Ethernet Blade**. The **Ethernet Blade Status** dialog box appears.



See the following table for descriptions of the elements on the **Ethernet Blade Status** dialog box.

Element	Description
Type	The type of blade.

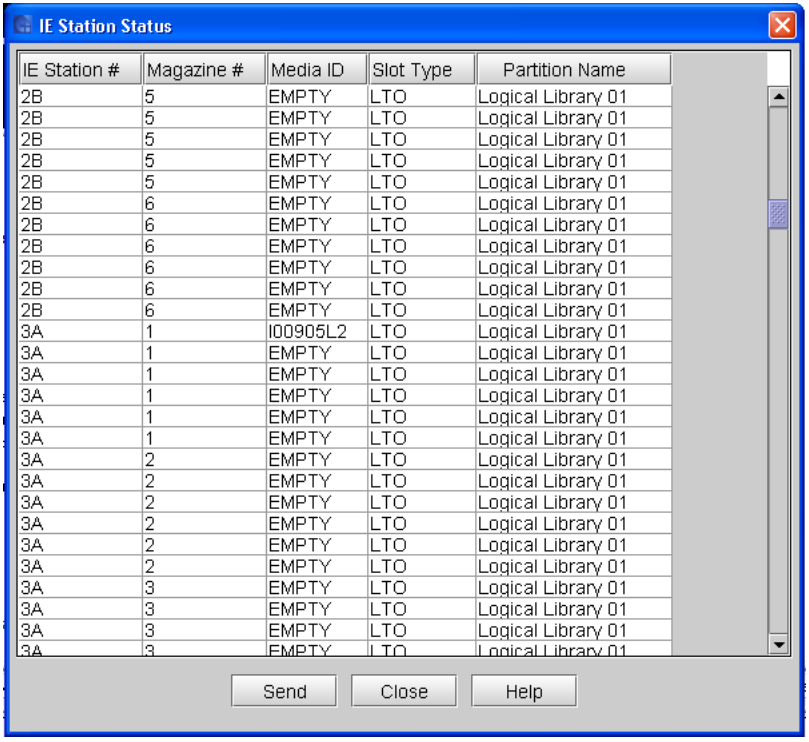
Element	Description
Location	The location of the blade by means of a coordinate system. For information about location coordinates, see Understanding Location Coordinates on page 449.
Firmware Version	The firmware level of the blade.
Serial Number	The serial number of the blade.

3 From the **Ethernet Blade Status** dialog box, you can Mail, save, or print status information by using the **Send** button (see Mailing, Saving, and Printing Status Information on page 538.

Monitoring I/E Station Status

The **I/E Station Status** dialog box displays detailed information about the magazine slots in the I/E stations within the currently selected partition. If you are working in the physical library, status information appears for all magazine slots in all I/E stations. You can perform this procedure while viewing either the physical library or a partition.

1 Click **Monitor > I/E Station** or use the **I/E** toolbar button. The **I/E Station Status** dialog box appears.



The following table describes the elements on the **I/E Station Status** dialog box.

Element	Description
IE Station #	All single door I/E stations are numbered starting with 1 at the control module. All double door I/E stations are numbered with a number and a letter - for example 2A and 2B--the frame number (1-16), with A as the left I/E station and B the right.
Magazine #	The number of the I/E station magazine (numbered from top to bottom in the I/E station).
Media ID	The cartridge barcode or the word EMPTY.
Slot Type	The media type (for example, LTO).
Partition Name	The name of the partition to which the I/E station is assigned.

2 From the **IE Station Status** dialog box, you can perform the following tasks:

- Change the sorting of magazine slots in the status list (for example, by I/E station number or partition name) by clicking the column heading by which you want the magazine slots sorted. Repeatedly clicking a column heading toggles between ascending and descending order.
- Mail, save, or print status information by using the **Send** button (see Mailing, Saving, and Printing Status Information on page 538).

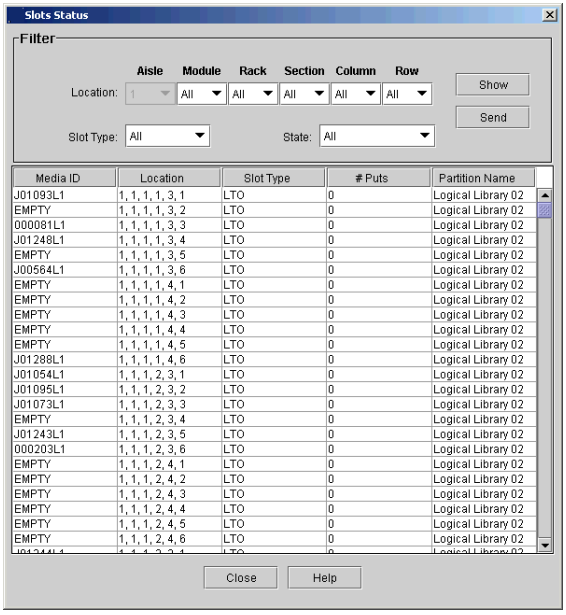
Monitoring Slot and Extended I/E Slot Status

Note: To view slot status for Extended I/E slots, use the procedure below.

The **Slots Status** dialog box displays detailed information about the slots in the currently selected partition. If you are working in the physical library, you can view status information for all slots. Because the number of slots in a physical or partition can be quite large, you can select a subset of the available slots. You can perform this procedure while viewing either the physical library or a partition.

1 Click **Monitor** > **Slots**. The **Slots Status** dialog box appears.

Note: For Extended I/E, click **Monitor > Extended I/E Slots**.



The following table describes the elements on the **Slots Status** dialog box.

Element	Description
In the **Filter** area:	
Location: Aisle	The location of slots by aisle number.
Location: Module	The location of slots by module number.
Location: Rack	The location of slots by rack number.
Location: Section	The location of slots by section number.
Location: Column	The location of slots by column number.
Location: Row	The location of slots by row number.

Element	Description
In the **status list** area:	
Media ID	The slot barcode.
Location	The location of the slot (see Understanding Location Coordinates on page 449).
Slot Type	The type of slot media (for example, LTO).
# Puts	The number of puts during the library's history.
Partition Name	The name of the partition to which the slot is assigned.

2 From the **Slots Status** dialog box, you can perform the following tasks:

- Change the sorting of slots in the status list (for example, by location or slot type) by clicking the column heading by which you want the slots sorted. Repeatedly clicking a column heading toggles between ascending and descending order.
- Use filtering criteria to select the slots that you want to appear in the status list on the dialog box (see Filtering Slots From the Status List on page 521).
- Mail, save, or print status information by using the **Send** button (see Mailing, Saving, and Printing Status Information on page 538).

Filtering Slots From the Status List

You can specify the slots that you want to appear in the status list by selecting location, slot type, and state criteria from the **Filter** area of the **Slots Status** dialog box.

1 Use one or more of the following drop-down lists to specify the slots that you want to appear in the status list:

- To specify slots by location, click the appropriate option from each of the **Location** drop-down lists: **Aisle**, **Module**, **Rack**, **Section**, **Column**, and **Row**. The defaults are set to **All** unless a drop-down list does not have more than one option. For example, the **Aisle** drop-down list is always set to **1** by default because only one aisle exists in the library. Therefore, the drop-

down list also is grayed out and selections cannot be made from it.

These selections correspond to location coordinates for the physical library. For example, to select all slots in the drive-side rack of the control module, click **1** for module, **1** for rack, **All** for section, **All** for column, and **All** for row. For more information about location coordinates, see Understanding Location Coordinates on page 449.

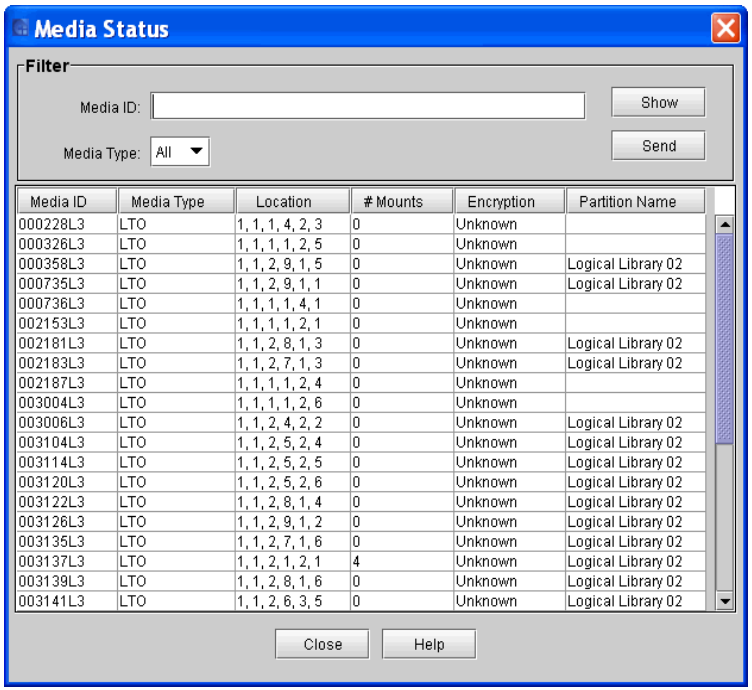
- To specify slots by media type, click **All** or a specific media type, such as **LTO**, from the **Slot Type** drop-down list. Only media types that are currently used in the library appear in the drop-down list. The default is set to **All**.
- To specify slots by slot state, click **All**, **Occupied**, or **Empty** from the **State** drop-down list. The default is set to **All**.

2 Click **Show**.

Monitoring Media Status

The **Media Status** dialog box displays detailed information about the media in the currently selected partition. If you are working in the physical library, you can view status information for all media. Because the number of media in a physical or partition can be quite large, you can select a subset of the available slots. You can perform this procedure while viewing either the physical library or a partition.

1 Click **Monitor** > **Media**. The **Media Status** dialog box appears.



The following table describes the elements on the **Media Status** dialog box.

Element	Description
In the **Filter** area:	
Media ID	The cartridge barcode (allows the asterisk [*] wildcard character).
Media Type	The type of cartridge (for example, LTO).
In the status list area:	
Media ID	The cartridge barcode.
Media Type	The type of cartridge (for example, LTO).
Location	The location of the cartridge (seeUnderstanding Location Coordinates on page 449).

Element	Description
# Mounts	The number of mounts within the history of the library.
Encryption	Reports whether the media is encrypted. The values are Encrypted, Not Encrypted or Unknown.
Partition Name	The name of the partition to which the cartridge is assigned. **Note:** When viewed from a Active Vault partition, this column is named **Source Partition** and reports the partition from which the media came.
Source Partition	This column appears when the library view is set to an Active Vault partition. It reports the partition from which the media came.

2 From the **Media Status** dialog box, you can perform the following tasks:

- Change the sorting of media in the status list (for example, by location or media type) by clicking the column heading by which you want the media sorted. Repeatedly clicking a column heading toggles between ascending and descending order.
- Use filtering criteria to select the media that you want to appear in the status list on the dialog box (see Filtering Media From the Status List on page 524).
- Mail, save, or print status information by using the **Send** button (see Mailing, Saving, and Printing Status Information on page 538).

Filtering Media From the Status List

You can specify the media that you want to appear in the status list by selecting media ID and media type criteria from the **Filter** area of the **Media Status** dialog box.

1 Use one or both of the following elements to specify the media that you want to appear in the status list:

- To specify a media item by media ID, type the exact barcode that is associated with a particular cartridge in the **Media ID** text box. You also can use the asterisk (*) as a wild card character to represent one or more characters in the media ID. This will list all media for IDs that match the designated pattern. For

example, if you set the **Media ID** value to "J00*", any media with IDs that start with "J00" will appear in the status list.

- To specify media by media type, click **All** or a specific media type, such as **LTO**, from the **Slot Type** drop-down list. Only media types that are currently used in the library appear in the drop-down list. The default is set to **All**.

2 Click **Show**.

Monitoring Sensor Status

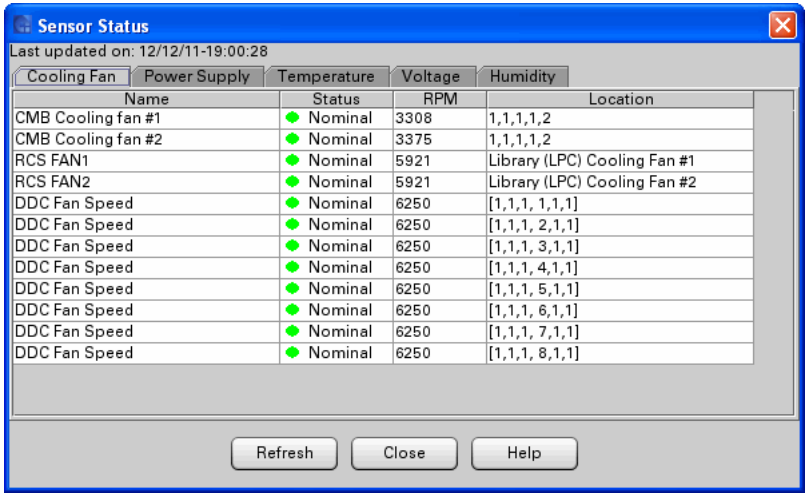
The **Sensor Status** dialog box displays detailed information about the library's power and cooling systems, such as operational statuses, temperatures, voltages or wattages, and fan speeds in rotations per minute (RPM). You can perform the following procedures while viewing either the physical library or a partition.

Accessing the Sensor Status Dialog Box

Click **Monitor > Sensors**. The **Sensor Status** dialog box appears with the **Cooling Fan** tab displayed.

Displaying Cooling Fan Information

1 To display detailed information about the library's cooling fans, click the **Cooling Fan** tab on the **Sensor Status** dialog box.



The following table describes the elements on the **Cooling Fan** tab.

Element	Description
Name	The name of the cooling fan sensor.
Status	The status of the cooling fan. If the fan speed is within normal operating limits, the status is nominal. Otherwise, a warning or alarm is indicated.
RPM	The current speed of the fan in rotations per minute (RPM).
Location	The location of the cooling fan within the library. Locations of cooling fans for control management blades (CMBs) are indicated by means of a coordinate system. For information about location coordinates, see Understanding Location Coordinates on page 449.

2 To view current information, click **Refresh**.

Displaying Power Supply Information

1 To display detailed information about the library's power supplies, click the **Power Supply** tab on the **Sensor Status** dialog box.

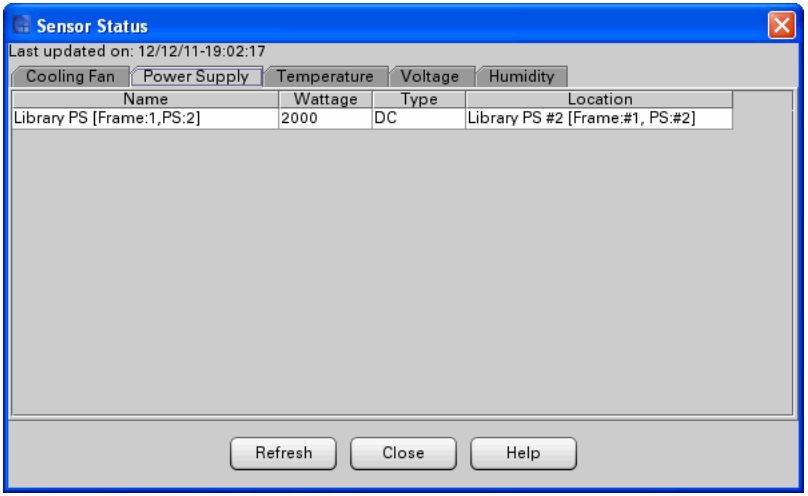


Table 44 on page 527 describes the elements on the **Power Supply** tab.

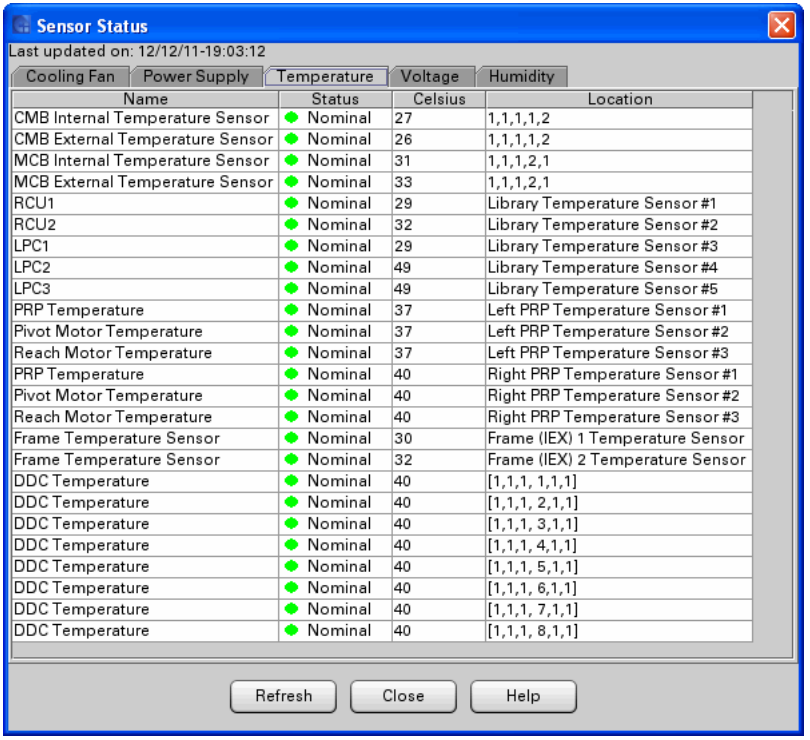
Table 44 Power Supply tab

Element	Description
Name	The name of the power supply sensor.
Wattage	The amount of power in watts.
Type	The type of power (AC or DC).
Location	The location of the power supply within the library.

2 To view current information, click **Refresh**.

Displaying Temperature Information

1 To display temperature status information for various library components, click the **Temperature** tab on the **Sensor Status** dialog box.



Name	Status	Celsius	Location
CMB Internal Temperature Sensor	Nominal	27	1,1,1,1,2
CMB External Temperature Sensor	Nominal	26	1,1,1,1,2
MCB Internal Temperature Sensor	Nominal	31	1,1,1,2,1
MCB External Temperature Sensor	Nominal	33	1,1,1,2,1
RCU1	Nominal	29	Library Temperature Sensor #1
RCU2	Nominal	32	Library Temperature Sensor #2
LPC1	Nominal	29	Library Temperature Sensor #3
LPC2	Nominal	49	Library Temperature Sensor #4
LPC3	Nominal	49	Library Temperature Sensor #5
PRP Temperature	Nominal	37	Left PRP Temperature Sensor #1
Pivot Motor Temperature	Nominal	37	Left PRP Temperature Sensor #2
Reach Motor Temperature	Nominal	37	Left PRP Temperature Sensor #3
PRP Temperature	Nominal	40	Right PRP Temperature Sensor #1
Pivot Motor Temperature	Nominal	40	Right PRP Temperature Sensor #2
Reach Motor Temperature	Nominal	40	Right PRP Temperature Sensor #3
Frame Temperature Sensor	Nominal	30	Frame (IEX) 1 Temperature Sensor
Frame Temperature Sensor	Nominal	32	Frame (IEX) 2 Temperature Sensor
DDC Temperature	Nominal	40	[1,1,1, 1,1,1]
DDC Temperature	Nominal	40	[1,1,1, 2,1,1]
DDC Temperature	Nominal	40	[1,1,1, 3,1,1]
DDC Temperature	Nominal	40	[1,1,1, 4,1,1]
DDC Temperature	Nominal	40	[1,1,1, 5,1,1]
DDC Temperature	Nominal	40	[1,1,1, 6,1,1]
DDC Temperature	Nominal	40	[1,1,1, 7,1,1]
DDC Temperature	Nominal	40	[1,1,1, 8,1,1]

Table 45 on page 528 describes the elements on the **Temperature** tab.

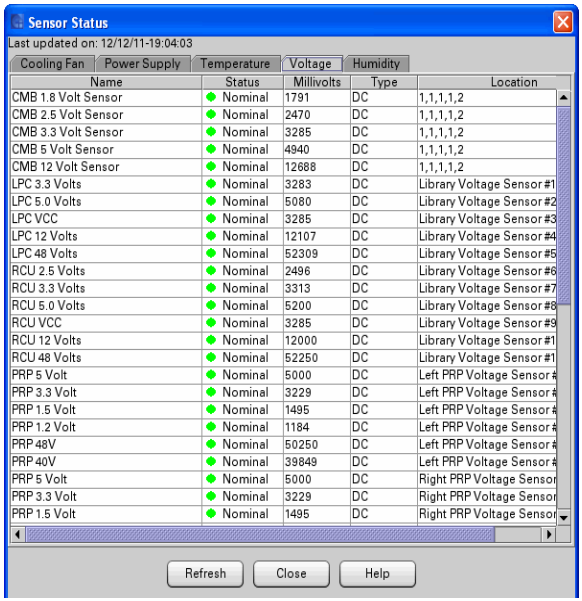
Table 45 Temperature tab

Element	Description
Name	The name of the temperature sensor.
Status	The temperature status in the vicinity of the sensor. If the temperature is within normal operational limits, the status is nominal. Otherwise, a warning or alarm is indicated.
Celsius	The sensor's temperature reading in degrees Celsius.
Location	The location of the temperature sensor within the library. Control management blade (CMB) locations are indicated by means of a coordinate system. For information about location coordinates, see Understanding Location Coordinates on page 449.

2 To view current information, click **Refresh**.

Displaying Voltage Information

1 To display voltage status information for various library components, click the **Voltage** tab on the **Sensor Status** dialog box.



Name	Status	Millivolts	Type	Location
CMB 1.8 Volt Sensor	Nominal	1791	DC	1,1,1,1,2
CMB 2.5 Volt Sensor	Nominal	2470	DC	1,1,1,1,2
CMB 3.3 Volt Sensor	Nominal	3285	DC	1,1,1,1,2
CMB 5 Volt Sensor	Nominal	4940	DC	1,1,1,1,2
CMB 12 Volt Sensor	Nominal	12688	DC	1,1,1,1,2
LPC 3.3 Volts	Nominal	3283	DC	Library Voltage Sensor #1
LPC 5.0 Volts	Nominal	5080	DC	Library Voltage Sensor #2
LPC VCC	Nominal	3285	DC	Library Voltage Sensor #3
LPC 12 Volts	Nominal	12107	DC	Library Voltage Sensor #4
LPC 48 Volts	Nominal	52309	DC	Library Voltage Sensor #5
RCU 2.5 Volts	Nominal	2496	DC	Library Voltage Sensor #6
RCU 3.3 Volts	Nominal	3313	DC	Library Voltage Sensor #7
RCU 5.0 Volts	Nominal	5200	DC	Library Voltage Sensor #8
RCU VCC	Nominal	3285	DC	Library Voltage Sensor #9
RCU 12 Volts	Nominal	12000	DC	Library Voltage Sensor #1
RCU 48 Volts	Nominal	52250	DC	Library Voltage Sensor #1
PRP 5 Volt	Nominal	5000	DC	Left PRP Voltage Sensor #
PRP 3.3 Volt	Nominal	3229	DC	Left PRP Voltage Sensor #
PRP 1.5 Volt	Nominal	1495	DC	Left PRP Voltage Sensor #
PRP 1.2 Volt	Nominal	1184	DC	Left PRP Voltage Sensor #
PRP 48V	Nominal	50250	DC	Left PRP Voltage Sensor #
PRP 40V	Nominal	39849	DC	Left PRP Voltage Sensor #
PRP 5 Volt	Nominal	5000	DC	Right PRP Voltage Sensor
PRP 3.3 Volt	Nominal	3229	DC	Right PRP Voltage Sensor
PRP 1.5 Volt	Nominal	1495	DC	Right PRP Voltage Sensor

Table 46 on page 529 describes the elements on the **Voltage** tab.

Table 46 Voltage tab

Element	Description
Name	The name of the voltage sensor.
Status	The voltage status at the location of the sensor. If the voltage is within normal operational limits, the status is nominal. Otherwise, a warning or alarm is indicated.
Millivolts	The sensor's voltage reading in millivolts.
Type	The type of power at the location of the sensor (AC or DC).
Location	The location of the voltage sensor within the library. Control management blade (CMB) locations are indicated by means of a coordinate system. For information about location coordinates, see Understanding Location Coordinates on page 449.

2 To view current information, click **Refresh**.

Displaying Humidity Information

Gen 2 libraries display humidity information. A humidity sensor is attached to each robot.

1 To display humidity status information for various library components, click the **Humidity** tab on the **Sensor Status** dialog box.

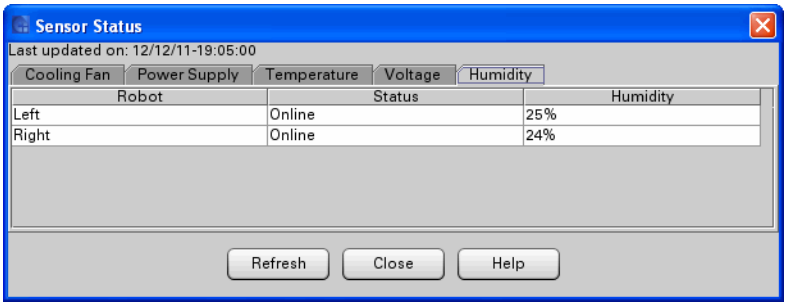


Table 47 on page 530 describes the elements on the **Humidity** tab.

Table 47 Humidity tab

Element	Description
Robot	Which robot (left or right) the humidity sensor is attached to. If the library has only one robot, this column displays “Left.”
Status	Robot’s online or offline status.
Humidity	The humidity of the interior of the library at the location of the sensor.

2 To view current information, click **Refresh**.

Monitoring Users Status

The **Users Status** dialog box displays detailed information about users who are currently logged on to the library. You can perform this procedure while viewing either the physical library or a partition.

1 Click **Monitor > Users**. The **Users Status** dialog box appears.

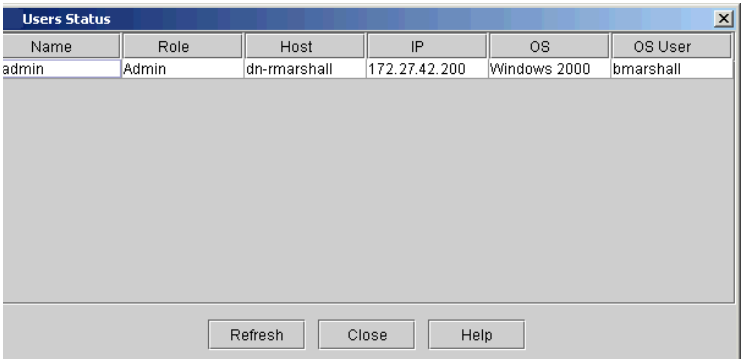


Table 48 on page 531 describes the elements on the **Users Status** dialog box.

Table 48 User Status

Element	Description
Name	The name of the user who is currently logged on to the library.
Role	The type of user (for example, User or Admin).
Host	The name of the host computer from which the user is connected to the library.
IP	The IP address of the host computer.
OS	The host computer's operating system.
OS User	The name of the user who is currently logged on to the host computer.

2 To view current information, click **Refresh**.

Monitoring Partition Status

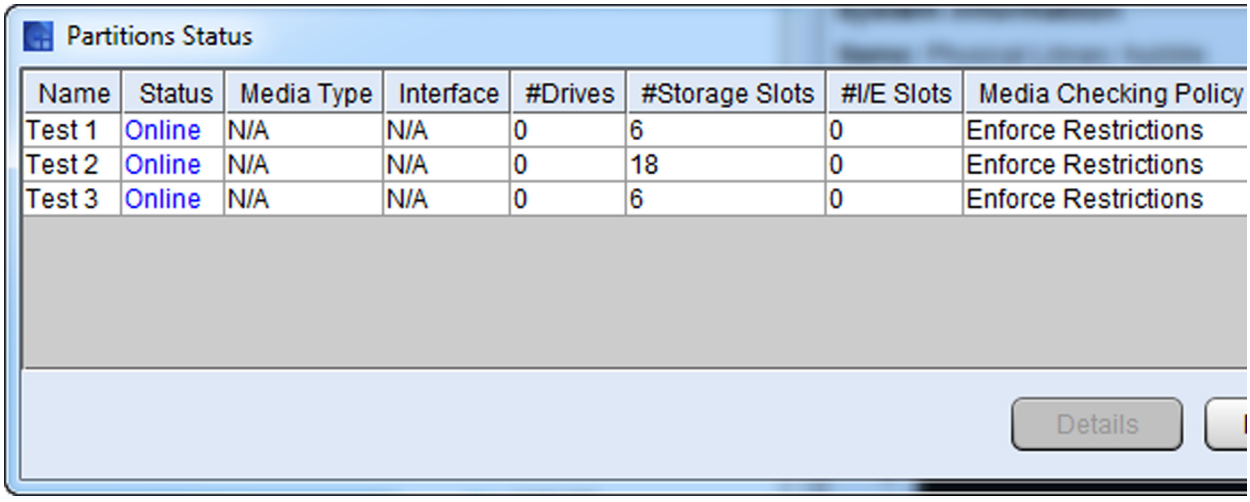
If you want to see settings and information for a partition but do not need to make changes, you can view partition status and partition details. Unlike modifying a partition, viewing the status and details does not require you to take a partition offline.

1 Make sure that you are viewing the physical library. From the **View** menu, click the name of the physical library.

2 On the menu bar, click **Monitor** > **Partitions** > **Status**. The **Partitions Status** dialog box appears with a list of all logical partitions in the library and information about each partition.

Figure 56 Partitions Status Dialog box

Left side of dialog box



Right side of dialog box

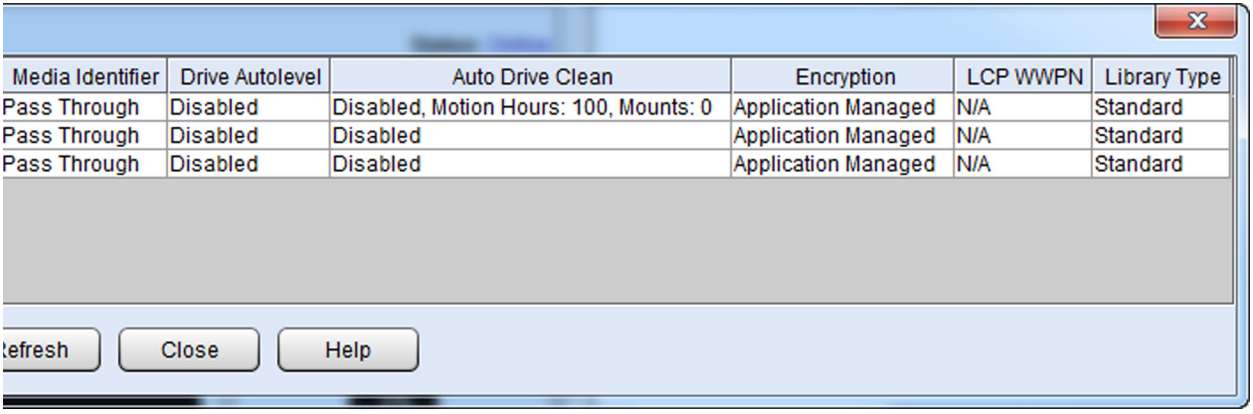
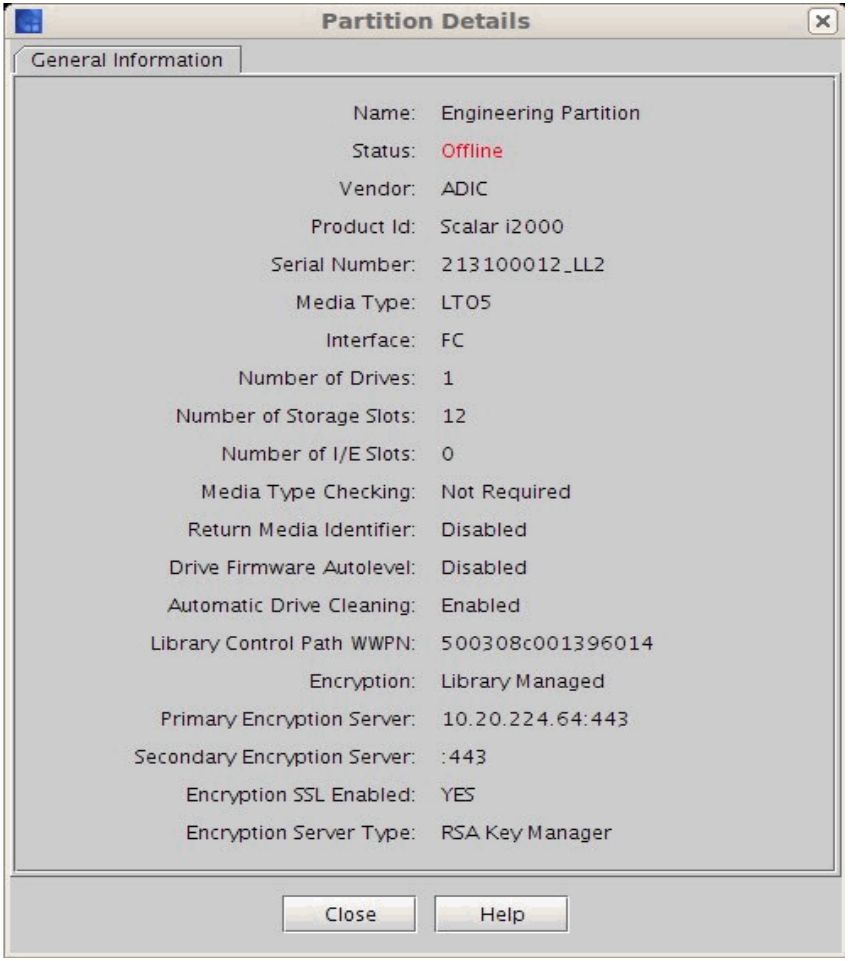


Table 49 on page 533 describes the elements on the **Partitions Status** dialog box.

Table 49 Partition Status

Element	Description
Name	The name of the partition.
Status	The status of the partition (Online or Offline).
Media Type	The type of media used in the partition (LTO-1, LTO-2, LTO-3, LTO-4, LTO-5, or LTO-6).
Interface	The type of interface used to connect to the host (FC).
#Drives	The number of tapes drives in the partition.
#Storage Slots	The number of storage slots in the partition.
#I/E Slots	The number of I/E station slots in the partition.
Media Type Checking	The current setting for media type checking (Required, Not Required, or Disabled).
Media Identifier	The current setting for return media identifier (Suffix, Pass Through, Prefix, or Disabled).
Drive Autolevel	The current setting for drive firmware autoleveling (Enabled or Disabled).
Auto Drive Clean	The current setting for automatic drive cleaning (Enabled or Disabled) as well as the number of motion hours set for each drive cleaning.
Encryption	Defines the encryption method for the partition. The values are Not Supported, Application Managed, or Library Managed. If the partition is enabled for FIPS, “FIPS” appears in parentheses.
LCP WWPN	The Library Control Path (LCP) World Wide Port Name (WWPN) for a partition. A WWPN will only be listed if control path or control path failover is used to present the partition to the SAN.
Library Type	Logical library/partition type - either Standard or Library Managed. If library managed, the type of library managed partition is listed in parentheses (for example, AMP, EDLM, or VAULT).

3 To see additional details for a partition, click the partition in the list, and then click **Details**. The **Partition Details** dialog box appears. It shows additional information about the partition, such as vendor, product ID, and serial number.



4 Click **Close** to close the **Partition Details** dialog box.

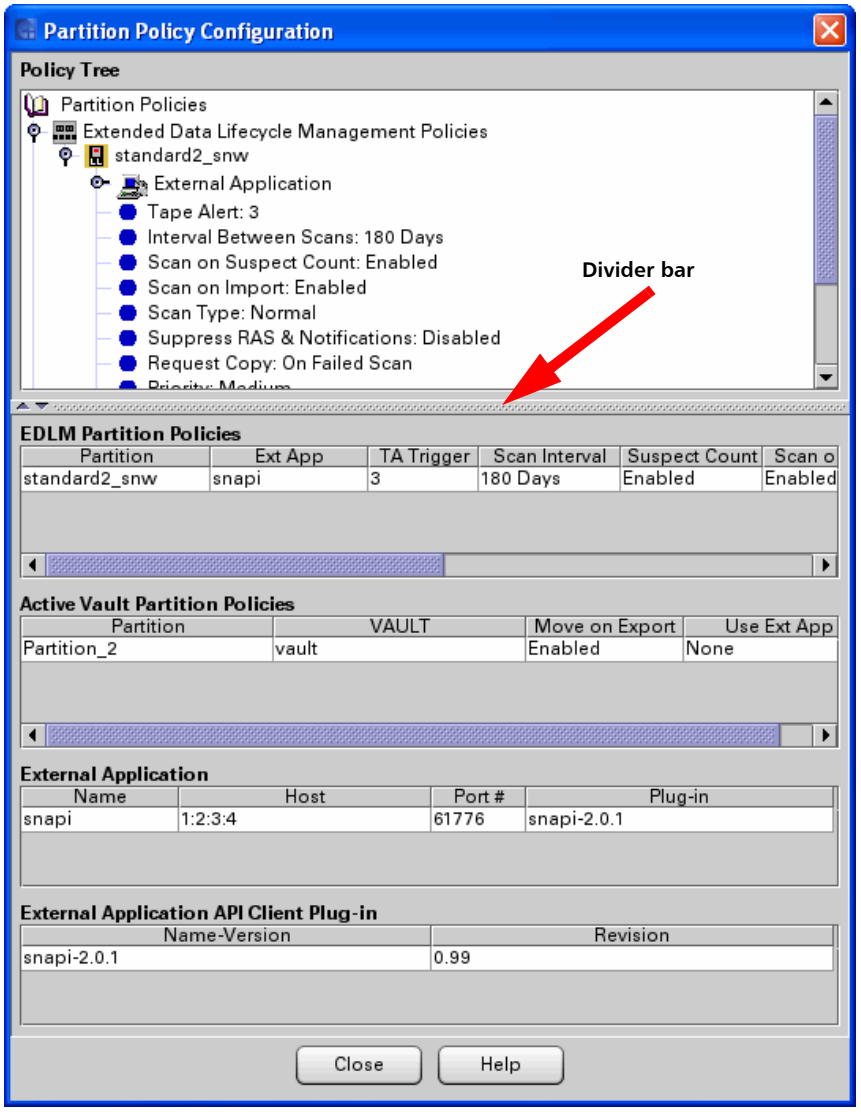
5 Click **Close** to return to the **Partitions Status** dialog box.

Monitoring Partition Policies

To view EDLM or Active Vault policies configured on partitions, click **Monitor > Partitions > Policies** from the LMC.

The Partition Policy Configuration screen appears. You can click the items in the **Policy Tree** section to expand them, or view the information in the **Policies** sections below. The **Policies** sections contain tables with information about EDLM and Active Vault policies, as well as external application and API client plug-in information.

You can click and drag the horizontal divider bar below the Policy Tree section to create more or less viewing space for the Policy Tree section if desired. You can also click the up/down arrows on the left side of the divider bar to hide or display the Policies sections.

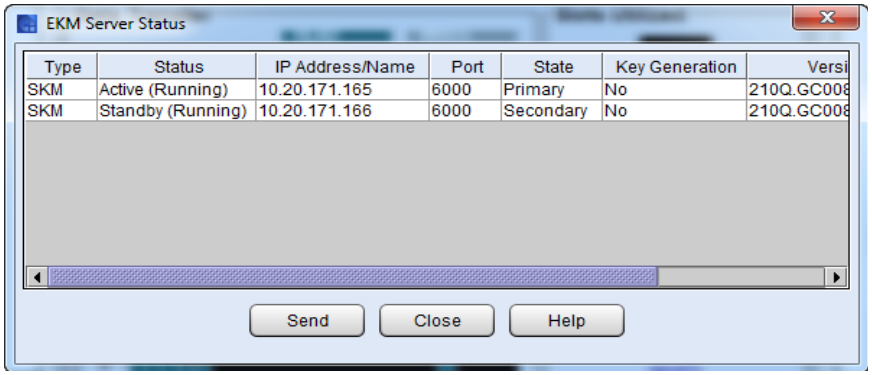


Monitoring EKM Server Status

For each server configured, you can monitor the server using the EKM Server Status dialog box.

1 From the **View** menu, click the name of the physical library or partition.

2 On the menu bar, click **Monitor** > **EKM Servers**. The **EKM Server Status** dialog box appears.



For each server, the **EKM Server Status** dialog box displays the following information - the table describes the elements on the EKM **Server Status** dialog box.

Element	Description
Type	The encryption server type (Q-EKM, SKM, KMIP, or RKM).
Status	The current status of the server: **Note: Note:** When the server indicates a "Running" status, this server will receive the next key request. **Q-EKM** — Active, Standby or Not Configured **SKM** — Active Running, Standby Running or Down, or Not Configured **KMIP** — Active Running, Standby Running or Down, or Not Configured **RKM** — Active Running or Down, Standby Running or Down, or Not Configured
IP Address/Name	The IP or host name of the server.
Port	The server port number: **Q-EKM**— Default 3801 for non-SSL and 443 for SSL **SKM** — default 6000 **KMIP** — 5696 **RKM** — 443

Element (Continued)	Description
State	Whether the server is Primary or Secondary.
Key Generation	For SKM only: **Yes** — encryption key generation in progress **No** — encryption key generation not in progress. Q-EKM, KMIP, and RKM — n/a
Version	For SKM only: Software version number
Serial Number	For SKM only: Server serial number

3 You can mail, save, or print status information by using the **Send** button (see Mailing, Saving, and Printing Status Information on page 538).

Mailing, Saving, and Printing Status Information

The **Send** button on each of the following status dialog boxes enables you to send status information to e-mail addresses:

- System Status
- Drive Status
- IO Blade Status
- SCSI Channel Status
- Fibre Channel Status
- Ethernet Blade Status
- I/E Station Status
- Slots Status
- Media Status

If you are accessing the LMC from a remote client, **Send** also enables you to save the information to a file or print it.

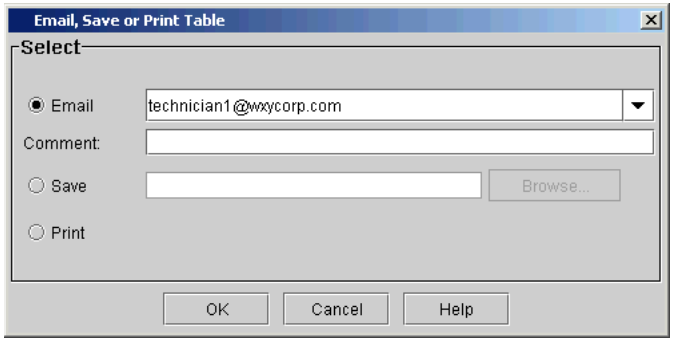
Note: You can mail, save, or print status information from a remote client. However, you cannot save or print the information from the library's touch screen.

The information that is sent will be the same as what the status dialog box appears at the time that you click **Send**.

Note: Before you perform the following procedure, you must make sure that e-mail is appropriately configured in the LMC so that the library can send information to the recipient. See Configuring E-mail on page 177.

1 Make sure that the status dialog box displays the status information that you want to send.

2 Click **Send**. The **Email, Save or Print Table** dialog box appears.



3 Perform one of the following tasks:

- To indicate that you want to send the information as an e-mail message to a recipient, select **Email**, and then either type an e-mail address in the **Email** text box or select an existing address from the drop-down list. You can type a comment in the **Comment** text box to send with the information.
- To indicate that you want to save the information, select **Save**, and then either type in the **Save** text box a path and a file name to which you want the information saved or click **Browse** to specify a location and a file name.

  Note: The **Save** option is available to remote client users only. It appears grayed out on the touch screen.

- To indicate that you want to send the information to a printer, select **Print**.

Note: The **Print** option is available to remote client users only. It appears grayed out on the touch screen.

4 To send, click **OK**.

Mailing or Saving the Configuration Record

Use the **Email Configuration Record** dialog to:

- Send the configuration record to a selected e-mail address
- Save the configuration record to a specified .txt file

For information about the configuration record, see About the Configuration Record on page 242.

Before you can e-mail the configuration record, the library e-mail account must be configured. For information on configuring the library e-mail account, see Configuring E-mail on page 177.

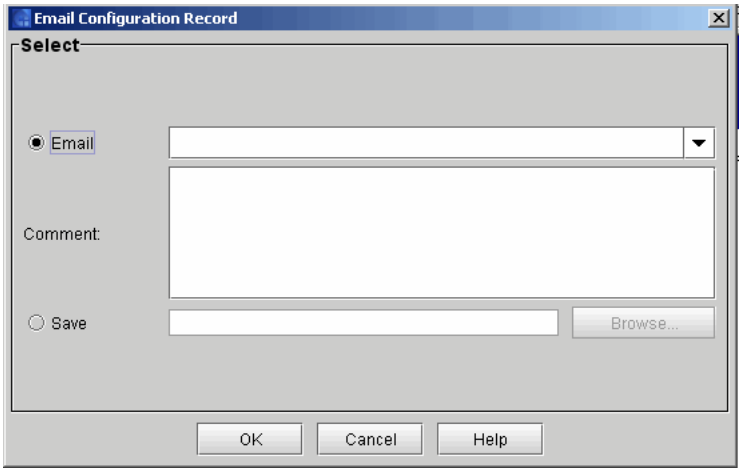
Note: Only users with administrative privileges can e-mail or save the configuration record.

Mailing the Configuration Record

To e-mail the configuration record:

1 Log on as an administrator.

2 From the menu bar, click **Monitor** > **Email Configuration Record**. The **Email Configuration Record** dialog box appears.



3 Click **Email** and select the destination e-mail address.

> **Note:** You can only specify one e-mail address. If you need to send the configuration record to multiple destinations, repeat this procedure for each e-mail address.

4 Use the **Comment** box to type any additional information you want to include in the e-mail message.

5 Click **OK** to send the configuration record and your comment text to the specified e-mail address and close the **Email Configuration Record** dialog box.

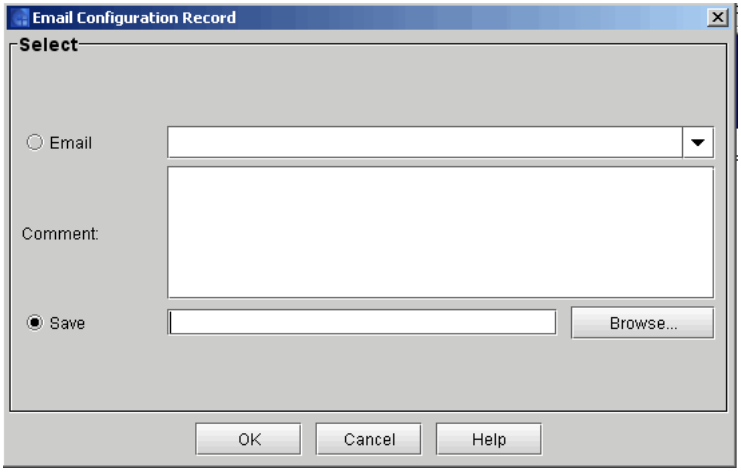
The e-mail message includes both the configuration record information and your comments as embedded text with "Library Configuration Information" as the subject.

Saving the Configuration Record

To save the configuration record:

1 Log on as an administrator.

2 From the menu bar, click **Monitor** > **Email Configuration Record**. The **Email Configuration Record** dialog box appears.



3 Click **Save** and use the **Browse** function to specify the file name and location.

4 Click **OK** to save the configuration record to the specified location and close the **Email Configuration Record** dialog box.

Maintenance Actions

If you are experiencing system problems, make a quick check of subsystems and components before looking for a service ticket or contacting technical support. Your service representative might ask you to check these things or, if you are an administrator, you might be asked to run a diagnostic procedure or upload new firmware.

Administrative users have access to the all the commands on the **Tools** menu. Use this menu to test the drives, as well as to capture a snapshot, to update firmware, and to use the **Teach** tool. The **Tickets** command on the **Tools** menu displays tickets that the library creates when it detects issues within its subsystems. For more information about the Tickets command, see Troubleshooting Your Library on page 35. For a summary of user privileges defined by physical library, partition, and command menu, see Table 37 on page 435.

Is the Access Door Closed?

Library operations are put into a **Not Ready** state when the access door is opened. If library operations have stopped, check whether the access door is shut and the **Robotics Enabled** indicator is solid green.

Is a Cartridge Old?

Cartridges can become old and less dependable. If you experience problems reading, writing, or otherwise using a cartridge, try the following courses of action:

- Use the **Monitor > Media** command to determine the number of mounts for the cartridge, and then compare that number to other cartridges in the system. If the cartridge has been used excessively, replace it with a new cartridge.
- Ask an administrator to put the cartridge in a different drive, and then use the **Tools > Drives** command to check the error count. If the error count continues to increase, replace the old cartridge with a new cartridge.
- If you have received a message about read/write failures, first copy the data from the failing cartridge, and then replace it with a new cartridge.

Using Library Explorer

You can use the **Library Explorer** feature to view a graphical presentation of all the drives, cartridges, and slots in the library. The **Library Explorer** can display all library elements according to physical location in any configuration, from one to seventeen modules, and one drive up to the maximum number of 192 drives.

You can access the Library Explorer when viewing either the physical library or an individual partition (from the **View** menu). When viewing from a partition, you only see the elements belonging to that partition in the graphical display.

The **Library Explorer** features are available to administrator and service users, along with non-administrative users who have limited access to library functions. Users who do not have administrative privileges can perform all Operations options available to non-administrative users directly from the **Library Explorer** dialog boxes.

You can use the Library Explorer to directly perform the following tasks:

- Locate an element by entering its address

- Locate a cartridge by entering the media barcode
- Load and unload drives
- Move cartridges
- Perform inventory
- Import and export
- View drive details
- Perform all drive related functions
- View partition resources
- View the location of cleaning tapes

To use the Library Explorer:

1 From the **Tools** menu, click **Library Explorer**. The **Library Explorer** dialog box appears.

2 You can display library data using either the **Select Filter** options or clicking on a particular module in the **Select Module** area. In addition, there is a button toward the bottom of the screen called **Partition View**. If you click on this button, the displayed information is color-coded according to partition so it is easy to see where all the elements in each partitions are located.

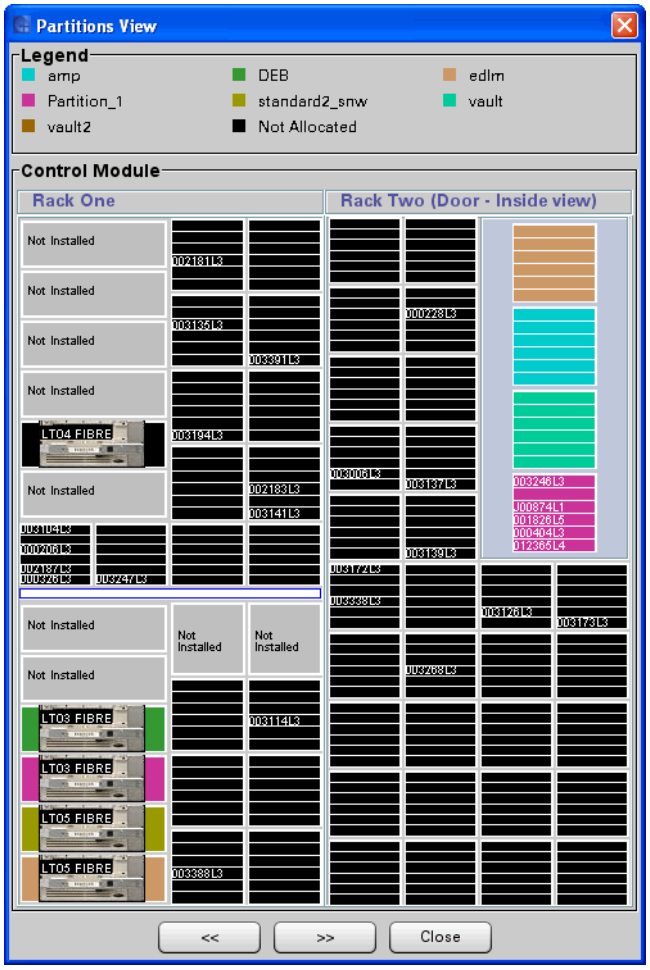
- In the **Select Filter** area, you can search for and display specific criteria according to device type and location coordinates, or by **Media ID**.
  - Select the **Device Type** filter, and then from the **Type** drop-down list, click the appropriate device type: Storage, IE (I/E Station), or Drive. Click **Show**.

    The Control **Module** dialog box displays a graphical view of the library elements according to your **Type** filter choices.
  - To search for a specific cartridge according to the cartridge's barcode, select the **Media ID** filter, type the barcode in the **Media ID** field, and then click **Show**.

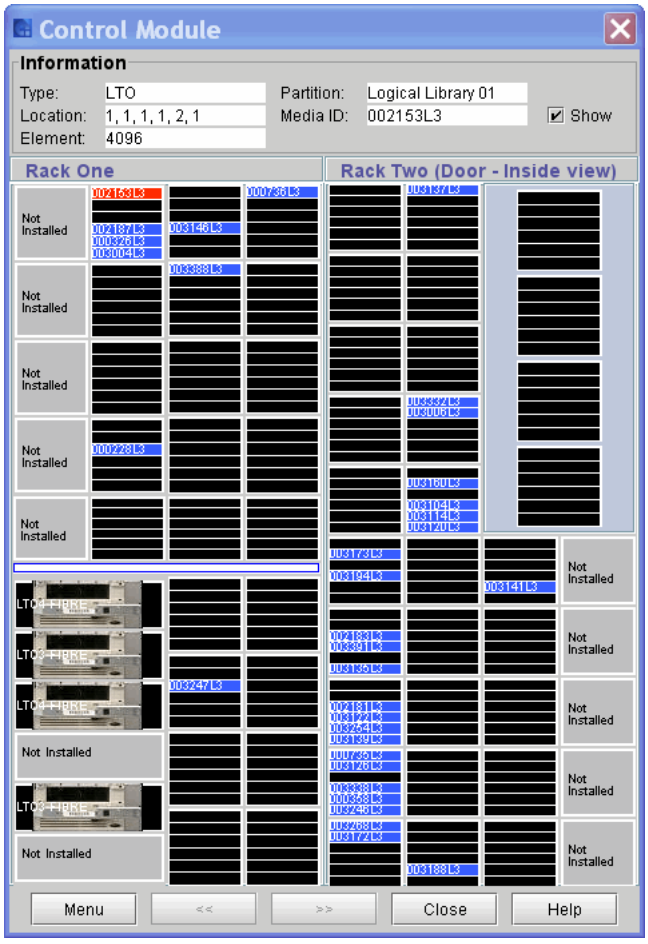
    The **Module** dialog box displays the specific cartridge highlighted in red within the module where it is located.
  - To search for a specific cartridge according to the element address, select the **Element Address** filter, type the element address in the field, then click **Show**. You must be in partition view to filter using the **Element Address.**
- In the **Select Module** area, you can select a specific module in your library to view. On a multi-module library, all modules are represented.
  - In the **Select Module** area, click on the module you want to view. The **Module** dialog box displays the current configuration of Rack one and Rack two (Door - Inside view) according to the module you chose.

    Note: The Rack two (Door - Inside view) view is MIRROR image of the outside view, so I/E station B is on the left, and I/E station A is on the right.
- If you click the **Partition View** button, the graphical display opens at the left-most module. The upper portion of the screen displays a legend showing which colors represent each

partition. You can use the right/left arrows at the bottom of the screen to scroll through all library modules.



3 If you chose to search for an element by its address, or chose to locate a cartridge by its media barcode, your search result appears in red in the **Control Module** dialog box.



4 To return to the **Library Explorer** dialog box, click **Close**. The **Library Explorer** dialog box appears.

Understanding the Graphical Display

You can access Library Explorer Control Module from both the physical and partition views. If you are in a partition view, you can view slots and drives pertaining to that particular partition.

- The **Library Explorer Module** dialog box displays the current configuration of Rack One and Rack Two (Door - Inside view) according to the module you chose.
- The Rack Two (Door - Inside view) view is MIRROR image of the outside view, so I/E station B is on the left, and I/E station A is on the right.
- Slots containing cartridges are blue. Empty slots are black. Your search result appears in red.
- Details concerning the particular cartridge, drive, or slot appear in the Information area.

The **Information** area displays the following details:

- Type
- Location
- Element
- Partition
- Media ID
- Barcode numbers appear on slots containing cartridges. If you do not want to view the barcode information, clear the **Show** check box.
- If you click on a specific slot or drive, that slot or drive is highlighted in red, and details about the slot or drive appear in the Information area.
- If you hover your mouse over a specific segment in the module a tool tip appears, displaying the coordinates of that particular segment.
- To move from one module to another, click on the arrows at the bottom of the dialog box.

Accessing Library Operations

To access available library operations for a specific drive or slot, you can either click on **Menu** or right click on the drive or slot. You can perform the following operations, depending on what library view you are using. From the **View** menu, click the name of the physical library or partition.

- Drive Details

- Inventory
- Loading Drives
- Unloading Drives
- Move Media
- Importing Cartridges
- Exporting Cartridges

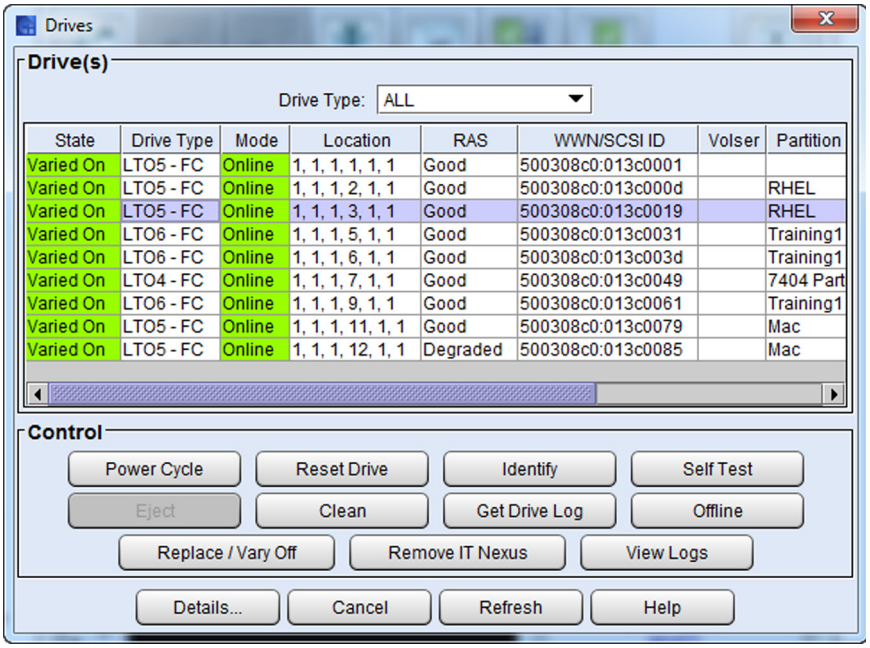
Drives

The **Drives** dialog box enables you to do the following:

- Cycle power to drives
- Reset drives
- Identify drives
- Run a pass/fail test for LTO-type drives
- Eject tape cartridges from drives
- Clean drives
- Send the logs by e-mail or save drive logs
- Take drive online or offline
- Vary drives on or off
- Remove drive reservations

Drive information on this dialog box is automatically refreshed whenever a drive is added or removed.

1. Log on as an administrator.
2. Make sure that you are viewing the physical library. From the **View** menu, click the name of the physical library.
3. Click **Tools > Drives**. The **Drives** dialog box appears.



The following table describes the elements on the **Drives** dialog box.

Element	Description
In the **Drive(s)** area:	
Drive Type drop-down list	Enables you to select the type of drives you want to list on the **Drives** dialog box (for example, **LTO1** for LTO-1 tape drives). **All** lists every drive in the library.
State	The state of the drive (Varied On, Varied Off, or Pending [if in transition]).
Drive Type	The type of drive (for example, LTO2 - FC).
Location	The location of the drive by means of a coordinate system. For information about location coordinates, see Understanding Location Coordinates on page 449.
RAS	The status of the drive as reported by the RAS system (for example, Good or Failed).

Element	Description
WWN/SCSI ID	Indicates either: • For Fibre drives only, the World Wide Name of the drive, or • For SCSI drives only, the SCSI ID of the drive
Volser	If a cartridge is loaded in the specified drive, the volume serial number of the cartridge.
Partition Name	The name of the partition to which the drive is assigned.
Serial #	The tape drive's serial number.
Firmware Version	Tape version of firmware on the tape drive.
In the **Control** area:	
Power Cycle	Cycles power to the specified drive by removing the power and then restoring it. In general, you should try to reset drives before you cycle power to them.
Reset Drive	Resets the specified drive without cycling the power.
Identify	Causes status LEDs on the back of the specified drive to blink rapidly so that you can identify it. When you click **Identify**, a message appears that informs you that you can now identify the drive by the rapidly blinking LED on the back of it. After you find the drive, click **OK** to stop the rapid blinking.
Self Test	For LTO-type drives only, runs a pass/fail test on the specified drive. This button is available only when you select an LTO-type drive.
Eject	Ejects any currently loaded tape from the specified drive.
Clean	Enables the drive cleaning process (see Cleaning a Drive on page 556).
Get Drive Log	Enables you to mail or save the log of a Fibre drive that is attached to an I/O blade (see Mailing, Saving, and Printing Test Logs on page 642). This button is available only for I/O blade-attached Fibre drives that are properly connected and configured. If the button is not available for a Fibre drive, verify that it is properly connected to the I/O blade and that communication is established between them.

Element	Description
Replace/Vary Off or Activate/Vary On	Powers off or on the specified tape drive within the drive sled. The label of the button toggles between **Replace/Vary Off** and **Activate/Vary On**. Each use of this button updates the drive information in the **Drive(s)** area. Use this button when you replace drives.
Remove IT Nexus	Allows the library to clear drive reservations and media removal preventions.
View Logs	View any saved drive logs.

The **Details** button displays the **Drive Details** dialog box. For more information, see Viewing Drive Details on page 552.

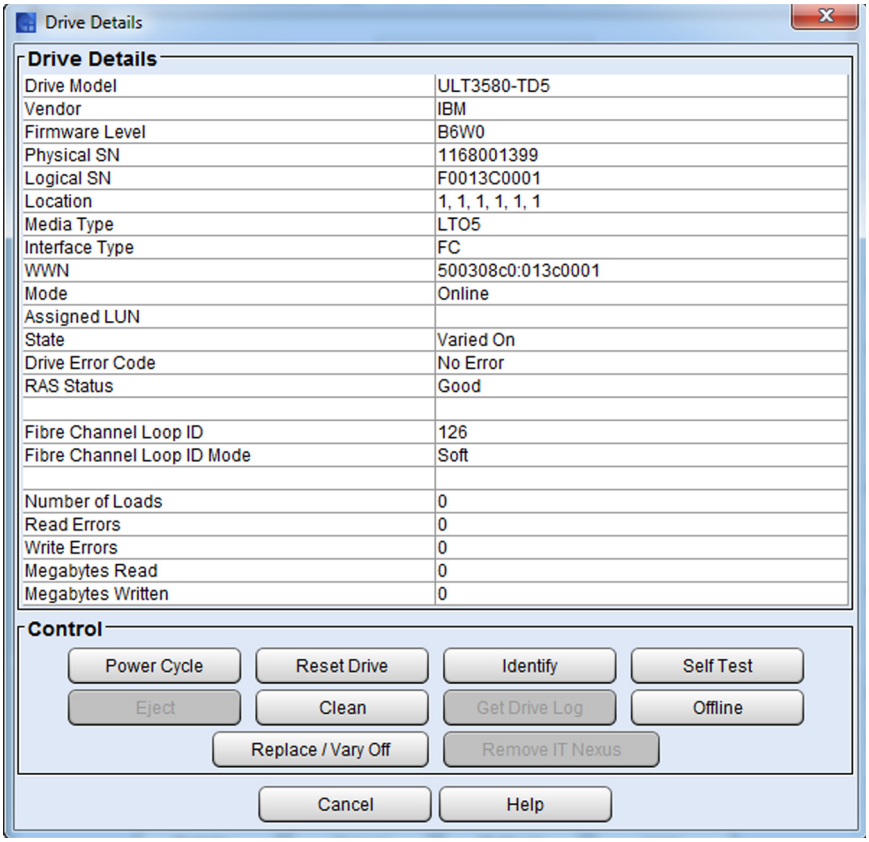
4 In the **Drive(s)** area, click the appropriate drive row to highlight it.

5 Perform operations in either the **Fibre Channel Parameters** area or the **Control** area of the **Drives** dialog box.

Viewing Drive Details

1 On the **Drives** dialog box in the **Drive(s)** area, click the appropriate drive row to highlight it.

2 Click **Details**. The **Drive Details** dialog box appears.



The **Drive Details** area of the **Drive Details** dialog box displays detailed information about the selected drive.

The following table describes the elements that appear in this area. For descriptions of elements in the **Fibre Channel Parameters** and **Control** areas, see Drives on page 549.

Element	Description
Drive Model	The brand name of the drive model.
Vendor	The drive vendor.
Firmware Level	The firmware version that is currently installed on the drive.
Physical SN	The serial number of the particular drive.

Element	Description
Logical SN	The logical serial number that the library assigns to a drive in a specific location. This is not the serial number of the particular drive (see **Physical SN** in this table). If a drive is replaced by another drive in the same library location, the logical serial number remains the same. From the host's perspective, the replacement drive is the same as the original one. If the logical serial number addressing feature is disabled for the library, **Disabled** appears in this field.
Location	The location of the drive by means of a coordinate system. Refer to Understanding Location Coordinates on page 449.
Media Type	The type of drive (for example, **LTO2** for LTO-2 tape drives).
Interface Type	The type of interface (FC or SCSI).
WWN	For Fibre drives only, the World Wide Name of the drive. This field does not appear for SCSI drives.
Mode	The drive Online/Offline mode.
Assigned LUN	The assigned logical unit number.
State	The tape drive vary off (ready for replacement) and vary on (tape drive activation) state.
Drive Error Code	The tape drive error code.
RAS Status	The status of the drive as reported by the RAS sub-system (for example, Good or Failed).
Fibre Channel Loop ID	For Fibre drives only, the loop ID assigned to the drive.
Fibre Channel Loop ID Mode	For Fibre drives only, the way in which the loop ID is assigned to the drive (Hard or Soft).
Number of Loads	The number of loads during the drive's history.
Read Errors	The number of read errors that have occurred during the drive's history.
Write Errors	The number of write errors that have occurred during the drive's history.
Megabytes Read	The amount of data in megabytes that the drive has read during its history.
Megabytes Written	The amount of data in megabytes that the drive has written during its history.

3 To return to the **Drives** dialog box, click **Cancel**.

Mailing and Saving Drive Logs

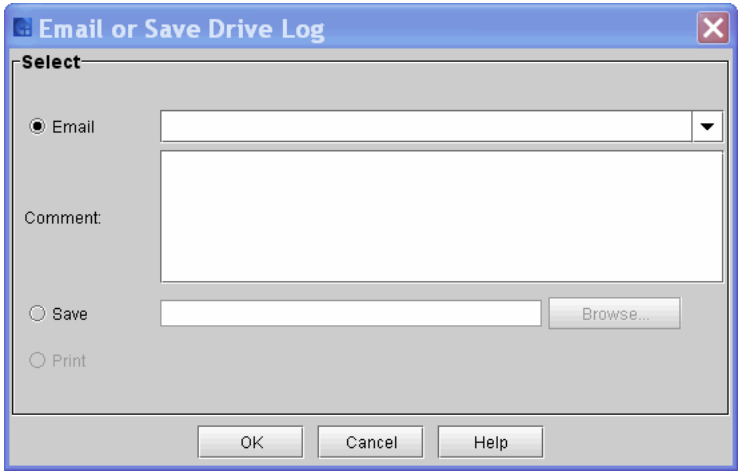
The **Get Drive Log** button on the **Drives** dialog box enables you to send drive logs to e-mail addresses. If you are accessing the LMC from a remote client, **Get Drive Log** also enables you to save the information to a ZIP file.

Note: You can mail or save logs from a remote client. However, you cannot save logs from the library's touch screen.

Before you perform the following procedure, you must make sure that e-mail is appropriately configured in the LMC so that the library can send logs to the recipient. For more information about configuring e-mail, see Configuring E-mail on page 177.

---

1 From the **Drives** dialog box, click **Get Drive Log**. The **Email or Save Drive Log** dialog box appears.



2 Perform one of the following tasks:

- To indicate that you want to send the log as an e-mail message to a recipient, select **Email**, and then either type an e-mail address in the **Email** text box or select an existing address from the drop-down list. You can type a comment in the **Comment** text box to send with the log.

- To indicate that you want to save the log, select **Save**, and then either type in the **Save** text box a path and a file name to which you want the information saved or click **Browse** to specify a location and a file name.

  Note: The **Save** option is available to remote client users only. It appears grayed out on the touch screen.

3 To send, click **OK**.

Cleaning a Drive

Use the **Drives** dialog box to manually initiate a drive cleaning operation. When cleaning a drive, you can use cleaning media inserted in the I/E station or media in an assigned cleaning magazine.

Note: If the host application coordinates drive cleaning, or if periodic drive cleaning is enabled for the partition, you do not need to manually initiate a drive cleaning operation to perform routine cleaning tasks. In these cases, routine cleaning is handled by the host application or the library, and you should manually initiate a drive cleaning operation only as part of a troubleshooting procedure.

Before you manually initiate a drive cleaning operation, you must add cleaning media to the library. The cleaning media must be appropriate for the type of drive being cleaned.

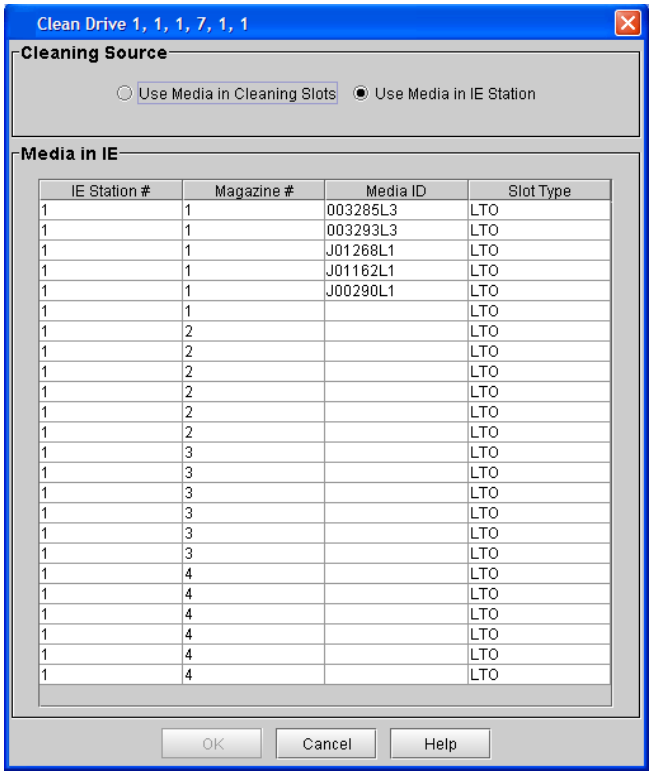
There are two ways to add cleaning media to the library:

- Insert cleaning media into the I/E station and close the I/E station door.
- Configure drive cleaning by assigning cleaning magazines and importing cleaning media. For more information on configuring drive cleaning, see Configuring Drive Cleaning on page 217.

After adding cleaning media to the library, manually initiate a drive cleaning operation.

1 Select **Tools > Drives** to display the **Drives** dialog box.

2 Select a drive in the list, and then click **Clean**. The **Clean Drive** dialog box appears.



3 Under **Cleaning Source**, select an option:

- To use cleaning media inserted in the I/E station, click **Use Media in IE Station**, and then click a piece of cleaning media in the list.
- To use cleaning media in an assigned cleaning magazine, click **Use Media in Cleaning Slots**.

4 Click **OK**.

The drive cleaning operation is initiated, and the **Clean Drive** dialog box closes. Once the cleaning operation completes, the cleaning media is returned to the I/E station or assigned cleaning magazine.

Note: The system does not display a message when the cleaning operation is completed.

Remove Drive Reservations

When tape drive is setup for advanced path failover and a host is lost or locked up such that it cannot remove host or application applied reservations and/or media removal preventions for a tape drive, the reservation must be manually removed. This frees up the drive to be available by other hosts or applications.

The Remove IT Nexus button allows the Library User/Admin to remove all host reservations applied to any tape drive.

Note: The Remove IT Nexus button applies for HP LTO-5 or greater drives and is used only when a host is not able to remove or clear reservations and/or media removal preventions.

Use the **Drives** dialog box to manually remove all drive reservations, persistent and non-persistent. To remove a drive reservation:

1. Select **Tools > Drives** to display the **Drives** dialog box.
2. Select a drive in the list, and then click **Remove IT Nexus**. A warning dialog box displays stating that removing the reservation may cause a loss of data.
3. Click **Yes**.
4. A dialog box displays indicating that the operation was a success.
5. Click **OK**.

Working With Connectivity

The **Connectivity** dialog box enables you to do the following:

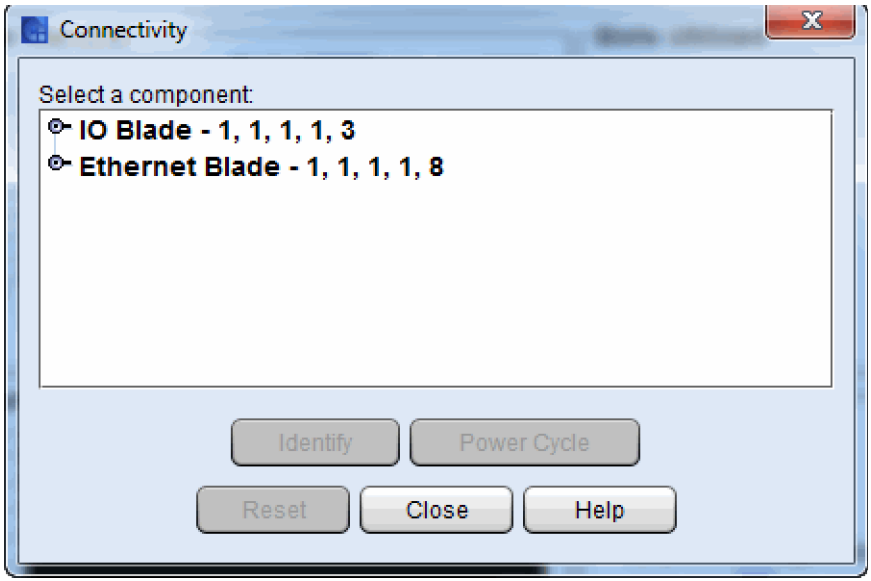
- Reset an I/O blade
- Reset the Fibre Channel port on an I/O blade
- Power cycle an EEB or I/O blade
- Visually locate a specific EEB or I/O blade in the library

To reset or identify port/blade connectivity:

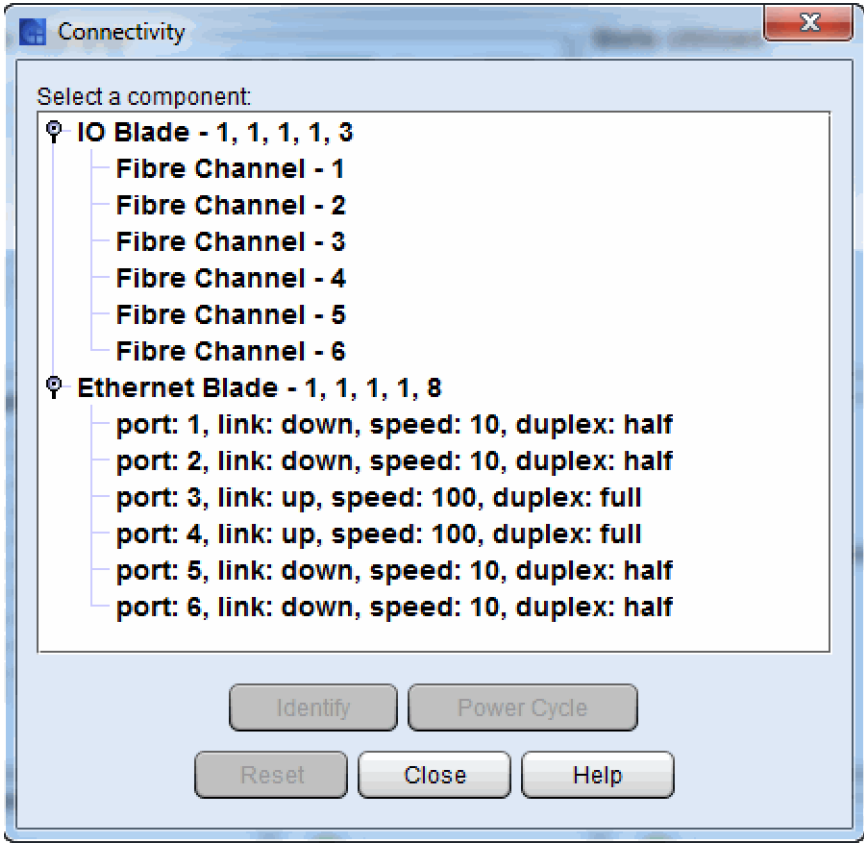
1. Log on as an administrator.
2. Make sure that you are viewing the physical library. From the **View** menu, click the name of the physical library.

3 Click **Tools > Connectivity**. The **Connectivity** dialog box appears with the EEB and all I/O blades in the library listed.

Note: If the physical library is not offline, you receive a message that asks you whether you want to take it offline. Click **Yes**.



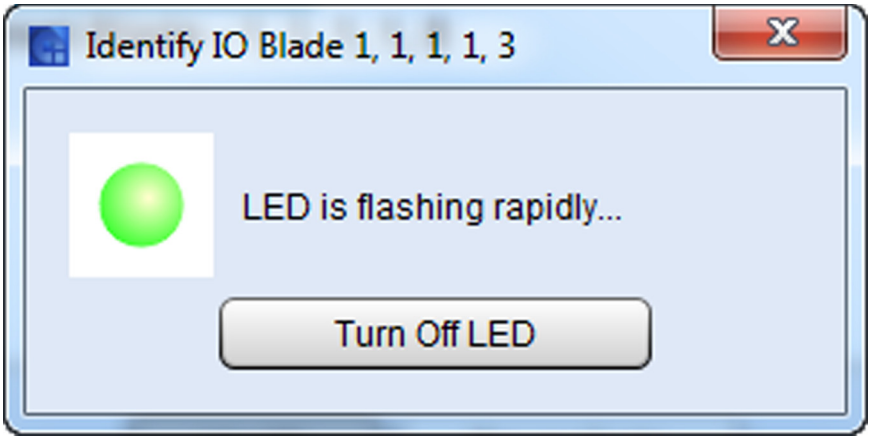
4 To display the ports for a specific blade, click the name of the blade (EEB or I/O blade). For information about location coordinates, see Understanding Location Coordinates on page 449.



5 Perform one of the following tasks:

- To reset either an entire I/O blade, an individual Fibre Channel port on an I/O blade, or an EEB, select the blade or port and click **Reset**.
- To power cycle an I/O blade or EEB, select the blade and click **Power Cycle**.
- To cause the LEDs on an EEB or I/O blade to blink rapidly so that you can find it in the library, select the blade, and then click **Identify**. After you locate the I/O blade, click **Turn Off LED**.

  When you click **Identify**, the following dialog box appears.



6 After you find the I/O blade, click **Turn Off LED**.

Capturing Snapshots

The **Capture Snapshot** command enables you to capture detailed information about the entire library in a single file and save it to disk or mail it to technical support. The captured information consists of configuration data, status information, and trace logs for library components, including the LMC, the MCB, the CMB, the robotics control subsystem (RCS), and the I/O blades.

Trace logs collect problem data for up to 72 hours of continuous library operation. They provide Quantum engineering personnel with vital library information for troubleshooting and solving problems. You should capture snapshots when technical support requests them.

Details about capturing snapshots include:

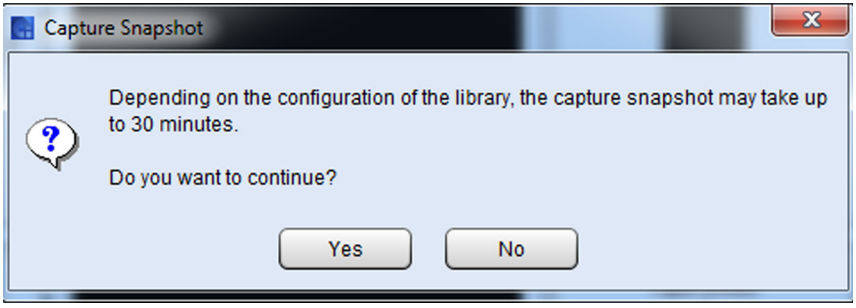
- Because the snapshot requires analysis by trained Quantum personnel, send captured snapshots to www.quantum.com/osr when Quantum requests them.
- Depending on the library configuration, capturing a snapshot can take as long as 30 minutes and the resulting file size can be large. Firewall file size limitations could prohibit you from mailing it. In addition, other library communications may be delayed up to 6 minutes during a snapshot capture.
- You can e-mail or save snapshots from a remote client. However, you cannot save snapshots from the library's touch screen but you

can e-mail them. You cannot print snapshots from either the remote client or the touch screen.

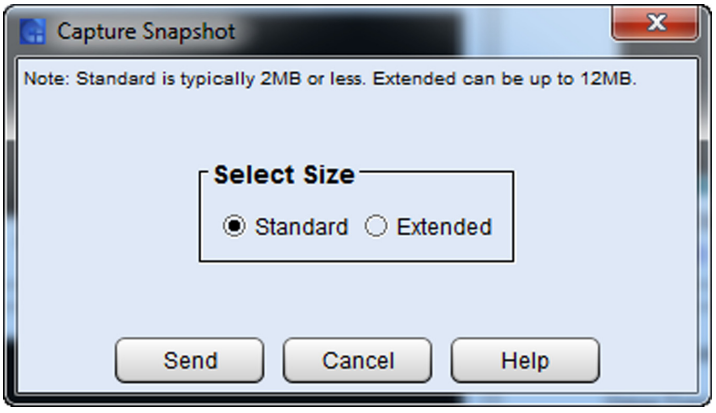
- Because snapshots do not contain binary data, secure sites allow them to be sent offsite.
- If you want to mail snapshots to e-mail addresses, you must make sure that e-mail is appropriately configured in the LMC before you perform the following procedure so that the library can send snapshots to the recipient. See Configuring E-mail on page 177.

To capture a snapshot:

1. Log on as an administrator.
2. Make sure that applications are not attempting to access the library.
3. Make sure that you are viewing the physical library. From the **View** menu, click the name of the physical library.
4. Click **Tools > Capture Snapshot**. The following message appears:

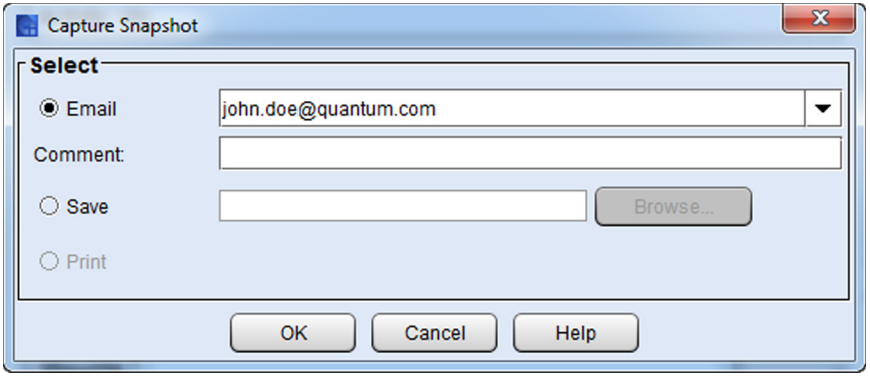


5. If you want to continue, click **Yes**. The **Capture Snapshot** dialog box appears.



The **Standard** option captures information about all library components. The **Extended** option captures a greater amount of historical event logging information.

6 Select **Standard** or **Extended**, and then click **Send**. The **Email, Save or Print Table** dialog box appears.



7 Perform one of the following tasks:

- To indicate that you want to send the snapshot as an e-mail message to a recipient, select **Email**, and then either type an e-mail address in the **Email** text box or select an existing e-mail address from the **Email** drop-down list. You can type a comment in the **Comment** text box to send with the snapshot.

  Note: Typically, you will send the snapshot to Quantum Support when requested to do so.

- To indicate that you want to save the snapshot, select **Save**, and then either type in the **Save** text box a path and a file name to which you want the snapshot saved or click **Browse** to specify a location and a file name.

  Note: The **Save** option is available to remote client users only. It appears grayed out on the touch screen.

8 To send, click **OK**.

Updating Library Software

To download library software to the library and perform various update operations, you can use the **Update Software** command to access the **Update Software Wizard**.

Note: This process may take 30 to 45 minutes.

Library software update files contain updates for one or more of the following library components:

- Management control blade (MCB)
- Robotics control unit (RCU)
- Robot(s)
- Tower(s)
- Control management blade (CMB)
- I/O blades
- Ethernet Control blade (EEB)
- Power and control subsystem (PIP) for blades
- Drive sleds

  Individual drive firmware image files contain updates for specific types of drives. Before you can update the library with a library software update file, you must use the Update Software Wizard to download the file to the MCB. You can use the **Update Software Wizard** to perform the following operations:

- Install new library software (including downloading and installing software)
- Reinstall the currently installed library software package

- Roll back library software to a previously installed package

You can perform all update operations while viewing the physical library. However, if you are viewing a partition, the only operations that are available to you is updating drive firmware (by using either firmware images or update tapes) for drives within the partition.

You can perform update operations from either the library's touch screen or a remote client on a remote host computer, with one exception. You cannot download images from the local touch screen.

During the software update process, the MCB distributes the various parts of the software package to the proper library components. The MCB also keeps track of the software components it updates so that you can roll those components back to a previous version.

After the library finishes installing new library software or rolling back library software to a previously installed level, the library automatically restarts. Any necessary autoleveling of library components begins after the library powers up and discovers library components.

Caution: As a result of restore, rescue, or revert operations, the library shuts down. You must have physical access to the library to bring the library back up. If you are performing a restore, rescue, or revert operation using remote access, the library will remain shut down until the library is directly powered back on.

If you choose to reinstall the currently installed software package, the robotics control unit (RCU), picker, and drive sleds are updated. Therefore, the library does not restart after the re-installation process completes. The re-installation procedure should be run only under specific circumstances. For more information, see Rolling Back to the Previous Build Package on page 576.

Note: Rollback and re-installation of current package options are viable recovery steps during a failed firmware upgrade, however these features should not be used as troubleshooting tools.

Accessing the Update Software Wizard

The **Update Software Wizard** gives you access to all of the library's software update operations.

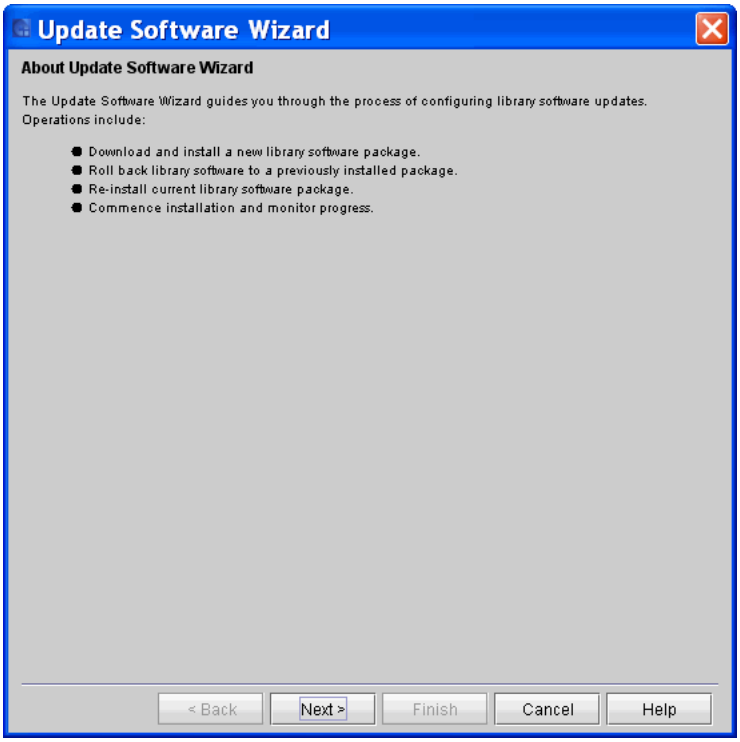
Note: Before performing a software upgrade, we recommend that you shut down and restart the library.

---

1. Log on as service.
2. You can access the **Update Software Wizard** while viewing either the physical library or a partition. From the **View** menu, click the name of the physical library or the appropriate partition.

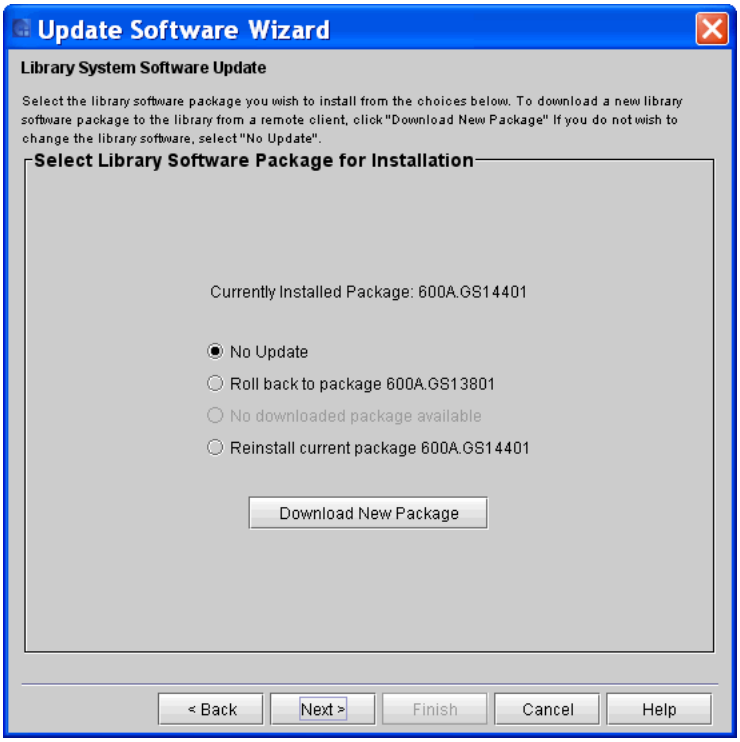
   Click **Tools > Update Software > Library**. The **Update Software Wizard** dialog box appears.

   Note: Each firmware release has specific upgrade instructions included with the release. These specific upgrade instructions need to be followed to ensure that the firmware upgrade will be successful. Contact Quantum Support to obtain specific drive firmware upgrade instructions.



This dialog box explains the operations you can perform by using the **Update Software Wizard**.

3 If you are ready to proceed, click **Next**. If you are not ready to proceed, click **Cancel**. The **Select Library Software Package for Installation** dialog box appears.



The remaining procedures in this section start with the **Library System Software Update** dialog box.

Installing New Library Software

To update your library software, you must download a new library software package to the library's management control blade (MCB) from the remote client's file system, and then install the downloaded software. You can perform the library software update from either the library's touch screen or a remote client, but you must perform the software download to the MCB from a remote client.

Note: If you are accessing the LMC using the remote client application, be aware that after you update the library software and the library restarts, you will not be able to view the LMC from the remote client application. You must update the client software to match the version of software you installed on the library.

Downloading a New Library Software Package

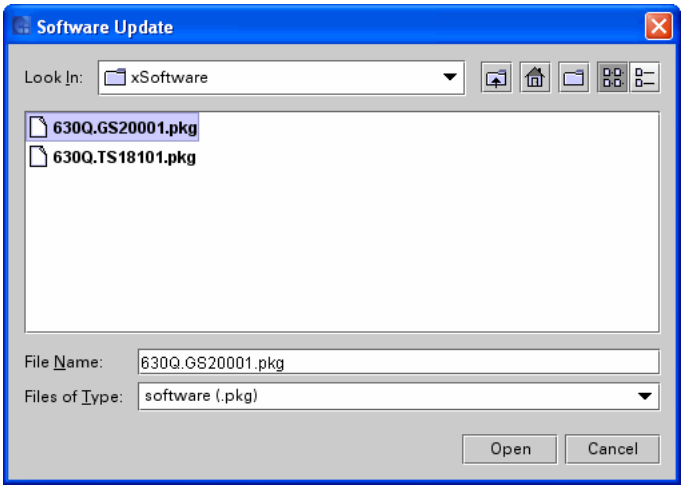
Before you install a new library software package, you must download the package to the library's MCB from the remote client's file system. You must perform the download from a remote client.

Note: Before you begin the following procedure, make sure that you have obtained the new library software package from Quantum and placed it in an accessible location on your laptop.

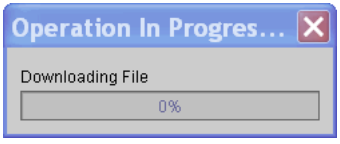
Caution: As a result of restore, rescue, or revert operations, the library shuts down. You must have physical access to the library to bring the library back up. If you are performing a restore, rescue, or revert operation using remote access, the library will remain shut down until the library is directly powered back on.

1 On the **Library System Software Update** dialog box, click **Download New Package**. The **Software Update** dialog box appears.

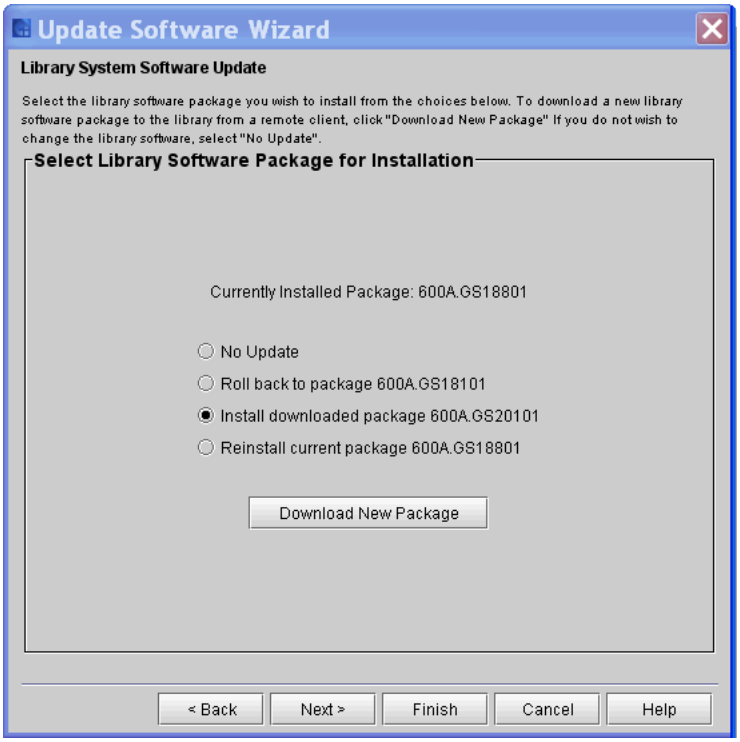
Note: If you are running the i8 software version, the library software file has a suffix of .pkg (for example, 300A.TS01701.pkg) shown in figure below. For software versions prior to i8, the filename suffix is .rpm.



2 Navigate to the location of the software file (with a **.pkg** extension) you want to download, click the file to highlight it, and then click **Open**. The **Operation in Progress** screen appears displaying the progress of the download.



The download process copies the software file from the remote file system to the library's MCB. When the download process completes, the **Library System Software Update** dialog box appears again with the **Install downloaded package** option automatically selected.



The version number of the software package appears at the end of the **Install downloaded package** option.

Installing a New Library Software Package

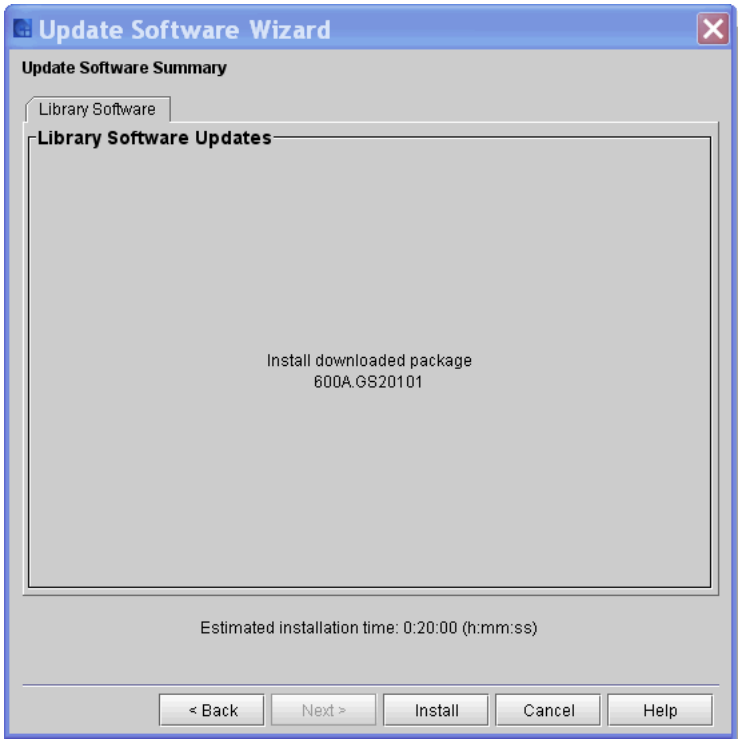
After you download the new library software package, you are ready to install it from either the library's touch screen or a remote client. This procedure assumes that you are working from a remote client.

1 On the **Library System Software Update** dialog box, select **Install downloaded package**.

Note: If you downloaded a software package and then began this procedure without closing the **Update Software Wizard - Library System Software Update** dialog box, **Install downloaded package** is already selected.

2 Click **Next**.

The estimated time for the installation is displayed.



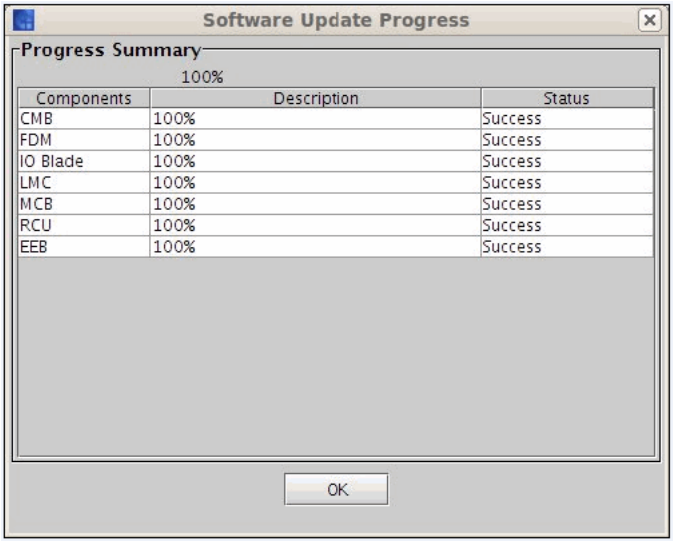
3 Click **Install.** A warning message appears asking you to take the library offline.

4 Click **Yes**.

Note: The library automatically logs off other users so that they cannot perform library operations while the library software update operation is in progress.

The Update **Software Summary** window appears asking if you want to continue.

5 Click **Yes.** The **Software Update Progress** screen appears displaying the progress of the installation.



Real-time progress information appears under **Progress Summary** in the **Description** and **Status** columns.

Once 100% success has been achieved for all components, the library is shutdown. This process could take several minutes.

6 Once complete, the **Software Update Progress** screen appears, click **OK**. The Attention message appears informing you that the software update was successful, the library will be rebooting, and that you have been automatically logged off from the system.

Note: If the software update was not successful, a RAS ticket is generates. Resolve all RAS tickets and begin the software update process again.

---

7 Click **OK**. The message **Library is being shutdown...** appears. This action may take a few minutes. The **Operation in Progress** screen appears.

8 Log off close the browser.

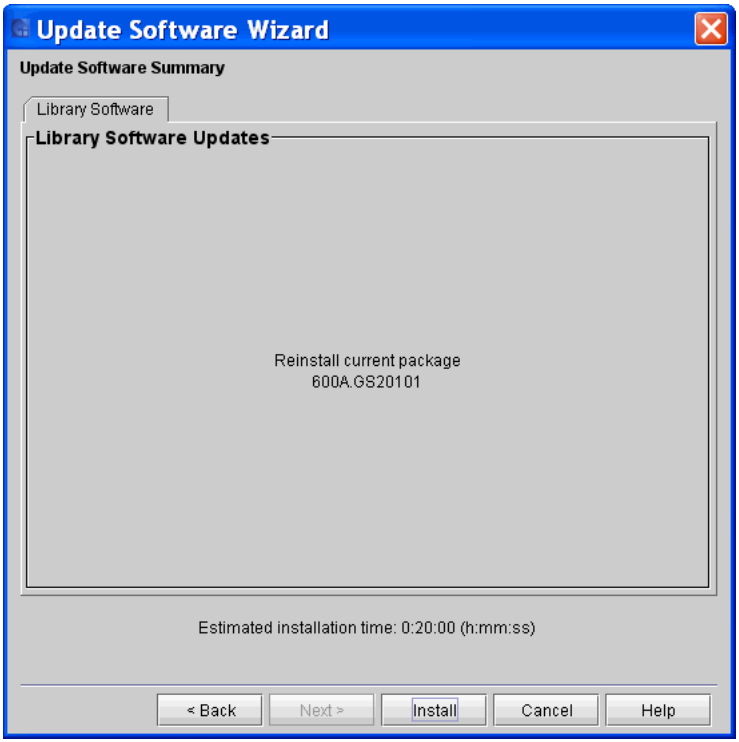
9 Launch the browser and log in again after the library has completed it's reboot process.

10 Click **Help > About**. Validate that the components reflect the correct firmware version.

Reinstalling Current Library Software

The reinstall feature enables you to re-establish the installation of the library software that is currently active on the MCB to the various remote devices, such as the RCU, I/O blades, and the CMB. Perform this procedure if the RCU has been replaced and you want to bring it to the level that is on the MCB.

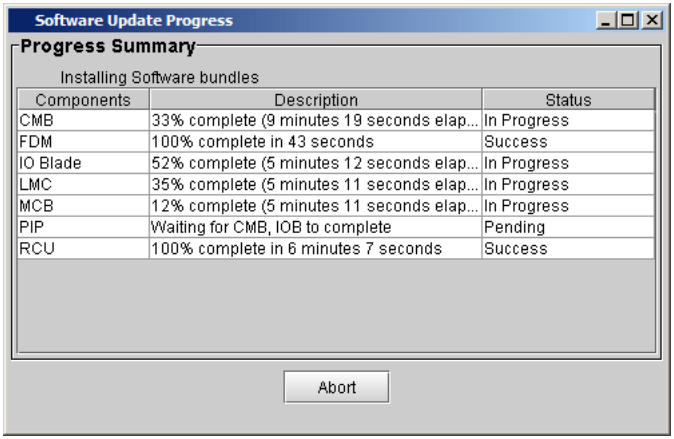
1. On the **Library System Software Update** dialog box, select **Reinstall current package**.
2. Click **Next.** The **Update Software Wizard** dialog box appears.



Click **Install**. The **Software Update Progress** dialog box appears.

Note: If the physical library is not offline, you receive a message that asks you whether you want to take it offline. Click **Yes**.

The library automatically logs off other users so that they cannot perform library operations while the library software update operation is in progress.



Real-time progress information appears under **Progress Summary** in the **Description** and **Status** columns.

Note: The components that already have the correct version loaded will transition to a "Success" status quickly during the reinstall process.

3 After the update process completes, click **OK**. Within approximately a minute after completing the update process, the RCU restarts.

Caution: Do not perform any library operations until the RCU is completely restarted.

Note: Before the RCU is restarted, the main menu **Activity** panel displays the message **WARNING: The Robotics is not Enabled**. This message indicates that the RCU is not yet ready. When the RCU is ready, the message disappears.

4 Bring the physical library online.

a From the LMC, click **Operations > Change Mode**.

b Select **Online**, and then click **OK**.

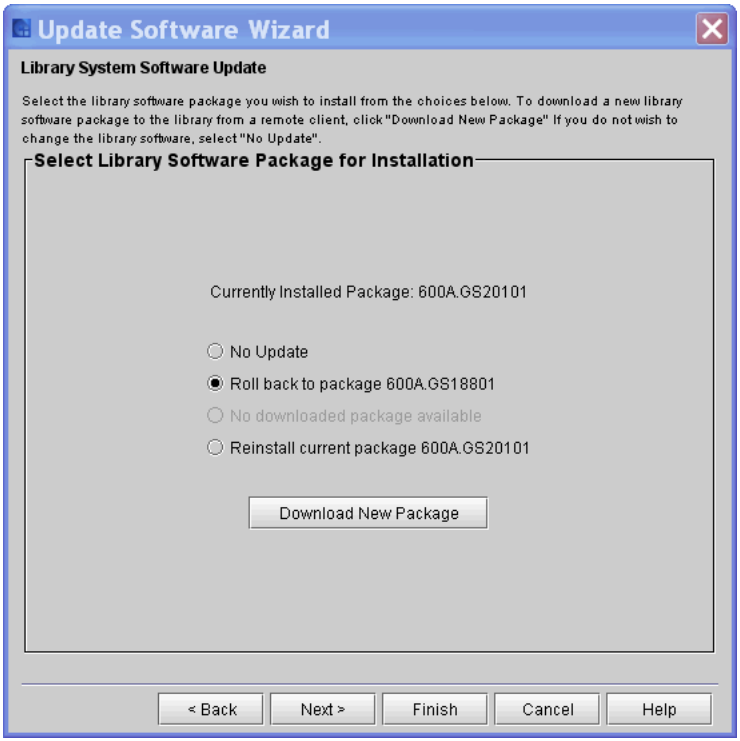
5 Click **Help > About**. Validate that the components reflect the correct firmware version.

Rolling Back to the Previous Build Package

1 On the **Library System Software Update** dialog box, select **Rollback to package.**

Note: Rolling back the firmware should NOT be used as a recovery tool for a failed firmware upgrade. If the firmware upgrade process has failed, capture the snapshot and escalate the issue.

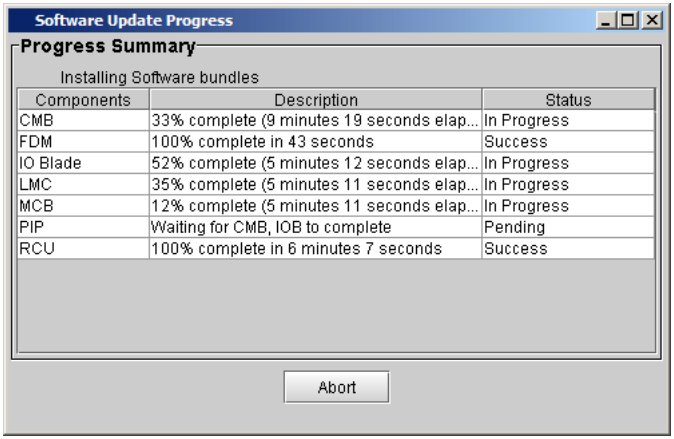
2 Click **Next.** The **Update Software Wizard** dialog box appears.



3 Click **Finish.** The **Software Update Progress** dialog box appears.

Note: If the physical library is not offline, you receive a message that asks you whether you want to take it offline. Click **Yes**.

The library automatically logs off other users so that they cannot perform library operations while the library software update operation is in progress.



Real-time progress information appears under **Progress Summary** in the **Description** and **Status** columns.

4 After the update process completes, click **OK**.

Within approximately a minute after completing the update process, the library will reinitialize.

Caution: Do not perform any library operations until the RCU is completely restarted.

5 Bring the physical library online.

- **a** From the LMC, click **Operations** > **Change Mode**.
- **b** Select **Online**, and then click **OK**.

6 Click **Help > About**. Validate that the components reflect the correct firmware version.

Updating Drive Firmware

Before you install a new drive firmware image, you must download it to the library's MCB from the remote client's file system. You must perform the download from a remote client.

It is important to make sure that the library is running the appropriate level of drive firmware, compatible with the drive type. To determine the appropriate drive firmware, see the library's *Release Notes* or contact Quantum technical support. If you want to update drive firmware by using I/O blades or Ethernet Expansion Blades (EEB), perform the procedure in this section. Drives that are not attached to I/O blades or Ethernet Expansion Blades must be updated by using update tapes.

You can perform drive firmware updates from either the library's touch screen or a remote client, but you must perform drive firmware downloads from a remote client.

Note: If you are viewing a partition, you can only set up update drive firmware for drives within the partition.

Note: Before you begin the following procedure, make sure that you have obtained the new drive firmware image from Quantum and placed it in an accessible location on your laptop.

Select **Tools > Update Software > Drives** to update drive brick firmware on one or more drives by using either update tapes or drive firmware images that you have downloaded to the library. This section includes the following subsections:

- Download Drive Firmware on page 578
- Updating Drive Firmware Using Firmware Images on page 581
- Updating Drive Firmware Using Update Tapes on page 583

Download Drive Firmware

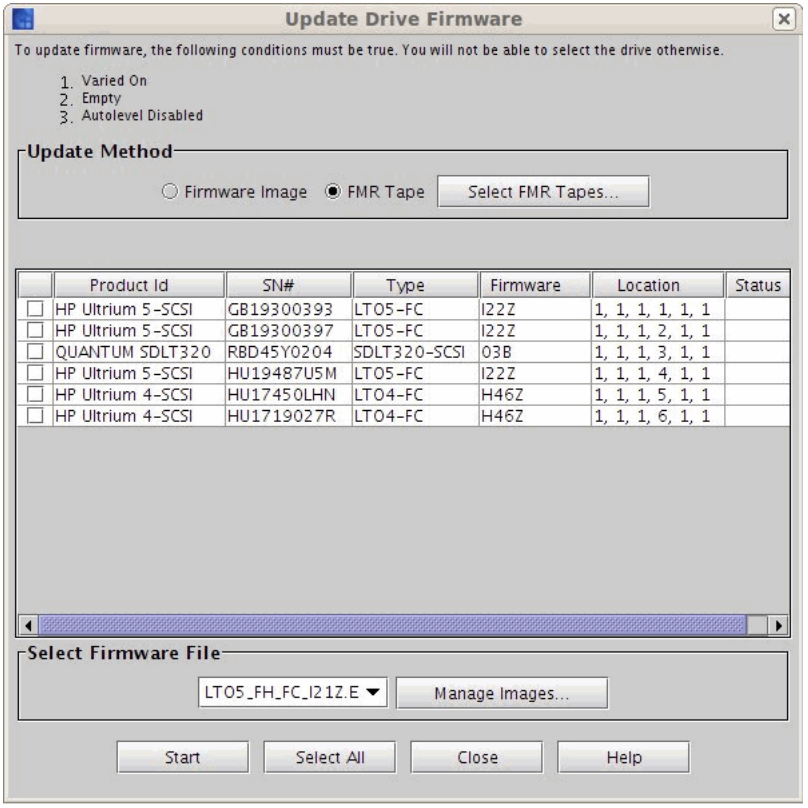
Note: Before performing a firmware upgrade, we recommend that you shut down and restart the library.

1. Log on as service.
2. You can access the **Update Drive Firmware** dialog box while viewing either the physical library or a partition. From the **View**

menu, click the name of the physical library or the appropriate partition.

Caution: If you are viewing a partition, drive firmware update operations affect drives that are within the partition only.

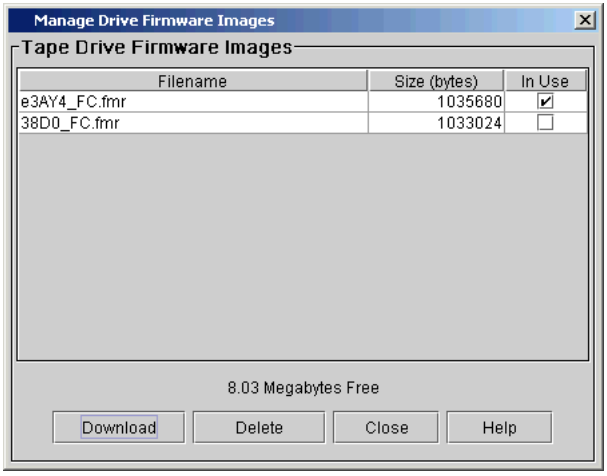
3 Click **Tools > Update Software > Drives**. The **Update Drive Firmware** dialog box appears.



From the **Update Drive Firmware** dialog box, you can update drive firmware by using either update tapes or drive firmware images that you have downloaded to the library. The table lists all drives in the library or, if you are currently viewing a partition, all drives in the partition. The **Manage Images** button enables you to download new drive firmware images to the library or delete drive firmware images

that the library currently stores. Drive images that are currently stored on the library are listed in the drop-down list in the **Select Firmware File** area.

4 On the **Update Drive Firmware** dialog box, click **Manage Images**. The **Manage Drive Firmware Images** dialog box appears.

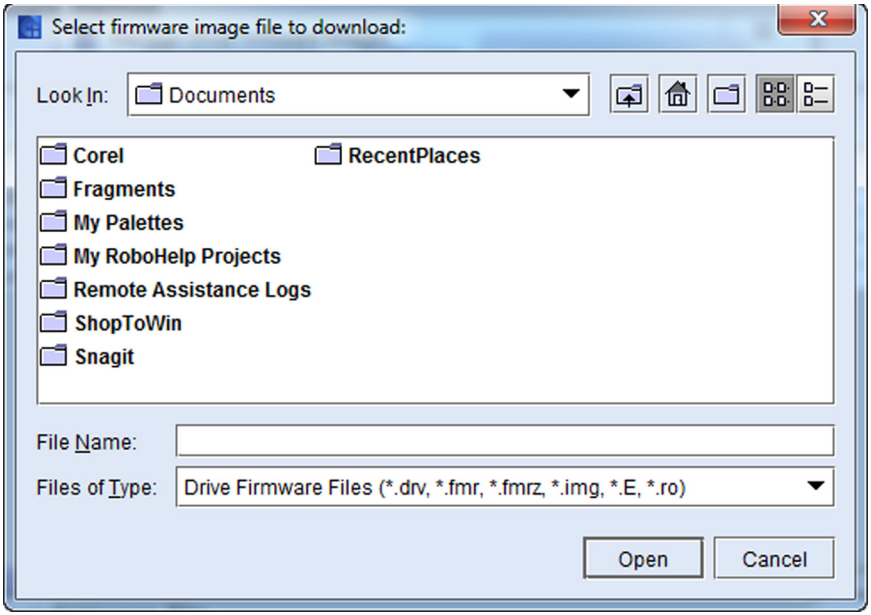


The library has enough space for 50 MB (with a maximum of 8 images) of drive firmware images.

If the **In Use** check box for a drive firmware image is clear, you can delete the image by clicking it to highlight it, and then clicking **Delete**.

The In Use check box indicates that the firmware image is set to auto-level all the drives to that firmware image in a specific partition.

5 To download a new drive firmware image, click **Download**. The **Select firmware image file to download** dialog box appears.



6 Navigate to the location of the drive firmware image file (with either a **.drv**, **.fmr**, .**frmz, .img**, **.E**, or **.ro** extension) you want to download, and then click the image file to highlight it.

7 Click **Open**.

The download process copies the drive firmware image from the remote file system to the MCB. After the download process finishes, the drive firmware image file is added to the list on the **Manage Drive Firmware Images** dialog box.

8 On the **Manage Drive Firmware Images** dialog box, click **Close**. The **Update Drive Firmware** dialog box appears again.

To update drive firmware by using downloaded firmware images, proceed to Updating Drive Firmware Using Firmware Images on page 581. To update drive firmware by using update tapes, proceed to Updating Drive Firmware Using Update Tapes on page 583.

Updating Drive Firmware Using Firmware Images

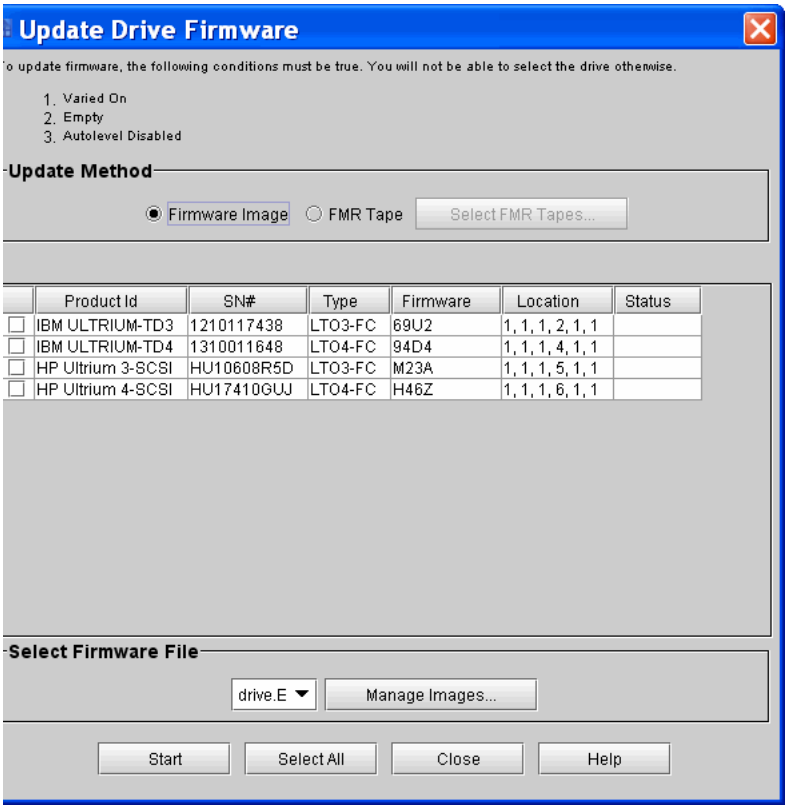
Caution: If you are viewing a partition, drive firmware update operations affect drives that are within the partition only.

Caution: Before you update drive firmware during this procedure, make sure that tapes are not mounted in any of the drives. If tapes are mounted in drives during the update process, the library loses knowledge of the cartridge home cell in storage, resulting in library and host inventory issues.

If you load a firmware image onto a drive that is the same version that is currently running on the drive, the upgrade will fail.

If host reservations exist on drives, it will fail the upgrade.

1 On the **Update Drive Firmware** dialog box, select **Firmware Image**.



Note: Drives that are not connected to I/O Blades or EEBs are listed, since drives not connected to I/O Blades can be updated using FMR Tapes. Refer to Updating Drive Firmware Using Update Tapes on page 583.

2 In the left-most column of the table under the **Update Method** area, select one or more check boxes that correspond to drives that you want to update with the same drive firmware image. Use the following rules to select drives:

- Do not select drives that are currently loaded.
- If you select more than one drive, make sure that they are all of the same drive type.
- Click **Select All** to select all drives. All drives must be of the same drive type.

Note: You can only perform firmware update for drives of the same product, such as HP or IBM, and type, for example LTO-4 or LTO-5.

3 From the drop-down list in the **Select Firmware File** area, click the drive firmware image you want to use to update the drives you selected.

Caution: The drop-down list includes all drive firmware images that are currently stored on the library, regardless of drive type. Be careful to select a drive firmware image that is compatible with the type of drive that you want to update. See the library's *Release Notes* for compatibility information or contact Quantum technical support.

4 Click **Start**. The library updates the firmware on each selected drive.

Updating Drive Firmware Using Update Tapes

It is important to verify that the library firmware version is compatible with the new drive firmware version. To determine the appropriate drive firmware, see the library's *Release Notes* or contact Quantum technical support. If you need to update drive firmware by using update tapes, perform the following procedure.

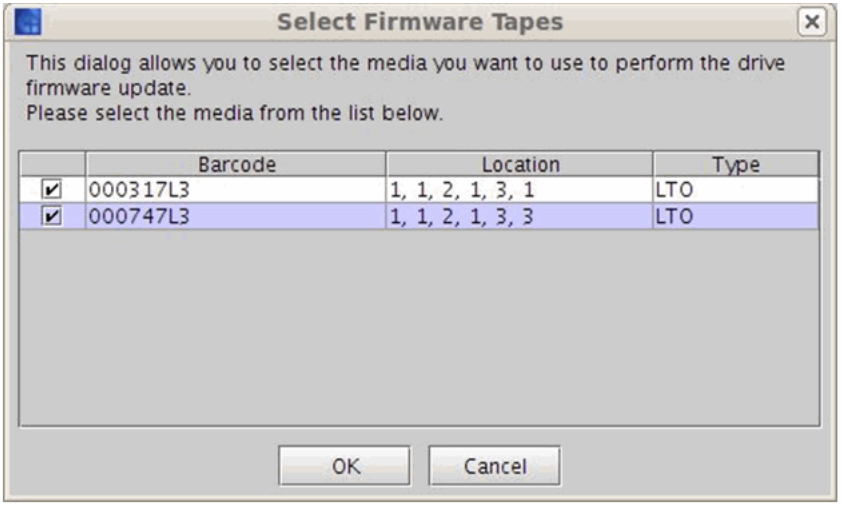
Note: If you are viewing a partition, drive firmware update operations affect drives that are within the partition only, and uses the I/E slots within the partition. If you are viewing the physical library, drive firmware update operations affect all drives.

1 Write down the barcode number on the tape before inserting it into the I/E Station.

2 From the **Physical Library** view, insert the firmware tape(s) into any I/E station slots in the library.

Note: If you are in the **Logical Library** view, insert the firmware tape(s) into I/E slots belonging to the partition of the current **Logical Library** view.

3 On the **Update Drive Firmware** dialog box, select **FMR Tape**. The **Select Firmware Tapes** dialog box appears.



4 Select the tape cartridges you want to use for the firmware update by checking the check boxes in the media table, and click **OK**.

Note: You can perform a firmware update only for drives of the same product (such as HP or IBM), and type (such as LTO-4 or LTO-5).

5 Click **Start**. A message **Updating do not power cycle the drive** is displayed above the drive table in red. The **Status** column in the drive table displays the status of the update.

Caution: The drive firmware image must be compatible with the drives that you will update with it. For more information, see the Customer Service Web site.

Teaching the Library (Configuration and Calibration)

The **Teach** command enables you to update the library's stored configuration and calibration information. Use this command after you replace a library component or whenever you need to assess the library's physical configuration (such as the number of modules and I/E stations, the locations of storage magazines and drives, and the types of media used in the library) or the position and alignment of library components.

Running Configuration Teach

Starting the configuration teach process causes the library to assess its contents, gathering information as follows:

- Number of modules
- Types of media
- Storage magazine locations
- Number of I/E stations and magazine type
- Types of drives
- Drive locations

If you change the library's physical configuration in any of these areas, you should initiate the configuration teach process (for example, when you add or remove storage or remove storage to add another component. The library will automatically perform a configuration teach, calibration teach, and inventory when an expansion module is added.

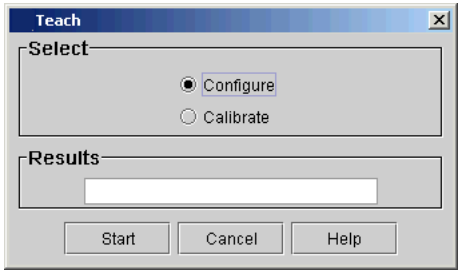
Note: During the configuration teach process, the library runs the calibration teach process. Afterwards, it automatically performs an inventory.

1 Log on as an administrator.

2 Make sure that you are viewing the physical library. From the **View** menu, click the name of the physical library.

3 Click **Tools > Teach**. The **Teach** dialog box appears.

Note: If the physical library is not offline, you receive a message that asks you whether you want to take it offline. Click **Yes**.



Configure is already selected by default.

4 Click **Start**.

During the configuration teach process, the picker moves to each storage magazine, I/E magazine, and drive in the library and stores information about them. Teach results appear in the **Results** text box when the process completes.

Running Calibration Teach

Starting the calibration teach process causes the library to assess the position and alignment of various library components through the use of calibration targets. Use this process to avoid cartridge-handling problems caused by rack, drive, or I/E station misalignments.

Rack alignment calibration targets are tabs that are located on special magazines. I/E station targets are small square holes that are located at the top and bottom of the I/E station. Whenever you perform work on the library that could affect the position of rack, drive, or I/E station

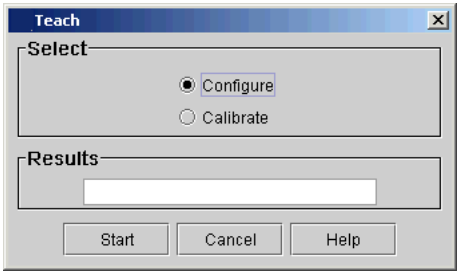
calibration targets, even slightly, you should initiate the calibration teach process.

1 Log on as an administrator.

2 Make sure that you are viewing the physical library. From the **View** menu, click the name of the physical library.

3 Click **Tools > Teach**. The **Teach** dialog box appears with **Configure** selected by default.

Note: If the physical library is not offline, you receive a message that asks you whether you want to take it offline. Click **Yes**.



4 Select **Calibrate**.

5 Click **Start**.

During the calibration teach process, the picker moves to the home position, which is X-Y coordinate position 0,0. Then, for each rack of each module, the picker moves to a magazine at the top and one at the bottom and stores those positions in coordinates relative to the 0,0 position. Teach results appear in the **Results** area when the process completes.

Note: Use the Physical Library command on the Setup menu to disable or enable automatic inventory after a calibration teach. For more information about this command, see Setting Up Policies for the Physical Library on page 170.

Saving and Restoring Library Configuration

The library's save and restore capabilities enable you to save a remote or local copy of configuration settings for the library's drives, I/O blades, and partitions, including the allocation of drives, storage magazines,

and I/E station magazines to each partition. If the library's current configuration becomes lost or unstable, you can use the LMC to apply the locally or remotely saved configuration image, which eliminates the need to reconfigure the entire library to bring it back to its original state.

Caution: You cannot apply an older firmware configuration to a new firmware library (i.e., i11.1.1 to i11.2.3).

The **Save and Restore Library Configuration** dialog box enables you to:

- Save a library's configuration settings as a remotely or locally stored image
- Restore, revert, or rescue the library by applying a remotely or locally stored image of a library's configuration settings.

Caution: As a result of restore, rescue, or revert operations, the library shuts down. You must have physical access to the library to bring the library back up. If you are performing a restore, rescue, or revert operation using remote access, the library will remain shut down until the library is directly powered back on.

Types of Configuration Image Files

There are three types of configuration images that correspond to the **Restore**, **Rescue**, and **Revert** commands:

- The restore image is stored on a remote file system and is created any time you use the **Save** command. You might restore the library's configuration, for example, if the library's locally saved configuration is lost because the Management Control Blade (MCB) is replaced. Because of the image's remote location, the **Save** and **Restore** commands are available only through the remote client.
- The rescue image is stored locally on the library's file system and is created any time you use the **Save Rescue** command. You might rescue the library's configuration, for example, if the library becomes unstable due to a configuration change and you want to roll back the library's configuration settings to a previous state. The

Save Rescue and **Rescue** commands are available from both the remote client and the library's touch screen.

- The revert image is automatically created and stored locally as the first step of any restore or rescue operation. The purpose of the **Revert** process is to revert to the last configuration that was used before a restore image was applied. If an incorrect restore image was applied, the **Revert** feature allows the MCB to revert back to its prior configuration.

  The **Revert** command is available from both the remote client and the local touch screen.

When to Save the Library Configuration

You should save the library configuration any time you make changes to the library hardware, software, or configuration. You can save the library configuration at any time.

Caution: It is the customer's responsibility to properly save the library configuration. If an MCB fails and needs to be replaced and the configuration was not saved properly, the library will need to be completely reconfigured manually.

CONFIG Button Alerts

To help you remember to save the configuration, the **CONFIG** button on the LMC main console toolbar indicates whether you have saved the current library configuration.

- **Green Check Mark — Good**. The current configuration has been saved. This can mean you saved the configuration locally on the library or to a remote location.
- **Yellow Exclamation Point — Warning**. The current configuration has not been saved.

Note: If you have never saved the configuration, then the icon will always show green/good, even if you change the configuration.

You can click the **CONFIG** button on the LMC toolbar to access the **Save and Restore Library Configuration** dialog box.

Figure 57 CONFIG Button - Good/Saved

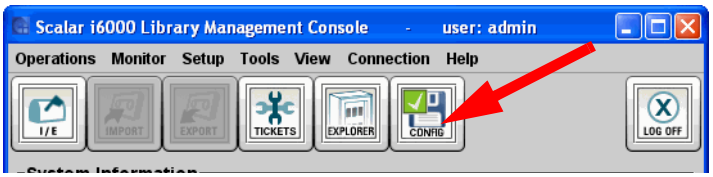
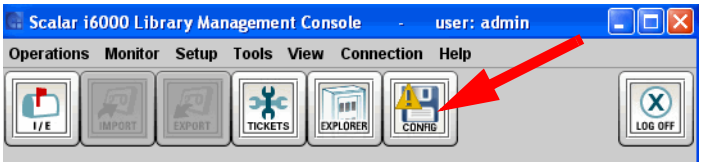


Figure 58 CONFIG Button - Warning/Unsaved



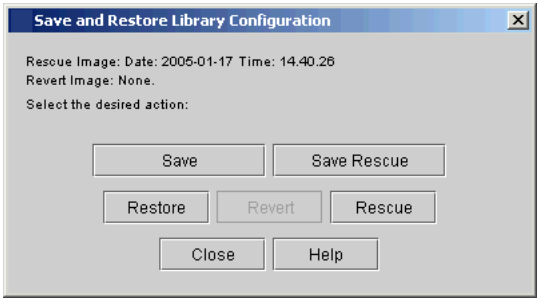
Saving a Remote Restore Image

Use the **Save** command to save a library configuration restore image on a remote file system. To make sure that the image captures all library configuration changes, save the image often.

1 Log on as an administrator from the remote client. The **Save** command is not available from the library's touch screen.

Click the **CONFIG** button on the LMC toolbar. The **Save and Restore Library Configuration** dialog box appears.

Alternatively, make sure that you are viewing the physical library (from the **View** menu, click the name of the physical library), then click **Tools > Save/Restore**.



2 Click **Save**.

3 Using the file chooser dialog box, specify a path to a directory on your remote file system in which to save the restore image. You only need to specify the path because the MCB determines the image file name.

4 To proceed, click **Open**. The library prompts you to decide whether you want to override the current rescue image that is stored locally on the library.

5 Click **Yes**.

The rescue image timestamp that appears on the **Save and Restore Library Configuration** dialog box will be updated to indicate that the file has changed.

If no rescue image exists, the library prompts you to decide if you want to generate one.

If the save operation succeeds, a message appears that indicates the name of the image file that was saved to the remote file system. If the save operation does not succeed, a message appears that describes the error that occurred.

Saving a Local Rescue Image

Use the **Save Rescue** command to save a library configuration rescue image locally on the library's file system. To make sure that the image captures all library configuration changes, you should save the image often.

1 Log on as an administrator from the remote client or from the library's touch screen. Click the **CONFIG** button on the LMC toolbar. The **Save and Restore Library Configuration** dialog box appears.

Alternatively, make sure that you are viewing the physical library (from the **View** menu, click the name of the physical library), then click **Tools > Save/Restore**.

2 Click **Save Rescue**. The save rescue operation starts.

If the save rescue image operation succeeds, a message appears that indicates that the rescue image file was saved to the library file system. The rescue image timestamp displayed on the **Save and Restore Library Configuration** dialog box will be updated to indicate that the file has changed.

If the save rescue operation does not succeed, a message appears that describes the error that occurred.

Restoring Library Configuration

Use the **Restore** command to restore a library using a configuration image that is saved on a remote file system.

If library configuration has occurred since the last time the image was saved, those changes will be lost when the older configuration is restored. The restore operation will succeed, but you will then need to reconfigure the library, including the partitions and mappings. Therefore, it is important to save the local rescue and/or remote restore image periodically, especially following hardware configuration changes.

Caution: Be cautious if you plan to use a saved library configuration image that is out of date. You might restore configuration information that you do not want, such as former passwords, partitions, mappings, and hardware configurations.

1 Log on as an administrator from the remote client. The **Restore** command is not available from the library's touch screen. Click the **CONFIG** button on the LMC toolbar. The **Save and Restore Library Configuration** dialog box appears.

   Alternatively, make sure that you are viewing the physical library (from the **View** menu, click the name of the physical library), then click **Tools > Save/Restore**.

2 Click **Restore**.

Note: If the library is not offline, you receive a message that asks you whether you want to take it offline. Click **Yes**.

3 Using the file chooser dialog box, locate the restore image file on the remote file system.

4 When you have located the file and are ready to proceed, click **Open**.

Note: Because the management control blade (MCB) determines the name of the restore image file, you might not know the file name when you are searching for it on the remote file system. The file name always includes the library serial number, date stamp, and time stamp, in that order and separated by underscores.

An example file name might look like this:

213100020_2004-02-18_13.23.47.tar.gz

The serial number encoded in the image file must match the library serial number. A serial number mismatch will result in an message and the operation will not continue.

When image file compatibility has been established, the library reboots itself and continues with restoring the configuration. The reset operation could take minutes to complete. If you are near the library and can see the library's touch screen, normal behavior is when two "working" messages appear and the touch screen goes dark when the LMC server restarts. From the remote client, a message appears that indicates that the LMC server is reconnecting to the client. After it reconnects, the LMC server performs a discovery.

If the restore operation succeeds, a message appears that indicates that the operation succeeded.

If the restore operation fails at any point, the library generates a RAS ticket that contains details about the failure. Perform a revert or rescue operation to return the library to a stable configuration.

5 After the restore operation has completed on the library, close and restart the remote client.

6 If you have not done so already, make sure that the robotics are enabled and bring the library back online so that data input and output can continue.

Rescuing Library Configuration

Use the **Rescue** command to restore a library using the configuration rescue image that is saved locally on the library's file system.

Caution: Be cautious if you plan to use a saved library configuration image that is out of date. You might restore configuration information that you do not want, such as former passwords, partitions, mappings, and hardware configurations.

If library configuration has occurred since the last time the image was saved, those changes will be lost when the older configuration is restored. The restore operation will succeed, but you will then need to reconfigure the library, including the partitions and mappings. Therefore, it is important to save the local rescue and/or remote restore image periodically, especially following hardware configuration changes.

1. Log on as an administrator from the remote client. The **Restore** command is not available from the library's touch screen. Click the **CONFIG** button on the LMC toolbar. The **Save and Restore Library Configuration** dialog box appears.

   Alternatively, make sure that you are viewing the physical library (from the **View** menu, click the name of the physical library), then click **Tools > Save/Restore**.

2. Click **Rescue**.

Note: If the library is not offline, you receive a message that asks you whether you want to take it offline. Click **Yes**.

3 At the prompt, make sure that all data input and output has stopped. Click **Yes** to continue.

When the system determines that it can reconfigure the library using the saved image, a message dialog box appears that informs you that the library will reboot itself. The reset could take minutes to complete. If you are near the library and can see the library's touch screen, normal behavior is when two "working" messages appear and the touch screen goes dark when the LMC server restarts. From the remote client, a message appears that indicates that the LMC server is reconnecting to the client. After it reconnects, the LMC server performs a discovery.

As the MCB reboots, the I/O blades, MCB, LMC server, and robotics control unit (RCU) change to the configuration settings stored in the rescue image. Each I/O blade is also reset.

When the LMC has restarted, reconnected, and completed its discovery operation, a message appears that indicates that the library has been restored to its previous configuration.

If the operation succeeds, a message appears that indicates that the operation completed successfully.

If the operation fails at any point, the library generates a RAS ticket that contains details about the failure. Perform a revert or rescue operation to return the library to a stable configuration.

4 If you have not done so already, make sure that the robotics are enabled and bring the library back online so that data input and output can recommence.

Reverting Library Configuration

If a restore or rescue operation fails before completion, it can cause the library to become unstable. The Revert command allows you to roll back the partial configuration changes that occurred during the attempted restore or rescue. The Revert command will only be available if a revert image has been saved. A Revert image is saved the first time a restore or rescue operation is attempted.

1 Log on as an administrator from the remote client or from the library's touch screen. Click the **CONFIG** button on the LMC toolbar. The **Save and Restore Library Configuration** dialog box appears.

Alternatively, make sure that you are viewing the physical library (from the **View** menu, click the name of the physical library), then click **Tools > Save/Restore**.

2 Click **Revert**.

Note: If the library is not offline, you receive a message that asks you whether you want to take it offline. Click **Yes**.

3 At the prompt, check whether all library data input and output has stopped. To continue, click **Yes**.

When the system determines that it can reconfigure the library using the saved image, a message dialog box appears that informs you that the library will reboot itself. The reset could take minutes to complete. If you are near the library and can see the library's touch screen, normal behavior is when two "working" messages appear and the touch screen goes dark when the LMC server restarts.

As the MCB reboots, the I/O blades, MCB, LMC server, and robotics control unit (RCU) change to the configuration settings stored in the rescue image. Each I/O blade is also reset.

When the LMC has restarted, reconnected, and completed its discovery operation, a message appears that indicates that the library has been restored to its previous configuration.

If the operation succeeds, a message appears that indicates that the library has been restored to its previous configuration.

If the operation fails at any point, the library generates a RAS ticket that provides that contains details about the failure. Perform a revert or rescue to return the library to a stable configuration.

4 If you have not done so already, make sure that the robotics are enabled and bring the library back online so that data input and output can recommence.

Viewing the Drive Resource Utilization Reports

The Drive Resource Utilization Reporting (DRUR) feature enables you to view and manage your tape drive resources. The data provided through DRUR can help you determine the proper work load distribution between the drives in your library. DRUR provides you with up to twelve months of historical data for each SN drive installed, and includes MB read and written, mounts, and media motion time.

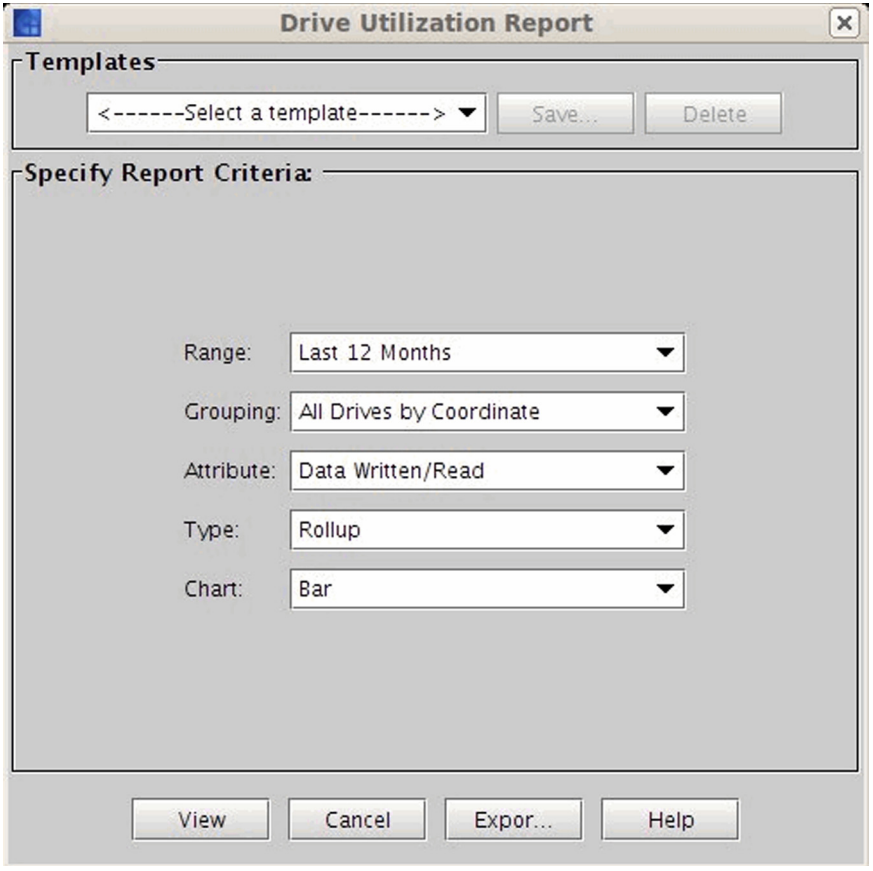
Note: The DRUR feature requires a license key to use. For more information, see Enabling Licenses on page 115.

You can view the DRUR data in summary reports and graphs, which you can then export from the library into a PDF document. You also can export and save the data as comma delimited text files (.csv). A .csv file is a plain text file that stores basic database-style information in a simple format, with one record on each line, and each field within that record separated by a comma.

DRUR data is based on the actual drive serial number (SN), not the logical drive serial number. The data tracked and reported through the DRUR feature is data that has been accumulated while the drive SN has been installed in the library.

Note: You can e-mail, save, or print reports from a remote client. However, you cannot save or print reports from the library's touch screen.

1. Log on as administrator.
2. Make sure that you are viewing the physical library. From the **View** menu, click the name of the physical library.
3. From the **Tools** menu, click **Reports > Drive Utilization**. The **Drive Utilization Report** dialog box appears.



4 In the **Specify Report Criteria** section, you can use the following criteria filters to view and export specific data:

- Range
  - Current Month
  - Last Month
  - Last 3 Months
  - Last 6 Months
  - Last 12 months
- Grouping

    - **All Drives by Coordinate**: Presents the sum total of all attributes for all drives in the library.
    - **All Drives by Physical SN**: Presents the sum total of all attributes for all drives according to the physical drive SN.
    - **All Partitions**: Presents a comparison of all drives grouped by partition in the physical library.
    - **Selected Drive by Coordinate**: Graph is based on an individual drive according to the library system coordinates. For example, 1,1,1,1,1,1.
    - **Selected Drive by Physical SN**: Graph is based on an individual physical drive SN.
    - **Selected Partition**: Graph is based on an individual partition in the physical library.
    - **All Media**: Presents all media for all drives.
    - **Select Media**: Presents selected media by media ID.
- Attribute
    - Data Written/Read
    - Mount Count
    - Media Motion Time
    - Total Read and Write
- Type
    - **Rollup**: A device x-axis for the display of attributes by drive or library.
    - **Trend**: A time scale x-axis for the display of the trend of the particular attribute.
- Chart: Choose from the following charts to visually display your data:
    - Bar
    - Bar 3D
    - Line
    - Stacked Area
    - Stacked Bar

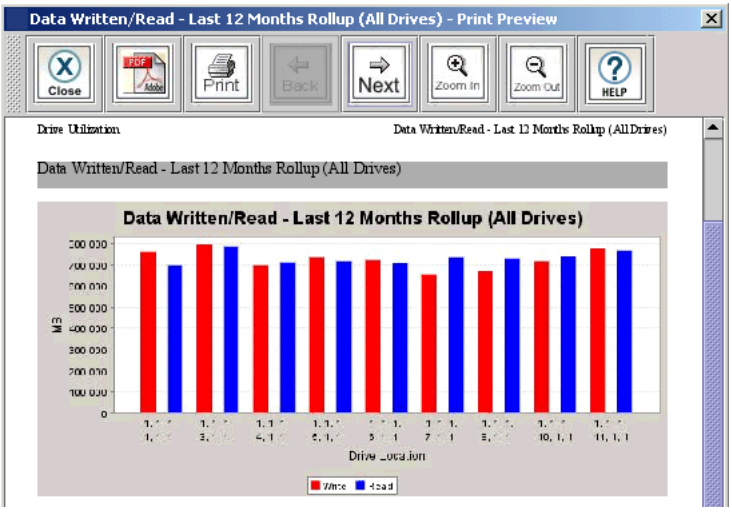
- Stacked Bar 3D
- Pie
- Pie 3D

5 To directly send or save the data, click **Export**.

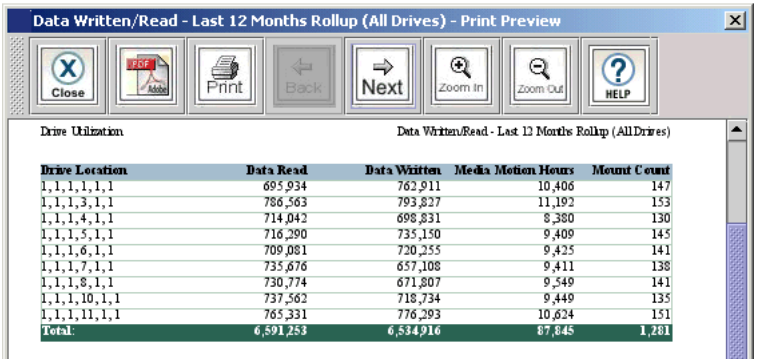
- To export data, in the **Export Raw Data** dialog box, select **E-mail** to send the data in .csv file format.
- To save the data, select **Save**. In the **Save** text box, type the path and file name, or click **Browse** to select a save location.

6 Optionally, save the report criteria as a template. Refer to Saving a Report Template on page 601

7 To view a report according to the criteria selected, click **View,** and then click **Preview**. The report appears graphically according to the type of chart you selected.



8 To view the next page of the report, click the **Next** icon on the toolbar.



9 In the report viewer, you can perform the following tasks:

   a To save the report as an Adobe Portable Document Format (PDF) file, click the **Adobe PDF** icon on the toolbar.

   b In the **Saving Report to PDF** dialog box, enter the appropriate information, and then click **Confirm** to convert the report into a PDF file.

   c To print the report, click the **Print** icon on the toolbar.

Saving a Report Template

If you frequently generate the Drive Resource Utilization Report with the same set of report criteria, save the criteria as a template. Loading the template recalls the saved report criteria and lets you quickly generate a report based on the saved criteria.

1 On the menu bar, click **Tools > Reports > Drive Utilization**. The **Drive Utilization Report** dialog box appears.

2 Under **Specify Report Criteria**, click criteria options in the lists to customize the content and appearance.

3 Under **Templates**, click **Save**.

4 Type a name for the template, and click **OK**. The template appears in the list under **Templates**.

5 To load the saved report criteria at a later time, click the template in the list, and then click **View** to generate the report.

6 To close the **Drive Utilization Report** dialog box, click **Cancel**.

Setting Up Advanced Reporting Options

Reports let you see information about your library at a glance, and help you identify trends and changes over time. You can manually generate reports as needed. In addition, if the advanced reporting options feature is licensed for your library, the LMC can automatically generate reports and e-mail them to designated recipients at specified times.

Note: The Advanced reporting feature is available via *remote* access only.

The LMC can automatically generate and e-mail the following reports:

- Drive Utilization Report
- Tickets Report
- LUN Mapping Report
- Media Reports
  - Integrity Analysis
  - Usage
  - Security
  - Moves
- Library Configuration Report
- Partition Utilization Report

To automatically generate reports, set up one or more scheduled jobs using advanced reporting options. You can specify when and how often the report is generated, what report templates are used, and which e-mail recipients receive the report. You can also edit and delete scheduled jobs.

Note: To automatically send reports to recipients, the library must be configured for sending e-mail. For more information, see Configuring E-mail on page 177.

Saving Report Criteria Templates

To schedule a job for a report, that report must have at least one template. A template is a saved set of report criteria that customize the content and appearance of a report.

Before setting up advanced reporting options, use the **Report Criteria** dialog box to save one or more templates for each report you want to automatically generate.

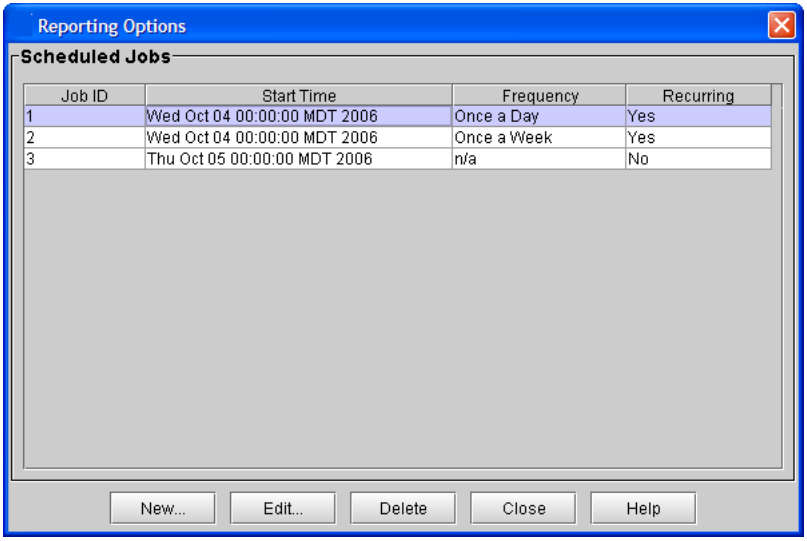
1. On the menu bar, click **Tools > Reports**, and then click **Drive Utilization**, **Tickets, LUN Mapping, Media (Integrity Analysis, Usage, Security or Moves), Library Configuration or Partition Utilization**. The appropriate report criteria dialog box appears.
2. Under **Specify Report Criteria**, click criteria options in the lists to customize the content and appearance of the report.

   For more information about choosing report criteria, see Generating Media Integrity Analysis Reports on page 62, Generating the Tickets Report on page 75, or Viewing the Drive Resource Utilization Reports on page 596.
3. Under **Templates**, click **Save**.
4. Type a name for the template, and then click **OK**. The template appears in the list under **Templates**.
5. To close the report criteria dialog box, click **Cancel**.

Scheduling a New Job

To set up a report to be automatically generated, first schedule a new job, and then set job options.

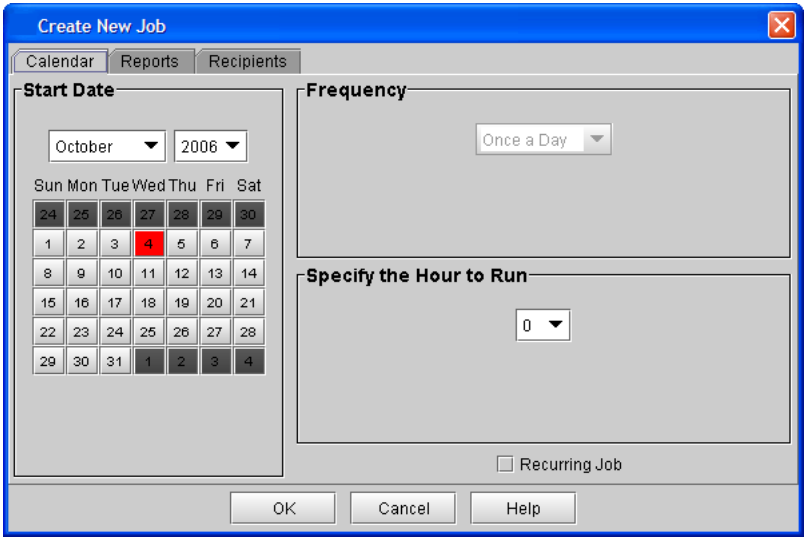
1. On the menu bar, click **Tools > Reports > Reporting Options**. The **Reporting Options** dialog box appears.



2 Click **New**. The **Create New Job** dialog box appears with the **Calendar** tab selected.

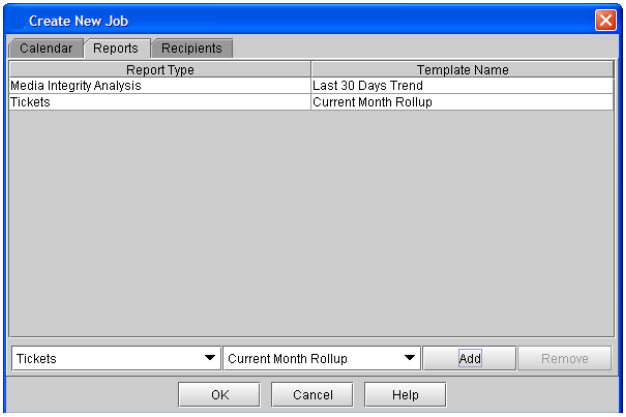
3 Specify time and recurrence options:

- Under **Start Date**, click the day, month, and year when you want the report to be generated for the first time. The current date is selected by default.
- Under **Specify the Hour to Run**, click the value that corresponds to the time of day when you want the report to be generated. The values in the list correspond to a 24-hour clock. For example, **0** is midnight, **10** is 10:00 a.m., and **20** is 8:00 p.m.
- (Optional) Select the **Recurring Job** check box, and then under **Frequency** click how often you want the report to be generated.



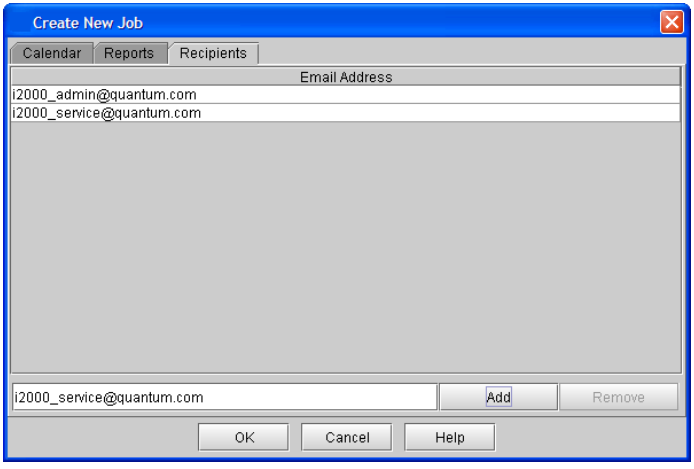
4 Click the **Reports** tab, and then add one or more reports to the job.

- To add a report, click a report in the reports list, and then click a template in the templates list. Click **Add** to add the report to the job. You can add more than one report to a job.
- If you need to remove a report from a job, click the report, and then click **Remove**.
- If there are no templates available for the report you choose, you need to save a template for the report before you can schedule a job. For more information on saving a template, see Saving Report Criteria Templates on page 602.



5 Click the **Recipients** tab, and then add one or more e-mail recipients to the job.

- To add a recipient, type an e-mail address in the box, and then click **Add**. You can add more than one recipient to a job.
- If you need to remove a recipient from a job, click the recipient, and then click **Remove**.



6 Click **OK**. The new job appears in the list of scheduled jobs. The LMC will generate the report at the specified time and send it to the designated e-mail recipients.

Note: If a yellow caution icon appears next to a scheduled job on the **Reporting Options** dialog box, it means there is a problem with the job. For example, the date for the job might be in the past. To correct the problem, edit the job to change job options. For more information about editing scheduled jobs, see Editing Scheduled Jobs on page 607.

7 Click **Close** to close the **Reporting Options** dialog box.

Editing Scheduled Jobs

If you need to make changes to a scheduled job, edit it to change job options. You can change any job options, such as the date, time, report template, or e-mail recipients.

1 On the menu bar, click **Tools** > **Reports** > **Reporting Options**. The **Reporting Options** dialog box appears.

2 Under **Scheduled Jobs**, click the job you want to change, and then click **Edit**. The **Edit Job** dialog box appears.

3 Change job options as needed on the **Calendar**, **Reports**, and **Recipients** tabs.

4 Click **OK**.

5 Click **Close** to close the **Reporting Options** dialog box.

Note: If the start date for a scheduled job is in the past, and it is not a recurring job, the report will not be generated. To correct this problem, edit the scheduled job and choose a start date that is in the future.

Deleting Scheduled Jobs

If you no longer need a scheduled job, delete it.

1 On the menu bar, click **Tools** > **Reports** > **Reporting Options**. The **Reporting Options** dialog box appears.

2 Under **Scheduled Jobs**, click the job you want to delete, and then click **Delete**. A dialog box appears asking if you are sure you want to delete the selected job.

3 Click **Yes**. The job is deleted from the list of scheduled jobs.

4 Click **Close** to close the **Reporting Options** dialog box.

Working With Verification Tests

A collection of verification tests are available to assist you or a customer service engineer (CSE) in determining whether the library is properly installed, configured, and operational. Running the tests is an important part of ensuring that the system is working correctly.

Note: Because resolving an issue often involves complex technical procedures, such as removing and replacing FRUs, and because verification tests often require preparation and trained interpretation of results, it is recommended that a CSE perform the tests.

There are four types of verification test that help diagnose problems with the library:

- Install Test on page 609
- Smaller library configuration requires about 1 hour and the larger configurations require as long as 6 hours to run the Install Test. Partial Test on page 609
- FRU Test on page 609
- Custom Test on page 610

These verification tests provide the following:

- Fully automated tests
- Tests to determine problems with installation
- Detailed problem analysis
- Full system tests or individual field replaceable unit (FRU) tests
- Logs of installation and configuration tests
- Graphical reports showing passed and failed results
- No affect to integrity of data

To perform these tests, the accessor assembly must be ready and functional, and the library must be powered on. In addition, the library must be in an offline state, and at least one scratch tape must be inserted in the I/E station.

Test Descriptions

This section describes the verification tests and their associated *sub-tests* that are available.

Note: Refer to Sub-test Descriptions on page 610 for descriptions of each sub-test.

Install Test

The Install Test enables you to verify that the library's installation and configuration is complete and functioning correctly. The Install Test automatically runs the following individual sub-tests:

- Library alignment test
- Picker assembly test
- I/E station assembly test
- Get/Put test
- Scanner fiducial test

Smaller library configuration requires about 1 hour and the larger configurations require as long as 6 hours to run the Install Test. **Partial Test**

The Partial Test performs the selected sub-tests to test an area or range of the library configuration. The available sub-tests include:

- Frame test - This test includes the same individual tests as the Install Test, but enables you to specify a range of modules rather than testing all modules.
- Configuration test - This test includes the picker assembly and scanner fiducial tests.

Both tests enable you to select a range of modules and racks to test. For example, if you have a four-module library, you can select to test only modules 3 and 4. The Frame test performs the same operations as the installation verification test, except there are frame and rack range parameters available.

FRU Test

The FRU test enables you to verify the replacement of a FRU. When the FRU test is selected, you can select any of the following sub-tests:

- Accessor Assembly
- Picker Assembly
- Drive Sled Assembly
- IE Assembly
- Scan Barcode

When one of the sub-tests is selected, you may be prompted to enter additional information. For example, the **Select FRU** dialog box has tabs along the top to select individual drives, I/E stations, and scratch tapes.

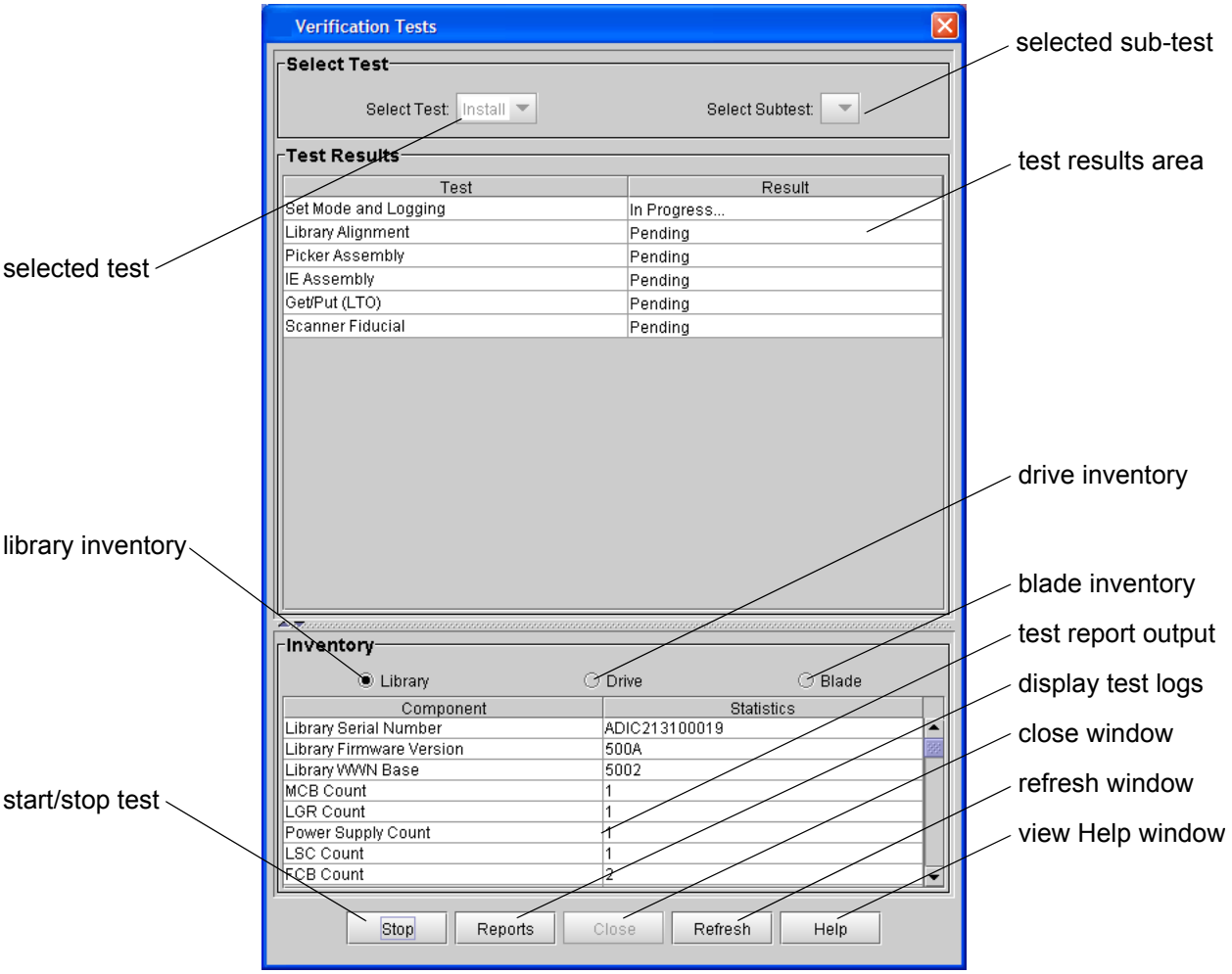
Custom Test

The Custom test enables you to run the Library Alignment sub-test on a per-rack basis.

Sub-test Descriptions

Use the **Verification Tests** dialog box to select the test and sub-test, to start the test, and view results. Figure 59 shows the parts of the **Verification Tests** dialog box. To display the dialog box, click **Tools > Verification Tests**.

Figure 59 Verification Tests Dialog Box



Library Alignment Test

The library alignment test performs the following tasks:

- Performs accessor X-axis and Y-axis travel test (also calls the FRU accessor assembly test)
- Calibrates library and checks calibration offsets by comparing them to the default values for the drives and I/E stations

- Checks magazine offsets
- Checks collected offset alignments for magazines, I/E stations, and drive sleds
- Checks joint alignment quality

Get/Put Test

The Get/Put test performs the following tasks:

- Performs a Get/Put of a scratch tape in the top and bottom slots of each magazine that supports the scratch tape's media
- Performs a Get/Put of existing media if no scratch tape is found or if the top or bottom is occupied
- Moves a scratch tape to one row in each frame to test cross-frame alignment
- Uses a scratch tape to perform a Get/Put in each compatible drive

Accessor Assembly Test

The accessor assembly test performs the following tasks:

- Checks for the module terminator (the terminator on the LBX board in the last expansion module)
- Checks the joint alignment (makes sure all the joints on the X-axis are flush)
- Performs two passes around the library to ensure the X-axis and Y-axis encoders are reading correctly and the belts are not slipping
- Tests the calibration sensor
- Checks the alignment of the accessor to the control module

Picker Assembly Test

The picker assembly test performs the following tasks:

- Performs pivot left and right check
- Performs reach and retract five times
- If the LMC gets its side done, performs a Get/Put of the selected cell
- Scans the control module serial number to make sure the scanner is reading properly

Drive Sled Assembly Test

The drive sled assembly test performs the following tasks:

- Calibrates the drive sled
- Checks the quality of the sled's fiducial
- Performs Get/Put to the drive

Scan Barcode Test

The scan barcode test performs the following tasks:

- Moves to selected cell coordinate and scans the barcode label
- Checks to ensure the label reads the same from top to bottom
- Verifies the quality of the barcode labels and checks to make sure barcode labels are in a readable position

I/E Station Assembly Test

The I/E station assembly test performs the following tasks:

- Locks and unlocks the I/E station
- Calibrates the I/E station and check offsets collected
- Checks each magazine's fiducial in the I/E station
- Performs Get/Put tests on all the I/E station cells

Scanner Fiducial Test

The scanner fiducial test performs the following tasks:

- Scans and checks each magazine fiducial
- Scans and checks each drive sled fiducial
- Tests the calibration sensor
- Calibrates and checks repeatability, up to three times for failed calibration targets

Understanding the Verification Test Inventory

The verification tests generate inventory lists that provide specific information about the library's configurations. Inventory lists for the library, drives, and blades are available. On the **Verification Test** dialog

box, select the type of inventory list that you want to see (**Library**, **Drive**, or **Blade**).

Library Inventory

This inventory list provides the following statistics and information:

- Library serial number
- Library firmware version
- Library WWN base
- Count for frame, tower, drives, I/E magazine, storage magazine, LGR, IEX, LMD, CMB, EEB, LSC, MCB, and FCB
- Serial number for frame, tower, power supply, LMD, EEB, IEX, FCB, CMB, MCB, and LSC
- Application firmware version for EEB, FCB, CMB, MCB, KGR, and LSC
- Boot firmware version for CMB, MCB, LGR, and LSC
- Pip firmware version for CMB and MCB
- Number of cartridges, I/E stations, frames, towers, drives, and aisles

Note: If an inventory is performed that includes a varied off tower, you will receive a warning message allowing you to continue with the inventory or cancel the request so the tower can be varied on. If you continue, the tower will not be included in the results of the inventory.

Drive Inventory

This inventory list provides the following information about each drive:

- Drive type
- Type of interface
- Physical serial number
- Logical serial number
- Firmware version
- Sled serial number
- Sled application firmware version
- Sled boot firmware version

Blade Inventory

This inventory list provides the following information about each Fibre Channel I/O blade:

- Location of each blade
- Serial number
- Firmware version

Test Results

The results of all subtests appear on the **Verification Tests** dialog box after each individual test is completed. See Table 50 for an explanation of test results.

Table 50 Test Results

Test Results	Explanation
PASSED	Completed the test without reported errors.
FAILED	An error has been found and needs to be corrected. A fatal error, or an error that causes a part of the system to become disabled, will halt the test.
INCOMPLETE	This portion of a test was incomplete due to an interruption or a portion of the test was run (for example, no scratch tape was used so must only use existing tapes). An incomplete will occur when the door is opened, an abort command is issued, or when the **Robotics Enable** button is pressed.
SKIPPED	This portion of the test was skipped. The cause is that either a scratch tape was not present or the library was not configured for the test.
WARNING	A warning is additional information about the test that the user should know. For example, if a calibration failed, but the stored offsets are analyzed, a warning should be posted that states that the offset check might not be accurate.
STOPPED	The test was interrupted. The log will show the result to provide a record of test interruption.

Note: A single problem in the library can cause failed results in multiple tests. After taking action to correct a failed result, run tests that yielded failed results again.

Verification Test Graphical Reports

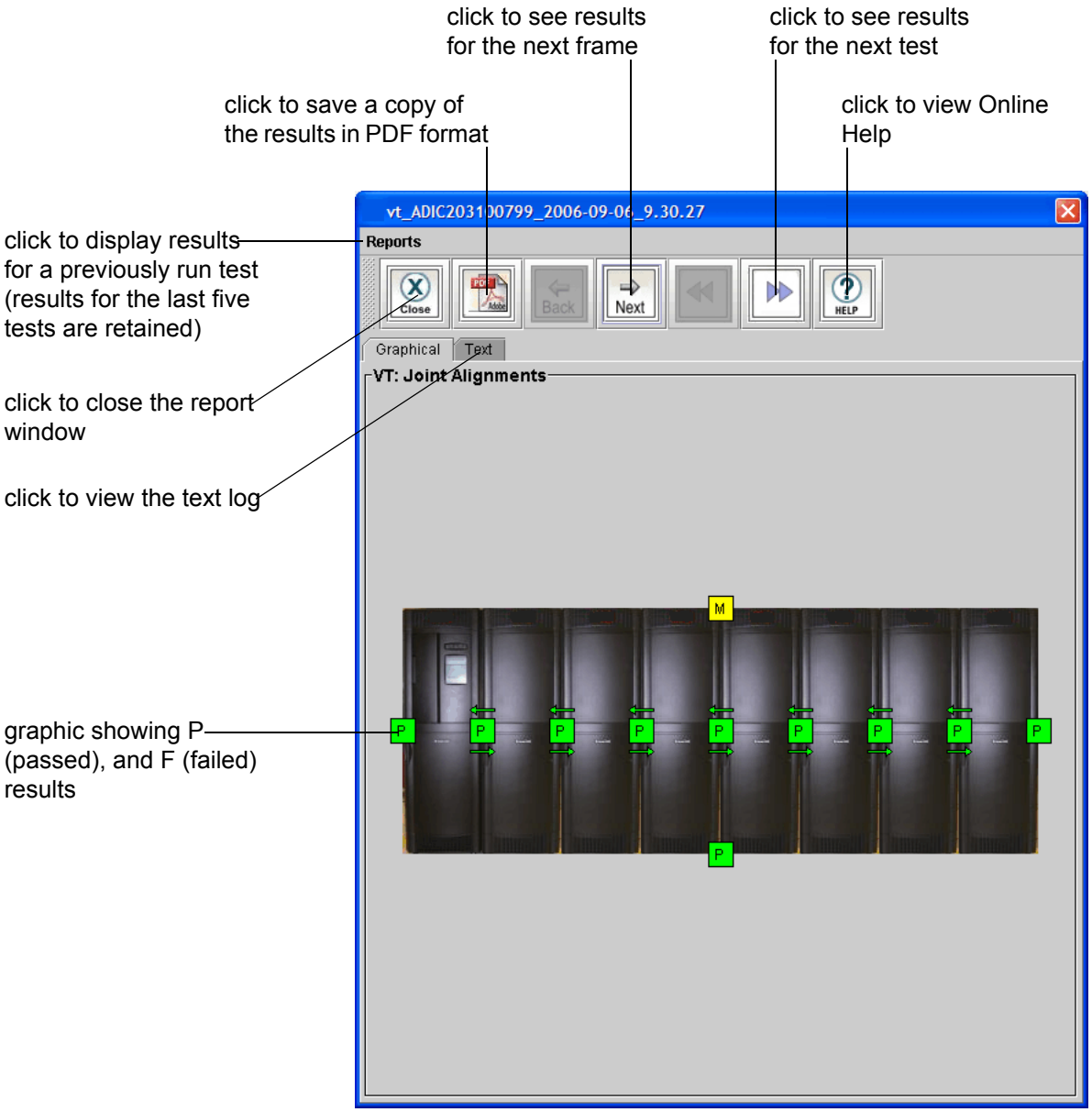
Some verification tests produce graphical reports that let you easily see if the test generated passed or failed results. Each result is shown in a different color:

- **P** - passed (green)
- **F** - failed (red)

There are eight types of graphical reports. Each individual test generates two or more graphical reports (except for the scan barcode test, which does not generate graphical reports). The following sections show an example of each type of graphical report and actions to take to correct a failed result.

To view the graphical reports for a test, click **Reports** on the **Verification Tests** dialog box. Figure 60 on page 617 shows the parts of the report window.

Figure 60 Report Window



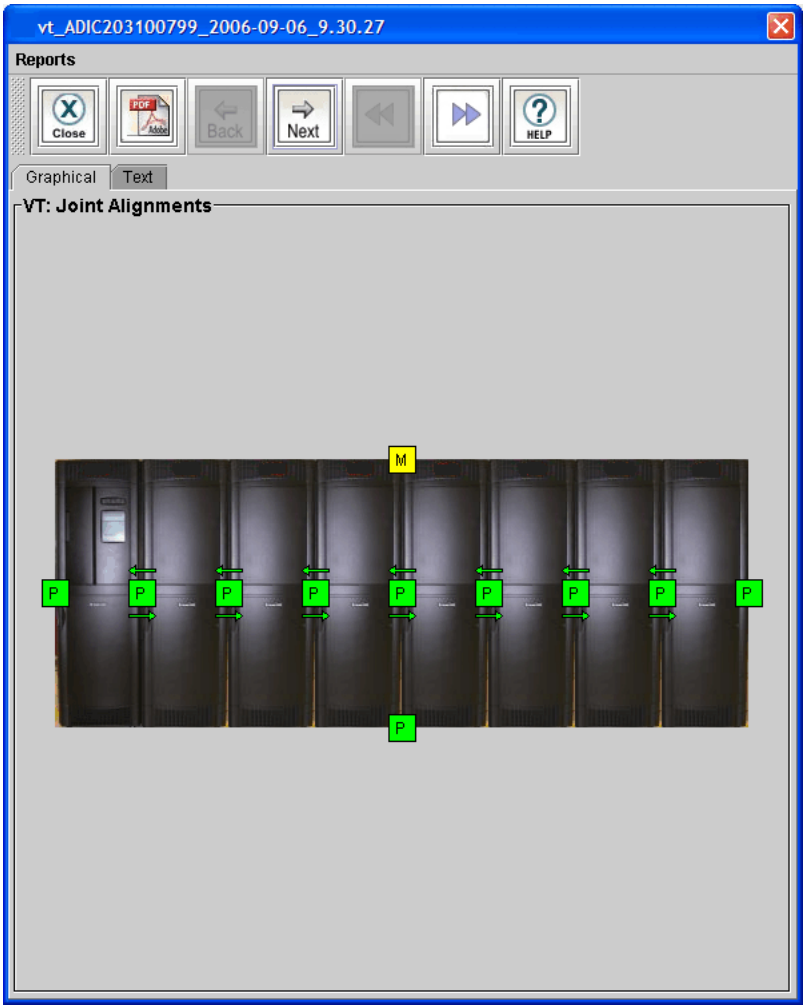
Joint Alignments

The Joint Alignments graphical report shows the results for tests of alignment between frames. It also shows the results for tests of accessor travel to all corners of the library.

- If the graphical report shows one or more failed results for joint alignment, realign the middle X-axis rail and check the alignment of the top and bottom X-axis rails at the location of the failure.
- If all the joints passed testing but accessor movement failed, manually move the accessor down the aisle in each direction to locate any places where motion of the accessor is not smooth or is restricted. Then realign the middle X-axis rail and check the alignment of the top and bottom X-axis rails at the location of the failure.

See Figure 61 on page 619.

Figure 61 Joint Alignments Graphical Report



Vertical Alignments

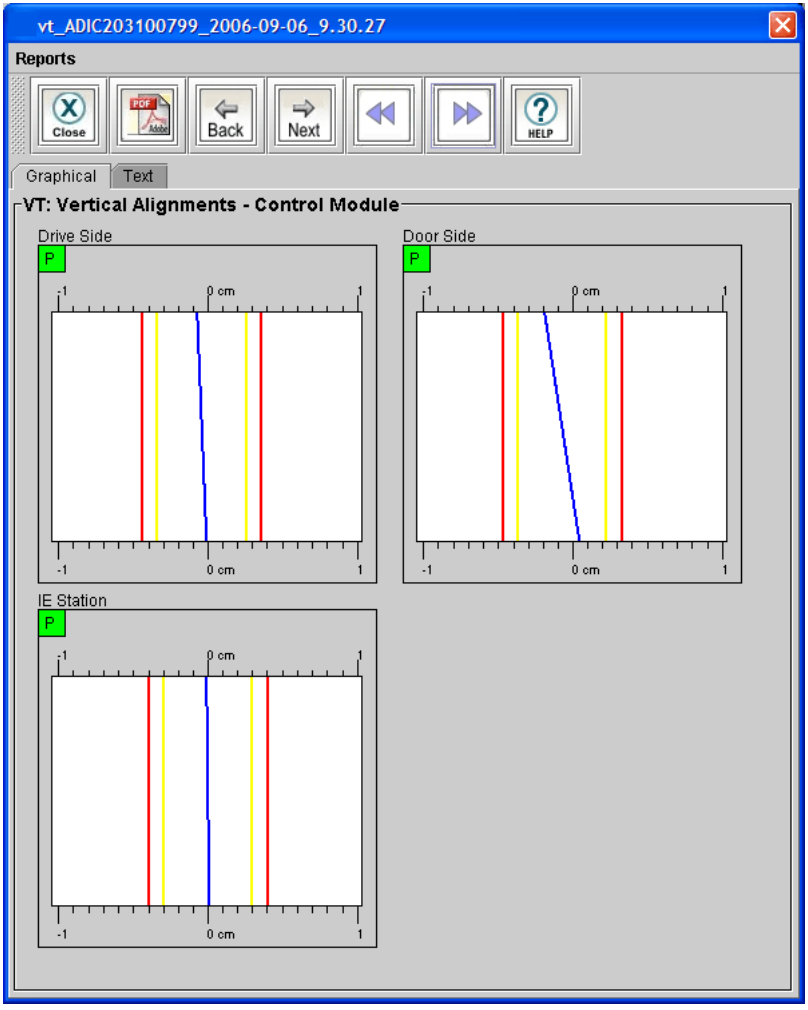
The Vertical Alignments graphical report shows the results for test of vertical alignment of tape magazines on the drive-side and door-side of each frame, and for vertical alignment of each I/E station.

- If the graphical report shows a failed result for the drive-side or door-side, make sure that all tape magazines are installed properly on that side and that the calibration targets are correctly snapped on to the magazines.

- If the graphical report shows a failed result for the I/E station, make sure the I/E station and front door are completely shut.
- If running the test again still generates failed results, realign the middle X-axis rail and check the alignment of the top and bottom X-axis rails at the location of the failure.

See Figure 62 on page 620.

Figure 62 Vertical Alignments Graphical Report



Horizontal Alignments

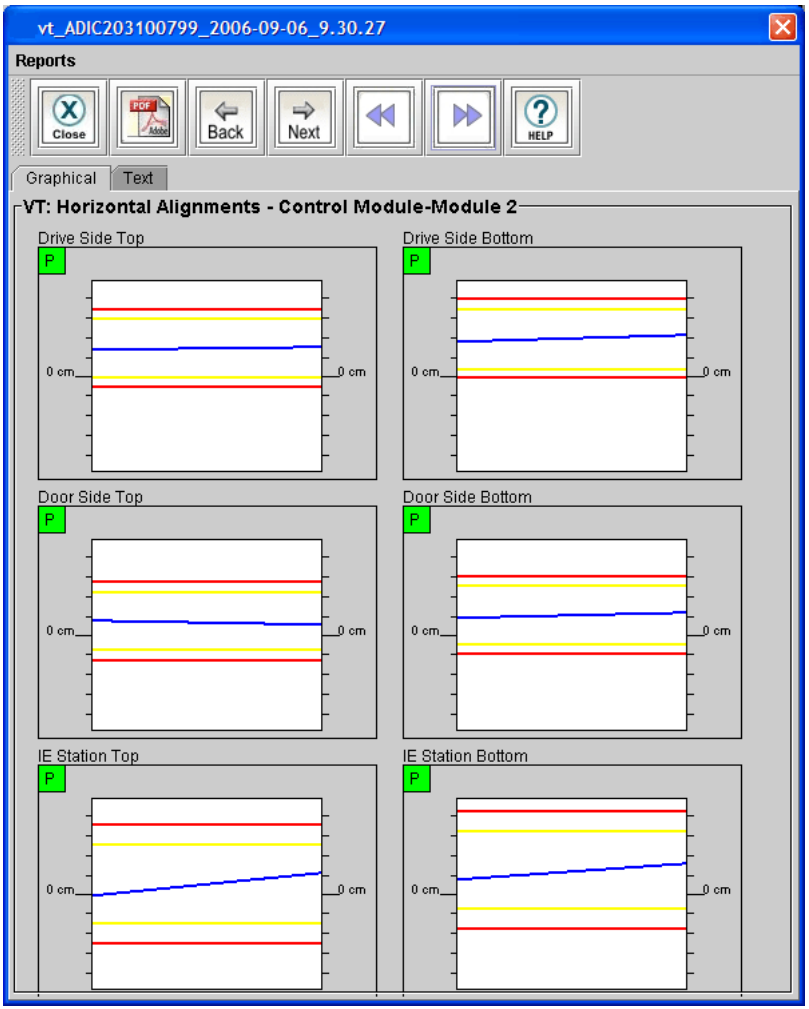
The Horizontal Alignments graphical report shows the results for tests of horizontal alignment of tape magazines on the drive-side and door-side across frames, and for horizontal alignment of I/E stations across frames.

Note: This graphical report is not generated for libraries with only one frame.

- If the graphical report shows a failed result for the drive-side or door-side, make sure that all tape magazines are installed properly on that side and that the calibration targets are correctly snapped on to the magazines.
- If the graphical report shows a failed result for the I/E station, make sure the I/E station and front door are completely shut.
- If running the test again still generates failed results, realign the middle X-axis rail and check the alignment of the top and bottom X-axis rails at the location of the failure.

See Figure 63 on page 622.

Figure 63 Horizontal Alignments Graphical Report



Calibration Offsets

The Calibration Offsets graphical report shows the results for tests of tape magazine, drive sled, and I/E station offsets compared to predefined tolerances. Reports are generated for drive-side and door-side for all frames.

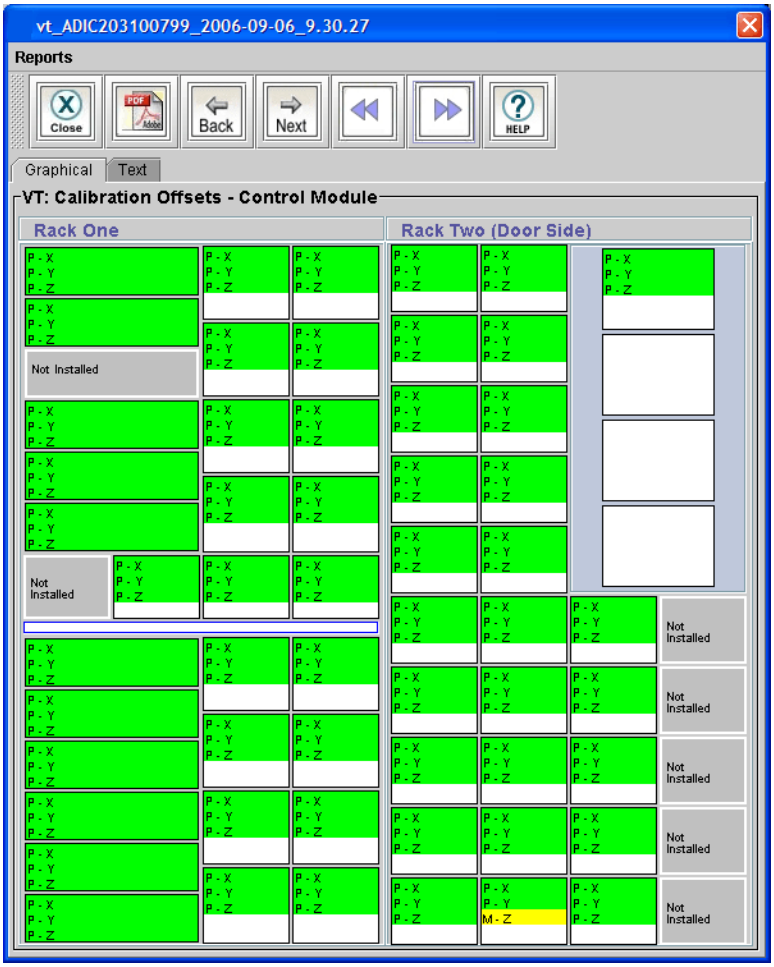
- If the graphical report shows a failed result for one or more tape magazines, make sure the magazines at the location of the failure

are installed properly and that the calibration targets are correctly snapped on to the magazines.

- If the graphical report shows a failed result for the I/E station, make sure the I/E station and front door are completely shut.
- If running the test again still generates failed results, realign the middle X-axis rail and check the alignment of the top and bottom X-axis rails at the location of the failure.

See Figure 64 on page 623.

Figure 64 Calibration Offsets Graphical Report



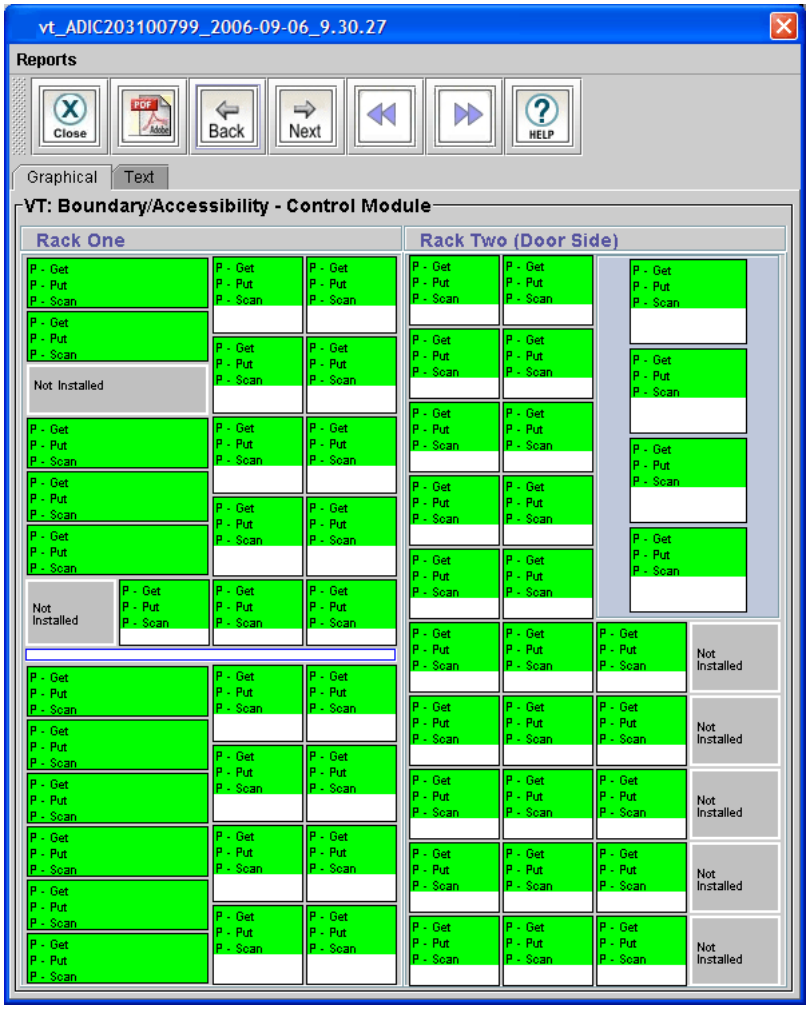
Boundary/Accessibility

The Boundary/Accessibility graphical report shows the results for tests of the accessor while performing Get, Put, and Scan functions for all tape magazines and drive sleds. (This tests whether magazines and sleds are within the maximum allowable movement range of the accessor.)

- If the graphical report shows a failed result for one or more tape magazines, make sure the magazines at the location of the failure are installed properly and that the calibration targets are correctly snapped on to the magazines.
- If the graphical report shows a failed result for the I/E station, make sure the I/E station and front door are completely shut.
- If running the test again still generates failed results, realign the middle X-axis rail and check the alignment of the top and bottom X-axis rails at the location of the failure.

See Figure 65 on page 625.

Figure 65 Boundary/ Accessibility Graphical Report



Get/Put

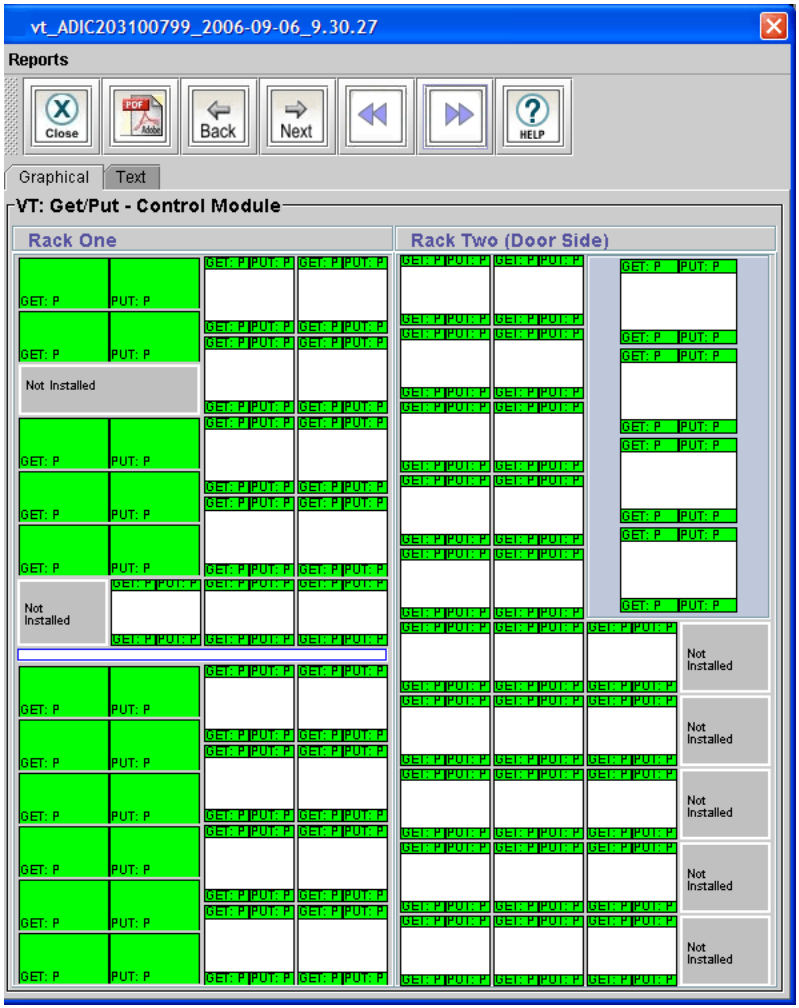
The Get/Put graphical report shows the results for tests of the picker assembly while performing one Get and one Put function for each tape magazine. The picker will use the selected scratch tape or the existing tape if it finds one at the target.

- If the graphical report shows a failed result for one or more tape magazines, make sure the magazines at the location of the failure are installed properly.

- If there are multiple failed results in an area, review the area to make sure it is not prone to problems. Also run the library alignment test (part of the installation verification or partial frame test) to make sure the library is level.
- If there are a large number of issues, use rubbing alcohol to clean the picker fingers and the detents in the side of the tapes.
- If the problems persist, you may need to replace the picker assembly.

See Figure 66 on page 627.

Figure 66 Get/Put Graphical Report



Scan Fiducials

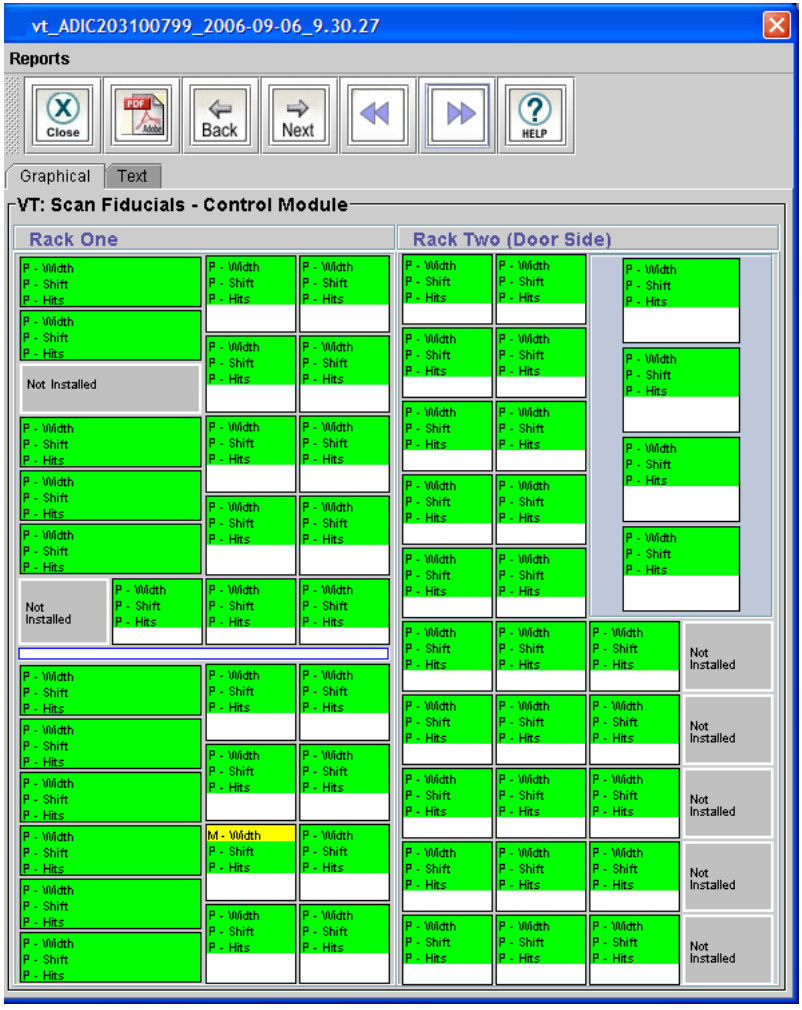
The Scan Fiducials graphical report shows the results for tests of the fiducial barcode on each tape magazine and drive sled, including the width, expected Y position (shift), and the number of hits the scanner receives while traveling up and down. (Only known magazines are tested.)

- If the graphical report shows a failed result for one or more tape magazines, replace the affected magazines.

- If there are multiple failed results, run the library alignment test (part of the installation verification or partial frame test) to make sure the library is level.
- If the library is level and there are multiple failed results, the scanner should be inspected and replaced if necessary.

See Figure 67 on page 628.

Figure 67 Scan Fiducials Graphical Report



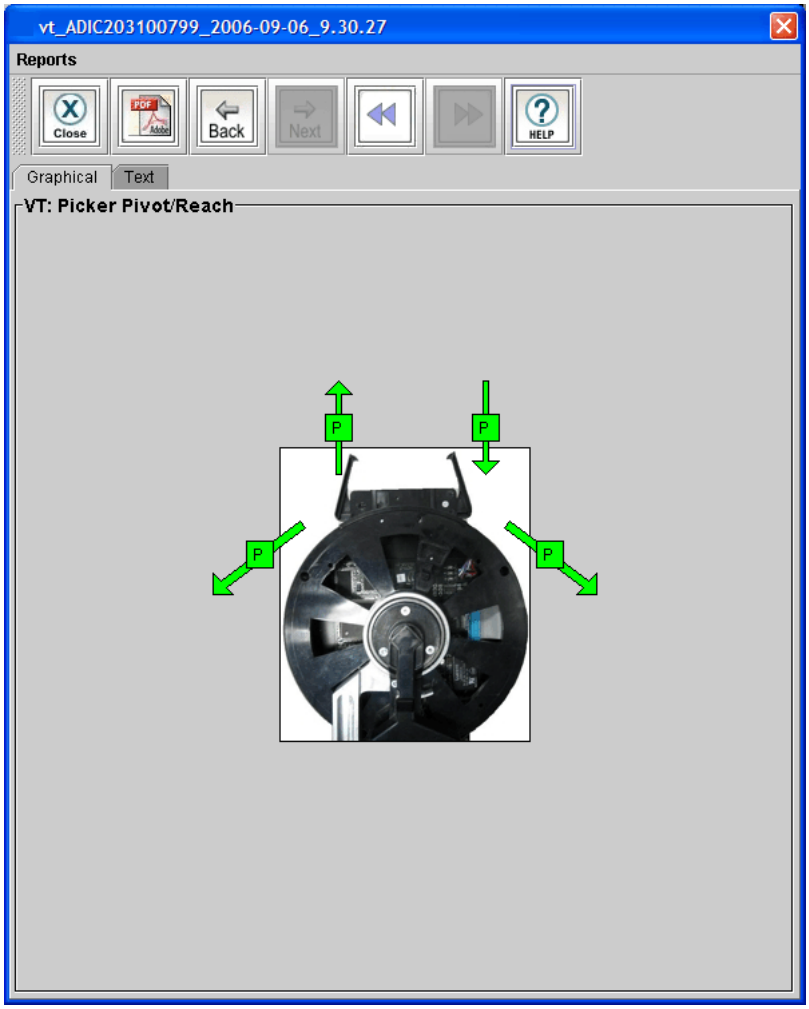
Picker Pivot/Reach

The Picker Pivot/Reach graphical report shows the results for tests of the picker while performing rotation and reach/retract actions.

- If the graphical report shows one or more failed results, inspect the picker. It should rotate easily by hand, and the fingers should spring into a clamped position. Make sure both rotation axis belts are free of debris. Also make sure that the storage is correctly seated in the I/E station and that the I/E station and front door are completely shut.
- If the problems persist, you may need to replace the picker assembly.

See Figure 68 on page 630.

Figure 68 Picker Pivot/Reach Graphical Report



Verification Test Logs

Each verification test produces a test log that details all information and results from the individual tests and subtests. In addition, the log includes information to help you understand the test results and to help resolve any problems encountered. To view a test log, click **Reports** on the **Verification Tests** dialog box to display the report window, and then click the **Text** tab.

You can view results for the five most recent tests. Click **Reports**, and then click the test results you want to view.

This log file is appended with data as each test finishes. You can repeat the test if any problems are found and fixed. If the **Verification Tests** dialog box was not closed during the retesting, all results are contained in one log file.

To save the information that the test generates, click **Send**. If you are using the remote LMC client, you can choose to save the log to your hard drive. If you choose to save directly to your hard drive, the report listing and test log are combined into one text file.

Figure 69 on page 632 shows an example of a test log. It provides the following information:

- The test output is from the library alignment test.
- In dual-robotics libraries, the test output is for the robot on which the test was run (the currently active robot).
- The test title is always shown between rows of equal signs.
- A brief guide for understanding coordinates and offsets used in the test results is provided near the beginning of the log.
- The X-axis and Y-axis limits applied by this test are shown. FAILED output is placed between brackets; for example, (30) and [45].
- The results of the subtest appear between dashed lines.
- Coordinates are represented as A (aisle), F (frame), R (rack), S (section), C (column), and R (row).
- All location values are in 0.1 mm.
- All results that you should review are identified with four arrows (>>>>) in the column to the left of the detailed results.
- At the end of every test, summary results of every subtest are given. The overall test result appears between asterisk lines, and a summary of subtest results follows. See Figure 69 on page 632.

Figure 69 Example Test Log Output

```
================================================================
             TEST ACCESSOR LIBRARY ALIGNMENT
================================================================
Library  serial number = 203100119
MCB time: 02/26/2010 05:02:47.39
Library Reserved for VT Testing.

  Checking input parameters...
     PASSED    0x00       Start Frame          OK
     PASSED    0x00       End Frame            OK
     PASSED    0x00       Start Rack           OK
     PASSED    0x00       End Rack             OK

--------------------------------------------------------------------------
                    GUIDE TO VERIFICATION TEST LOG
 COORDINATES
    A F R S C R  = aisle, frame, rack, section, column, row
    Index        = internal RCS number for a location
 OFFSETS
    Marginal offsets appear in (), Failed appear in []
    Predicted X Offset is the average of the previous frame's X offsets.
      This number is used to check the offset found against the tolerances.
--------------------------------------------------------------------------

Using frames 1 to 1, racks 1 to 1.

Checking XY Travel...

  Verifying Frame Terminator Corresponds with Hard Stops...
      This test uses the accessor to push up against the outside edge
      of the library. A hard-stop should be installed in the X and Y
      rail that limits the accessor's movement. If the frame terminator
      (installed on the last frame's LBX card) does not agree with the
      hardstops, this test will fail.

    PASSED: Max X hardstop matches frame terminator.
    PASSED: Max Y hardstop matches frame terminator.
      Position Stats         X  |   Y
        Set Limits:       3255 | 16731
        Hardstop Test:    3285 | 16740
      Move Details           X  |   Y
        Max Current:      2011 |  747
        Min Current:       371 |  698
        Following Error:    27 |    2
        Position Error:      0 |    0
```

Running the Verification Tests

This section provides instructions for starting the installation verification test, partial test, FRU operational test, and custom test.

To stop a test, disable the robotics by pressing the **Robotics Enable** button on the operator panel or by clicking **Stop** on the **Verification Tests** dialog box. Control will be returned to you as soon as the current command is completed.

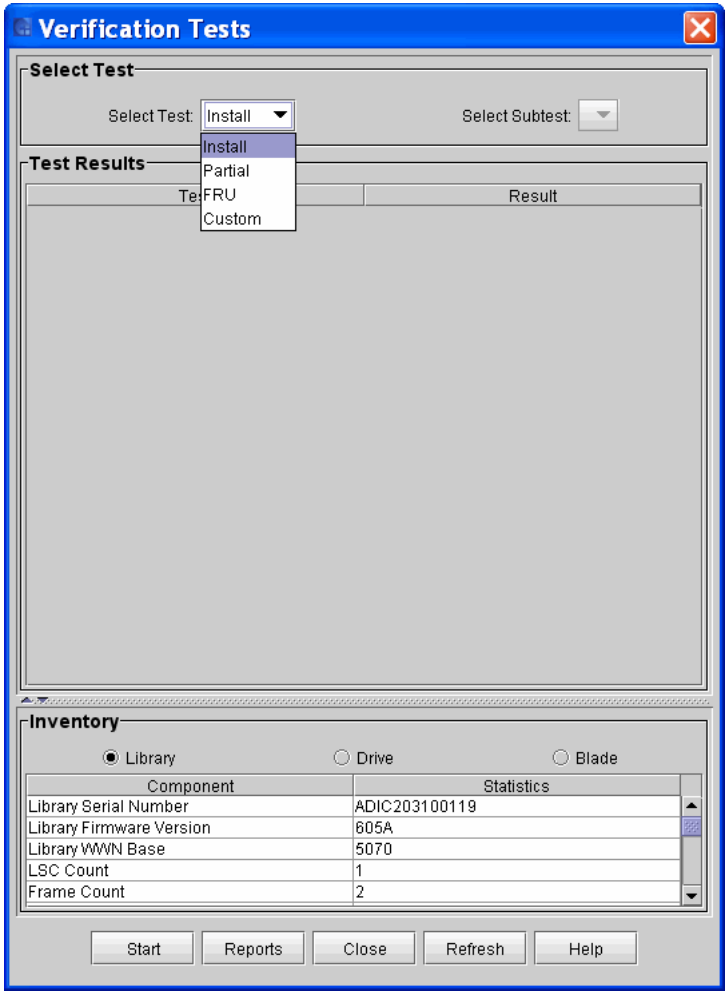
The test results appear after the tests complete. The different reports (**Library Report**, **Drive Report**, and **Blade Report**) will be generated and viewable in the **Reports** area of the **Verification Tests** dialog box.

If a typical user logs on while an administrator is logged on and running a verification test, testing will continue unaffected. Only one administrator can be logged on at any given time.

Install Verification Test

When the Install verification test is running, no one else can log on to the library. The message, "Verification Test is Running," appears in the **Activity** area of the main LMC display.

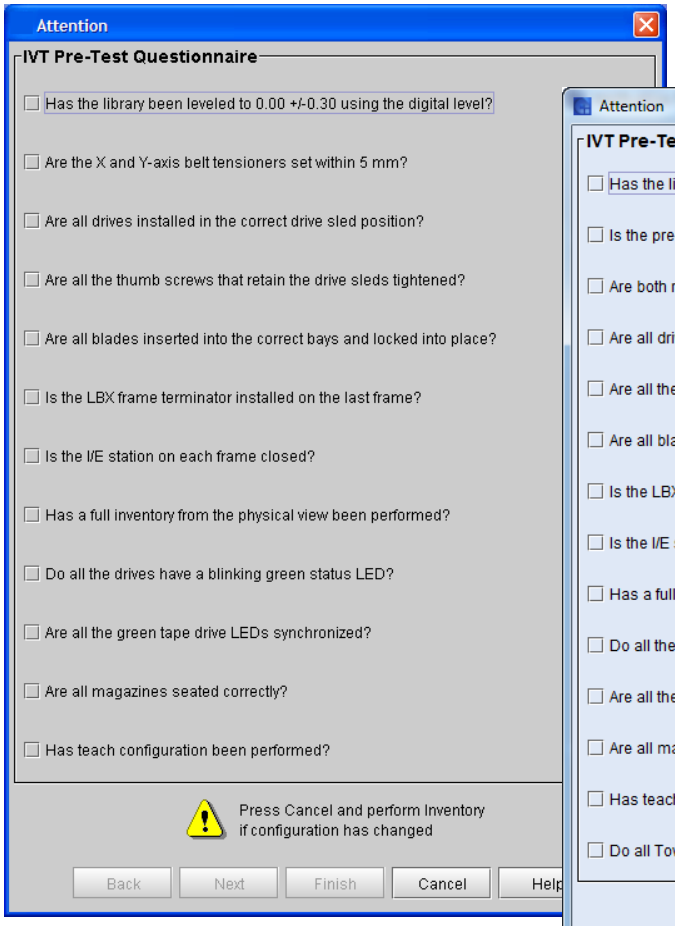
1. Log on as an administrator.
2. Make sure that you are viewing the physical library. From the **View** menu, click the name of the physical library.
3. Click **Tools > Verification Tests**. The **Verification Tests** dialog box appears.



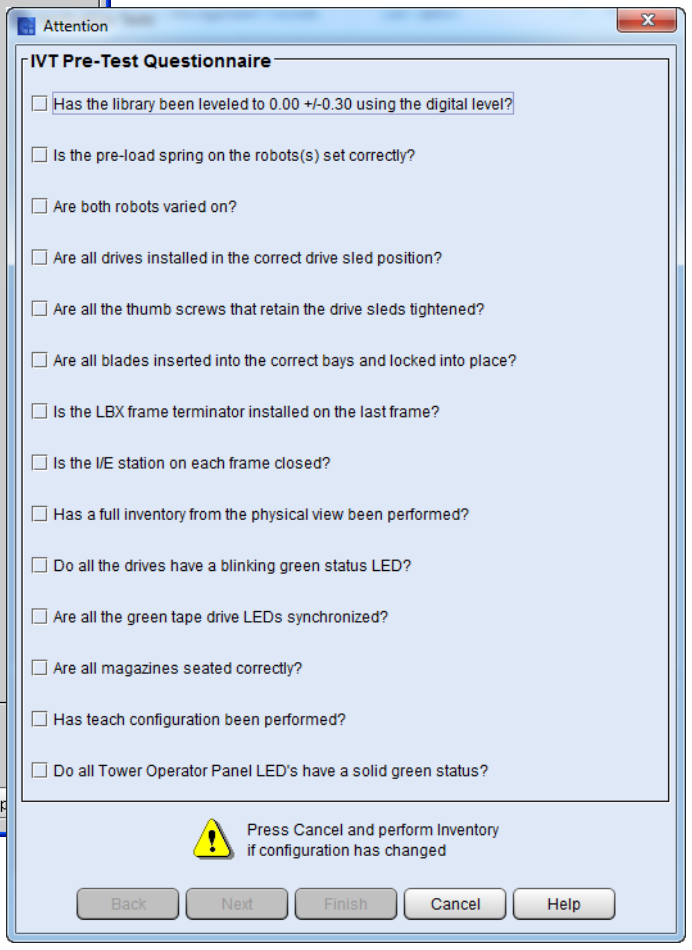
4 From the **Select Test** drop-down list, click **Install**.

5 Click **Start**.

6 If prompted to take the library offline, click **Yes**. The **IVT Pre-Test Questionnaire** appears.



Gen 1 Pre-test Questionnaire



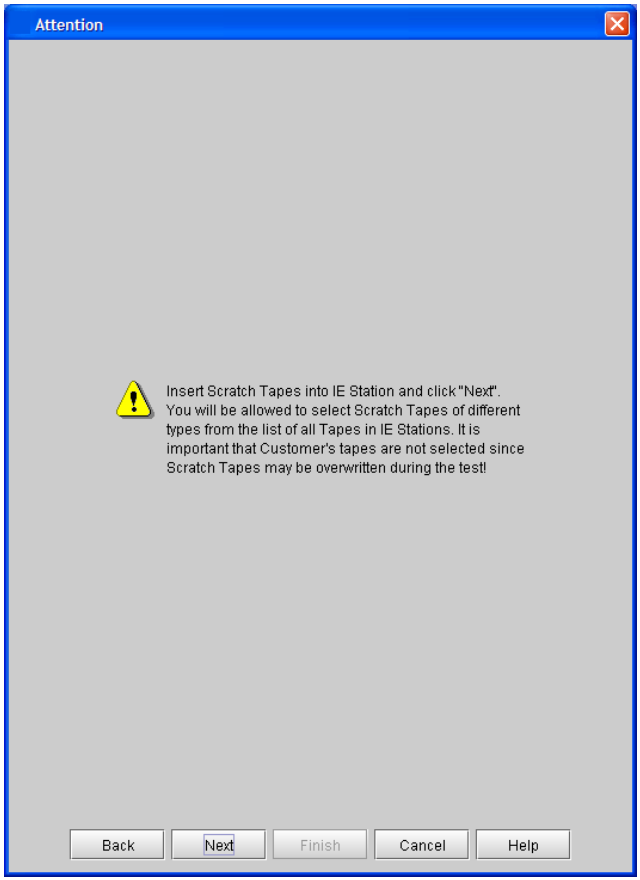
Gen 2 Pre-test Questionnaire

7 Complete the pre-test questionnaire by clicking inside the box next to the questions.

You cannot continue with the installation verification test until you have completed and verified the question requests on this questionnaire.

Note: Make sure you physically verify each of the questions on the questionnaire. Each of the items listed can cause the installation verification test to have unexpected behavior and unreliable results. The tests must be re-run if they fail.

8 After you complete the questionnaire, click **Next**. The following dialog box appears.



9 Insert a “scratch” cartridge into the I/E station, and then click **Next**.

Note: Make sure that your scratch tapes are formatted and contain no data that cannot be overwritten. Scratch tapes must have barcode labels with valid volume serial (volser) numbers on them. Also, you might find it useful to write down the volser number so that you can identify your scratch tapes.

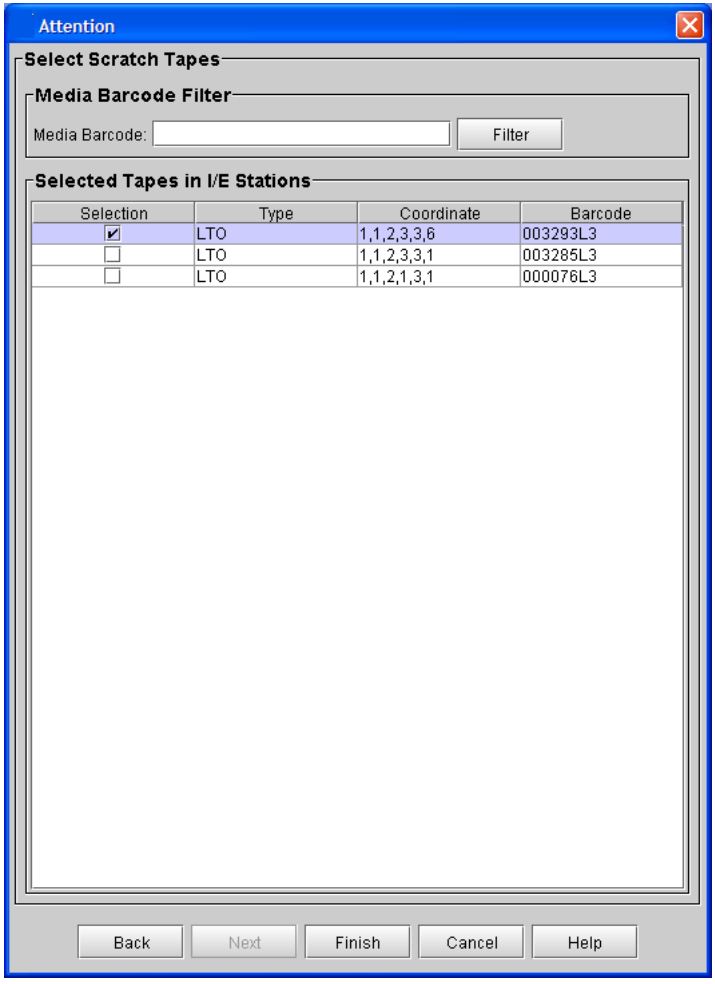
This procedure will not damage any cartridges that are already installed in the library.

If the scratch cartridge becomes lodged in a drive or magazine, it must be manually removed from the library. If not removed, the cartridge will become part of the partition the next time the accessor assembly is enabled.

The I/E station will be locked until the inventory is complete.

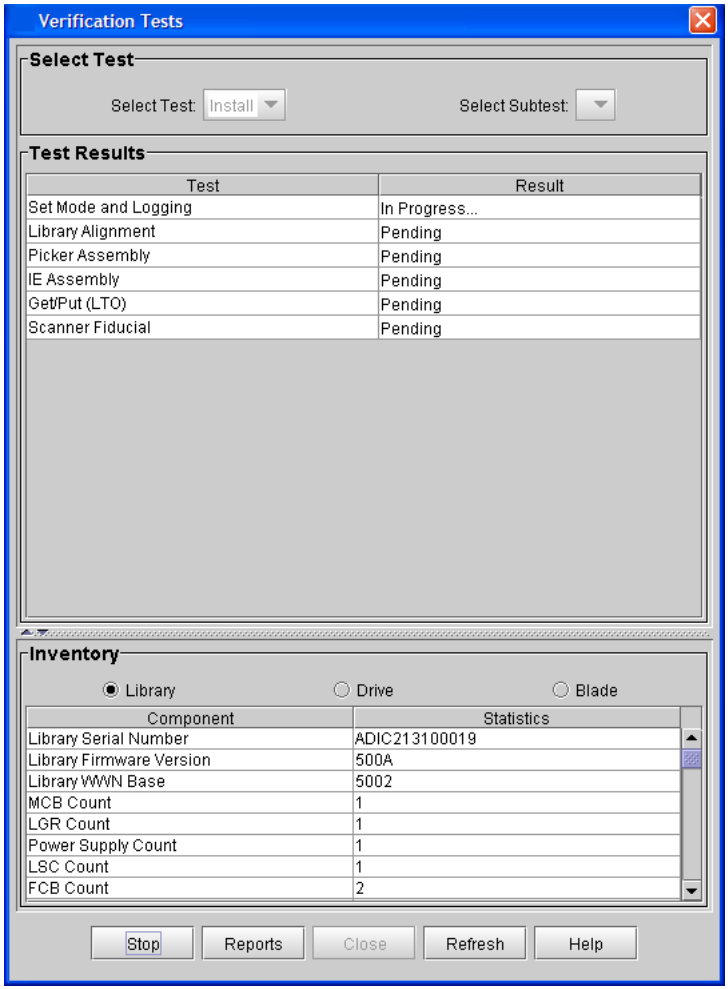
10 Select a scratch cartridge of each media type listed on the following dialog box.

Note: You can select one scratch cartridge per media type. Each test that requires a scratch cartridge will call the media types as needed.



11 After you select the cartridges, click **Finish**.

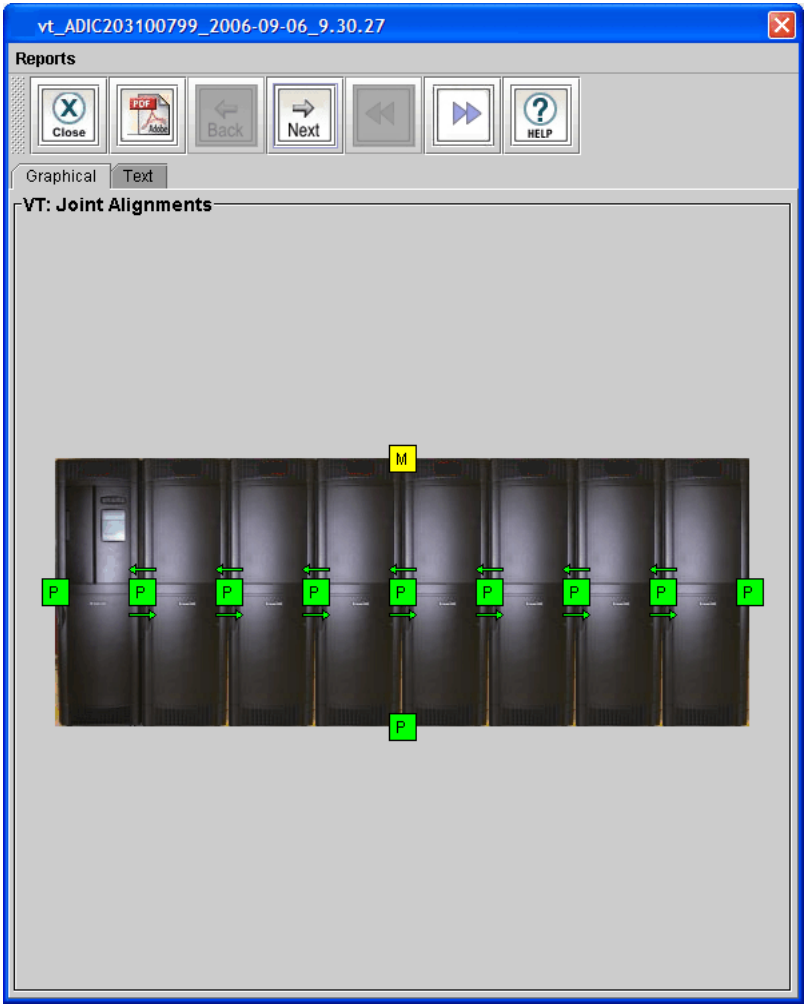
As the tests run, the library will generate RAS tickets if problems are discovered. You must close the **Verification Tests** dialog box to view those tickets. Return to the **Verification Tests** dialog box to view test results.



12 After the test is complete, click **Reports** to view the test results.

The report window appears with the **Graphical** tab displayed.

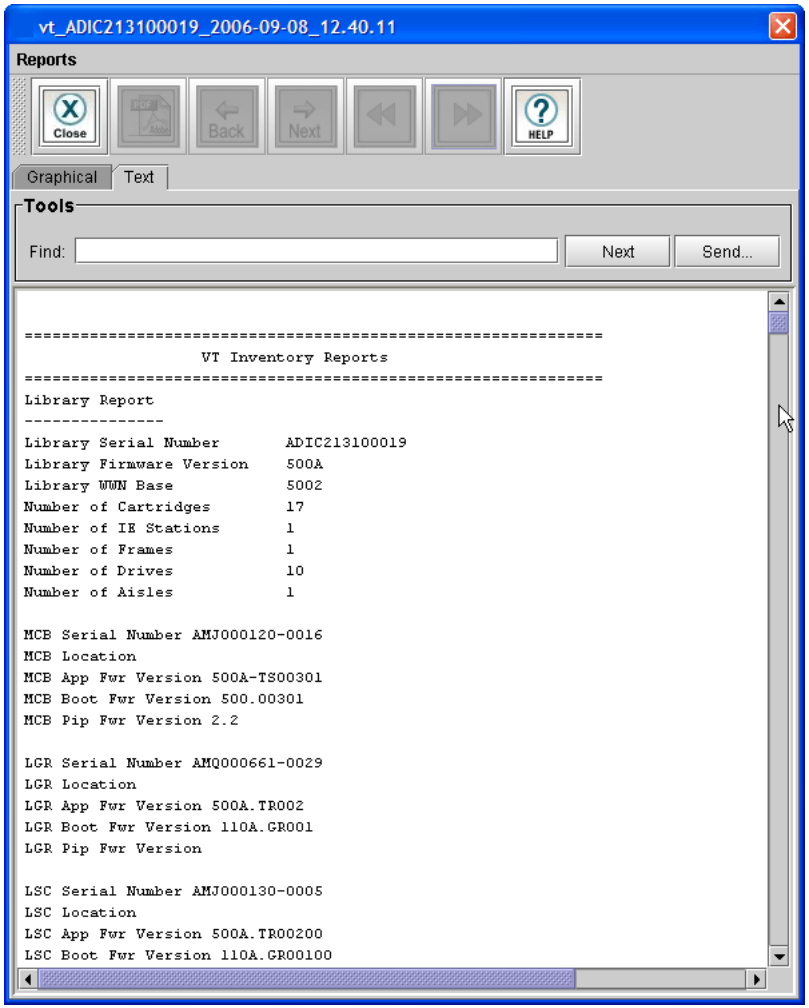
- Use the **Graphical** tab to view graphical reports and to quickly identify areas where failed results occurred.
- Use the toolbar to navigate between graphical reports or to save the results in PDF format. For more information about how to work with graphical reports, see Verification Test Graphical Reports on page 616.



13 For more detailed test results, click the **Text** tab to view the test log generated by the LMC.

14 Review the test log to find failed test results, and to see troubleshooting information. For information about how to interpret test logs, see Verification Test Logs on page 630.

15 To e-mail the test log, print it, or save it as a text file, click **Send** and then specify the output location. For more information, see Mailing, Saving, and Printing Status Information on page 538.



16 To see the results for a previous test, click **Reports**, and then click a test. The LMC saves the most recent five test results.

17 When you are done working with the test results, click **Close** to close the result window.

18 If you are done performing verification tests, click **Close** to close the **Verification Tests** dialog box.

Mailing, Saving, and Printing Test Logs

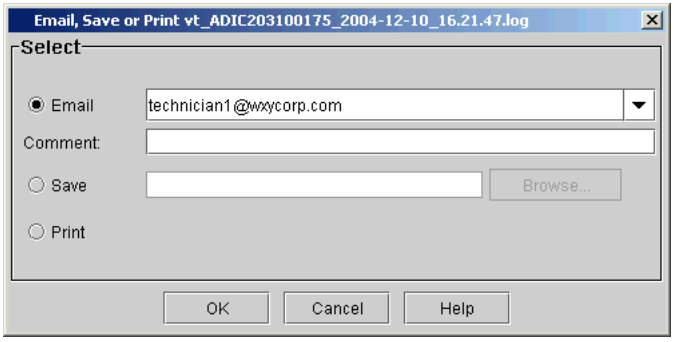
The **Send** button on the **Text** tab on the report window enables you to send a verification test log to e-mail addresses. If you are accessing the LMC from a remote client, **Send** also enables you to save the log to a file or print it.

Note: You can mail, save, or print verification test logs from a remote client. However, you cannot save or print logs from the library's touch screen.

The information that is sent will be the same as what the **Text** tab appears at the time that you click **Send**.

Note: Before you perform the following procedure, you must make sure that e-mail is appropriately configured in the LMC so that the library can send logs to the recipient. See Configuring E-mail on page 177.

1. Make sure that the **Text** tab on the report window displays the log that you want to send.
2. Click **Send**. The **Email, Save or Print** dialog box appears.



3. Perform one of the following tasks:
   - To indicate that you want to send the log as an e-mail message to a recipient, select **Email**, and then either type an e-mail address in the **Email** text box or select an existing address from the drop-down list. You can type a comment in the **Comment** text box to send with the log.

- To indicate that you want to save the log, select **Save**, and then either type in the **Save** text box a path and a file name to which you want the log saved or click **Browse** to specify a location and a file name.

Note: The **Save** option is available to remote client users only. It appears grayed out on the touch screen.

- To indicate that you want to send the log to a printer, select **Print**.

Note: The **Print** option is available to remote client users only. It appears grayed out on the touch screen.

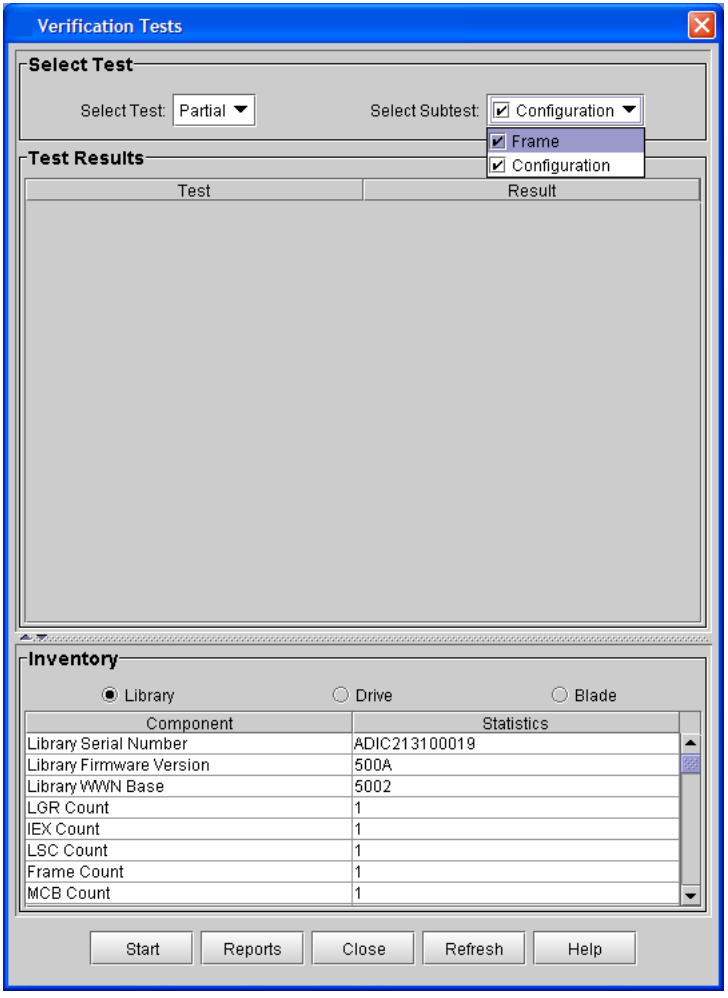
4 To send, click **OK**.

Partial Tests

1 Log on as an administrator.

2 Make sure that you are viewing the physical library. From the **View** menu, click the name of the physical library.

3 Click **Tools > Verification Tests**. The **Verification Tests** dialog box appears.

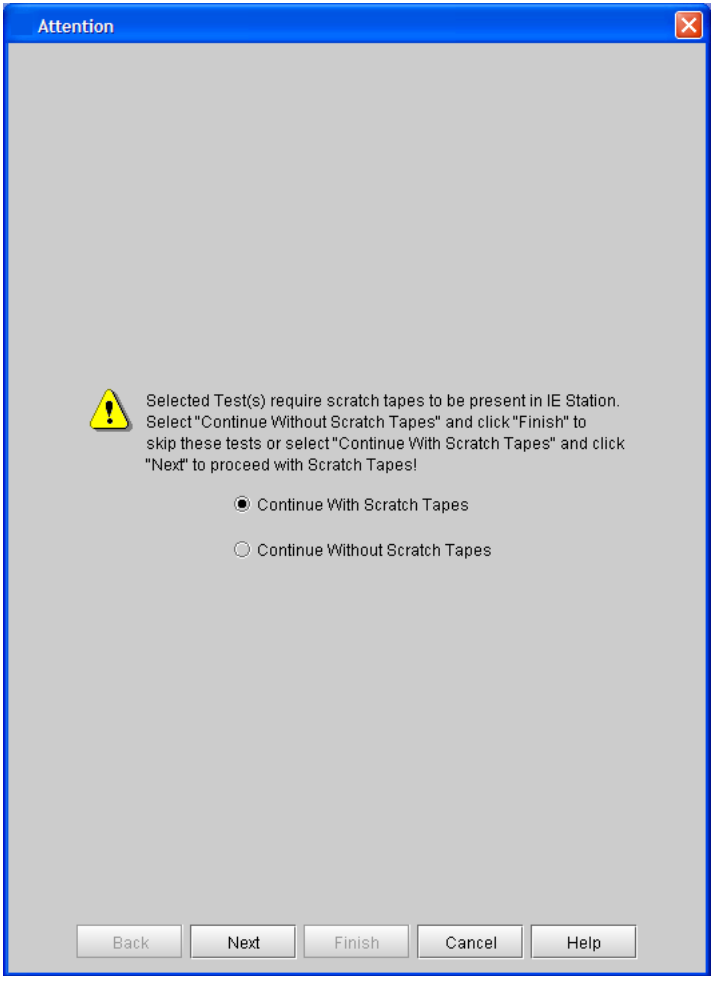


4 From the **Select Test** drop-down list, click **Partial**.

5 From the **Select Subtest** drop-down list, click either **Frame** or **Configuration** or both. A check mark indicates the test is selected.

6 Click **Start**.

7 If prompted to take the library offline, click **Yes**. The following dialog box appears.



8 Select either **Continue With Scratch Tapes** or **Continue Without Scratch Tapes**, and then click **Next**.

9 If you selected **Continue With Scratch Tapes**, insert a “scratch” cartridge into the I/E station, and then click **Next**.

Note: Make sure that your scratch tapes are formatted and contain no data that cannot be overwritten. Scratch tapes must have barcode labels with valid volume serial (volser) numbers on them. Also, you might find it useful to write down the volser number so that you can identify your scratch tapes.

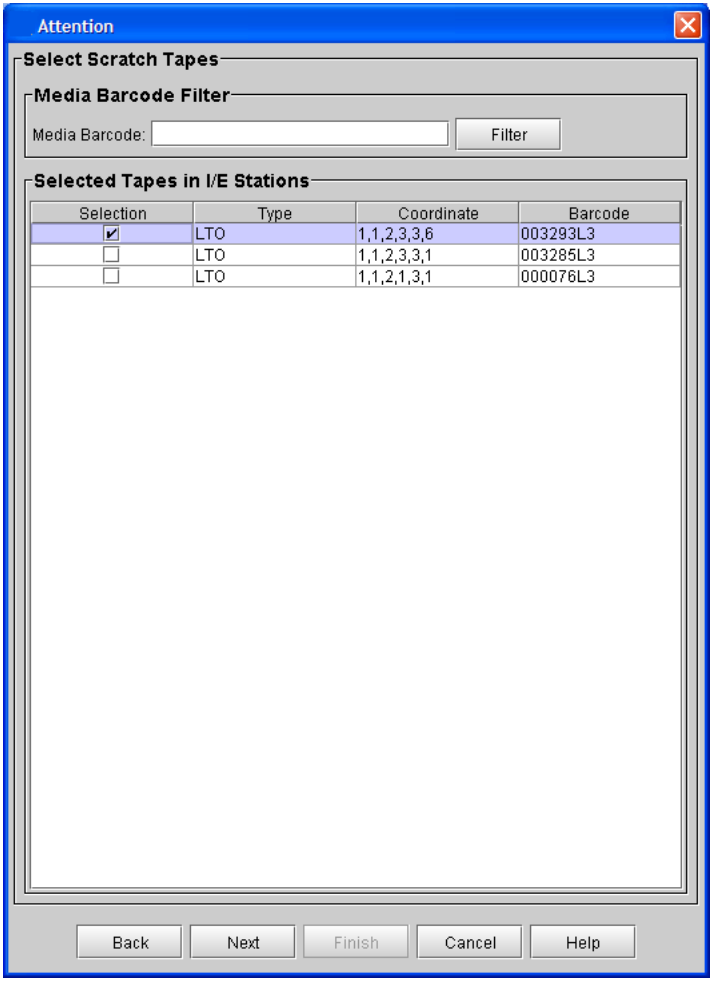
This procedure will not damage any cartridges that are already installed in the library.

If the scratch cartridge becomes lodged in a drive or magazine, it must be manually removed from the library. If not removed, the cartridge will become part of the partition the next time the accessor assembly is enabled.

The I/E station will be locked until the inventory is complete.

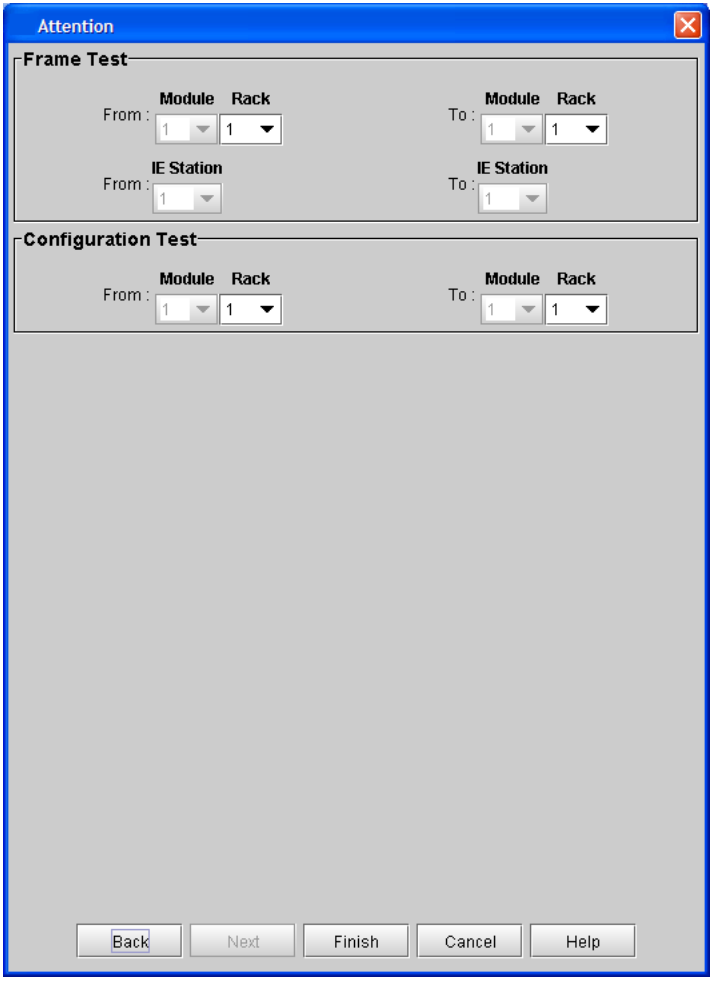
10 Select a scratch cartridge of each media type listed on the following dialog box, and then click **Next**.

Note: You can select one scratch cartridge per media type. Each test that requires a scratch cartridge will call the media types as needed.

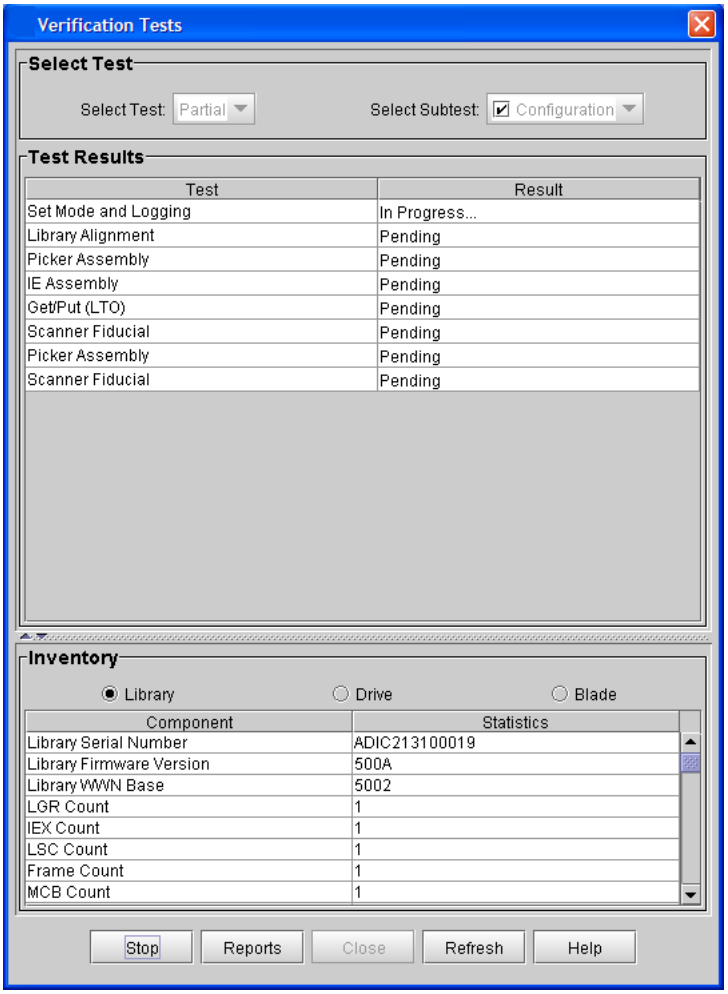


11 Select the number of the frame and racks where the tests are to be performed.

The following example shows both the frame and configuration tests because both were selected.



Test progress is shown in the **Verification Tests** dialog box.



12 After the test is complete, click **Reports** to view the test results.

For more information about how to work with graphical reports, see Verification Test Graphical Reports on page 616.

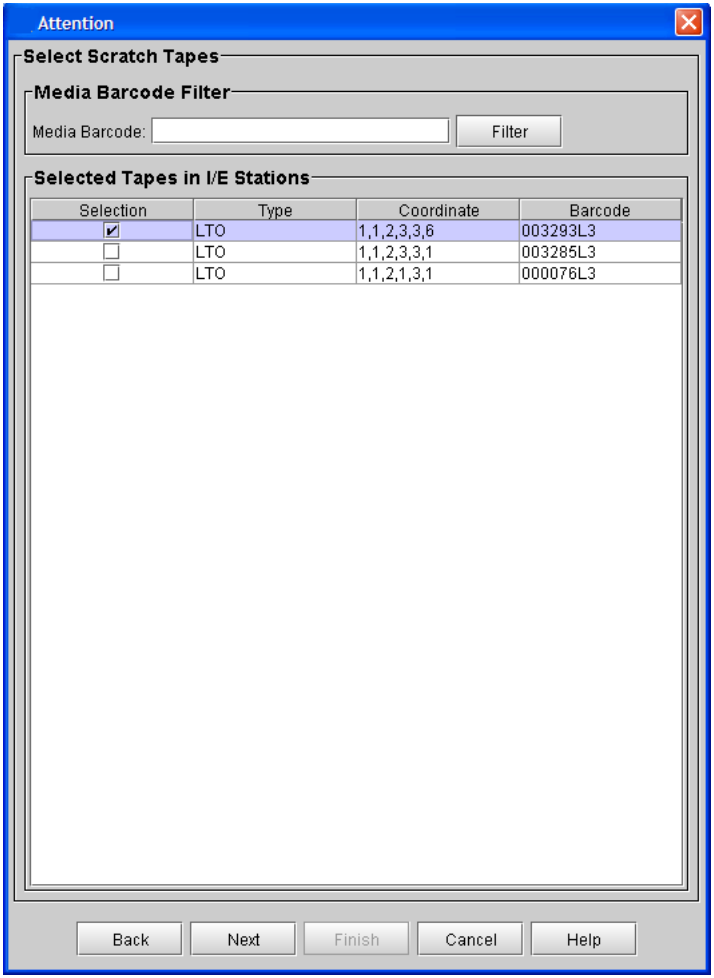
For information about how to interpret test logs, see Verification Test Logs on page 630.

For information how to e-mail, print, or save text logs, see Mailing, Saving, and Printing Test Logs on page 642.

FRU Operational Tests

There are two ways to run the FRU operational tests. You can select the FRU test from the **Verification Tests** dialog box. Alternatively, you can run the test from the **Ticket Details** dialog box if that FRU is supported by the verification tests.

The screens displayed by the FRU operational tests vary, depending on which subtest was selected. For example, if you click **Picker Assembly**, **IE Assembly**, or **Drive Sled Assembly**, the following dialog box appears for selecting a scratch tape.

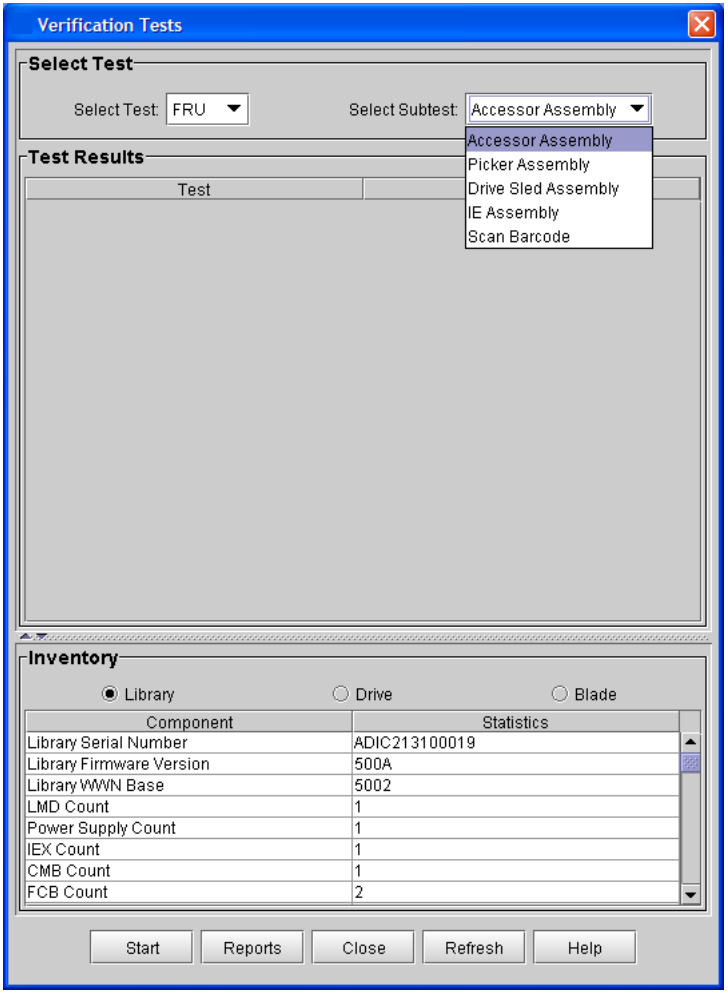


Running FRU Operational Tests from Verification Tests Dialog Box

1 Log on as an administrator.

2 Make sure that you are viewing the physical library. From the **View** menu, click the name of the physical library.

3 Click **Tools** > **Verification Tests**. The **Verification Tests** dialog box appears.



FRU tests are available for the **Accessor Assembly**, **Picker Assembly**, **Drive Sled Assembly**, **IE Assembly**, and **Scan Barcode**. You can only test one FRU at a time. The following steps provide

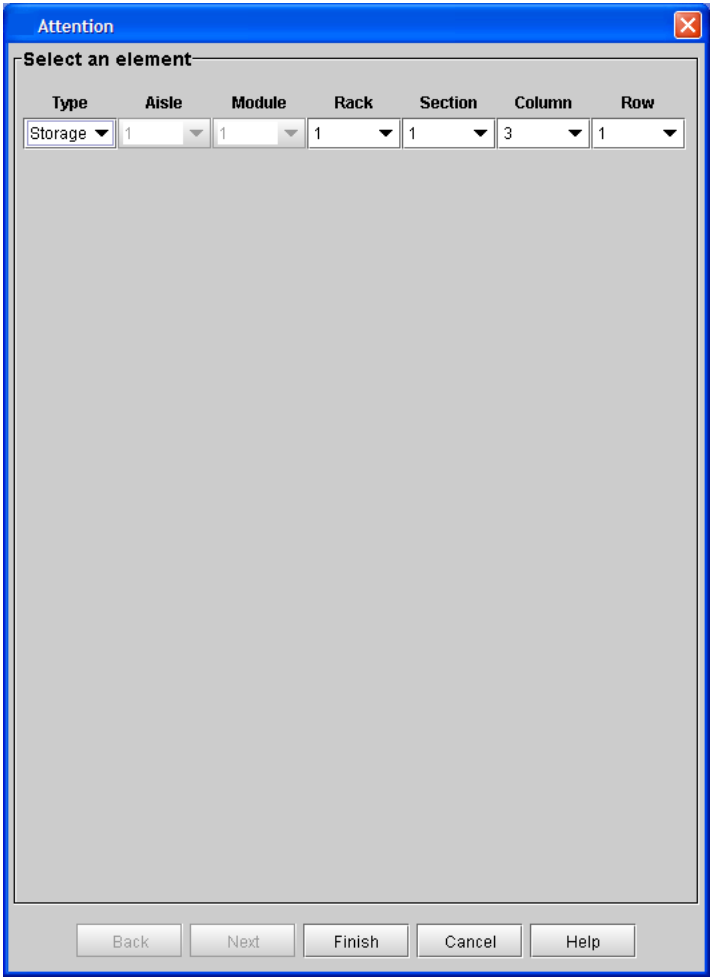
instructions for running the **Scan Barcode** test. The other tests provide similar windows and functionality for the other FRUs.

4 From the **Select Test** drop-down list, click **FRU**.

5 From the **Select Subtest** drop-down list, click **Scan Barcode**.

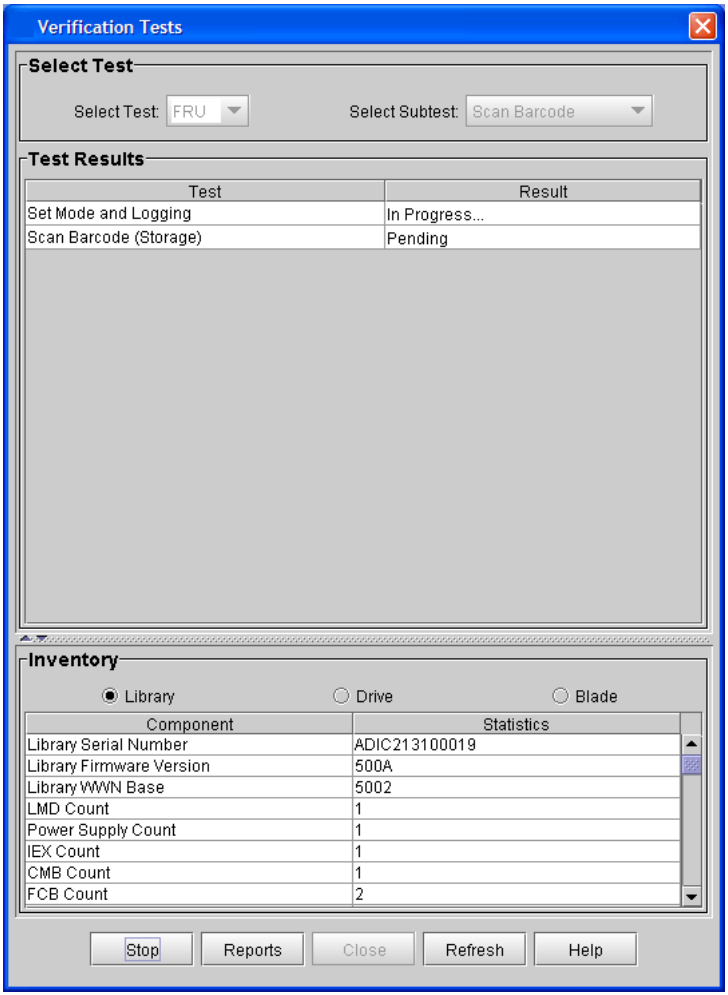
6 Click **Start**.

7 If prompted to take the library offline, click **Yes**. The following dialog box appears.



This dialog box enables you to enter any coordinate address in the library (aisle, module, rack, section, column, and row). The address does not need to be occupied by a drive or cartridge.

8 Click **Finish**. Test progress is shown in the **Verification Tests** dialog box.



9 After the test is complete, click **Reports** to view the test results.

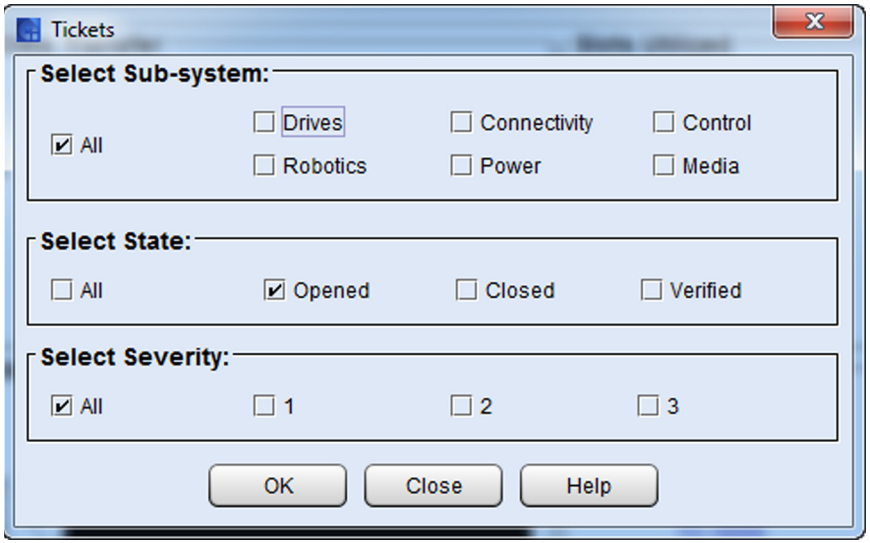
For more information about how to work with graphical reports, see Verification Test Graphical Reports on page 616.

For information about how to interpret test logs, see Verification Test Logs on page 630.

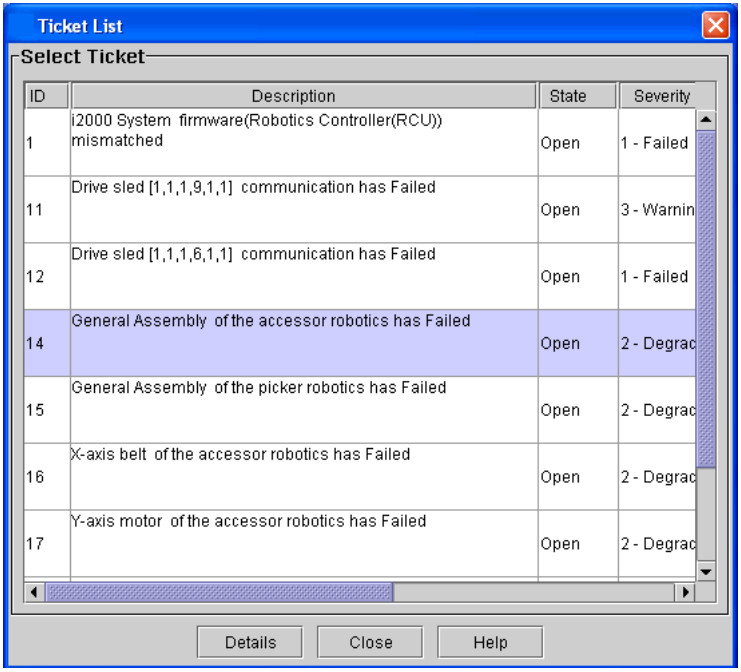
For information how to e-mail, print, or save text logs, see Mailing, Saving, and Printing Test Logs on page 642.

Running FRU Operational Tests from Ticket Details Dialog Box

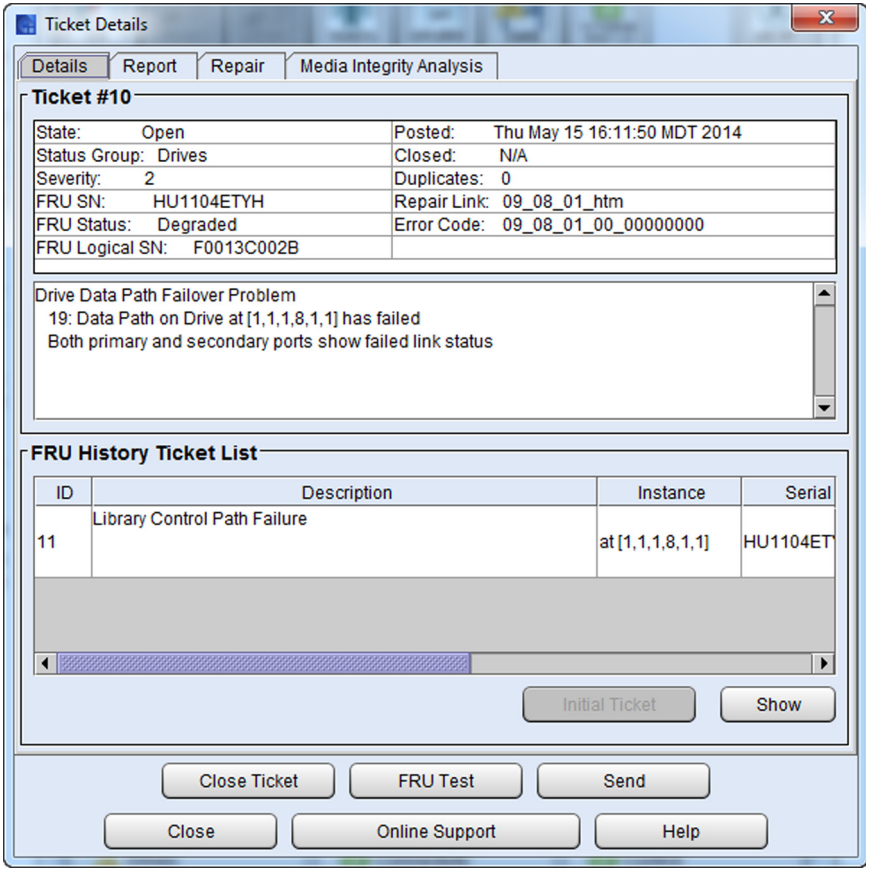
1. Log on as an administrator.
2. Make sure that you are viewing the physical library. From the **View** menu, click the name of the physical library.
3. Click **Tools > Tickets**. The **Ticket** dialog box appears.



4. From the **Tickets** dialog box, click the categories of the tickets you want to view and click **OK**. The **Ticket List** dialog box appears.



5 Click a ticket to highlight it, and then click **Details**. The **Ticket Details** dialog box is displayed.



6 From the **Ticket Details** dialog box, click **FRU Test**.

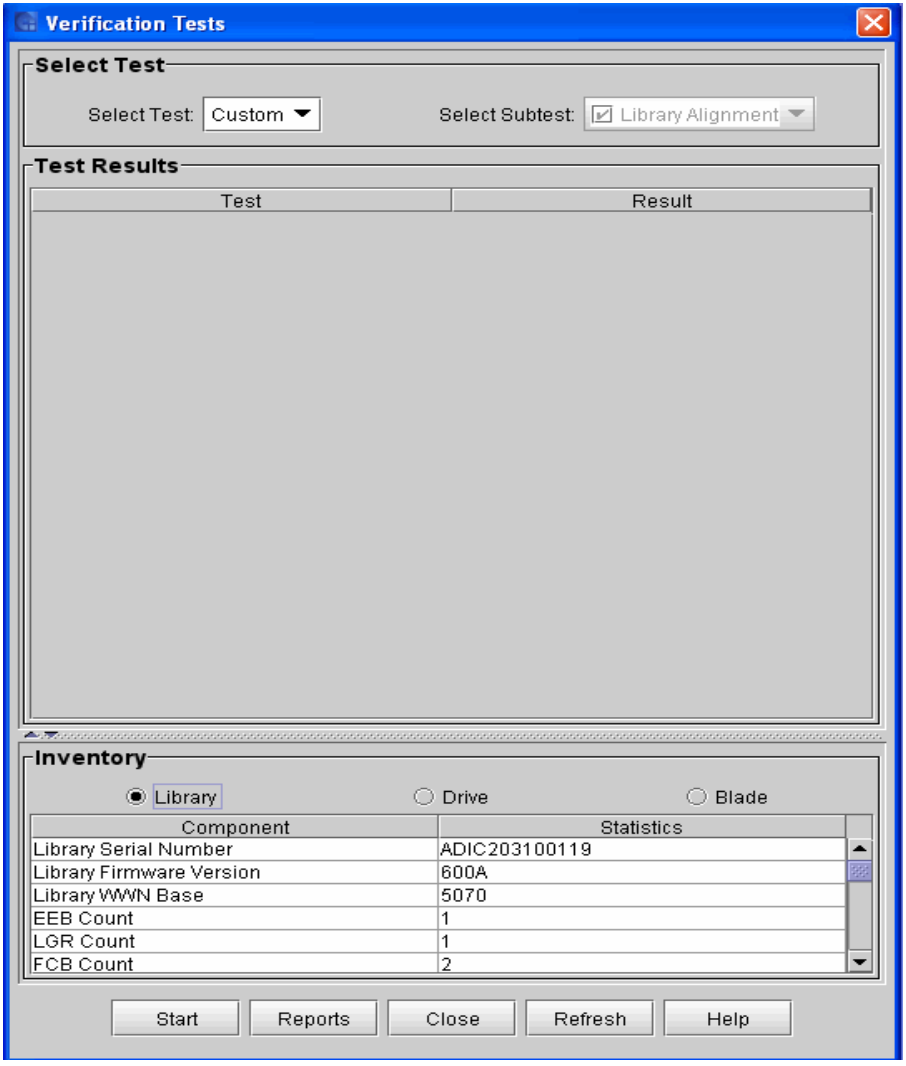
After the FRU test successfully verifies that the FRU has PASSED, all tickets associated with the failure are transitioned to the Verify state.

Custom Tests

The Custom test enables you to run the Library Alignment sub-test.

1 Make sure that you are viewing the physical library. From the **View** menu, click the name of the physical library.

2 Click **Tools > Verification Tests**. The **Verification Tests** dialog box appears.

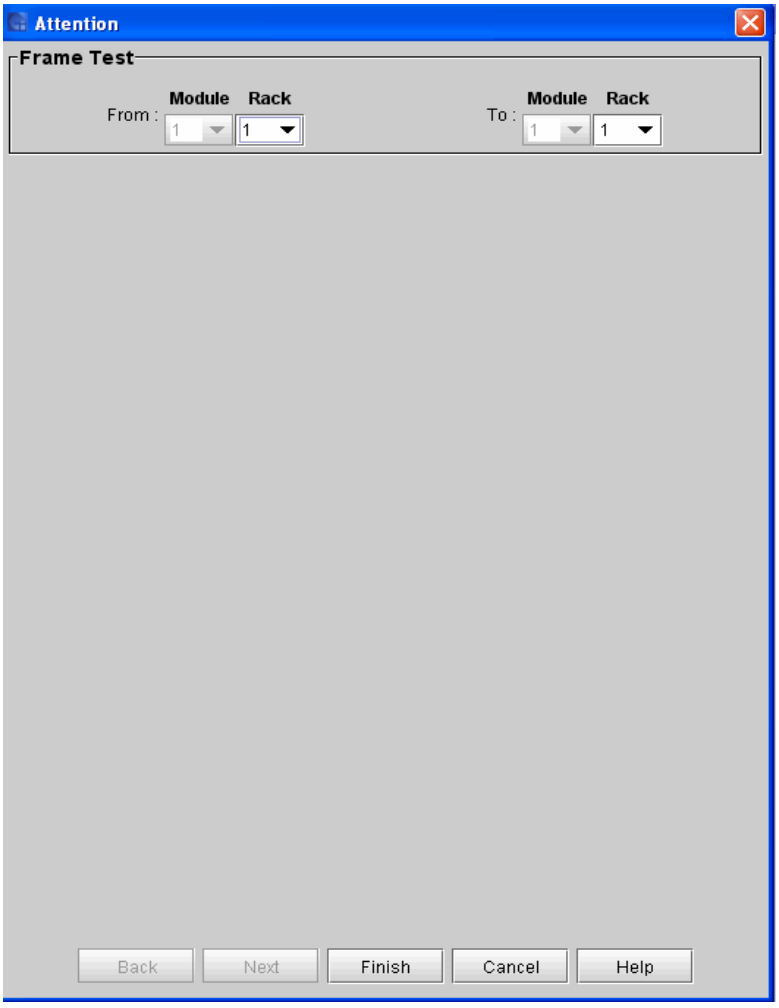


3 From the **Select Test** drop-down list, click **Custom**. The **Select Subtest** field defaults to the Library Alignment subtest and cannot be changed.

4 Click **Start**.

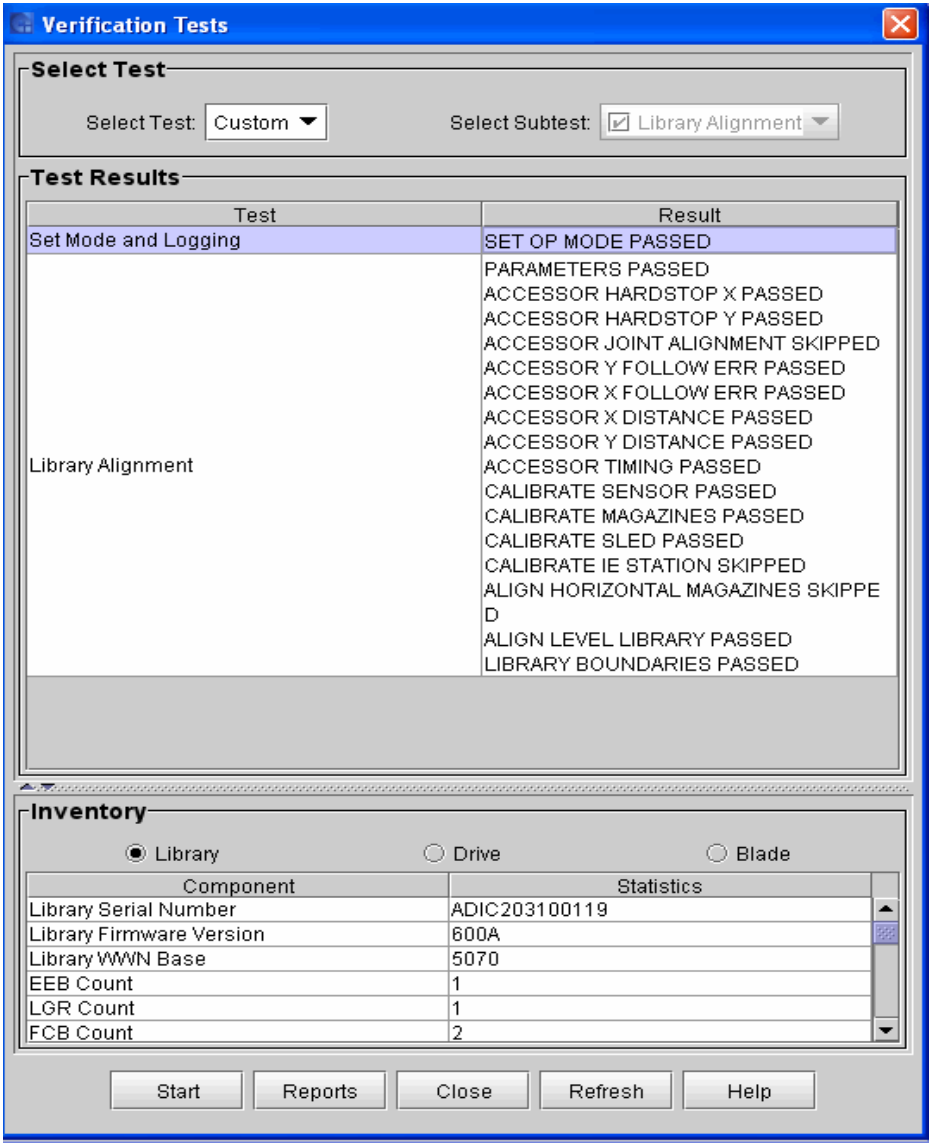
5 If prompted to take the library offline, click **Yes**.

6 Click **Start.** The following dialog box appears.



7 Select the starting **Module** (frame) and **Rack** as well as the ending **Module** (frame) and **Rack** where you want to perform the tests.

8 Click **Finish**. The test is initiated. Test progress is shown in the **Verification Tests** dialog box.



9 After the test is complete, click **Reports** to view the current or historical reports.

For more information about how to work with graphical reports, see Verification Test Graphical Reports on page 616.

For information about how to interpret and save test logs, see Verification Test Logs on page 630.

Using the Partitions Defragmentation Tool

Typically, partitions in a library are physically contiguous. That is, all tape slots that belong to a partition are adjacent to one another in the library. However, if a partition is enlarged, or if an expansion module is added to a library, it is possible that some or all partitions in the library will no longer be physically contiguous. In this case, the slots that belong to a partition are not all adjacent to one other, and the partition is fragmented. Fragmentation can make bulk loading media more difficult.

Defragmenting partitions reassigns slots in the library so that all slots in each partition are physically contiguous with one another. In addition, media is moved as needed to make sure it resides in the correct partition. In the process, tapes are first moved from their old location to the I/E station, and then are moved to their new location in the library.

Note: Only partitions that contain an I/E station can be defragmented. Also, at least one magazine in the I/E station must be empty. Partitions that do not contain an I/E station cannot be defragmented and will be skipped.

Caution: Depending on the size of the library, defragmenting partitions can be a time-consuming process.

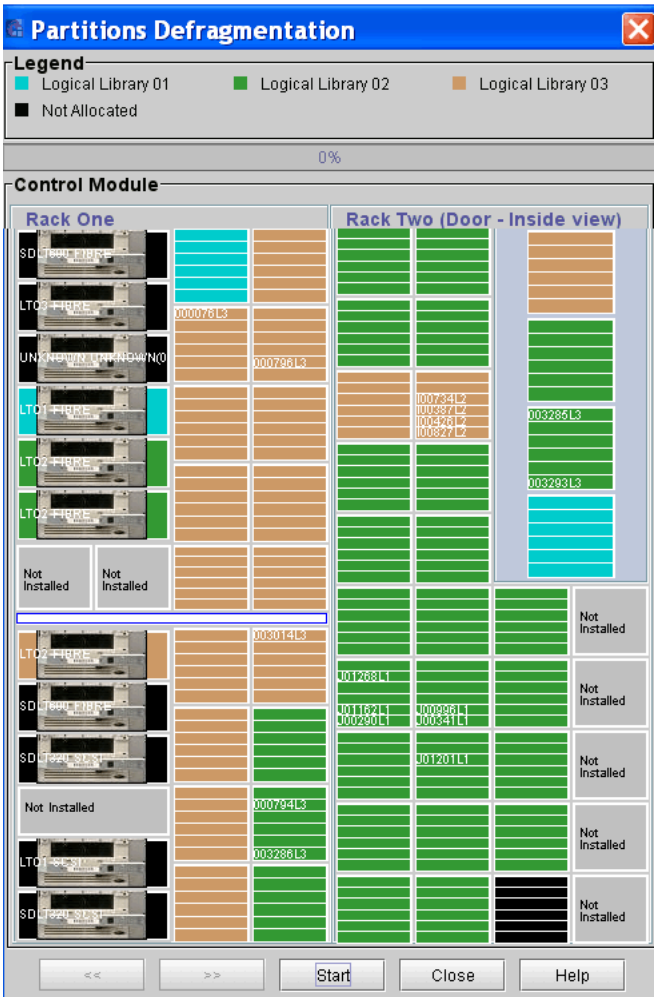
Defragmenting Partitions

After enlarging a partition or adding an expansion module to the library, check for partition fragmentation, and then defragment partitions if necessary.

1. Log on as an administrator.
2. Make sure that you are viewing the physical library. From the **View** menu, click the name of the physical library.
3. Click **Tools > Partitions Defragmentation**. The **Partitions Defragmentation** dialog box appears. This dialog box shows a graphical representation of the tape magazines in the library.

Magazines are color-coded indicating to which partition they belong.

If the library has more than one frame, click the arrow buttons to display the next or previous frame. If one or more partitions are fragmented, you can defragment them.



4 To begin defragmenting partitions, click **Start**. A dialog box appears notifying you that partitions that do not have a free I/E station slot cannot be defragmented and will be skipped.

5 Verify that the I/E station in each partition has at least one free slot, and then click **Yes**. A dialog box appears notifying you that all partitions must be taken offline before defragmenting can begin.

6 Click **Yes** to take all partitions offline.

The partitions defragmentation operation starts. A progress bar at the top of the **Partitions Defragmentation** dialog box displays the percentage complete for the operation.

When defragmenting is complete, a dialog box appears prompting you to take all partitions online.

7 Click **Yes** to take all partitions online.

8 Click **Close** to close the **Partitions Defragmentation** dialog box.

Canceling Defragmentation

Depending on the size of the library, defragmenting partitions can be a time-consuming process. If needed, you can click **Abort** on the **Partitions Defragmentation** dialog box to cancel the defragmentation operation at any time. When prompted, click **Yes** to confirm the action.

After you cancel defragmentation, the library finishes moving the current magazine (and any media it contains), then defragmentation stops. If you cancel defragmentation, no tapes will be stranded, and all media will still be assigned to the correct partition. You can resume defragmentation at a later time by clicking **Start** on the **Partitions Defragmentation** dialog box.

Recovering After Defragmentation is Interrupted

If a defragmentation operation fails (for example, if a power interruption occurs or the robotics go offline), no tapes will be stranded, and all media will still be assigned to the correct partition. However, it is possible that some media which was in the process of being moved will remain in the I/E station.

In this case, simply import the media into the library. The media will automatically be moved to a magazine in the correct partition. For more information about importing media, see Importing Cartridges Into Partitions on page 683.

Cycling Library Power

If library firmware seems to be at fault, or the robot will not move, or a circuit board has gone down, try recycling power to the library. Cycling library power involves shutting down the library, powering it off, and then powering it on. For more information, see Shutting Down/ Rebooting the Library on page 475, Powering Off the Library on page 477, and Powering On the Library on page 477.

Caution: Do not cycle library power for a drive problem. Use Tools > Drives to power cycle the individual drive.

Removing Lodged Cartridges

It is very unlikely that a cartridge will become lodged in the robot. If this happens, contact technical support. It also is very unlikely that a cartridge will become lodged in a drive. If this happens, it is not difficult to remove it.

Removing a Cartridge From a Drive

Required tools: None

1. On the operator panel, press the **Robotics Enabled** button to turn off power to the picker and return it to the home position. The power is on to all other components.
2. Open the access door. Aisle power is disabled.
3. On the drive, press the **Eject** button, and then remove the cartridge.
4. Close the access door. The power is on.
5. On the operator panel, press the **Robotics Enabled** button to enable the picker.

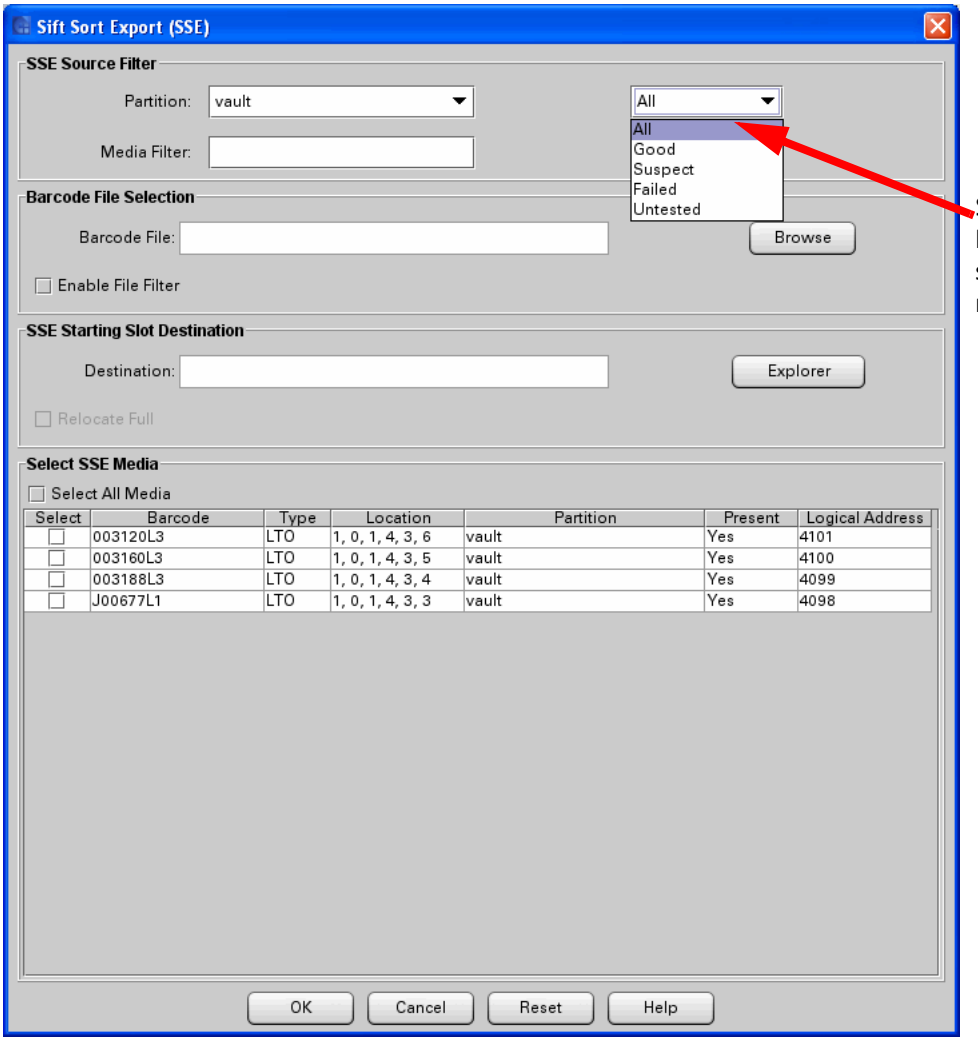
Using Sift Sort

The Sift/Sort/Export functionality is to facilitate bulk movement of cartridges from their standard slot locations to either specific storage area within the library or the I/E station (the default setting will be the left upper storage area within the library).

The default mode of operation is to relocate cartridges in sort order within the library, based on slot number or other logical grouping. This sort function helps you to quickly locate like-cartridge ID's, view all daily/weekly/monthly tapes easily (if a barcode nomenclature is implemented)

Exporting Media via Sift/Sort

1. Log on as an administrator.
2. From the **Tools** menu, select **Sift Sort > Export**. The **Sift Sort Export** dialog box appears.



Sort by EDLM scan test result

You may choose to filter by partition or by barcode.

3 To filter by partition, in the **SSE Source Filter** area, do the following:

a Select a **Partition** from the drop down list.

b If EDLM is licensed on the library, you can filter media in the EDLM library managed partition and partitions with EDLM policies configured according to their media scan test result.

From the drop-down list to the right of the **Partition** drop-down list, select All, Good, Suspect, Bad, or Untested.

c To use an additional filter, in the **Media Filter** field, type the search string and click **Filter**.

For example, to filter all media containing the character 8, type *8*.This field is case sensitive.

The appropriate media appears in the **Select SSE Media** section below.

4 Optionally, in the **Barcode File Selection** section, you can filter using a file using a "user-supplied" file (that lists barcodes).

a Click **Browse** to locate the appropriate file.

b Clicking **Enable File Filter** tells the interface to filter out barcodes contained in that file.

If the barcodes in that file do not belong to the particular partition selected, those barcodes are highlighted in red in the **Select SSE Media** section and are not selectable.

5 Once you have selected media to sift sort, in the **SSE Starting Slot Destination** area, click **Explorer** to select a coordinate location graphically by clicking on a cell.

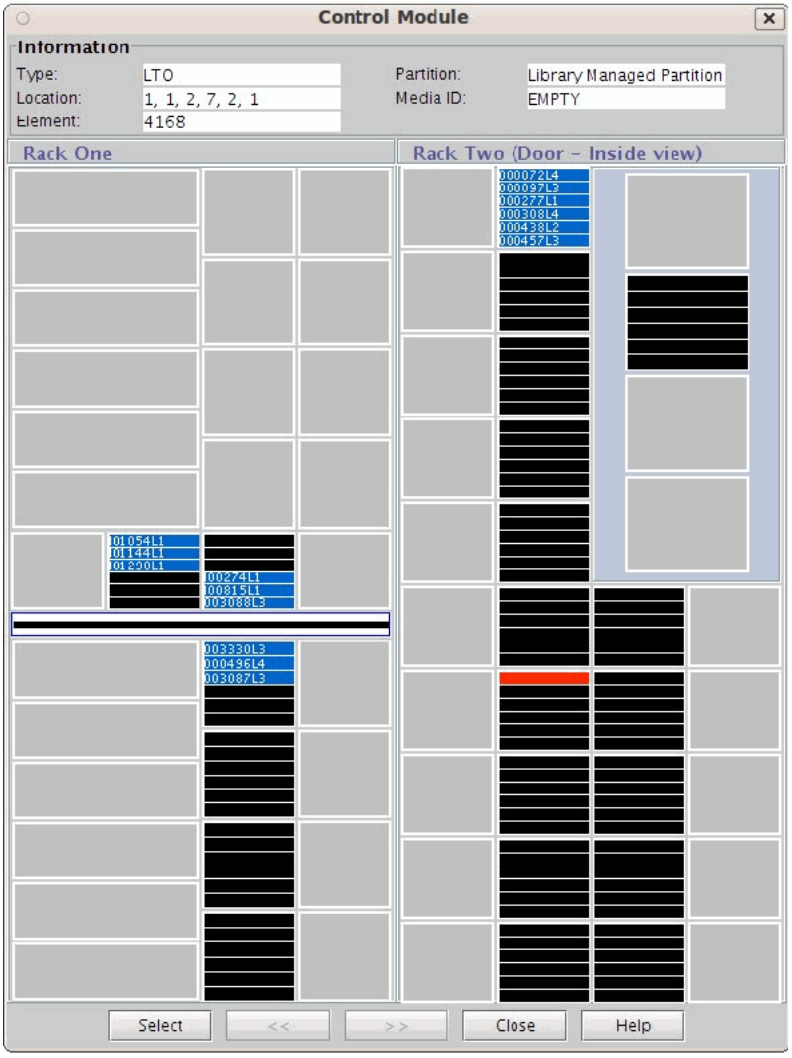
6 To relocate a cartridge to the last empty slot of the destination element selected, ensure **Relocate Full** check box is checked.

Note: The **Relocate Full** box is checked as the default condition.

When **Relocate Full** is checked, any tapes in the destination area will be moved to the lowest available element address location in the partition.

When **Relocate Full** is not checked, tapes that exist in the destination area will not be moved (skipped).

7 Click **OK**. The **Control Module** screen appears.



Based on the selections you made on the **Sift Sort Export** screen, the **Control Module** screen displays the available storage locations.

8 Click the desired storage location slot for the export function. The coordinates and details for that location appear in the **Information** area of the screen.

9 Click **Select**. The **Sift Sort Export** screen appears.

Capturing Sift Sort Screen Shot

Use the **Capture Sift Sort** screen to capture a picture of the last sift sort export you performed. The picture can be saved to a file on your local work station or e-mailed to a recipient.

1. Log on as an administrator.
2. From the **Tools** menu, select **Sift Sort > Capture Report**. The **Capture Sift Sort** screen appears.
3. On the top of the screen, click the circle next to the type of capture you want to perform - BMP, GIF, PNG, or JPEG.
4. Click **Capture**. The **Capture Sift Sort Export** screen appears.
5. Send the capture via email or save it on your computer.

   E-mail the capture

   a. Click the circle next to **Email.**
   b. Either type the email address or select one from the drop down list. The **Comment** section is enabled for entry.
   c. In the **Comment** section, you can include a note to the recipient, or any comments about the capture.

   Save the capture

   a. Click **Save**, and then click **Browse** to locate the location where you want to save the capture on your computer.

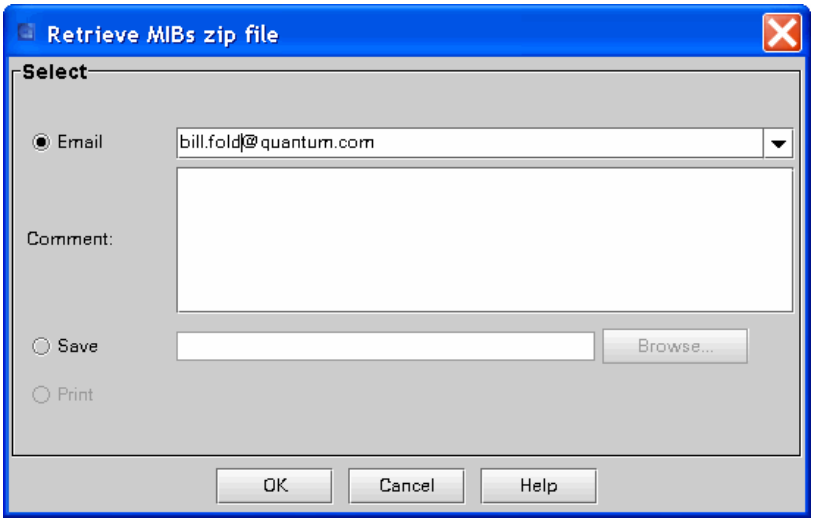
Retrieving MIBs

The Tools menu's Retrieve MIBs option allows you to retrieve the Scalar i6000 MIB files, which can be compiled into your SNMP Management tools. After retrieving the MIB files, you can extract the contents and then use a third-party SNMP tool such as Landesk or HP Operations Manager.

Emailing or Saving an MIB File

1. Log on as an administrator.

2 From the **Tools** menu, select **Retrieve MIBs**. The **Retrieve MIBs zip file** dialog box appears.



3 Send the MIB file via email, or save it on your computer.

E-mail the MIB File

a Click the circle next to **Email**.

b Either type the email address or select one from the drop down list. The **Comment** section is enabled for entry.

c In the **Comment** section, you can include a note to the recipient, or any comments about the MIB file.

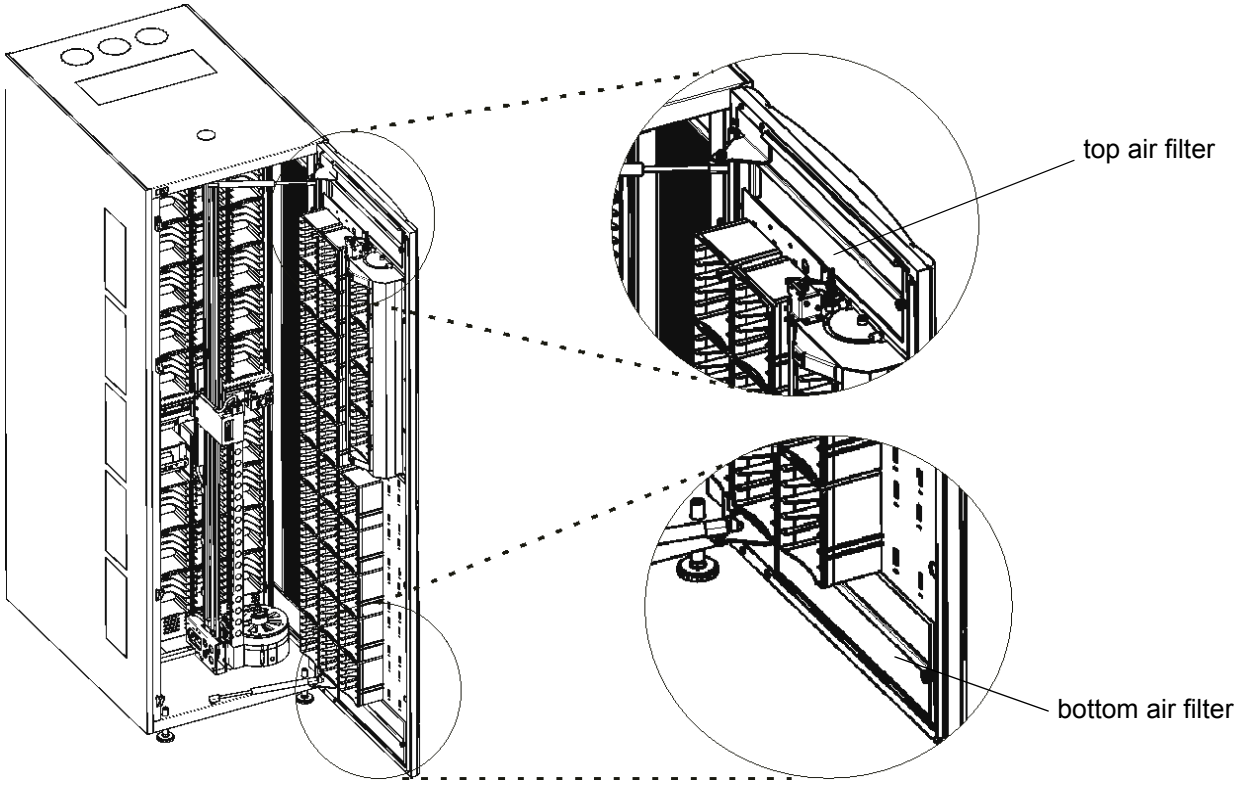
Save the MIB File

a Click **Save**, and then click **Browse** to navigate to the location where you want to save the MIB file on your computer.

Maintaining Air Filters

The access door of each control and expansion module has two air filters: one located at the top, and the other located at the bottom, as shown in Figure 70.

Figure 70 Top and Bottom Air Filters



Many factors exist that contribute to the need to regularly service the air filters. For example, the total number of tape drives and the operating environment greatly affect the rate at which debris accumulates in the air filters.

With the maximum number of tape drives operating in a normal data center environment, you should check the filters every two years. If you see dust and debris on the inlet side of the filters, remove the filters and use water and a mild soap to clean them. The materials in the filters should last for the life of the product. However, if abnormal contamination occurs, you should replace them. To order filters, contact your service representative.

Removing an Air Filter

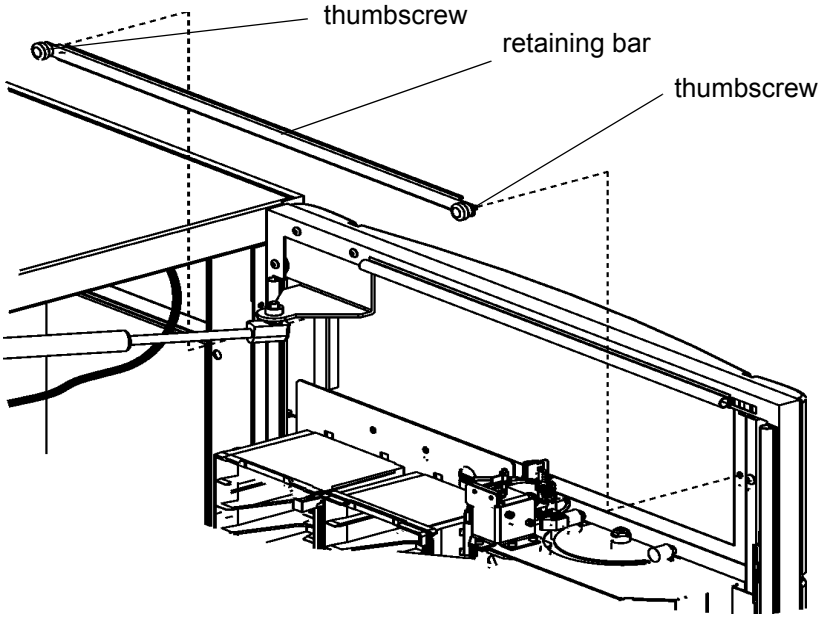
Use these instructions to remove either a top or bottom air filter.

Required tools: #1 Phillips screwdriver
FRU ID: 1001 (air filter)

1. Take the library offline.

   For information about taking the library offline, see Changing the Library's State on page 465.

2. On the operator panel, press **Robotics Enabled** to turn off power to the picker and return it to the home position. The power is on to all other components.
3. Open the access door. Aisle power is disabled.
4. Use the Phillips screwdriver to unscrew the two retaining thumbscrews. The screws remain attached to the retaining bar.



5. Remove the air filter.
6. Use water and a mild soap to clean the air filter.
7. Allow them to dry.

Replacing an Air Filter

Use these instructions to replace either a top or bottom air filter.

Note: Make sure that the air filter is completely dry before placing it back in the access door.

Required tools: #1 Phillips screwdriver
FRU ID: 1001 (air filter)

1 Take the library offline.

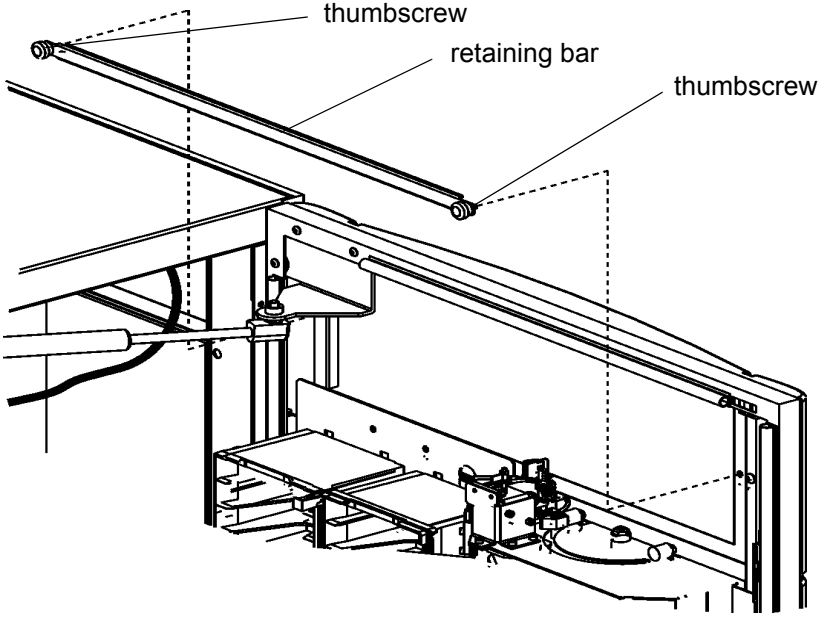
For information about taking the library offline, see Changing the Library's State on page 465.

2 On the operator panel, press **Robotics Enabled** to turn off power to the picker and return it to the home position. The power is on to all other components.

3 Open the access door. Aisle power is disabled.

4 Place the filter in the opening.

5 Place the retaining bar over the filter to hold it in place. Use the Phillips screwdriver to tighten the two retaining thumbscrews.



6 Close the access door.

7 On the operator panel, press **Robotics Enabled** to enable the picker.

8 Bring the library online. See Changing the Library's State on page 465.

Robot, Tower and Power Rail Health Checks

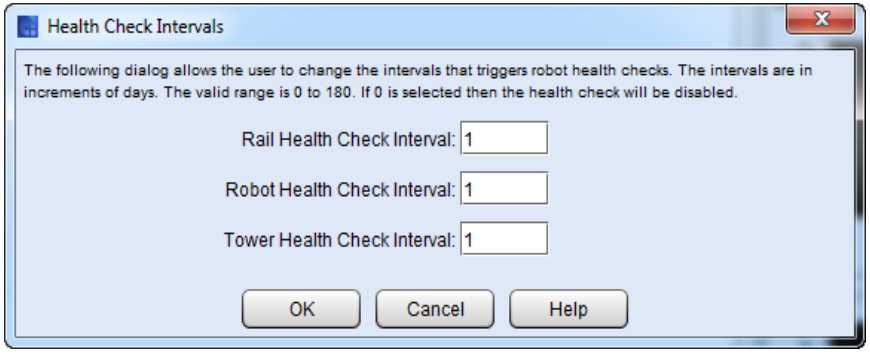
The library automatically performs health checks on the robot(s), towers and robot power rails. If problems are found, a RAS ticket is generated.

By default, the library performs each check once per day. You can change how often the library performs these checks. The interval can be set in increments of days, from once per day to once per year. You can also set it to never run. Quantum recommends a once-per-day health check for the robots, towers and power rails.

To change the health check interval:

1 Select **Setup > System Settings > Health Check Intervals**.

2 The **Health Check Intervals** screen appears. The intervals for rails, robot, and towers (if applicable) are displayed.



3 Change any of the intervals by typing in a new value in the field. The check is performed every time the interval has elapsed. If you type zero, the health check will never be performed.

Note: The intervals are in increments of days. Accepted values are form 0 (health check never performed) to 180.

Chapter 16
Working With Cartridges and Barcodes

The Library Management Console (LMC) simplifies cartridge loading and unloading, importing and exporting, and moving and inventory operations. The maximum library can be configured to accommodate from 100 LTO cartridges to 7,146 LTO cartridges (for a single-robot library) or 7,224 LTO cartridges (for a dual-robot library). For libraries containing high-density expansion modules, the maximum capacities are 12,006 LTO cartridges (for a single-robot library) or 11,760 LTO cartridges (for dual-robot libraries) for the following drive types:

Note: A library with Gen 2 hardware does not support DLT tape drives and media.

- SCSI or Fibre LTO-1
- SCSI or Fibre LTO-2
- Fibre LTO-3
- Fibre LTO-4
- Fibre LTO-5
- Fibre LTO-6

Every partition in the library must contain at least one cleaning cartridge.

This chapter consists of the following sections:

Handling Cartridges Properly

To ensure the longest possible life for your cartridges, follow these guidelines:

- Select a visible location to post procedures that describe proper media handling.
- Ensure that anyone who handles cartridges has been properly trained in all procedures.
- Do not drop or strike cartridges. Excessive shock could damage the internal contents of cartridges or the casings themselves, rendering the cartridges unusable.
- Do not expose cartridges to direct sunlight or sources of heat, including portable heaters and heating ducts.
- Do not stack cartridges more than five high.
- The operating temperature range for LTO cartridges is 10º to 35ºC. The storage temperature range is 16º to 32ºC in a dust-free environment with a relative humidity range between 20% and 80% (non-condensing).
- If cartridges have been exposed to temperatures outside the ranges specified above, stabilize the cartridges at room temperature for the same amount of time they were exposed to extreme temperatures or 24 hours, whichever is less.
- Do not place cartridges near sources of electromagnetic energy or strong magnetic fields, such as computer monitors, electric motors, speakers, or x-ray equipment. Exposure to electromagnetic energy

or magnetic fields can destroy data and the embedded servo code written on the media by the cartridge manufacturer, rendering the cartridges unusable.

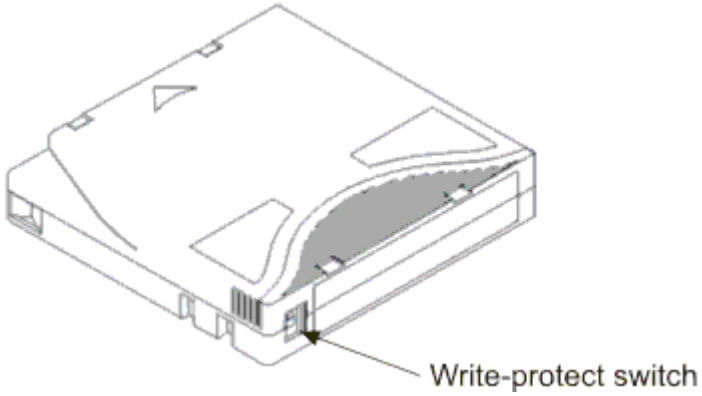
- Place identification labels only in the designated slots on the cartridges.
- If you ship cartridges, ship them in their original packaging or something stronger.
- Do not insert damaged cartridges into drives.
- Do not touch the tape or tape leader.
- Do not degauss cartridges that you intend to reuse.

Write-Protecting Cartridges

All cartridges have a write-protect (write-inhibit) switch to prevent accidental erasure or overwriting of data. Before loading a cartridge into the library, make sure that the write-protect switch is positioned correctly (either on or off).

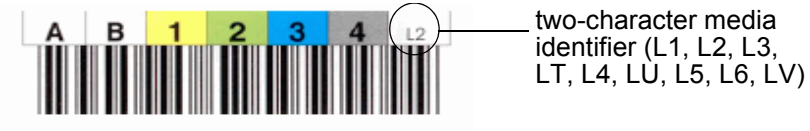
- For LTO cartridges, slide the red or orange write-protect switch to the right so that the padlock shows in the closed position. The switch is located on the left side of the cartridge front. See Figure 71 on page 678 for the location of the switch on an LTO cartridge.

Figure 71 Write-protect Switch on an LTO-1 Cartridge



Supported Barcode Formats

Quantum supplies industry standard LTO barcode labels with a length of 6 barcode characters + 2 media identifier characters. For advanced uses, your Quantum library supports tape cartridge barcode label lengths of up to 15 characters. However, refer to Barcode Label Requirements on page 679 for details as LTO barcode labels longer than 13 characters may not conform to the barcode label requirements when it is affixed to the LTO tape cartridge.



Barcode Label Requirements

Cartridges must have an external barcode label that is machine readable. Quantum-supplied barcode labels provide the best results. Barcode labels from other sources can be used, but they must meet the following requirements:

- ANSI MH10.8M-1983 Standard
- Font: Code 39 (3 of 9)
- Allowable characters: Uppercase letters A to Z and numeric values 0 to 9

  Note: Checksum characters are not supported on barcode labels.

- Number of characters: 5 to 15 (default for LTO is 6+2)
- Background reflection: Greater than 25 percent
- Print contrast: Greater than 75 percent
- Ratio: Greater than 2.2
- Module: Minimum 254 mm (10 mil)
- Print tolerance: ± 57 mm
- Length of the rest zones: 5.25 mm ± 0.25 mm
- No black marks may be present in the intermediate spaces or rest zones
- No white areas may be present on the bars

Installing Barcode Labels

Each cartridge in the library must have an external label that is operator and machine readable to identify the barcode number. Most manufacturers offer cartridges with the labels already applied or with the labels included that you can attach.

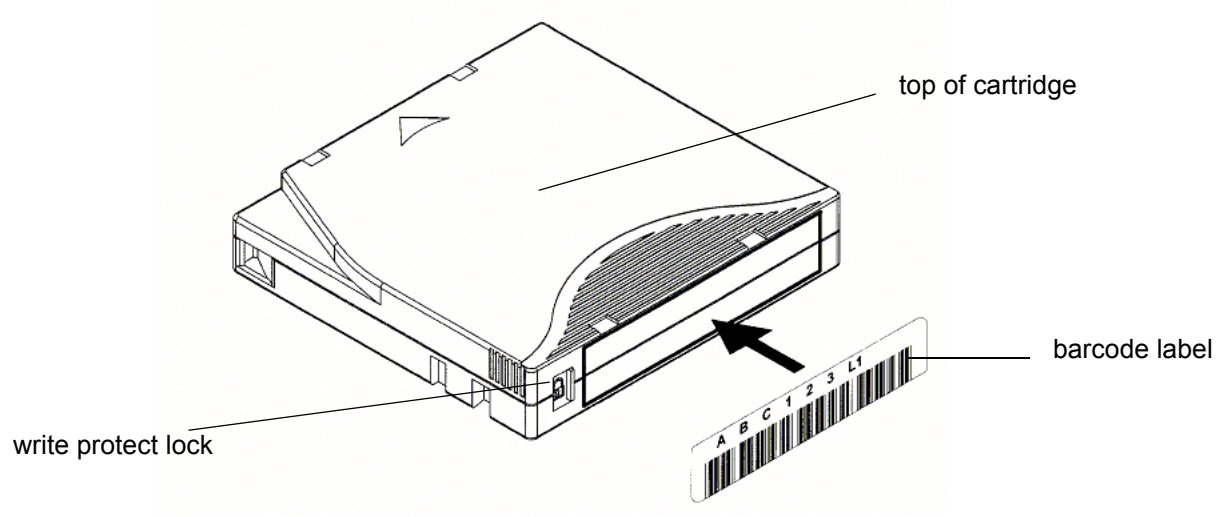
Note: Duplicate barcodes are not supported even if you have mixed media or multiple partitions in the library. If the library has cartridges with identical barcode labels, the library will issue a ticket notifying you of the problem. Areas in the LMC where media IDs are listed will show information for the first cartridge, but the cartridge with the duplicate barcode label will not be listed.

All barcode labels are applied to the front of a cartridge. Peel off the label and place it on the cartridge. Verify that label is oriented so that the numbers appear above the barcode. Figure 72 on page 681 shows an example of a barcode label being applied to an LTO cartridge.

Note: Barcode labels should be placed on the front of the tape with the barcode bars on the bottom and the human readable characters at the top.

Caution: Do not place any extra labels on the tapes other than on the front. Extra labels will cause tape handling issues, tapes getting stuck in drives and inventory operations to fail.

Figure 72 Applying Barcode Labels to Cartridges



Using Cleaning Cartridges

Most tape drives require occasional cleaning. A cleaning cartridge cleans accumulated debris from the tape drive and the read/write head.

Caution: You must use a separate cleaning cartridge for each partition in the library.

Backup applications or archive software applications use different techniques to automate the process of cleaning drives. These tools specify cleaning cycles based on cycle counts of the drive, drive requests, or regularly scheduled intervals.

The cleaning process itself requires certain considerations:

- Cleaning tapes must be labeled with a barcode. The preferred method of labeling a cleaning cartridge is to have **CLN** or **CLNU** as the prefix on the label. Any cartridge detected with a **CLN** or **CLNU** prefix will be considered a universal cleaning cartridge, regardless of any media identification extension. Cartridges containing a media identification of **C1**, **C2**, **C3**, **C4**, **C5, C6**, and **CU** will be considered cleaning cartridges and will be tracked and treated as a universal cleaning cartridge.
- Insert a cleaning tape just as you do any other data tape. For example, the most common method is by means of the I/E station using host application control.
- Cleaning tapes often have limited lives that can last only as long as 20 cycles. The controlling host application manages the number of uses of a cleaning tape. Errors can occur if a tape is inserted into a drive when the tape has already been used the maximum number of times.
- Export a cleaning tape just as you would export any other data tape.
- The concepts of physical and partitions must be considered when setting up cleaning procedures and methods. In general, cleaning cartridges must be treated in the same manner as data cartridges. Any physical cartridge (cleaning or data) can exist in only one partition. There can be no sharing of cleaning cartridges between partitions.

Managing and Moving Media

The LMC provides you with commands for:

- Importing Cartridges Into Partitions on page 683
- Exporting Cartridges From Partitions on page 685
- Loading Drives on page 686
- Unloading Drives on page 688
- Moving Media Within a Partition on page 689
- Moving Media Between Active Vault or AMP and Standard Partitions on page 690
- Taking Inventory on page 692

The following sections provide step-by-step instructions for performing these tasks.

Note: Unless the situation requires it, use the host application to move, load, unload, import, or export cartridges instead of doing so through the LMC. Using the host to move media makes sure that the host's view of the library remains in sync with the library's actual configuration.

Exception: When moving media into and out of library managed partitions, you must use the LMC since library managed partitions are not visible to hosts (see Moving Media Between Active Vault or AMP and Standard Partitions on page 690).

Importing Cartridges Into Partitions

When you first start using your library, open the door and manually insert, directly into storage slots, as many cartridges as you plan to use. The cartridges will not go back all the way if they are inserted incorrectly.

After your library begins operation, use the **Import Media** dialog box to add cartridges without interrupting library operations. Place cartridges in the I/E station. The scanner automatically reads the barcodes on new cartridges.

1 Make sure that you are viewing the partition into which you want to import a data cartridge. From the **View** menu, click the name of the appropriate partition.

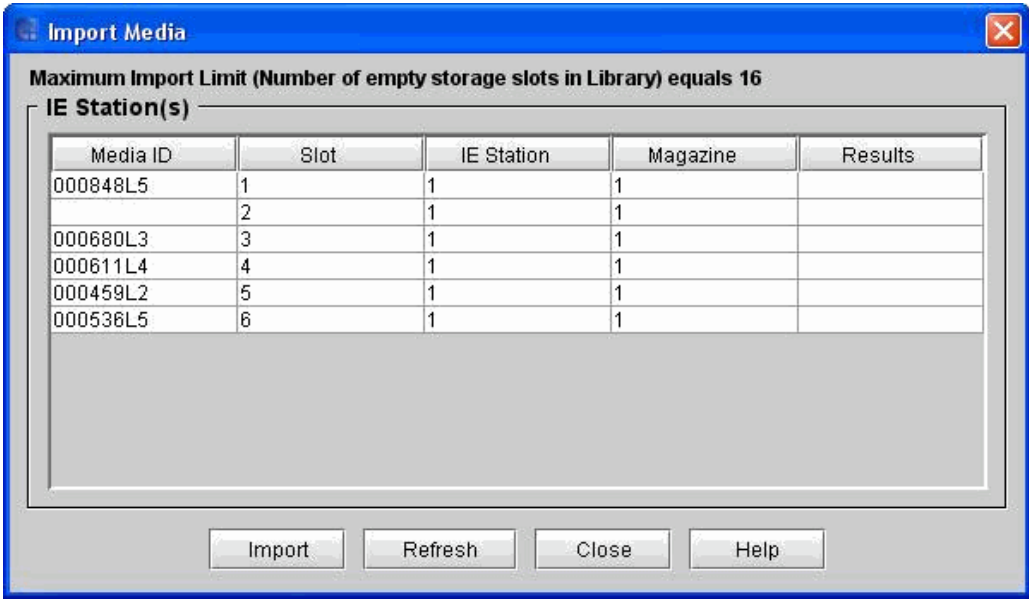
2 Insert a data cartridge into an appropriate I/E station. You can insert multiple cartridges up to the maximum number of slots in your I/E station.

3 To see which I/E stations are associated with a particular partition, click **Monitor** > **IE Station**.

4 Click **Operations** > **Import** or click the **Import** toolbar button.

If the partition is not offline, you receive a message that asks you whether you want to take it offline.

5 Click **Yes**. The **Import Media** dialog box appears with a list of cartridges in the I/E station displayed.



The following table describes the elements on the **Import Media** dialog box.

Element	Description
Media ID	The volume serial number of the cartridge.

Element	Description
Slot	The number of the slot in the I/E station magazine. To understand the location designation, see Understanding Location Coordinates on page 449.
IE Station	The number of the module. To understand the location designation, see Understanding Location Coordinates on page 449.
Magazine	The number of the magazine (section) where the slot is located, numbered from the top down. To understand the location designation, see Understanding Location Coordinates on page 449.
Results	"Imported" or "Failed".

6 Click a cartridge to highlight it, and then click **Import**.

The picker automatically moves the cartridge from the I/E station to the first available empty slot in that partition. You cannot manually specify the slot.

Exporting Cartridges From Partitions

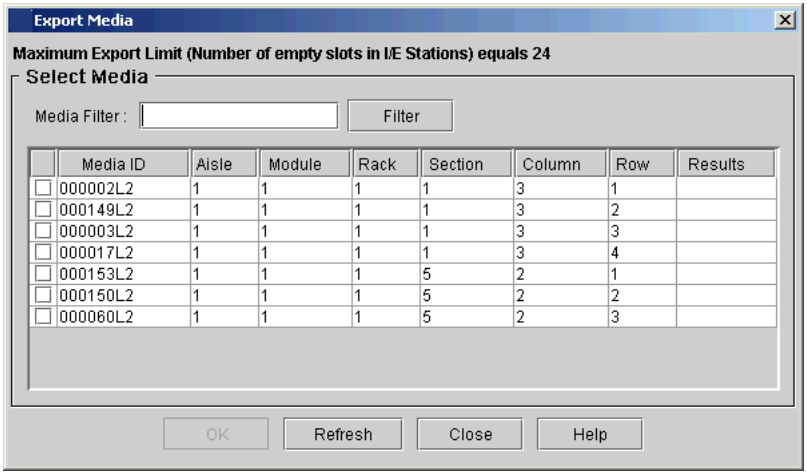
When partitions are created, specific I/E station slots are associated with that partition. When you export cartridges in a library with partitions, cartridges are exported to the partition's I/E station slots. You can only export cartridges if I/E station slots for that partition are empty.

1 Make sure that you are viewing the partition from which you want to export a data cartridge. From the **View** menu, click the name of the appropriate partition.

Click **Operations > Export** or click the **Export** toolbar button. The **Export Media** dialog box appears with a list of cartridges in the partition displayed.

Note: The physical library must be online.

If the partition is not offline, you receive a message that asks you whether you want to take it offline. Click Yes.



2 If you want to display one or more media IDs that match a particular pattern, type a media filter in the **Media Filter** text box, and then click **Filter**.

   Filter performs a search for media IDs that match a particular pattern. In the example, the media filter has been set to capture media IDs beginning with the string "J00."

3 Select the corresponding check box in the leftmost column for each cartridge that you want to export.

   The maximum number of slots that are available in the I/E station partition appears at the top of the table.

4 Click **OK**.

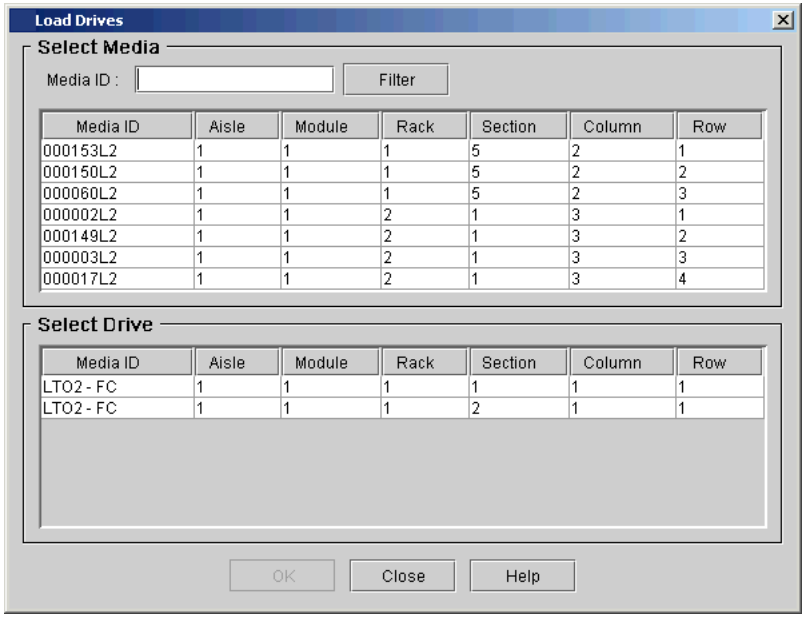
   All designated cartridges are exported to the I/E station slots that are associated with the partition. After the operation completes, the library automatically refreshes information in the table.

Loading Drives

The **Load Drives** dialog box enables you to load drives with cartridges from the current partition.

1 Make sure that you are viewing the partition from which you want to load drives. From the **View** menu, click the name of the appropriate partition.

2 Click **Operations** > **Drives** > **Load**. The **Load Drives** dialog box appears.



3 If you want to display one or more media IDs that match a particular pattern, type a media filter in the **Media ID** text box, and then click **Filter**.

Filter performs a search for media IDs that match a particular pattern. In the example, the media filter has been set to capture media IDs beginning with the string "J00."

4 Click the data cartridge to load into the drive to highlight it.

Note: You can load only one cartridge at a time.

The parameters used to define a cartridge are media ID (barcode) and location. Location is defined as a series of coordinates representing the aisle, module, rack, section, column, and row where a cartridge is located. See Understanding Location Coordinates on page 449.

The **Select Media** area shows the full slots.

5 Click the destination drive to receive the media to highlight it. The **Select Drive** area is populated with empty drives. You can select only one drive at a time.

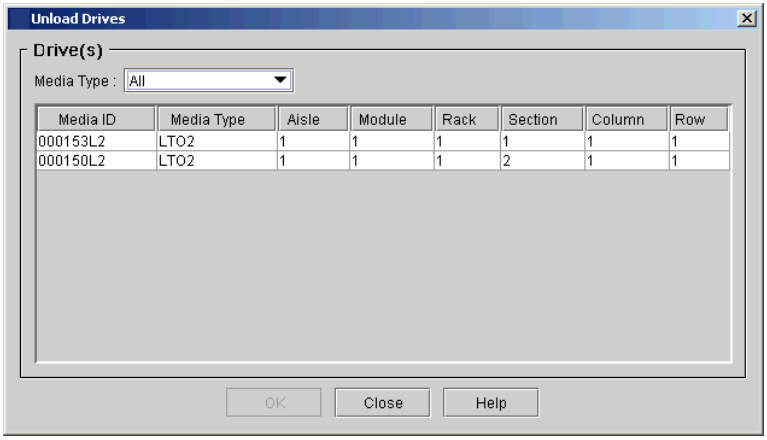
6 To load the data cartridge into the selected drive, click **OK**.

Unloading Drives

The **Unload Drives** dialog box enables you to rewind the cartridge in the drive, eject it, and return it to storage.

1 Make sure that you are viewing the partition from which you want to unload drives. From the **View** menu, click the name of the appropriate partition.

2 Click **Operations** > **Drives** > **Unload**. The **Unload Drives** dialog box appears.



3 If you want to display media IDs by media type, click the appropriate media type from the **Media Type** drop-down list.

4 Click the drive you want to unload to highlight it. You can only unload one drive at a time.

The parameters used to define a cartridge are media ID (volume serial number) and location. Location is defined as a series of coordinates representing the aisle, module, rack, section, column, and row where a cartridge is located. SeeUnderstanding Location Coordinates on page 449.

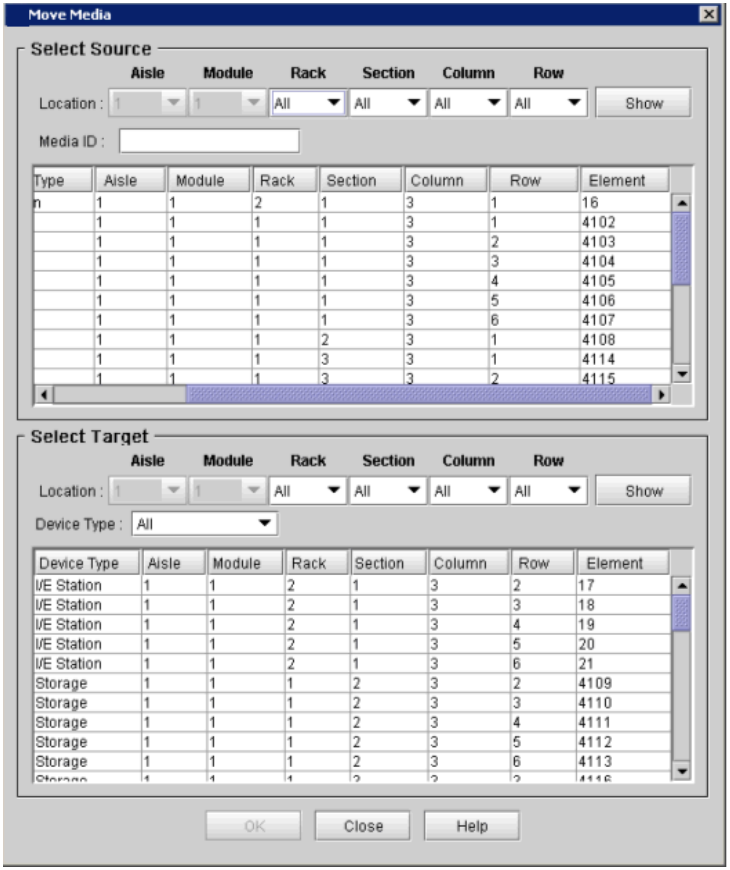
5 Click **OK**. The library rewinds the data cartridge, unloads it from the drive, and returns it to storage.

Moving Media Within a Partition

The **Move Media** dialog box enables you to move media from one location to another within a partition.

Note: Only one cartridge can be moved at a time.

1. Make sure that you are viewing the partition within which you want to move media. From the **View** menu, click the name of the appropriate partition.
2. Click **Operations** > **Move Media**. The **Move Media** dialog box appears.



The table in the **Select Source** area lists slot locations with cartridges, and the table in the **Select Target** area lists slot locations without cartridges.

You can limit the cartridges that are listed in the **Select Source** table in the following ways:

- To list cartridges by location, click the arrows next to the location coordinate boxes at the top of the **Select Source** area, click the appropriate numbers or **All**, and then click **Show**. For information about location coordinates, see Understanding Location Coordinates on page 449.
- To list a particular cartridge by media ID, type the volume serial number of the cartridge in the **Media ID** text box, and then click **Show**. You also can type a partial volume serial number, such as "K00", to list all cartridges within the specified location coordinates that have a volume serial number containing the specified string of characters.
- You also can limit the slot locations that are listed in the **Select Target** table by device type. From the **Device Type** drop-down list, click **I/E Station**, **Storage**, or **Drive**.

3 In the **Select Source** table, click the media ID for the cartridge that you want to move to highlight it. If necessary, you can use the scroll bar to display additional media IDs for cartridges that are in drives or I/E stations.

4 In the **Select Target** table, click the destination for the cartridge that you want to move to highlight it. If necessary, you can use the scroll bar to display additional slot locations.

5 Click **OK**. The media moves to the new location.

Moving Media Between Active Vault or AMP and Standard Partitions

The library does not allow you to move media directly between one standard partition and another standard partition. However, you are allowed to move media directly from a standard partition to a library managed partition, and vice versa. Library managed partitions include Active Vault, Automated Media Pool (AMP), and Extended Data Lifecycle Management (EDLM) partitions.

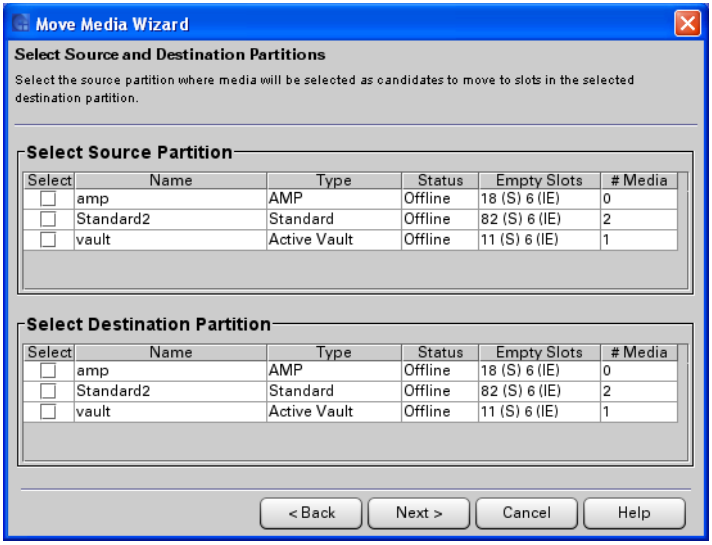
Note: Manual movement between library managed partitions and standard partitions will require inventory reconciliation with the backup application managing the standard partition.

Note: Moving media between a standard partition and a library managed partition will take the standard partition offline during the operation.

1 Make sure that you are viewing the physical library. From the **View** menu, click the name of the physical library.

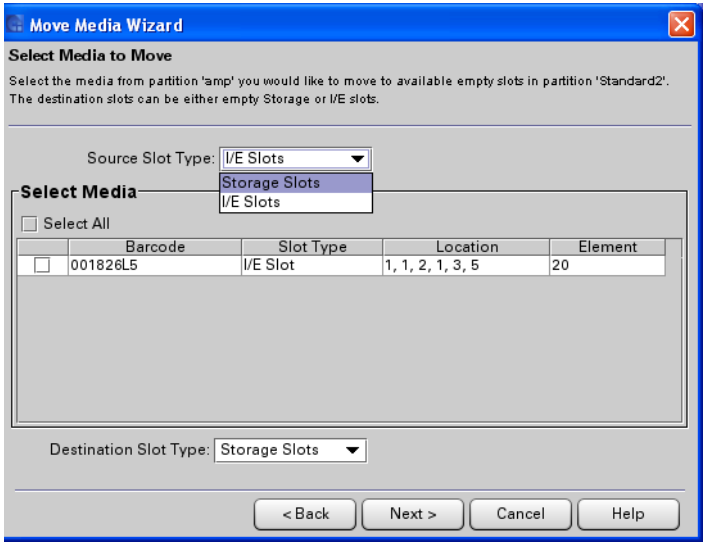
2 Click **Operations > Move Media**. The **Move Media Wizard** appears.

3 Click **Next**. The **Select Source and Destination Partitions** screen appears.



4 Select a source partition from the **Select Source Partition** section and select a destination partition from the **Select Destination Partition**. You cannot move media between library managed partitions or between standard partitions.

5 Click **Next**. The **Select Media to Move** screen appears.



6 From the **Source Slot Type** drop-down list, select the area from which you want to move the media (Storage Slots or I/E Slots).

7 From the **Select Media** list, select the tape(s) you want to move.

8 From the **Destination Slot Type** drop-down list, select the area to which you want to move the media (Storage Slots or I/E Slots).

9 Click **Next**. The **Media Move Completion Page** appears, listing source location, destination location, and which media will be moved.

10 Click **Finish**.

11 Click **Close**.

Taking Inventory

The **Inventory** command causes the library to scan all storage locations, drives, and I/E stations. The library automatically performs an inventory when doors are closed or the library's configuration information is changed in any way. You can configure inventories to automatically occur whenever the power is cycled, or you can perform an inventory whenever you want by clicking **Operations® Inventory**. To enable automatic inventories, see Setting Up Policies for the Physical Library on page 170.

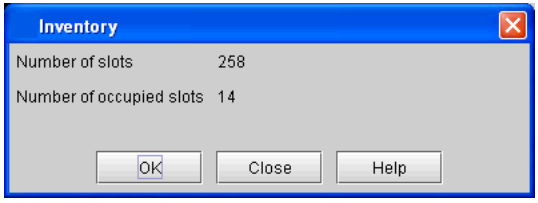
1 Log on as an administrator.

2 You can perform this procedure while either viewing the physical library or a partition. From the **View** menu, click the name of the physical library or the appropriate partition.

Click **Operations** > **Inventory**. The **Inventory** dialog box appears.

Note: If you want to perform an inventory of the physical library, and it is not offline, you receive a message that asks you whether you want to take it offline. Click **Yes**.

If you want to perform an inventory of a partition, and if the physical library is offline, you receive a message asks you whether you want to take the physical library online. Click Yes. Also, if the partition is online, you receive a message that asks you whether you want to take it offline. Click **Yes**.



This dialog box shows the total number of slots and the number of occupied slots in the physical library or the partition, depending on the view you chose.

3 To perform an inventory, click **OK**.

The inventory process take a few minutes to complete.

4 When the "Inventory completed successfully" message appears, click **OK**.

Appendix A
Frequently Asked Questions

This appendix answers some questions that are most often asked about the library.

Where do I find installation instructions?

The library requires that a trained Quantum Support Engineer perform the installation.

Where are error messages described?

When the library detects issues, it sends you e-mail notifications and creates tickets that provide you with detailed information about the issues and corrective actions you can perform. A ticket can direct you to obtain further help from technical support. For more information about troubleshooting, see Troubleshooting Your Library on page 35.

How do I clean a drive?

You can set up automatic drive cleaning when you manually create a partition (see Creating Partitions Manually on page 126) or you can manually clean drives at your discretion (see Configuring Drive Cleaning on page 217).

How do I know when the drives need cleaning?

If you do not have periodic drive cleaning configured (see Creating Partitions Manually on page 126) for your drives, a diagnostic ticket is generated when a drive needs to be cleaned.

What is a partition?

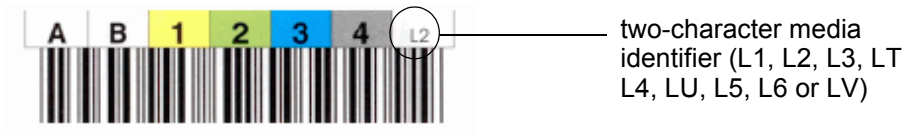
A partition is an abstraction of a single underlying physical library that presents the appearance of multiple, separate libraries for purposes of file management, access by multiple users, or dedication to one or more host applications. It is a collection of real physical elements, combined to create a grouping that is different from the physical library, and is often dedicated to a single host application. For example, you can choose to run one software application in one partition, and a different software application in a second partition. For a more information, see Working With Partitions on page 118. To learn how to create a partition, see Creating Partitions on page 124.

Where can I find the library's serial number?

The serial number appears in the **ID** column for the first line of output on the **System Status** dialog box (**Monitor® System**). Use the serial number when contacting technical support for assistance.

How many characters can be in the barcodes?

For LTO media barcodes, the library dynamically supports 1 to 14 characters for volume serial number plus a two-character media type identifier. The image below is an example of a supported LTO barcode label.



What barcode formats are supported?

Cartridges must have an external barcode label that is machine-readable to identify the volume serial number. A barcode must use only uppercase letters A to Z and/or numeric values 0 to 9. The library currently supports Code 39 (3 of 9) type barcode labels.

What do I do if I lose my password?

Contact technical support and they will tell you how to reset the password. See Getting More Information or Help on page xiii.

What do I do if I lose power during a backup?

If your library contains a redundant power supply, it is unlikely that power will ever be completely unavailable to the library.

The library should recover even if power goes out completely during a backup. If power remains off, press the **Power** button and leave it in the off position until you can obtain a reliable power source. When the power to the library is turned back on, the library will recover. You must re-run the backup using your application software.

If the library does not automatically come back up after a power outage, cycle library power. Cycling library power involves shutting down the library, powering it off, and then powering it on. For more information, see Shutting Down/Rebooting the Library on page 475, Powering Off the Library on page 477, and Powering On the Library on page 477. The blue LED on the power supply will be on and not blinking.

Appendix B
Network Port Settings

Table 1 describes the port and network details for customer site-to-site firewall settings.

Table 51 Network Port Settings

Port	Protocol	Description	Direction	TCP/UDP
22	SSH	SSH Access for CLI usage.	Inbound	TCP
25	SMTP	eMail Client	Outbound	TCP
53	DNS	DNS Client Model	Outbound	UDP+TCP
67-68	DHCP	DHCP Client	Outbound	UDP
80	HTTP	Library is a webserver for administration purposes	Inbound	TCP
80	HTTP	Library is a client for SKMv1	Outbound	TCP
123	NTP	NTP Client	Inbound/ Outbound	UDP
161	SNMP	SNMP queries and management	Inbound/ Outbound	UDP
162	SNMP	Trap output	Outbound	UDP

Port	Protocol	Description	Direction	TCP/UDP
389	LDAP	Non-secure LDAP client	Outbound	TCP
427	SLP	Service Locator Protocol	Inbound/ Outbound	UDP+TCP
443	HTTP	Secure Webserver	Inbound	TCP
443*	QEKM	Secure connections for QEKM encryption protocol. IBM Drives only	Outbound	TCP
443*	RKM	RSA key manager communications	Outbound	TCP
636	LDAPS	Secure LDAP Client	Outbound	TCP
1009-1108*	RMI	Java GUI RMI Connections, this is a bidirectional interface	Inbound/ Outbound	TCP
3801*	QEKM	Non secure connections for QEKM encryption protocol. IBM Tape drives only	Outbound	TCP
5696*	KMIP	KMIP Communication port on the server. Library uses non priviledged ports	Outbound	TCP
5988	SMIA	SMIS/OpenWBEM	Inbound	TCP
5989	SSMIS	Secure SMIS/OpenWBEM	Inbound	TCP
6000, 6001	SKM	SKM tape encryption protocol	Outbound	TCP
* user configurable. The default value is shown				

Glossary

This glossary consists of terms unique to the library along with some storage industry terminology.

A

Access door
Refers to the doors on either the control module or expansion module from which you can access the magazines and accessor assembly.

C

Capacity on demand (COD)
An Quantum library feature that enables users to have a large physical library, but users pay only for what capacity they are currently using. License upgrades enable more capacity to be added without a system interruption.

Control management blade (CMB)
A version of the MCB that has no I/O ports for Ethernet, SCSI, serial, or Fibre Channel. It is the controller board for the I/O management unit in expansion modules.

Control module
The first component of the library. It consists of an library management module, cartridges, drives, power, and an I/E station.

Control Path Failover (CPF)
The Scalar i6000 provides support for configuring the HP LTO-5 and LTO-6 drive for control path failover. To configure a control path failover drive, you must have a Storage Networking License (SNW).

When control path failover is used, one drive is assigned as the primary control path and another drive as the control path failover (secondary) drive. The control path failover drive is used whenever the primary control path drive fails or is inoperable.

D

Data path
One of the many possible paths that data can move over in the storage area network environment, potentially involving many components or connections between initiators and targets that have been set since the initial configuration occurred.

Data path failover

You can use Data Path Failover to allow an alternate data path when a preferred data path fails. Data Path Failover is provided as part of the Storage Networking license and applies to HP LTO-5 and LTO-6 Fibre Channel tape drives only.

The HP LTO-5 and LTO-6 Fibre Channel tape drives have two Fibre Channel ports. If you enable Data Path Failover on the tape drive, one port will be used as the “active port” for data transmission, and the other port will stand by to be used if the active port fails. If the tape drive loses its Fibre Channel link with the active port,

it will automatically “fail over” and use the standby port to continue drive operations.

DN
Distinguished Name

Drive pooling
Drives to be held in a pool (or pools) of drives. You can specify policy settings for the drive pools to configure how each pool will react to a drive failure and load balancing.

Drive sled position
A slot where a Fibre Channel or SCSI drives reside in the control module or expansion module in one of the two drive clusters.

There are six drive sled positions in each of the two drive clusters.

E

Encryption Key Management (EKM)
A generic term used to encompass any encryption key management solution.

Ethernet Expansion blade (EEB)
Provides Ethernet connectivity to 6 Ethernet drives. This connectivity is to the library's internal Ethernet and should not be connected to an external Ethernet source.

Expansion module
Expansion modules enlarge the library configuration by adding modules for additional media storage. You can add up eleven expansion modules to a library configuration. The first seven expansion modules may contain optional hardware, such as additional drives, I/O blades, and I/E stations.

F

FQDN
Fully Qualified Distinguished Name

I

I/E station
A door on the access door of the control module (or expansion modules) that contains magazines into which cartridges can be imported into or exported out of the library.

All single door I/E stations are numbered starting with 1 at the control module. All double door I/E stations are numbered with a number and a letter--for example 2A and 2B--the module number (1-8), with A as the left I/E station and B the right.

I/O management unit
A management and connectivity interface for the library. The control module and first seven expansion modules can have I/O management units installed. The I/O management unit may contain a CMB, FC
I/O blades and Ethernet Expansion blades.

L

Latchhook
The latches used to lock the printed circuit blades into place when they are inserted into the I/O management unit or library management module (LMM).

Library Management Console (LMC)
The management software client for the library. You can use the LMC either locally from the touch screen operator panel on the control module or remotely through a Web browser running a Java applet.

Library management module (LMM)
The connectivity interface for the three blades that provide intelligence and connectivity to the library through the control module. The management control blade (MCB), robotics control unit (RCU), and library motor drive (LMD) blades are installed in the LMM.

Library managed partition (LMP)
Partition in the i6000 that is like any other partition, except it is not visible to any backup applications or hosts. Allows the library to be able to manage the partition, rather than the backup application managing the partition. Use the LMP partition as a workspace for library to do value-added features outside environment — like EDLM (automated data integrity checking routine).

Linear Tape-Open (LTO)
A media technology that is open format. LTO comes in two formats, Accelis and Ultrium. Accelis is the fast access implementation, while Ultrium is the high capacity implementation.

M

Management control blade (MCB)
The library controller board, which resides in the LMM. The MCB has
I/O ports for Fibre Channel, Ethernet, serial, and SCSI.

P

Partition
A partition is a logical portion of the physical library that is viewed by the host as if it is a complete library. Partitions

present the appearance of multiple, separate libraries for purposes of file management, access by multiple users, or dedication to one or more host applications.

Picker
The robotic hand portion of the accessor assembly that handles cartridges.

Q

Quantum Encryption Key Manager (Q-EKM)
Quantum's encryption key management solution that supports IBM LTO-4, LTO-5, and LTO-6 FC and SAS tape drives.

R

RDN
Relative Distinguished Name.

S

Scalar Key Manager (SKM)
Quantum's encryption key management solutions that supports HP LTO-4, LTO-5, and LTO-6 FC and SAS tape drives.

Service door
The door on either the control module or expansion module that provides access to the I/O management unit, LMM, power supplies, drive sleds and other components.

Storage area network (SAN)
A dedicated, high-performance network whose primary purpose is the transfer of data along FC or high-speed Ethernet connections between servers, interconnect devices, and storage peripherals.

Storage networking (SNW)
A licensable feature that allows you to take advantage of the control path failover and host access configuration features of 8 Gb/s HP LTO-5 or LTO-6 tape drives, without those drives being connected to a 4 Gb/s /Fibre Channel I/O blade.

U

Universal drive sled (UDS)
A sheet metal case that houses LTO or SCSI drives in the drive clusters.

W

WORM
The Scalar i6000 library supports write once, read many technology in LTO-3 and greater tape drives. WORM allows non-erasable date to be written once and provides extra data security by prohibiting accidental data erasure.

X

X-axis
The horizontal position of the accessor assembly.

Y

Y-axis
The vertical position of the accessor assembly.

Index

T

U

V

W