Quantum

User's Guide User's Guide User's Guide User's Guide

Quantum Scalar *i*6000 Library

Scalar *i*6000

6-66879-01 Rev A

Scalar i6000 User’s Guide, 6-66879-01, May 2010, Made in USA.

Quantum Corporation provides this publication “as is” without warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability or fitness for a particular purpose. Quantum Corporation may revise this publication from time to time without notice.

COPYRIGHT STATEMENT

TRADEMARK STATEMENT

Quantum, ADIC, DLT, DLTtape, the Quantum logo, and the DLTtape logo are all registered trademarks of Quantum Corporation.

SDLT and Super DLTtape are trademarks of Quantum Corporation.

Other trademarks may be mentioned herein which belong to other companies.

REGULATORY AGENCY DOCUMENTATION APPLICABILITY

Scalar i6000 Automated Tape Library documentation is applicable to Regulatory Model Scalar i2000 Control Module and Regulatory Model Scalar i2000 Expansion Module components and installations.

Contents

Tables

Figures

Chapter 1

About This Guide and Your Product

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.

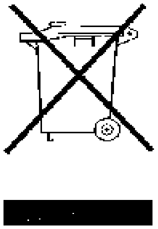
⚠ **WARNING** **THIS POWER BUTTON FUNCTIONS AS A POWER INTERRUPT ONLY. TO COMPLETELY REMOVE ALL POWER BEFORE SERVICING OR IN AN EMERGENCY, TURN OFF THE CIRCUIT BREAKER ON THE POWER DISTRIBUTION UNIT, AND THEN DISCONNECT THE POWER CORD FROM THE ELECTRICAL SOURCE.**

Mercury Statement

Required information

Hg 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.

WARNING **INDICATES A POTENTIALLY HAZARDOUS SITUATION WHICH, IF NOT AVOIDED, COULD RESULT IN DEATH OR BODILY INJURY.**

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

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

Other Documents you Might Need

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

- *Scalar i6000 Planning Guide* (6-66882)
- *Scalar i6000 Release Notes i8* (6-66883)
- *Scalar i2000/i6000 Maintenance Guide* (6-66880)
- *Scalar i6000 Installation Guide* (6-66881)
- *Scalar i6000 Unpacking Instructions* (6-66934)
- *System, Safety, and Regulatory Information Guide* (6-00618)

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 in the product box or at www.quantum.com/support

Getting More Information or Help Updated Contact Info

More information about this product is available on the Service and Support Web site at www.quantum.com/support. The Service and Support Web site contains a collection of information, including answers to frequently asked questions (FAQs). You can also access software, firmware, and drivers through this site.

For further assistance, or if training is desired, contact Quantum:

Global Call Handling:	1-800-284-5101
For additional contact information:	www.quantum.com/support
To open a Service Request:	www.quantum.com/osr

Chapter 2

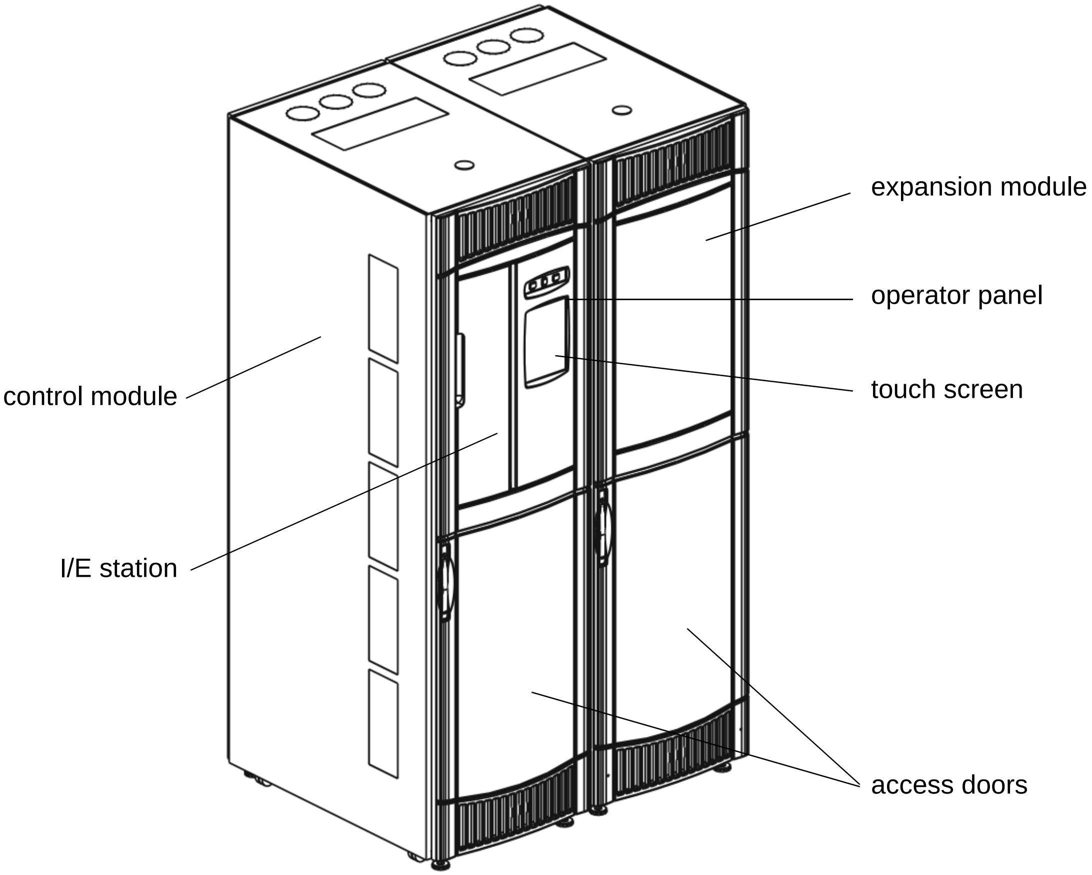
Description

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.

Figure 1 on page 8 shows a front view of the library, consisting of a control module and an expansion module.

Figure 1 Front View of a Control Module and Expansion Module



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 11 expansion modules as storage and tape drive requirements change.

Note Expansion modules in positions nine through twelve are storage-only modules and do not contain I/E stations or drives.

For LTO, the maximum library configuration can accommodate

- 1 control module,
- 0 to 11 expansion modules
- 102 to 5316 cartridges,
- 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.

For DLT, the maximum library configuration can accommodate:

- 1 control module,
- 0 to 7 expansion modules,
- 100 to 2910 cartridges,
- 1 to 96 tape drives,
- 1 to 8 20-slot Import/Export stations.

Note All 96 drives must be installed on the first eight modules of the system.

This chapter includes the following sections:

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 respectively).

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 324.

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 37.

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 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 or SCSI 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:

- SDLT-320 SCSI-interfaced drives can be connected to the SAN when they are directly connected to an external Storage Networking Controller (SNC) 5100. There is no area provided to mount the SNC inside the library modules, so you must plan for extra rack space near the library.
- FC and SCSI 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 or SCSI) 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 the LMC Applet (Web Browser) on page 265. For more information about the LMC, see Library Management Console (LMC) on page 271.

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 100 DLT or 102 LTO storage slots. The number of storage slots differs between media types because the library only supports full magazines for capacity on demand.

The library's license key must be enabled during installation to configure those parts of the library that are governed by additional licensing. Customer license keys are available from Quantum technical service.

The capacity on demand library can be expanded from a single module to up to 12 modules. With capacity on demand, you can purchase enough storage to accommodate your current needs. As your storage needs change, you can add storage in blocks of 100 cartridges without being required to purchase additional hardware. Capacity on demand begins at 100 cartridges and can be increased to as many as 5316 LTO or 2,910 DLT cartridges inside one library.

Control Module

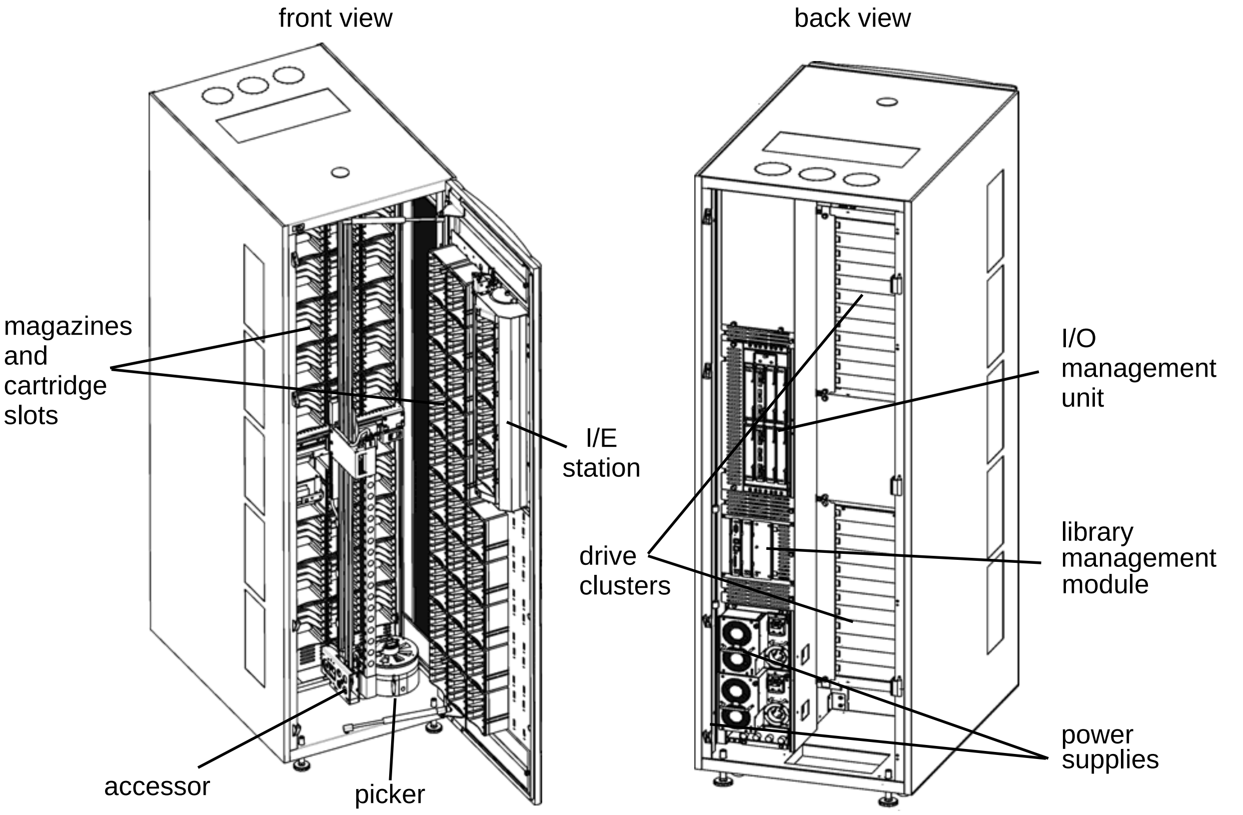
All library configurations include the control module, which contains the following components at a minimum (see figure 2 on page 14):

- Library management module (LMM)
- I/E station
- Tape drives
- Cartridge storage

- Operator panel
- Power system

The I/O management unit is optional for the control module. For more information about the I/O management unit, see I/O Management Units on page 20.

Figure 2 Front and Back View of the Control Module



Expansion Modules

Expansion modules enable the library to expand by adding space for tape drives, I/E stations, and cartridges. Each expansion module adds 300 to 456 LTO or 250 to 380 DLT cartridge slots, depending on the number of tape drives installed and whether an I/E station is installed (see figure 3 on page 16). The library's maximum configuration includes up to eleven expansion modules for a total of up to 12 modules. Expansion modules can only be added to the right of the control module.

Note Expansion modules in positions nine through twelve are storage-only modules and do not contain I/E stations or drives.

The expansion modules can accommodate the following components:

- I/O management unit (optional)
- Tape drives (optional)
- Cartridge storage
- I/E station (optional)
- AC power compartment (required only if drives are added)

If an expansion module contains only cartridges, all power is derived from the control module.

Figure 3 Expansion Module with 24 Slot I/E Station

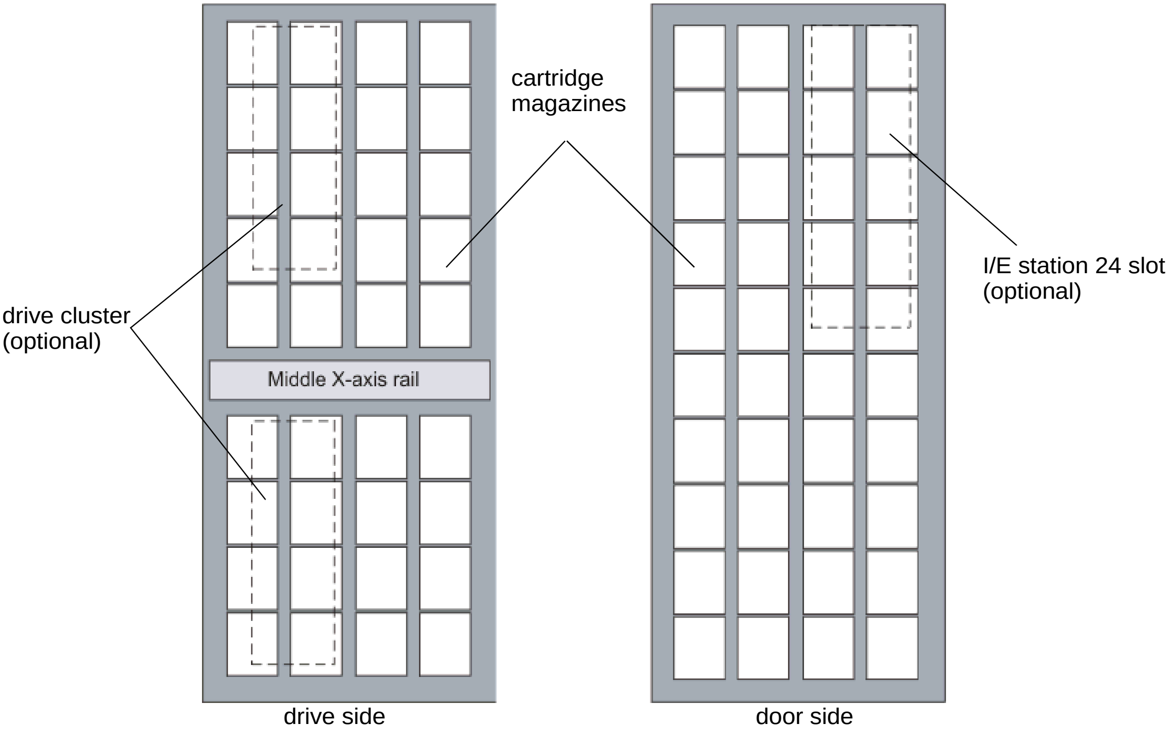
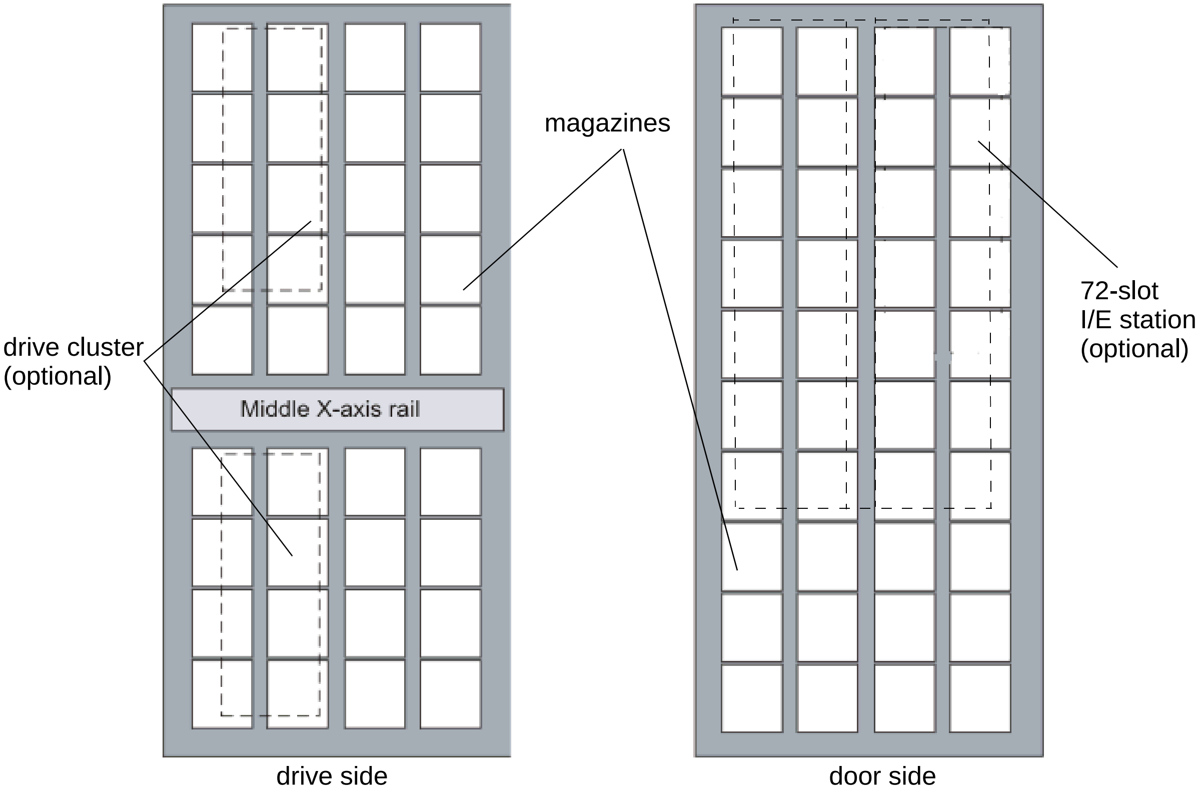


Figure 4 Expansion Module with 72 Slot I/E Station



I/E Station Options

An expansion module is designed for customers who have an increased need to import or export cartridges. An expansion module 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.

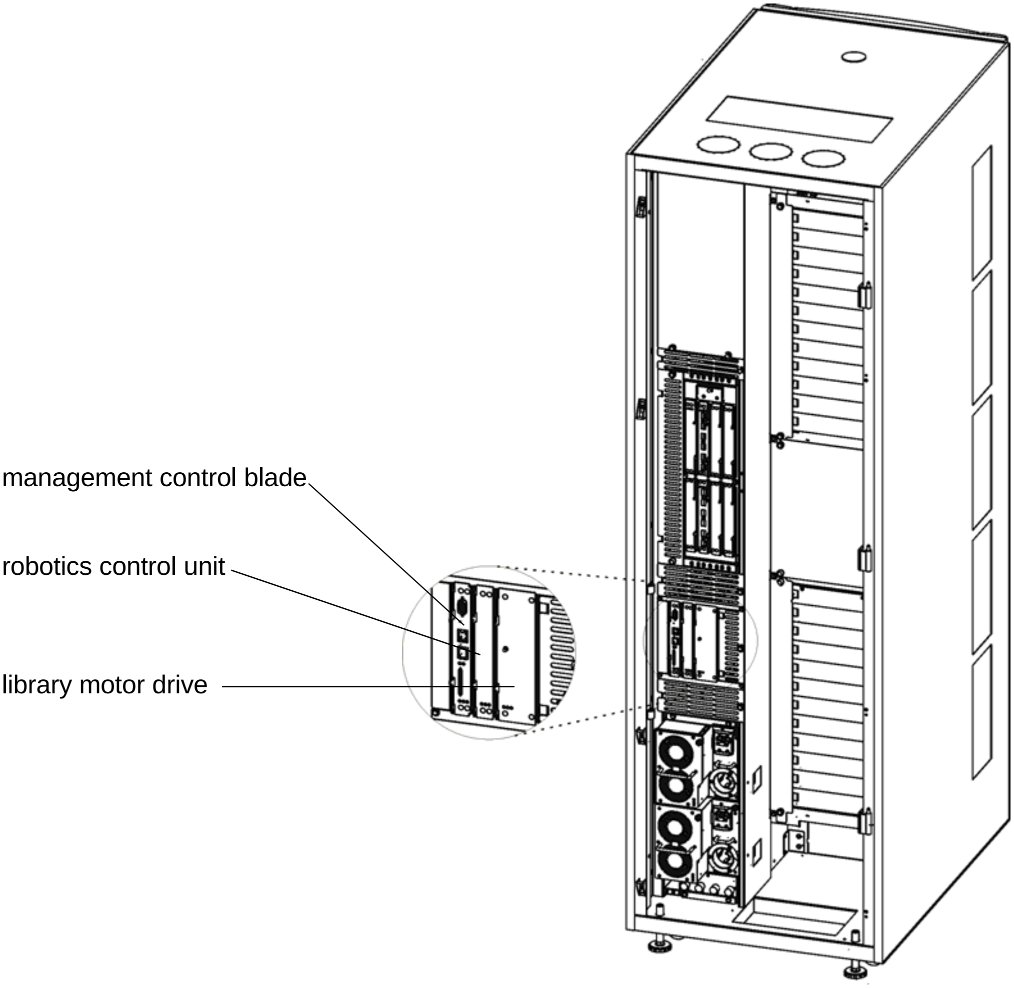
The 24-slot I/E station has a capacity of 24 LTO or 20 SDLT cartridges that are located in four removable magazines.

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. SDLT cartridges are not supported in the 72 slot I/E station.

Library Management Module

The library management module (LMM) controls and manages library hardware and software components. It enables both SAN-connected hosts and users who access the library using the operator panel to configure the library, obtain system status information, and perform various library functions. The LMM contains the management control blade (MCB), the robotics control unit (RCU), and the library motor driver (LMD), as shown in figure 5.

Figure 5 Library Management Module Boards



Management Control Blade (MCB)

The MCB is the primary point of intelligent management in the library. The MCB stores firmware and configuration data for itself as well as most other intelligent components in the library. It also contains the LMC, which enables local or remote users or hosts to operate, configure, and monitor the library. The MCB collects status information on other components in the library and issues notifications when problems occur.

Robotics Control Unit (RCU)

The RCU provides robotics intelligence that controls accessor movements and functions, including picker, pivot, and reach actions. It receives commands from hosts or users by way of the MCB.

Library Motor Driver (LMD)

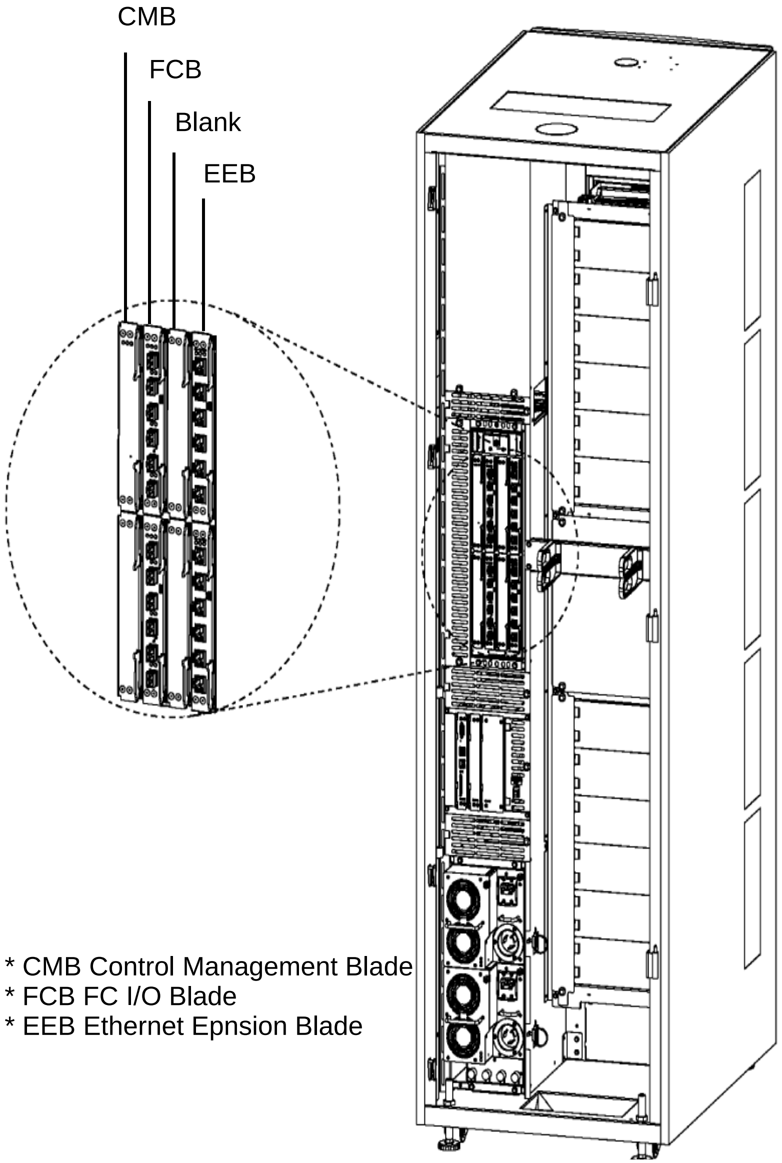
The LMD monitors wiring, fuses, and relays within the library. It regulates power levels and performs other power-related functions, such as disabling robotics when a library door opens.

I/O Management Units

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 six FC I/O blades, which provide FC connections for the Fibre Channel drives in the module. (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.

The I/O management unit supports the control management blade (CMB), the FC I/O blade, and the Ethernet Expansion Blade (EEB) as shown in figure 6 on page 21.

Figure 6 I/O Management Unit



* CMB Control Management Blade
* FCB FC I/O Blade
* EEB Ethernet Epnsion Blade

Control Management Blade (CMB)

The CMB performs unit status monitoring, including power and I/O present conditions, and internal network switch functions connecting I/O blades with the LMM. The CMB stores connectivity information for the I/O blades so that if you switch out an I/O blade, you do not have to reconfigure connectivity settings to drives. The CMB also enables you to update a drive's firmware without using a firmware update (FUP) tape.

FC I/O Blades

There are two different FC I/O blade types: 6404 that auto-negotiates up to 2 Gbps and 7404 that auto-negotiates up to 4 Gbps. Each FC I/O blade has an embedded controller that provides connectivity and features that enhance the performance and reliability of tape operations. Each blade provides two host communication ports and four connection ports to drives.

Note

Fibre Channel LTO-1, LTO-2, LTO-3, LTO-4, LTO-5 DLT-S4, and SDLT-600 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 drive to a blade; the I/O blade supports only 4 gigabits per second, but the drive supports 8 gigabits per second.

Ethernet Expansion Blade (EEB)

The Ethernet Expansion Blade (EEB) provides the option for Ethernet connectivity to each LTO-5 drive for MCB-to-drive communication purposes only. The EEB is not in the data path like the fibre I/O blade. The connection is at T100. This 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 drives. The EEB provides Ethernet connectivity to the library's internal Ethernet and should not be connected to an external Ethernet source.

Cartridge Accessor

The cartridge accessor moves cartridges between storage cells, tape drives, and I/E stations. 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^{o}. A barcode scanner on the picker assembly identifies cartridges located in storage cells.

Import/Export Stations

I/E stations enable you to import and export cartridges without interrupting normal library operations. The I/E station is installed on the front of the control module and, optionally, any of the first seven expansion modules in larger library configurations. See figure 1 on page 8 and figure 2 on page 14 to see the location of the I/E station.

Each 24-slot I/E station contains four removable magazines for a total of 24 LTO or 20 DLT tape cartridges. Each 72-slot I/E station contains twelve removable magazines for a total of 72 LTO tape cartridges.

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 112.

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, less 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 > Physical Library). Refer to Setting Up Policies for the Physical Library on page 159.
To configure a partition with Extended I/E segments, the user 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 Creating Partitions Manually Using Expert Mode on page 129.

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.

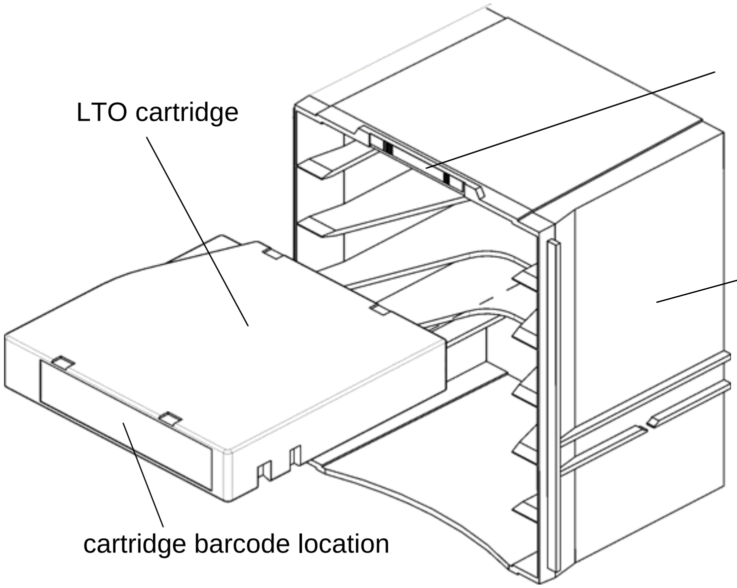
When you configure Extended I/E slots you must have at lease one physical I/E segment configured in the partition. The maximum number of physical and Extended I/E slots per partition is 240.

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 7.

Figure 7 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 (LTO or DLT). The library currently supports Code 39 (3 of 9) type barcode labels. For more information about tape cartridges, see Tape Drives on page 29. For additional specification information, see Barcode Requirements on page 506. For details about the use of drives and cartridges, see Mixed Media Support and Rules on page 33.

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 8. It contains the cartridge slots and provides flexibility when adding storage cartridges to a module.

Figure 8 Magazine and Drive Locations in the Control Module

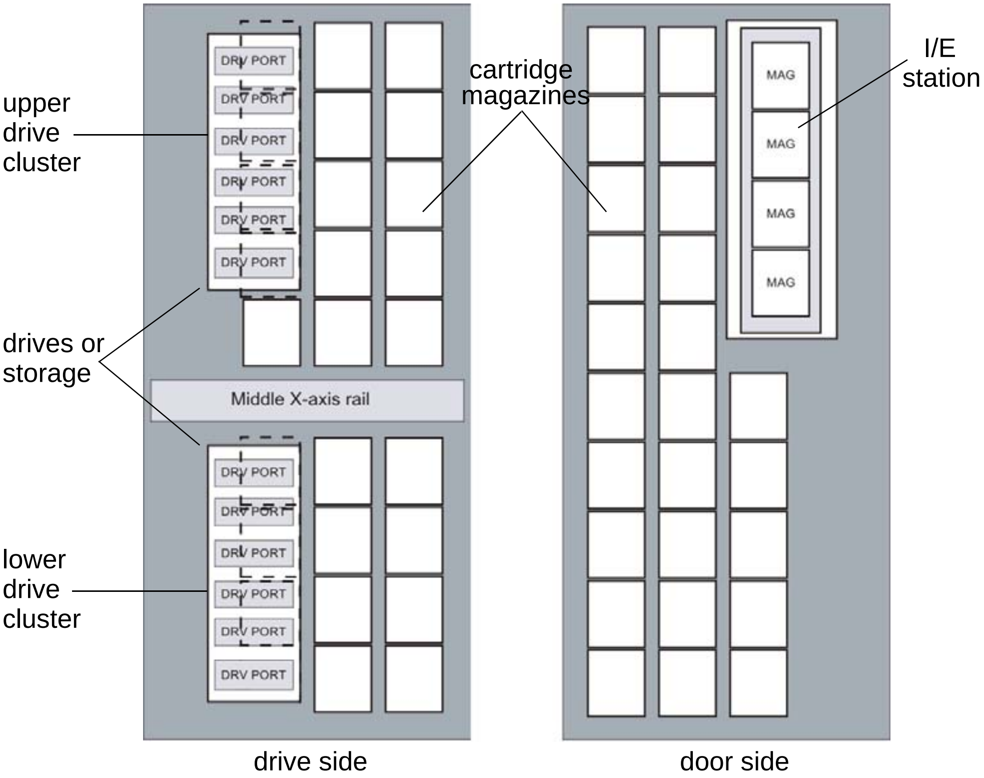
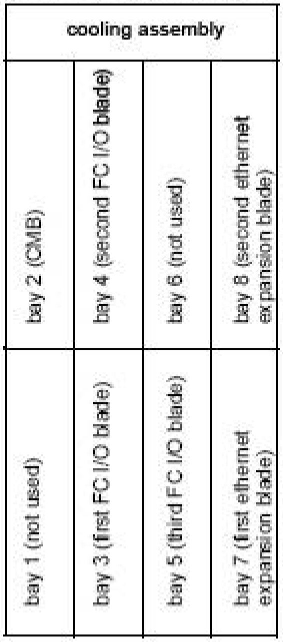


Figure 9 Expansion Module Magazine and Drive Locations in Control Module


cooling assembly
bay 2 (CMB)
bay 4 (second FC I/O blade)
bay 6 (not used)
bay 8 (second ethernet expansion blade)
bay 1 (not used)
bay 3 (first FC I/O blade)
bay 5 (third FC I/O blade)
bay 7 (first ethernet expansion blade)

There are two types of magazines: one for DLT and another for LTO. Because the two magazines are the same size, they can be mixed in the library. DLT magazines hold five cartridges, and LTO magazines hold six cartridges.

Table 1 Cartridge Capacities in Library Modules

Type of Cartridge	Cartridges per Magazine	Magazines per Control Module[a]	Magazines per Expansion Module[b]	Control Module Cartridge Capacity[c]	Expansion Module Cartridge Capacity[d]
DLT	5	44 min/50 max	50 min/76 max	220 min/250 max	250 min/380 max
LTO	6	44 min/50 max	32 min/76 max	264 min/300 max	192 min/456 max

a.The minimum is based on having 11 additional drives installed. The maximum is based on having one drive and one I/E station installed.

b.The minimum is based on having an I/E station and 12 drives installed. The maximum is based on having no drives or an I/E station installed.

c.The minimum is based on having 11 additional drives installed. The maximum is based on having one drive and one I/E station installed.

d. The minimum is based on having an I/E station and 12 drives installed. The maximum is based on having no drives or an I/E station installed.

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.

Support for WORM

The Scalar i6000 library supports WORM (write once, read many) technology in LTO-3, LTO-4, and LTO-5 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 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, or LTO-5 tape drive code are installed on a library with LTO-3, LTO-4, or LTO-5 tape drives, the WORM feature is supported whenever the operator uses WORM cartridges.

Tape Drives

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, or LTO-5 FC Multi-mode
- HP LTO-3, LTO-4, and LTO-5 FC Multi-mode
- Quantum SDLT-320 LVD–SCSI
- Quantum SDLT-600 FC
- Quantum DLT-S4 FC

⚠ **CAUTION** **Although the physical library can contain more than one media domain or drive domain, you cannot have a mix of domain types within a partition (for example, LTO and DLT).**

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).

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 the first seven expansion modules in the configuration. This enables you to have a total of 96 drives.

Note When you add drives, you lose storage slots.

Drives must be installed in bottom-to-top order in the control module before any are added to the first expansion module. There are two six-drive clusters in each of the first eight modules.

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

Figure 8 on page 26 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 33.

Fibre Channel LTO-1, LTO-2, LTO-3, LTO-4, LTO-5, DLT-S4, and SDLT-600 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 and SDLT drives follows.

LTO Drives

Five generations of LTO drives are supported, but they are not fully compatible as shown in Table 2.

Table 2 LTO Drive and Cartridge Compatibility

	LTO-1 Cartridge	LTO-2 Cartridge	LTO-3 Cartridge	LTO-3 WORM	LTO-4 Cartridge	LTO-4 WORM	LTO-5 Cartridge	LTO-5 WORM
LTO-1 Drives	Reads/ Writes	Not compatible	Not compatible	Not compatible	Not compatible	Not compatible	Not compatible	Not compatible
LTO-2 Drives	Reads/ Writes[a]	Reads/ Writes	Not compatible	Not compatible	Not compatible	Not compatible	Not compatible	Not compatible
LTO-3 Drives	Reads[b]	Reads/ Writes[c]	Reads/ Writes	Write Once, Read Many[d]	Not compatible	Not compatible	Not compatible	Not compatible
LTO-4 Drives	Not compatible	Reads	Reads/ Writes	Write Once, Read Many	Reads/ Writes	Write Once, Read Many[e]	Not compatible	Not compatible
LTO-5 Drives	Not compatible	Not compatible	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 size, which means they use the same magazines in the library.

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

DLT Drives

Five generations of DLT cartridges are supported in the library, but the drives are not fully compatible as shown in Table 3.

Table 3 DLT Drive and Cartridge Compatibility

	SDLT-600 Cartridges	SDLT-320 Cartridges	SDLT-220 Cartridges	SDLT-VS 160 Cartridges	DLT-S4 Cartridges
DLT-S4 Drives	Reads	Reads	Reads	Not compatible	Reads/Writes
SDLT-600 Drives	Reads/Writes	Reads	Reads	Reads	Not compatible
SDLT-320 Drives	Not compatible	Reads/Writes	Reads/Writes	Not compatible	Not compatible

The SDLT-600 tape drives support reading and writing to SDLT II cartridges. They also have a backward-read compatibility (BRC) mode. When in this mode, the SDLT-600 is capable of reading SDLT-220 and SDLT-320 tape formats in an SDLT I data cartridge, as well as the SDLT-VS160 tape format in the DLT tape VS1 data cartridge. The SDLT-600 tape drive will eject a data cartridge written in DLT formats other than DLT-VS160. All DLT cartridges are the same size, which means they will use the same magazines in the library.

The SDLT-320 SCSI tape drives are supported in the library, but they must be connected to an FC Host SAN by means of an external SNC 5100.

Mixed Media Support and Rules

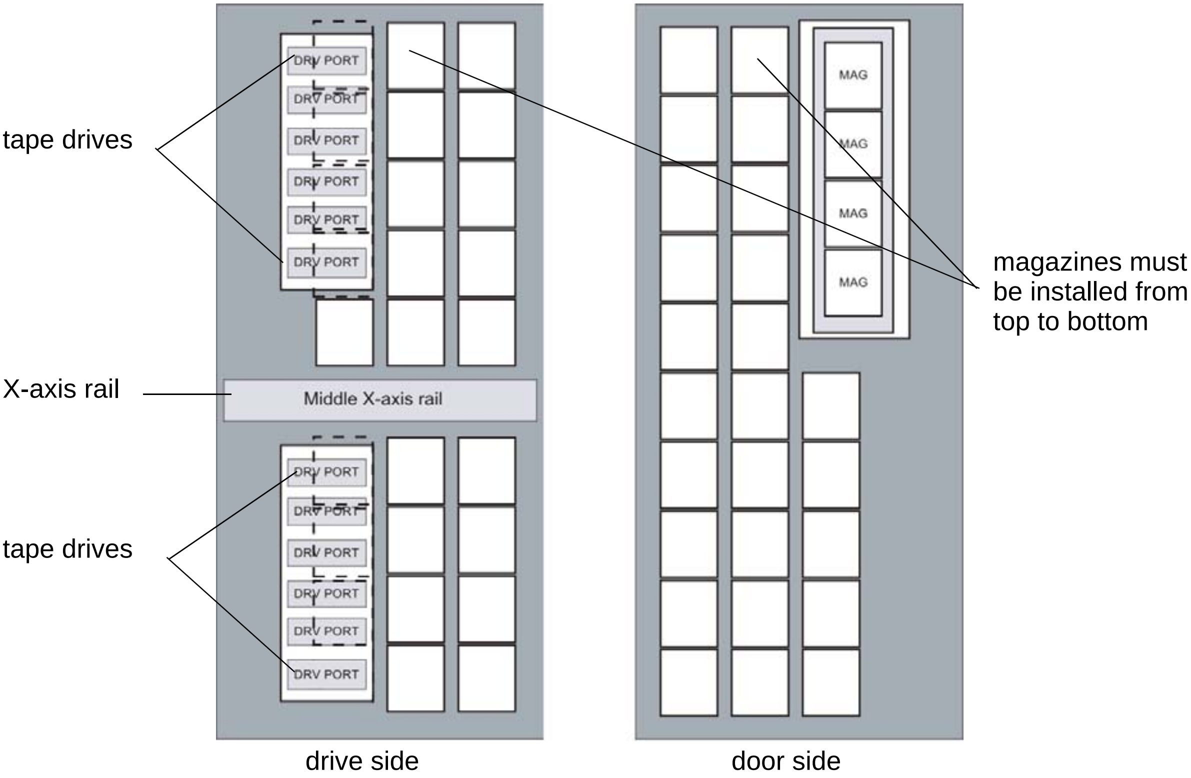
The library supports both LTO and DLT cartridges and drives in the same configuration, provided that you adhere to the following rules:

- When purchasing a library with mixed media, the new orders must specify the base system technology (either LTO or DLT) 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, SDLT-320, SDLT-600, DLT-S4.
- If you are loading cartridges into the library by using the I/E station, you must have a magazine of each of the two types of media in the I/E station (LTO and DLT).
- Mixed media can be within the 100 slot capacity increment, with the following restrictions:
    - DLT must be ordered in multiples of five because the magazines hold five cartridges.
    - LTO must be ordered in multiples of six because the magazines hold six cartridges.
    - Regardless of the mixed quantities of each media type, the total slots licensed will still be in multiples of 100.
- Field upgrades of the library to existing single media systems must specify a mixed media picker kit if mixed media will be used in the upgraded library.
- Drive types can be installed in any order. For example, an LTO drive can occupy the first drive position, a DLT drive can occupy the second, and another LTO can occupy the third drive position.

However, drives must be installed beginning in the lower most drive slot of the control module. Once the control module has 12 drives installed from bottom to top, you must move to the bottom drive position of the first expansion module.

- The library must include at least one drive for each type of cartridge used.
- Magazines must be installed in the control module beginning with the back rack (drive side). Once the back rack (drive side) is full, you must then install magazines in the door side, starting with the top left corner. See figure 10.
- The secondary media type is installed beginning at storage slot 4096 or the first media magazine. See figure 10.

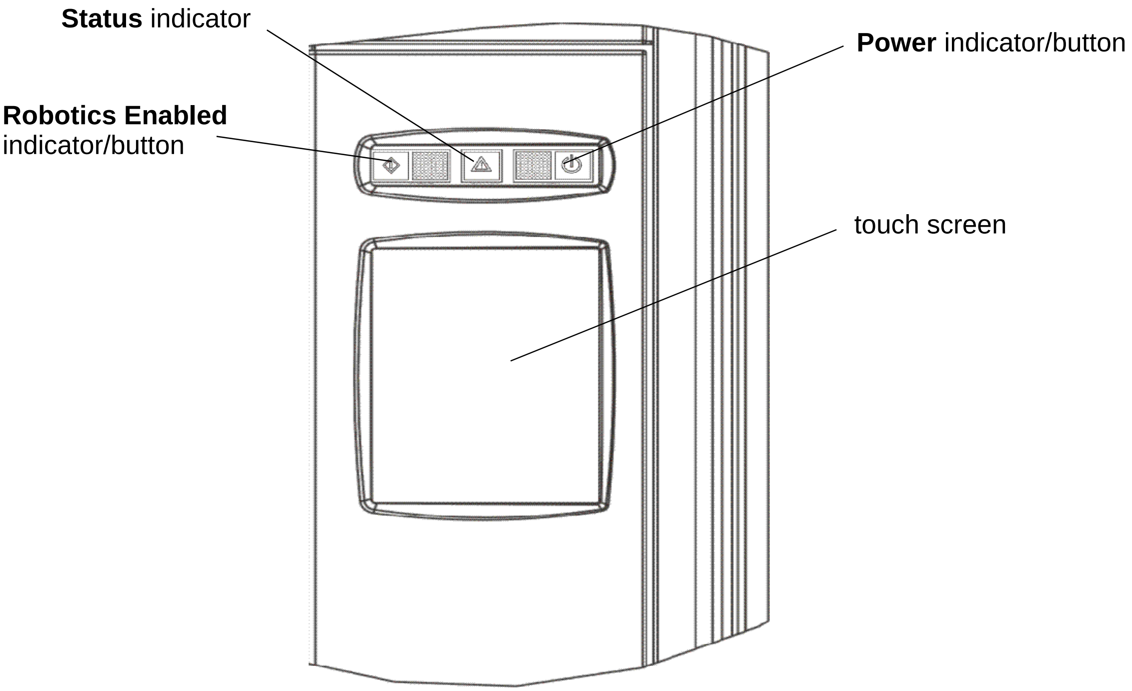
Figure 10 Magazine Installation Order



Operator Panel

The operator panel is located on the front of the control module and consists of indicators and a touch screen (see figure 11). The buttons are for library control and power, and the indicators provide library status.

Figure 11 Operator Panel


Status indicator
Robotics Enabled indicator/button
Power indicator/button
touch screen

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 Operator Panel and Library Management Console (LMC) on page 271.

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 (PDU)
- AC power cord

A single power switch, located on the access door, turns on and off all power for the control module and attached expansion modules. Each PDU 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.

Chapter 3

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.

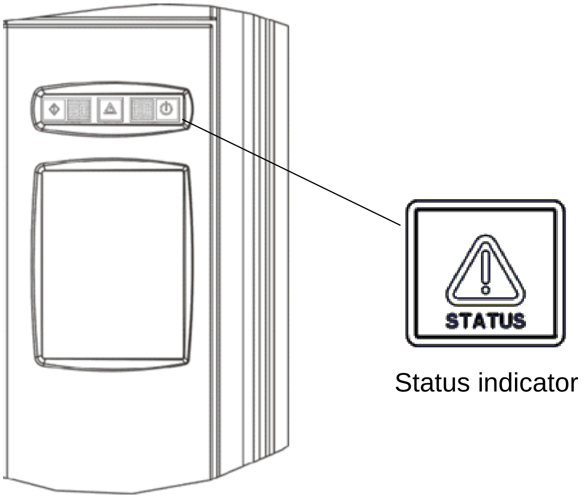
This chapter consists of the following sections:

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 first indication of issues is the status indicator on the indicator panel, as shown in Figure 12.

Figure 12 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 isolate field replaceable units (FRUs) that you must service or replace.

Note — Tickets can indicate failures or other serious problems, but they also can indicate warning conditions that you should investigate or other helpful information. For example, opening the library's access door or changing the library's configuration causes the library to create a ticket, but these situations would not indicate serious problems. However, you should investigate the tickets.

The library assigns a severity level to each ticket that it creates, and it notifies users of the ticket. Table 4 describes possible severity levels for tickets.

Table 4 Severity Levels Assigned to Tickets

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.

Table 4 Severity Levels Assigned to Tickets

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 library has two 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

Understanding Indicators on System Status Buttons

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 286. 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 4 on page 39. 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 43.

Understanding 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 4 on page 39. 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 (severity level 1 issues only) is techsup@quantum.com (Quantum technical support). To set up other e-mail addresses to receive notifications, see Configuring E-mail on page 164 and Setting Up E-mail Notifications on page 167.

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 enabled or disabled
- 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 Repair Pages on page 61.

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 43.

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 46).
2. View the details for the appropriate ticket (see Viewing Ticket Details on page 52).
3. View the reports that are associated with this ticket (see Viewing Ticket Details Reports on page 58.
4. View the ticket’s repair page (see Viewing Repair Pages on page 61).

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 52 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 58.

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 52.

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 52.

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 52.

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 Repair Pages on page 61.

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 Updated Contact Info on page 6. 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 70.

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 76.

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 47.

- 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 49.

- 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 49.

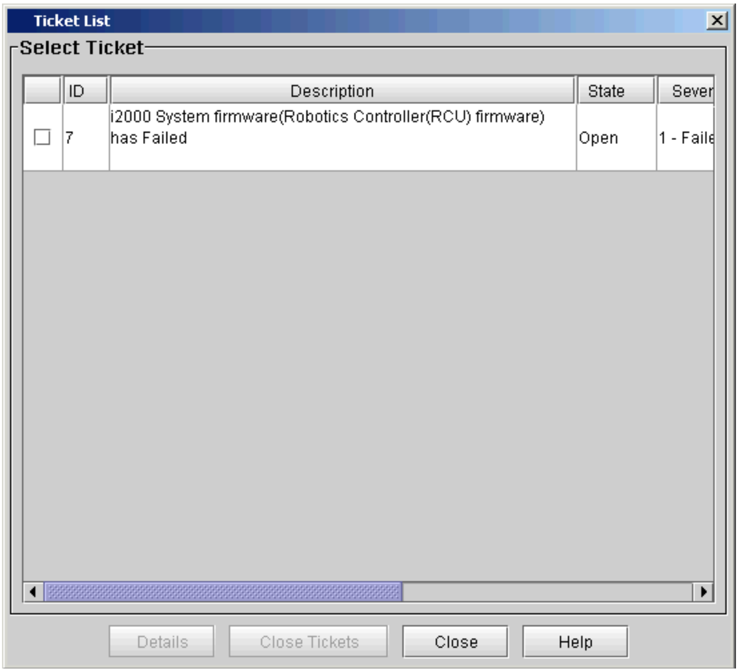
From the ticket list, you can select a ticket to view ticket details, associated reports, and a repair page.

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.



Ticket List

Select Ticket

	ID	Description	State	Sever
□	7	i2000 System firmware(Robotics Controller(RCU) firmware) has Failed	Open	1 - Faile

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

Element	Description
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 52.

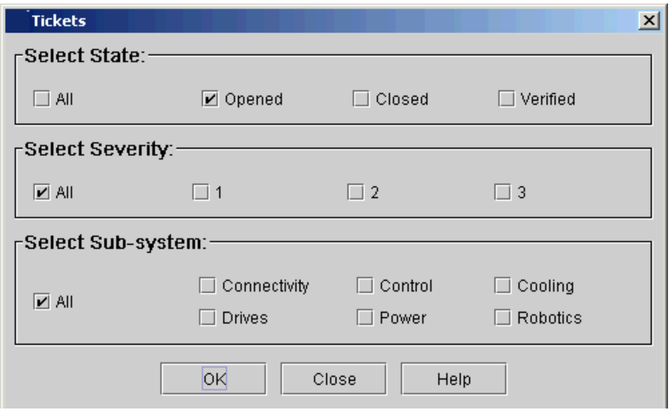
2 By default, the ticket list is sorted by ticket ID in ascending order with the oldest ticket at the top and the newest one at the bottom. To change the sorting (for example, by state or severity), click the column heading by which you want the tickets sorted. Repeatedly clicking a column heading toggles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



Tickets

Select State:
□ All ☑ Opened □ Closed □ Verified

Select Severity:
☑ All □ 1 □ 2 □ 3

Select Sub-system:
☑ All □ Connectivity □ Control □ Cooling □ Drives □ Power □ Robotics

This 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.

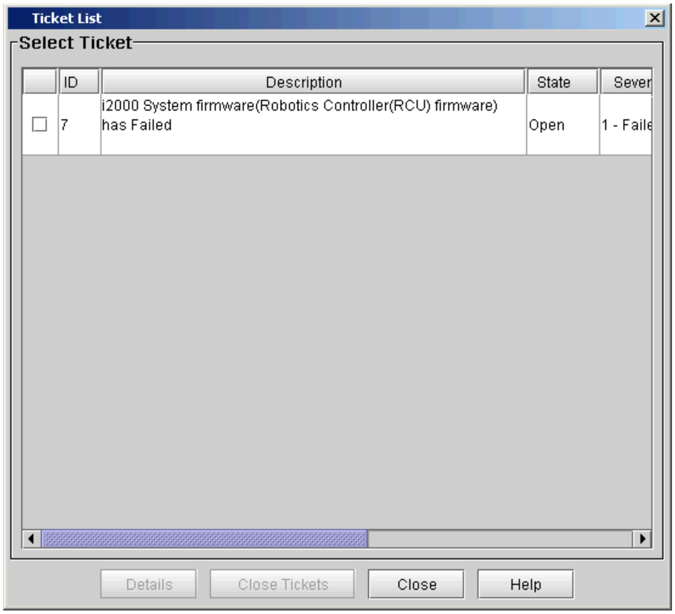
If you select a combination that does not produce a ticket list, a **No Tickets Found** error message appears.

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.



	ID	Description	State	Sever
□	7	i2000 System firmware(Robotics Controller(RCU) firmware) has Failed	Open	1 - Faile

For descriptions of elements on the **Ticket List** dialog box, see Using System Status Buttons to Display Ticket Lists on page 47.

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

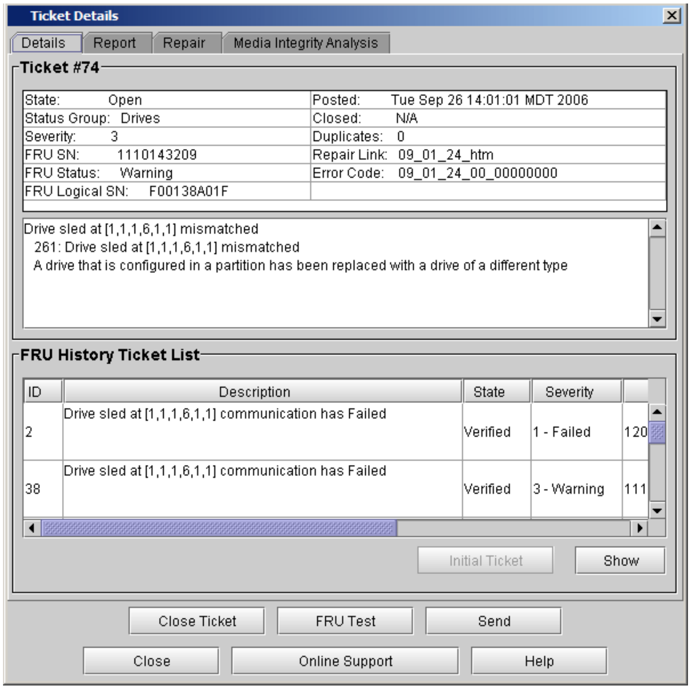
Tickets provide detailed information about the ticket itself, the reports that are associated with it, and a repair page that gives guidance for resolving the issue. These tickets provide important information about library conditions from which the issue emerged and helpful information for resolving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



Ticket #74

State: Open	Posted: Tue Sep 26 14:01:01 MDT 2006
Status Group: Drives	Closed: N/A
Severity: 3	Duplicates: 0
FRU SN: 1110143209	Repair Link: 09_01_24_htm
FRU Status: Warning	Error Code: 09_01_24_00_00000000
FRU Logical SN: F00138A01F	

```
Drive sled at [1,1,1,6,1,1] mismatched
  261: Drive sled at [1,1,1,6,1,1] mismatched
  A drive that is configured in a partition has been replaced with a drive of a different type
```

FRU History Ticket List

ID	Description	State	Severity	
2	Drive sled at [1,1,1,6,1,1] communication has Failed	Verified	1 - Failed	120
38	Drive sled at [1,1,1,6,1,1] communication has Failed	Verified	3 - Warning	111

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.

The following table describes the elements on the **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 Cooling 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.

Element	Description
In the **FRU History Ticket List** area:	
ID	The library-assigned identifier for the history ticket.
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 • Cooling • 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 56)
- 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 web site, 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 70)
- 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 430.

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.

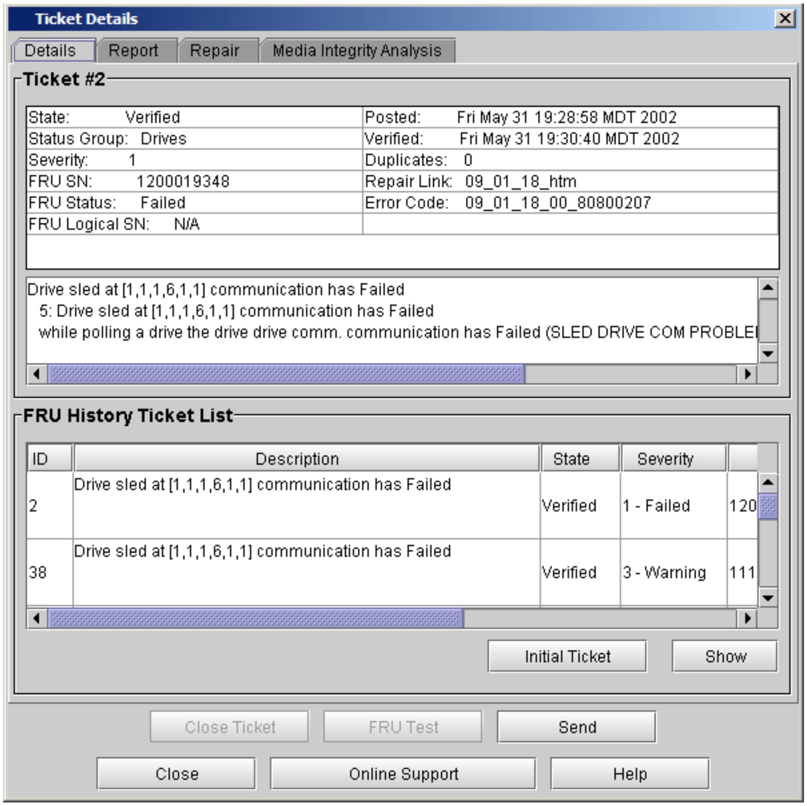
- Display report information (see Viewing Ticket Details Reports on page 58)
- Display the repair page (see Viewing Repair Pages on page 61)

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.
2. 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.



Ticket #2

State: Verified	Posted: Fri May 31 19:28:58 MDT 2002
Status Group: Drives	Verified: Fri May 31 19:30:40 MDT 2002
Severity: 1	Duplicates: 0
FRU SN: 1200019348	Repair Link: 09_01_18_htm
FRU Status: Failed	Error Code: 09_01_18_00_80800207
FRU Logical SN: N/A	

```
Drive sled at [1,1,1,6,1,1] communication has Failed
  5: Drive sled at [1,1,1,6,1,1] communication has Failed
  while polling a drive the drive drive comm. communication has Failed (SLED DRIVE COM PROBLEI
```

FRU History Ticket List

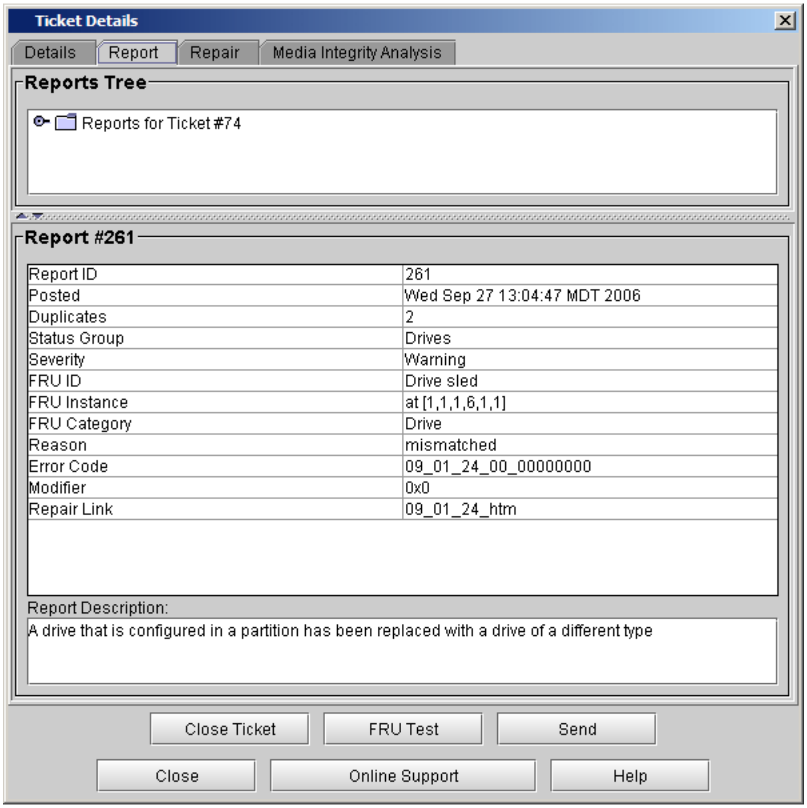
ID	Description	State	Severity	
2	Drive sled at [1,1,1,6,1,1] communication has Failed	Verified	1 - Failed	120
38	Drive sled at [1,1,1,6,1,1] communication has Failed	Verified	3 - Warning	111

3 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.



Report #261

Report ID	261
Posted	Wed Sep 27 13:04:47 MDT 2006
Duplicates	2
Status Group	Drives
Severity	Warning
FRU ID	Drive sled
FRU Instance	at [1,1,1,6,1,1]
FRU Category	Drive
Reason	mismatched
Error Code	09_01_24_00_00000000
Modifier	0x0
Repair Link	09_01_24_htm

Report Description:
A drive that is configured in a partition has been replaced with a drive of a different type

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

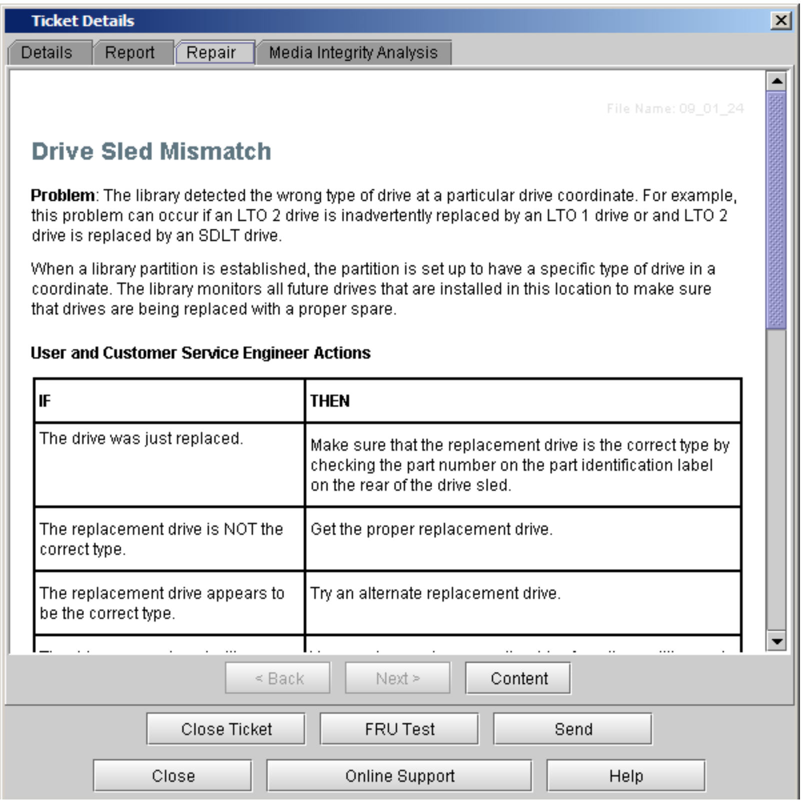
The following describes the elements on the **Report** tab:

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 Cooling 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 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.



File Name: 09_01_24

Drive Sled Mismatch

Problem: The library detected the wrong type of drive at a particular drive coordinate. For example, this problem can occur if an LTO 2 drive is inadvertently replaced by an LTO 1 drive or and LTO 2 drive is replaced by an SDLT drive.

When a library partition is established, the partition is set up to have a specific type of drive in a coordinate. The library monitors all future drives that are installed in this location to make sure that drives are being replaced with a proper spare.

User and Customer Service Engineer Actions

IF	THEN
The drive was just replaced.	Make sure that the replacement drive is the correct type by checking the part number on the part identification label on the rear of the drive sled.
The replacement drive is NOT the correct type.	Get the proper replacement drive.
The replacement drive appears to be the correct type.	Try an alternate replacement drive.

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

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 or generate tape alert reports from **Reports** on the menu. See Viewing Tape Alerts on page 63 or Generating Media Integrity Analysis Reports on page 65.

Note The **Media Integrity Analysis** feature requires a license key to use. For more information, see Enabling Licenses on page 110.

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 65.

Viewing Tape Alerts

To view tape alerts:

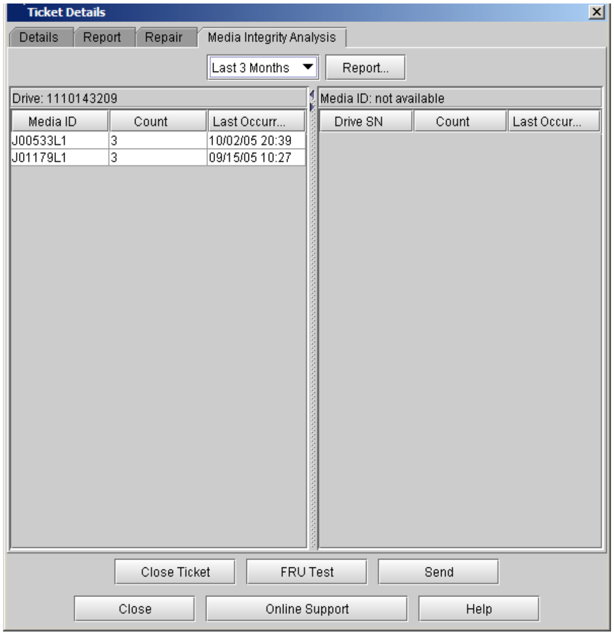
1 Click the **Media Integrity Analysis** tab on the **Ticket Details** dialog box.

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”.



Last 3 Months

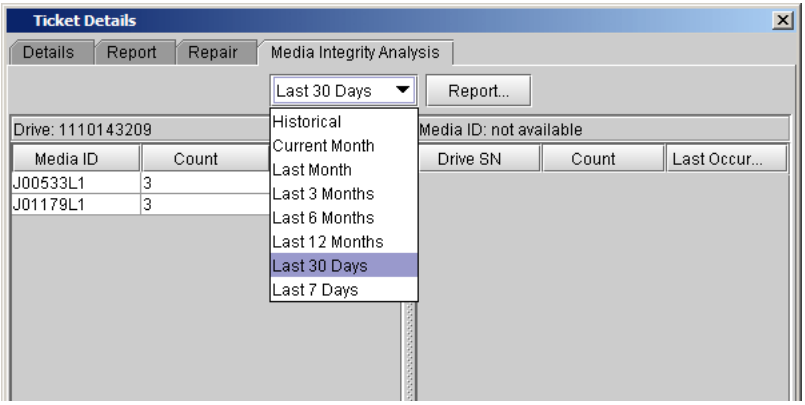
Drive: 1110143209

Media ID	Count	Last Occurr...
J00533L1	3	10/02/05 20:39
J01179L1	3	09/15/05 10:27

Media ID: not available

Drive SN	Count	Last Occur...

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



Last 30 Days

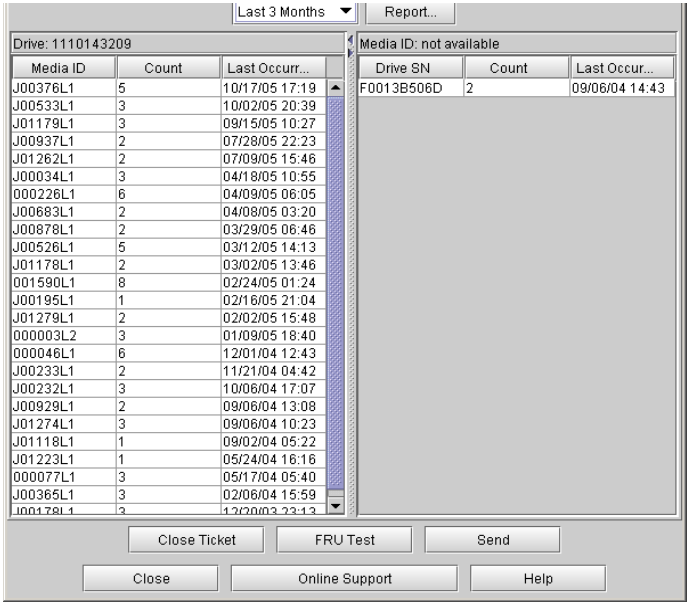
Drive: 1110143209

Media ID	Count
J00533L1	3
J01179L1	3

Media ID: not available

Drive SN	Count	Last Occur...

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



Drive: 1110143209

Media ID	Count	Last Occurr...
J00376L1	5	10/17/05 17:19
J00533L1	3	10/02/05 20:39
J01179L1	3	09/15/05 10:27
J00937L1	2	07/28/05 22:23
J01262L1	2	07/09/05 15:46
J00034L1	3	04/18/05 10:55
000226L1	6	04/09/05 06:05
J00683L1	2	04/08/05 03:20
J00878L1	2	03/29/05 06:46
J00526L1	5	03/12/05 14:13
J01178L1	2	03/02/05 13:46
001590L1	8	02/24/05 01:24
J00195L1	1	02/16/05 21:04
J01279L1	2	02/02/05 15:48
000003L2	3	01/09/05 18:40
000046L1	6	12/01/04 12:43
J00233L1	2	11/21/04 04:42
J00232L1	3	10/06/04 17:07
J00929L1	2	09/06/04 13:08
J01274L1	3	09/06/04 10:23
J01118L1	1	09/02/04 05:22
J01223L1	1	05/24/04 16:16
000077L1	3	05/17/04 05:40
J00365L1	3	02/06/04 15:59
J00178L1	3	12/20/03 23:13

Media ID: not available

Drive SN	Count	Last Occur...
F0013B506D	2	09/06/04 14:43

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

4 Go to Generating Media Integrity Analysis Reports on page 65.

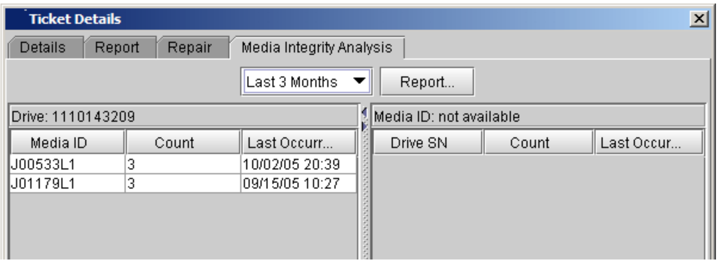
Generating Media Integrity Analysis Reports

This function allows you to generate reports using the criteria described in table 6 on page 77.

To generate tape alert reports:

1 Do one of the following:

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



Last 3 Months

Drive: 1110143209

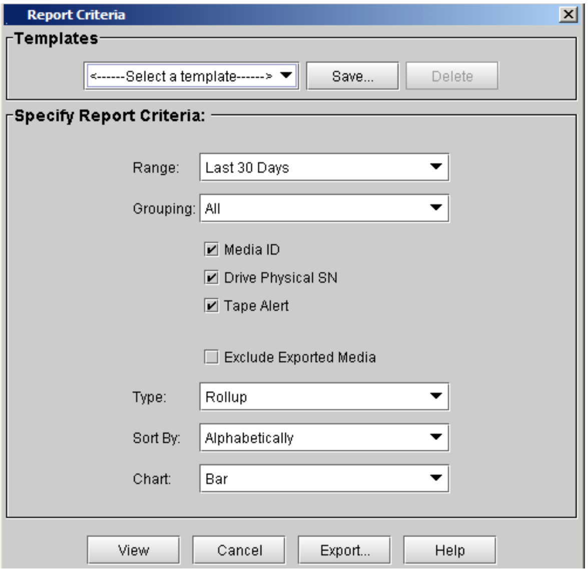
Media ID	Count	Last Occurr...
J00533L1	3	10/02/05 20:39
J01179L1	3	09/15/05 10:27

Media ID: not available

Drive SN	Count	Last Occur...

- On the menu bar, click **Tools**→ **Reports**→ **Media Integrity Analysis**.

  The **Report Criteria** dialog box appears.



<------Select a template------>

Range: Last 30 Days

Grouping: All

☑ Media ID

☑ Drive Physical SN

☑ Tape Alert

☐ Exclude Exported Media

Type: Rollup

Sort By: Alphabetically

Chart: Bar

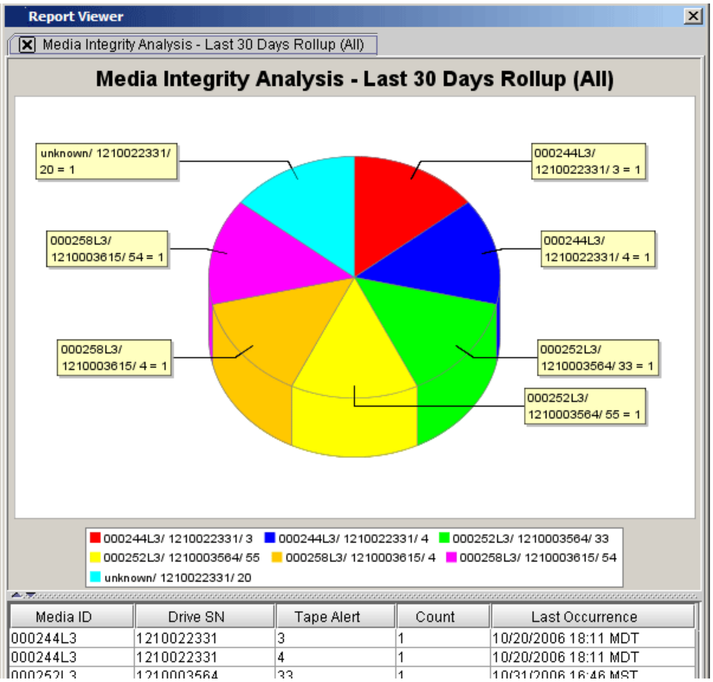
2 To view a report, select the report criteria described in the following and click **View.**

Table 5 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
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

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

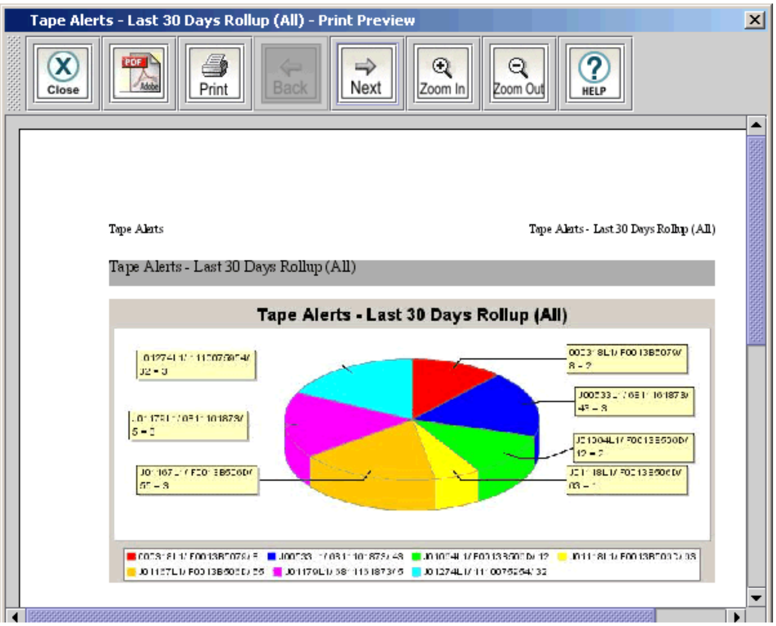
The **Report Viewer** dialog box appears. The content and appearance of the report varies depending on the selected criteria.


Report Viewer
☒ Media Integrity Analysis - Last 30 Days Rollup (All)
Media Integrity Analysis - Last 30 Days Rollup (All)
unknown/ 1210022331/ 20 = 1
000244L3/ 1210022331/ 3 = 1
000258L3/ 1210003615/ 54 = 1
000244L3/ 1210022331/ 4 = 1
000258L3/ 1210003615/ 4 = 1
000252L3/ 1210003564/ 33 = 1
000252L3/ 1210003564/ 55 = 1
🟥 000244L3/ 1210022331/ 3
🟦 000244L3/ 1210022331/ 4
🟩 000252L3/ 1210003564/ 33
🟨 000252L3/ 1210003564/ 55
🟧 000258L3/ 1210003615/ 4
🟪 000258L3/ 1210003615/ 54
🟦 unknown/ 1210022331/ 20

Media ID	Drive SN	Tape Alert	Count	Last Occurrence
000244L3	1210022331	3	1	10/20/2006 18:11 MDT
000244L3	1210022331	4	1	10/20/2006 18:11 MDT
000252L3	1210003564	33	1	10/31/2006 16:46 MST

3 Click **Preview**.

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

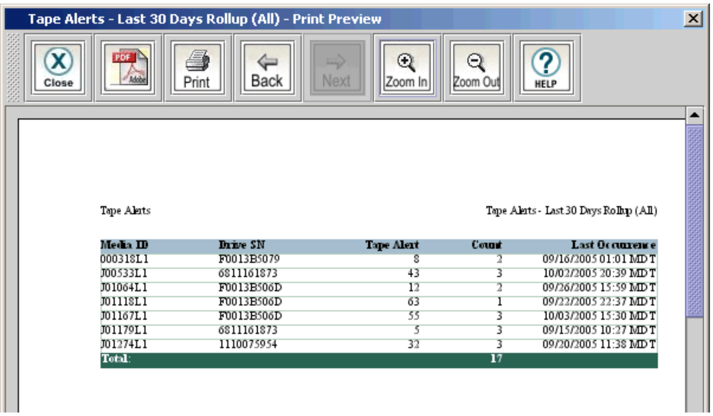

Tape Alerts - Last 30 Days Rollup (All) - Print Preview
Close
Adobe
Print
Back
Next
Zoom In
Zoom Out
HELP
Tape Alerts - Last 30 Days Rollup (All)

Tape Alerts

Tape Alerts - Last 30 Days Rollup (All)

Tape Alerts - Last 30 Days Rollup (All)

4 To view the next page of the report, click the **Next** icon on the toolbar.



Tape Alerts

Tape Alerts - Last 30 Days Rollup (All)

Media ID	Drive SN	Tape Alert	Count	Last Occurrence
000318L1	F0013B5079	8	2	09/16/2005 01:01 MDT
J00533L1	6811161873	43	3	10/02/2005 20:39 MDT
J01064L1	F0013B506D	12	2	09/26/2005 15:59 MDT
J01118L1	F0013B506D	63	1	09/22/2005 22:37 MDT
J01167L1	F0013B506D	55	3	10/03/2005 15:30 MDT
J01179L1	6811161873	5	3	09/15/2005 10:27 MDT
J01274L1	1110075954	32	3	09/20/2005 11:38 MDT
Total:			17	

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:

  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 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 5 on page 67 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 Understanding E-mail Notifications on page 41). 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 enabled or disabled
- Time stamps of recent activity
- Report summary
- Report details for the ticket

  The RAS repair page attachment is in HTML format.

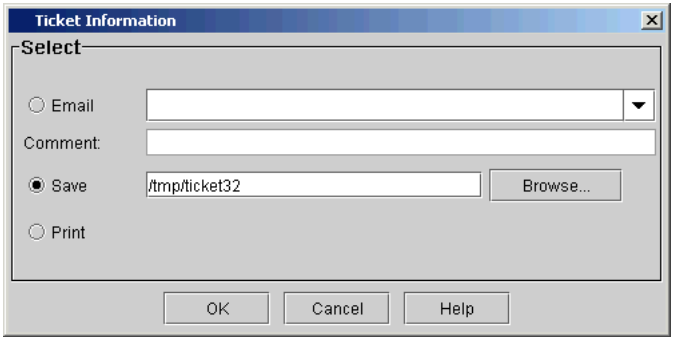
Note Before you perform the following procedure, you must make sure that e-mail is appropriately configured in the LMC so that the library can send ticket details to the recipient. See Configuring E-mail on page 164.

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 46 and Viewing Ticket Details on page 52.

2 Click **Send**.

The **Ticket Information** dialog box appears.



● Save /tmp/ticket32

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, seeWorking With Verification Tests on page 430.

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).
- The **FRU Test** button on the **Ticket Details** dialog box is not available. This means that an applicable verification test does not exist for the ticket's FRU.

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. SeeRunning 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 physically examining the FRU to make sure that 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 46 and Viewing Ticket Details on page 52.
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 46 and Viewing Ticket Details on page 52.
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.

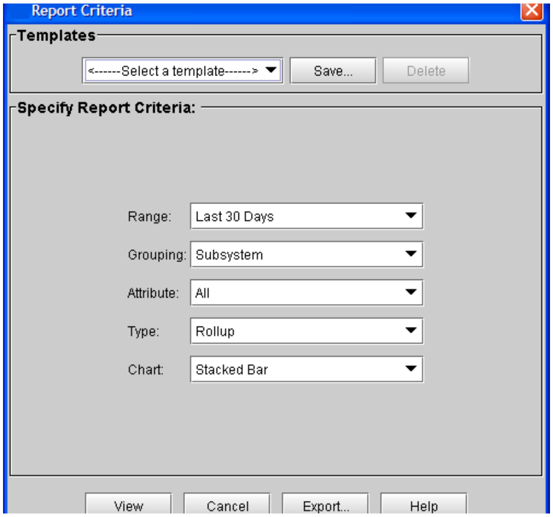
Specifying Tickets Report Criteria

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.



Report Criteria

Templates

<------Select a template------>

Specify Report Criteria:

Range: Last 30 Days
Grouping: Subsystem
Attribute: All
Type: Rollup
Chart: Stacked Bar

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

Table 6 on page 77 summarizes the available report criteria options.

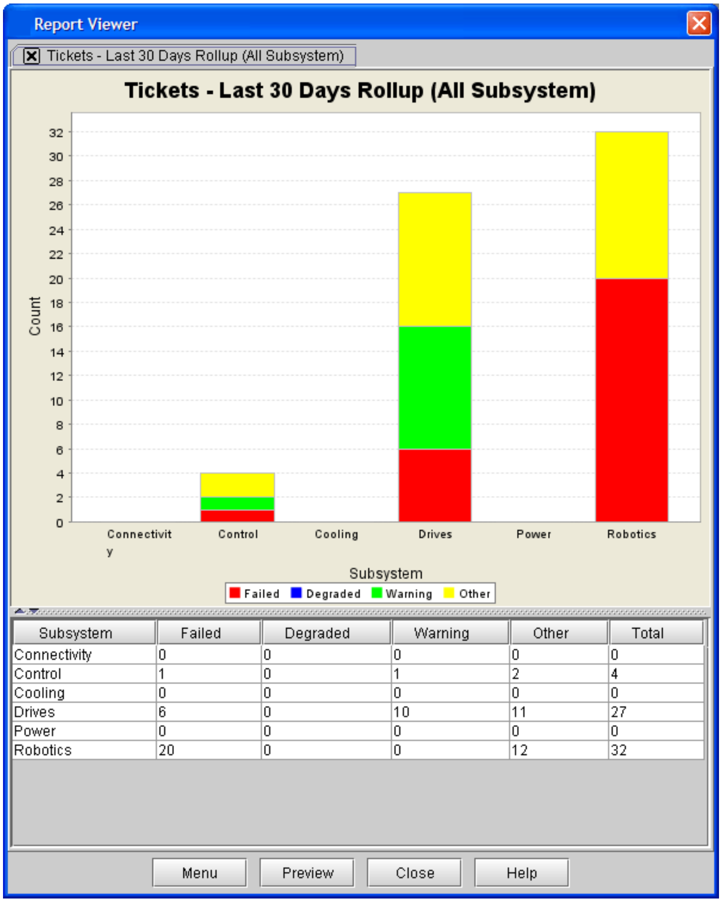
Table 6   Tickets Report Criteria Options

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.


Report Viewer
☒ Tickets - Last 30 Days Rollup (All Subsystem)
Tickets - Last 30 Days Rollup (All Subsystem)
Count
32
30
28
26
24
22
20
18
16
14
12
10
8
6
4
2
0
Connectivit y
Control
Cooling
Drives
Power
Robotics
Subsystem
🟥 Failed 🟦 Degraded 🟩 Warning 🟨 Other
Menu
Preview
Close
Help

Subsystem	Failed	Degraded	Warning	Other	Total
Connectivity	0	0	0	0	0
Control	1	0	1	2	4
Cooling	0	0	0	0	0
Drives	6	0	10	11	27
Power	0	0	0	0	0
Robotics	20	0	0	12	32

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

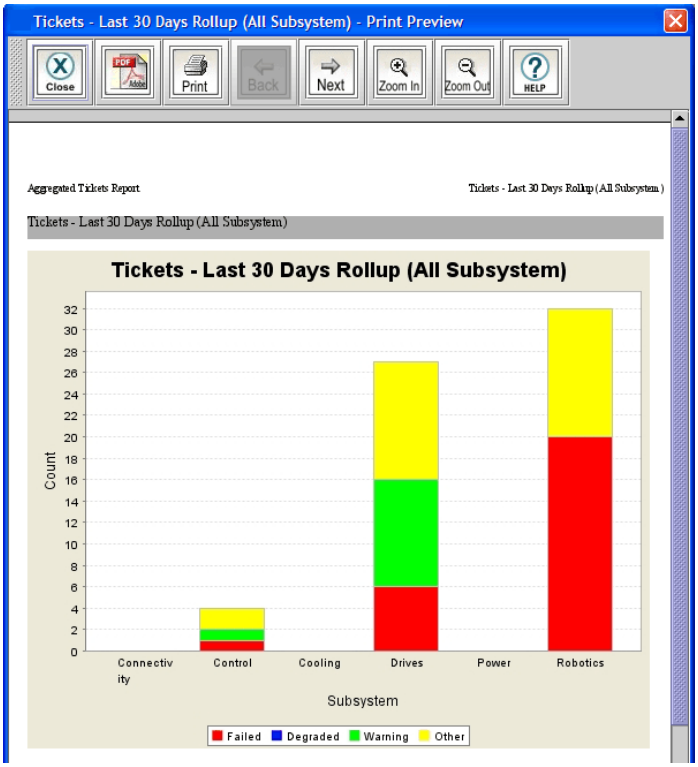
6 To close the **Report Criteria** dialog box, click **Cancel**.

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.


Tickets - Last 30 Days Rollup (All Subsystem) - Print Preview
Close
PDF Adobe
Print
Back
Next
Zoom In
Zoom Out
HELP
Aggregated Tickets Report
Tickets - Last 30 Days Rollup (All Subsystem)
Tickets - Last 30 Days Rollup (All Subsystem)
Tickets - Last 30 Days Rollup (All Subsystem)
Count
0
2
4
6
8
10
12
14
16
18
20
22
24
26
28
30
32
Connectivity
Control
Cooling
Drives
Power
Robotics
Subsystem
🟥 Failed
🟦 Degraded
🟩 Warning
🟨 Other

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 6 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 6 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**.

Interpreting LEDs

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

- Blade status LEDs
- Drive status LEDs
- Fibre port link LEDs (for Fibre drives and Fibre Channel I/O blades)
- MCB port LEDs
- LBX terminator LEDs
- Power supply status LEDs

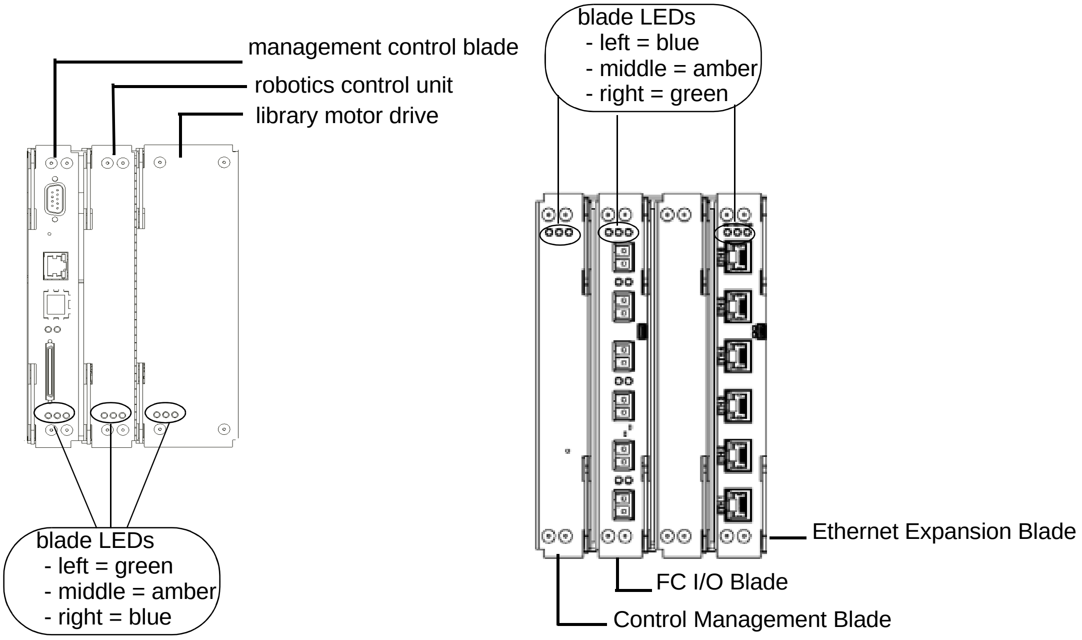
Interpreting Blade Status LEDs

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)
- I/O blade
- Robotics control unit (RCU)
- Library motor drive (LMD)

Figure 13 shows the locations and colors of the status LEDs on the five blades that can be in the library.

Figure 13 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 7 on page 85. For a description of how the blade status LEDs appear under normal conditions, see table 8 on page 86.

Table 7 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 8 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)
Amber	Solid off — no errors are detected; blade’s PIP 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.

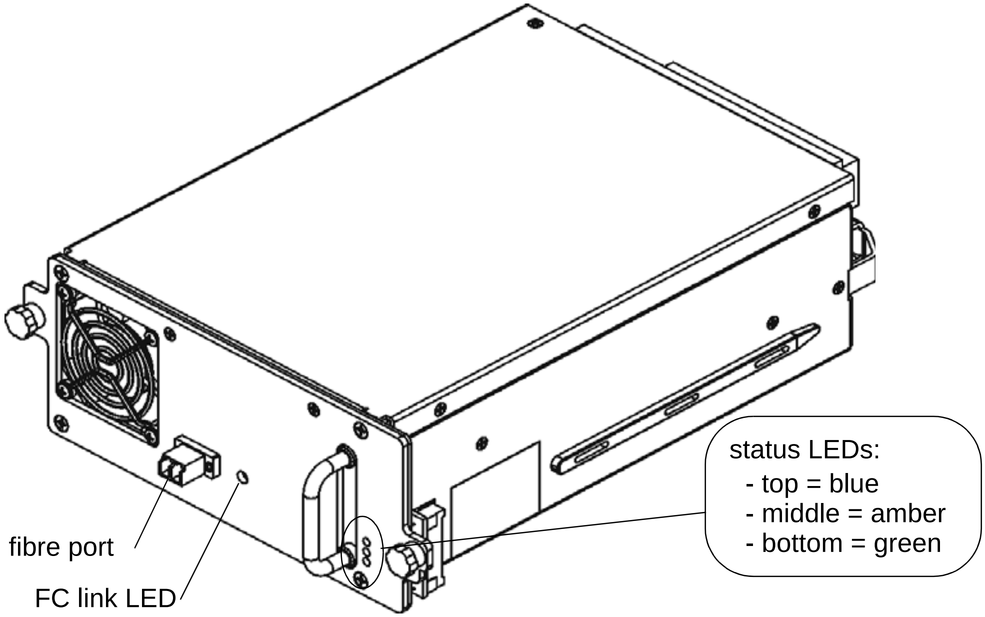
Interpreting Drive Status LEDs

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 9 on page 90 on page 133 are the same for Fibre Channel and SCSI drives in the UDS-2 drive sleds.

Figure 14 shows the locations of the status LEDs and the Fibre Channel link LED on the rear of a UDS-2 drive sled.

Figure 14 Rear View of Fibre Channel Drive Sled (UDS-2)



Note SDLT-600 Fibre drives do not have a Fibre Channel link LED.

Figure 15 shows the locations of the status LEDs and the Fibre Channel link LED on the rear of a UDS-3 drive sled.

Figure 15 Rear View of Fibre Channel Drive Sled (UDS-3 LTO-4 and LTO-5 Drives)

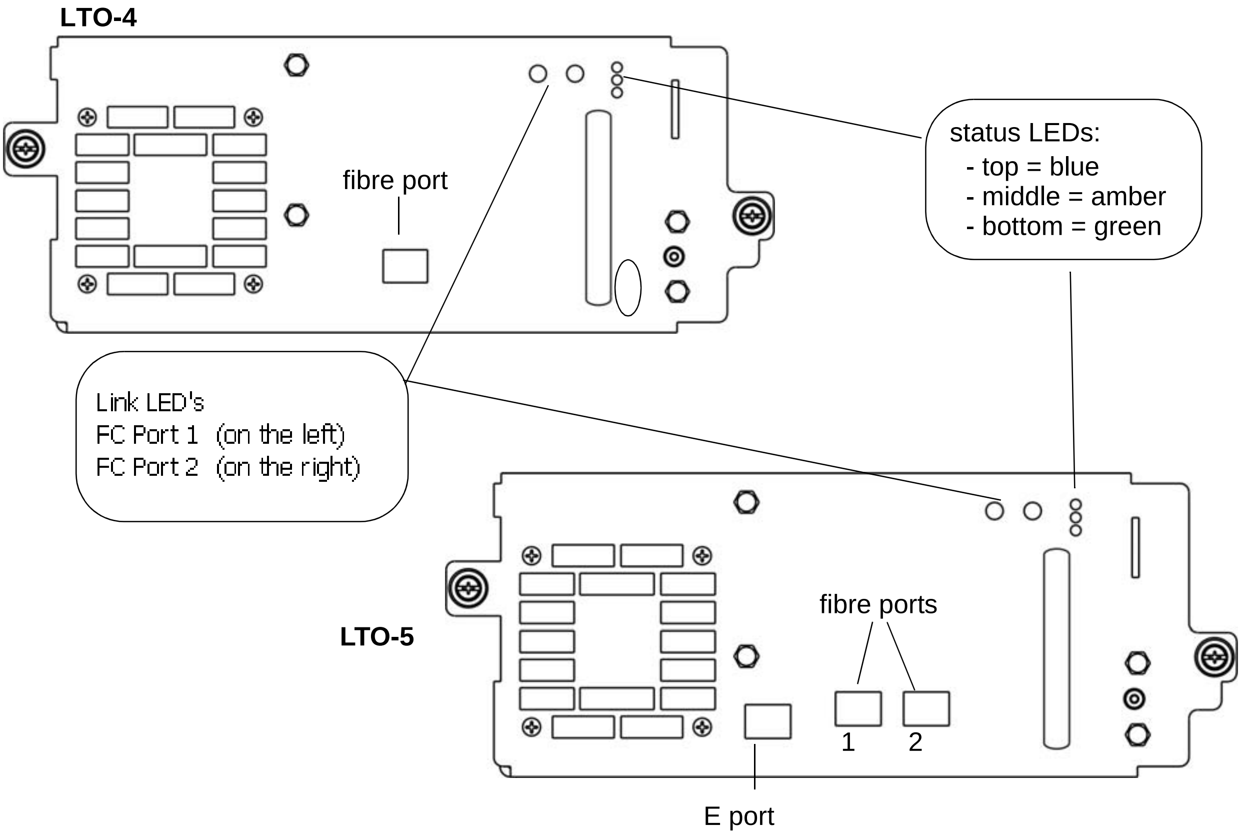


Table 9 on page 90 describes how to interpret the drive sled status LED activity that you might see on the rear of a UDS-2 or UDS-3 drive sled. For a description of how the blade status LEDs appear under normal conditions, see table 10 on page 91. For information about interpreting the drive link LED, see Drive Sled Fibre Channel Link LED on page 91.

Figure 16 shows Ethernet Connected Drive Sleds.

Figure 16 Ethernet Connected Drive Sleds

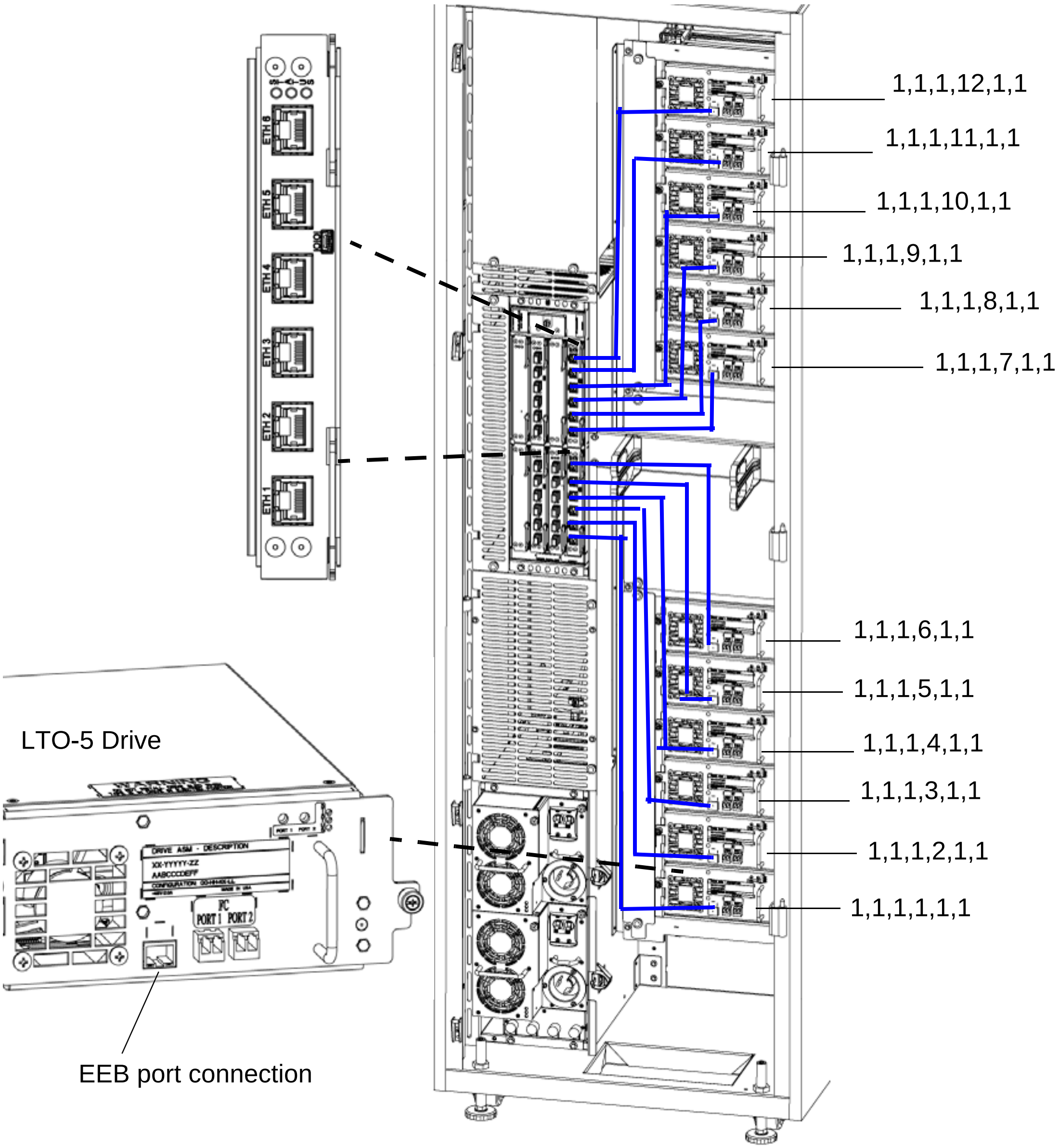


Table 9 Drive Sled Status LED States (UDS-2 and UDS-3)

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 10 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 14 on page 87 shows the location of the Fibre Channel link LED on the rear of the UDS-2 drive sled, and Figure 15 on page 88 shows the location of the Fibre Channel link LED on the rear of the UDS-3 drive sled.

Note SDLT-600 Fibre drives do not have a Fibre Channel link LED.

Table 11 describes how to interpret the Fibre Channel link LED activity that you might see on the rear of the UDS-2 drive sled. Table 12 on page 92 on page 135 describes the Fibre Channel link LED activity on the rear of the UDS-3 drive sled.

Table 11 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 12 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.

I/O Blade Fibre Port Link LED

The link LED for an 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 17 shows the locations of the I/O blade Fibre port link LEDs.

Figure 17 Locations - Colors of I/O Blade Fibre Port Link LEDs

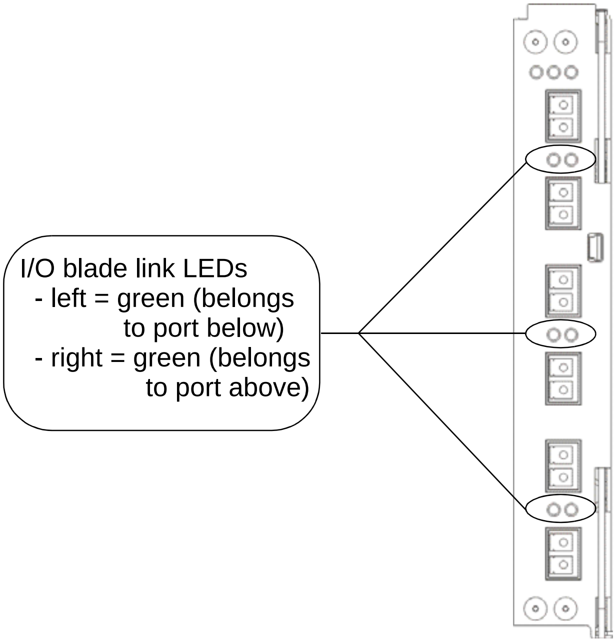

I/O blade link LEDs
- left = green (belongs to port below)
- right = green (belongs to port above)

Table 13 on page 94 describes how to interpret the link LED activity that you might see. There are two different models of I/O blade: 6404 and 7404. LED behavior varies based on which model is installed in the library.

Table 13 I/O Blade Link LED States

Blade Model	Possible Green LED States and Explanations
6404 2 gigabit/sec	• Solid on — the I/O blade has established a proper link and is ready to use. The drive detects light through the fiber optic cable. • Blinks slowly — the link is up and currently transporting commands. • Blinks rapidly — when the I/O blade is beginning to reboot or power up, all I/O blade link LEDs, along with the I/O blade's green status LED, blink rapidly to indicate that the blade is starting the Power On Self Test (POST). • Blinks with other link LEDs in a racetrack pattern — when all of the I/O blade link LEDs blink consecutively in a clockwise order, the blade is booting up. This pattern stops when the blade is powered and ready. If the pattern doesn't stop, the blade is unable to completely boot up. In this situation, follow the repair page instructions. • Solid off — the I/O blade does not detect light through the fiber optic cable.
7404 4 gigabit/sec	• Solid on — the 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 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 I/O blade, fibre port LEDs are off while the blade is booting up.

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 18 shows the locations and colors of the MCB Ethernet port LEDs.

Figure 18 Locations - Colors of MCB Ethernet Port LEDs

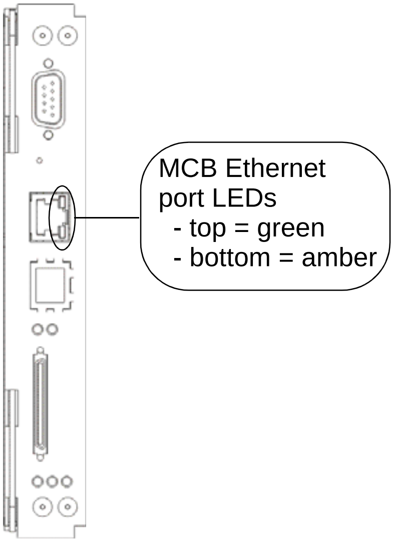


Table 14 describes how to interpret the Ethernet port LED activity that you might see.

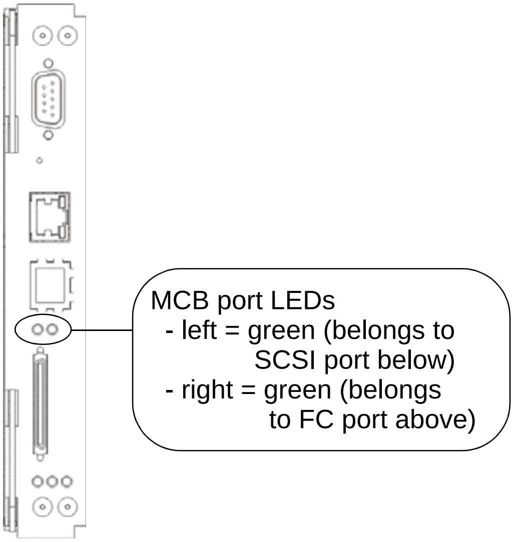
Table 14 Explanations of MCB Ethernet Port LED States

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 19 on page 97 shows the locations and colors of the LEDs.

Figure 19 Locations - Colors MCB FC / SCSI Port LEDs



MCB port LEDs
- left = green (belongs to SCSI port below)
- right = green (belongs to FC port above)

Interpreting LBX Terminator LEDs

The LBX terminator has two versions. Version 01 has four LEDs and Version 03 has 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 20 on page 98 shows the locations of the LEDs. Table 15 on page 98 describes how to interpret LED activity on the LBX terminator.

The terminator must be located in the LBX of the last expansion module, then the LED status should reflect the active modules correctly.

Figure 20 Locations of LBX Terminator LEDs (Version 01)

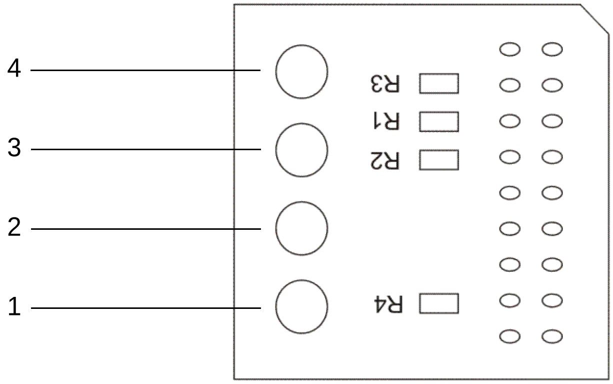


Table 15 LBX LED Version 01

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 21 shows the locations of the LEDs. Table 16 on page 100 describes how to interpret LED activity on the LBX terminator.

Figure 21 Locations of LBX Terminator LEDs (Version 03)

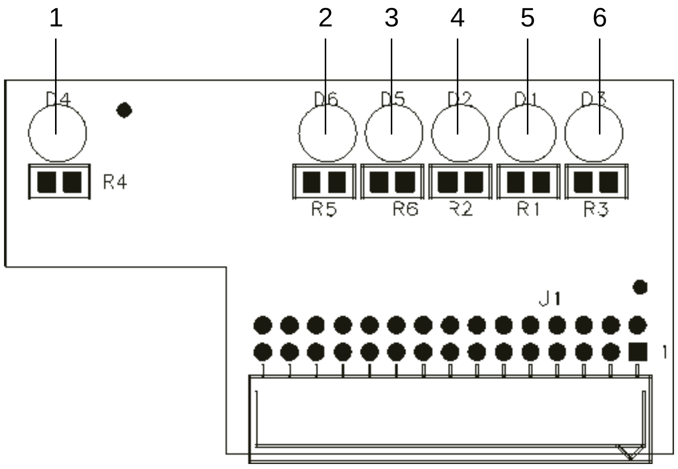


Table 16 LBX LED Version 03

LED On/Off Combinations						Explanation
1	2	3	4	5	6	
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.
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.

Interpreting Power Supply LEDs

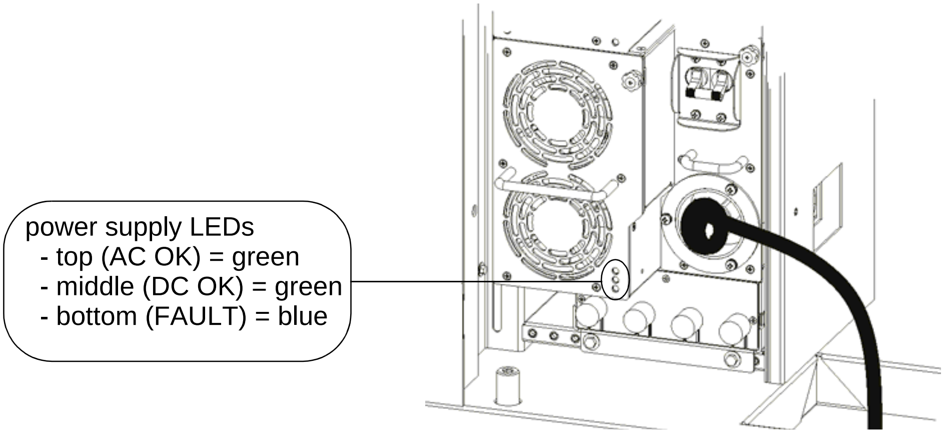
Power supply problems are reported in tickets. To physically identify a power supply, note the power supply number and module number in the ticket details. Modules can have up to two power supplies each. The top supply is #1 and the bottom supply is #2.

Note

The library can be physically configured to include up to seven expansion modules. If any of the expansion modules include drives, those modules also will have power supplies.

Figure 22 shows the locations and colors of the power supply LEDs.

Figure 22 Locations and Colors of Power Supply LEDs



power supply LEDs
- top (AC OK) = green
- middle (DC OK) = green
- bottom (FAULT) = blue

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

Table 17 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

Table 17 Explanation of Power Supply LED States (Continued)

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

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

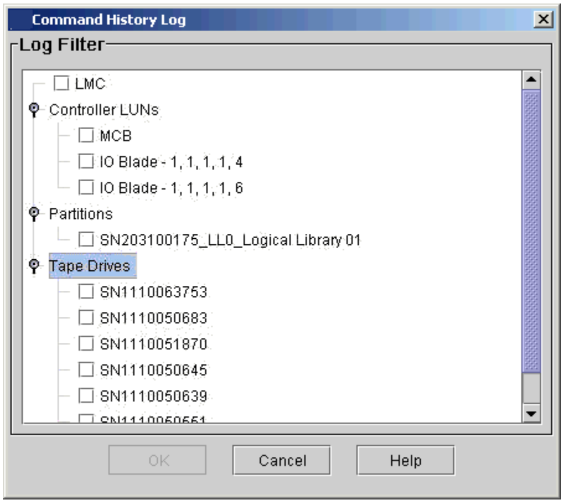
1 Log on as an administrator.

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.

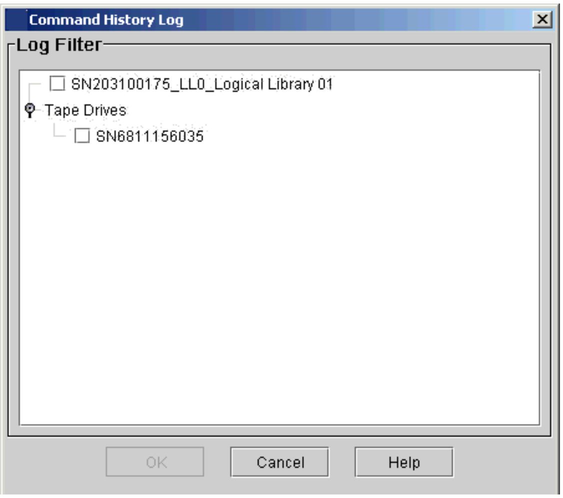
3 Click **Tools**→ **Command History Log**.

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.



- □ LMC
- Controller LUNs
  - □ MCB
  - □ IO Blade - 1, 1, 1, 1, 4
  - □ IO Blade - 1, 1, 1, 1, 6
- Partitions
  - □ SN203100175_LL0_Logical Library 01
- Tape Drives
  - □ SN1110063753
  - □ SN1110050683
  - □ SN1110051870
  - □ SN1110050645
  - □ SN1110050639
  - □ SN1110050661



□ SN203100175_LL0_Logical Library 01

Tape Drives

□ SN6811156035

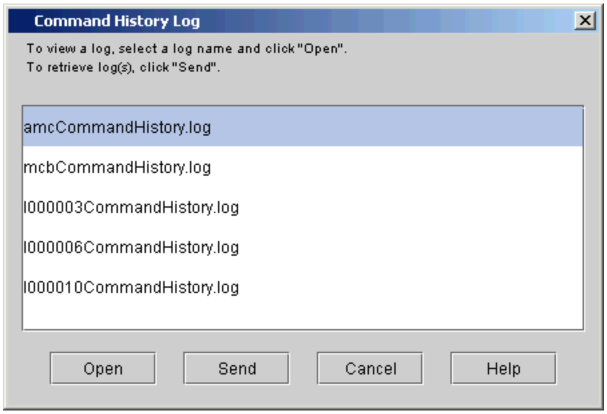
If logical serial number addressing is enabled on the **Physical Library** dialog box (**Setup**→ **Physical Library**), tape drives are listed according to their logical serial numbers. If logical serial number addressing is disabled, the drives are listed according to their physical serial numbers.

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.



To view a log, select a log name and click "Open".
To retrieve log(s), click "Send".

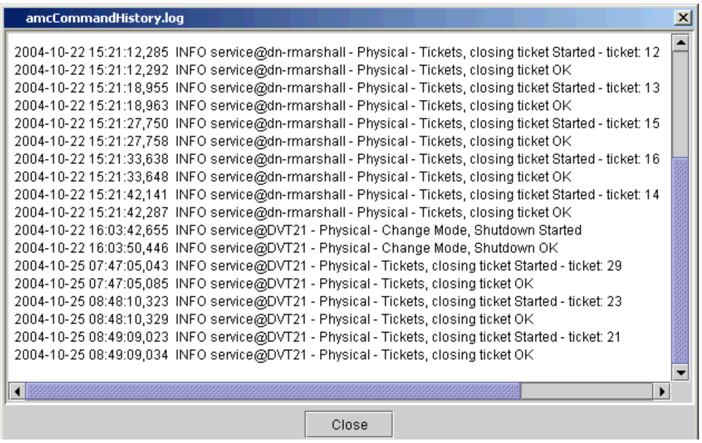
amcCommandHistory.log
mcbCommandHistory.log
l000003CommandHistory.log
l000006CommandHistory.log
l000010CommandHistory.log

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 106)

5 Click a log file to highlight it, and then click **Open**.

The contents of the log file appear.



```
2004-10-22 15:21:12,285  INFO service@dn-rmarshall - Physical - Tickets, closing ticket Started - ticket: 12
2004-10-22 15:21:12,292  INFO service@dn-rmarshall - Physical - Tickets, closing ticket OK
2004-10-22 15:21:18,955  INFO service@dn-rmarshall - Physical - Tickets, closing ticket Started - ticket: 13
2004-10-22 15:21:18,963  INFO service@dn-rmarshall - Physical - Tickets, closing ticket OK
2004-10-22 15:21:27,750  INFO service@dn-rmarshall - Physical - Tickets, closing ticket Started - ticket: 15
2004-10-22 15:21:27,758  INFO service@dn-rmarshall - Physical - Tickets, closing ticket OK
2004-10-22 15:21:33,638  INFO service@dn-rmarshall - Physical - Tickets, closing ticket Started - ticket: 16
2004-10-22 15:21:33,648  INFO service@dn-rmarshall - Physical - Tickets, closing ticket OK
2004-10-22 15:21:42,141  INFO service@dn-rmarshall - Physical - Tickets, closing ticket Started - ticket: 14
2004-10-22 15:21:42,287  INFO service@dn-rmarshall - Physical - Tickets, closing ticket OK
2004-10-22 16:03:42,655  INFO service@DVT21 - Physical - Change Mode, Shutdown Started
2004-10-22 16:03:50,446  INFO service@DVT21 - Physical - Change Mode, Shutdown OK
2004-10-25 07:47:05,043  INFO service@DVT21 - Physical - Tickets, closing ticket Started - ticket: 29
2004-10-25 07:47:05,085  INFO service@DVT21 - Physical - Tickets, closing ticket OK
2004-10-25 08:48:10,323  INFO service@DVT21 - Physical - Tickets, closing ticket Started - ticket: 23
2004-10-25 08:48:10,329  INFO service@DVT21 - Physical - Tickets, closing ticket OK
2004-10-25 08:49:09,023  INFO service@DVT21 - Physical - Tickets, closing ticket Started - ticket: 21
2004-10-25 08:49:09,034  INFO service@DVT21 - Physical - Tickets, closing ticket OK
```

Mailing and Saving Logs

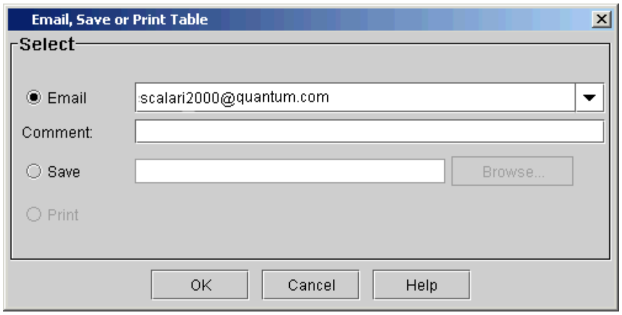
The **Send** button on the log-list view of the **Command History Log** dialog box enables you to send logs to e-mail addresses. If you are accessing the LMC from a remote client, **Send** also enables you to save the information to a file.

Note

- You can mail or save logs from a remote client. However, you cannot save logs from the library's touch screen.
- 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 164.

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.



Email, Save or Print Table

● Email: scalari2000@quantum.com

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 4

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:

- Configuring Screen Saver Preferences on page 255
- Working With Data Path Conditioning on page 257
- About the Configuration Record on page 259
- Setting Aisle Lights on page 261

For a brief overview of the LMC, see Library Management Console (LMC) on page 271.

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 142 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

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 capacity on demand (COD) or feature upgrade, such as when you want to enable the Drive Resource Utilization Reporting feature.
- 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.

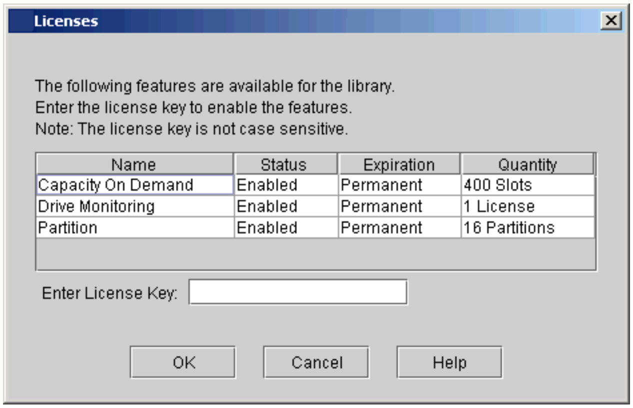
Note Authorized service personnel are involved in the first two situations. However, any administrator can activate additional storage slots.

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.



Licenses

The following features are available for the library.
Enter the license key to enable the features.
Note: The license key is not case sensitive.

Name	Status	Expiration	Quantity
Capacity On Demand	Enabled	Permanent	400 Slots
Drive Monitoring	Enabled	Permanent	1 License
Partition	Enabled	Permanent	16 Partitions

Enter License Key:

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

- The COD quantity is the number of slots licensed.
- The partition quantity is either 1 or 16. The only possible multiple number of partitions is 16.
- For features that are not licensed by quantity, such as the drive monitoring feature, **Quantity** is always set to 1.

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

Note You do not need to highlight the feature before you enter a license key.

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 or, if you are an end user, by contacting your inside sales representative.

5 Click **OK**.

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 112.

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.

A Library Managed Partition is like any other partition, except it is not visible to any backup applications or hosts. The LMP allows the library to be able to manage the partition, rather than the backup application managing the partition. The library uses the LMP to facilitate value-added features like MeDIA (automated data integrity checking routine). There can be only one LMP in the library.

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. The type of media determines the number of slots in the magazine. For example, an LTO magazine has six slots.
- 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 288.
- Drive — the read/write device for removable media.

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 partition consists of, at a minimum, one storage magazine and one drive. Neither the storage magazine nor the drive can be shared with another partition. Each partition is specific to a media type (for example, LTO-1, LTO-2) and a drive interface (for example, SCSI or Fibre). 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.

lthough the physical library can contain more than one media domain or drive domain, you cannot have a mix of domain types within a partition (for example, LTO and DLT). 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).

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 110.

Configuration controls, such as **FC Host**, **SCSI Host**, and **SNW** (Storage Networking) Host provide the means to permit host access to a particular partition. 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. When hosts are connected directly to drives, this is true exclusively. When the hosts connect through the MCB or an I/O blade, the library also has access to partition elements, such as drives and media. Each application can have a partition assigned to it. Each application uses its partition as if it were a dedicated physical library.

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

The media domain is the family of all cartridge types that can be stored in the same storage slot. Typically, a media domain represents all the generations and brands of a particular tape technology. Linear Tape Open (LTO), for example, has many generations and vendors, but all LTO cartridges are considered to exist in the same media domain.

Media Type

The media type is a particular generation of tape technology. Several media types can exist within one media domain. Using LTO again as an 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,and L5 to identify the LTO-1, LTO-2, LTO-3,LTO-4, and LTO-5 media types in a volume serial number.

Although the physical library can contain more than one media domain or drive domain, you cannot have a mix of domain types within a partition (for example, LTO and DLT). 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).

To create or modify a partition with mixed media, you must 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 a drive that does not have a matching 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 matching 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 18 explains the media type identifiers and assumptions.

Table 18 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
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

Table 18 Sampling of Media Type Identifiers (Continued)

Media Domain	Media Type	Identifier
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
DLT	SDLT-320	“S” as the last character in the barcode
DLT	SDLT-600	“2” as the last character in the barcode
DLT	DLT-S4	“S4” 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. For example, the library never runs a host command that moves an LTO cartridge from an LTO drive to a DLT storage slot, and vise versa.

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

Table 19 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 125.

Working with Library 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 Scalar i2000/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. For more information, refer to the *Scalar i6000 Installation Guide*.

Creating Partitions

You can create library partitions in three ways:

- By using the **Setup Wizard**
- **Automatic** mode
- **Manual** mode

The method you should choose depends on the circumstance and the level of control you want in allocating resources to the partition. In **Automatic** mode, the library assigns available system resources to create the number of partitions you specify. Automatic mode is not available if a partition already exists. **Manual** mode 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 With the Setup Wizard

If you are performing an initial configuration of your library, you can use the **Setup Wizard** to automatically create partitions using the available system resources. Using the **Setup Wizard** is part of the normal installation procedure for a library without I/O blades.

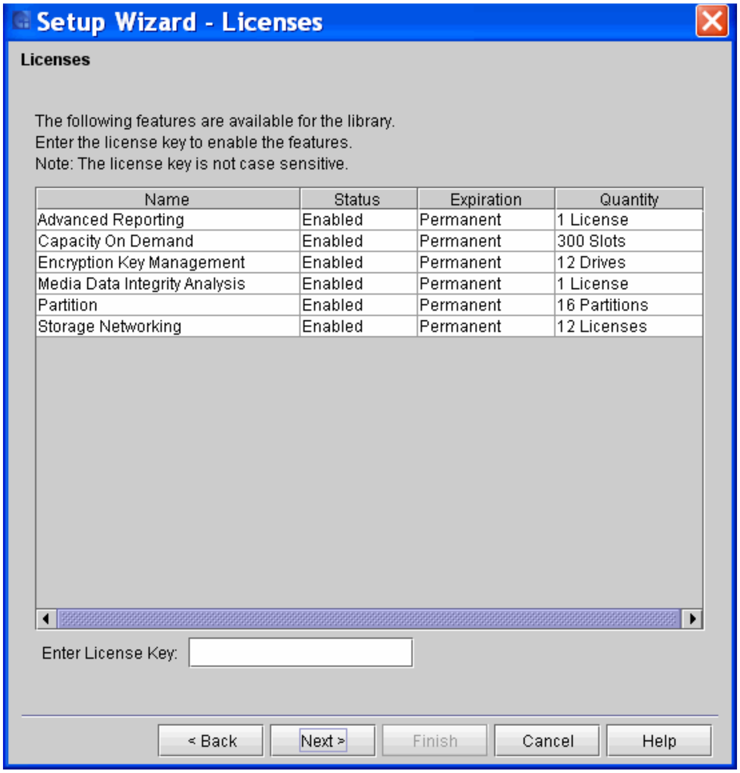
Note — **You should run the Setup Wizard *only* when you initially configure the library.**

At all other times, create partitions by using the **Partitions** command from the **Setup** menu.

1 Click **Setup > Setup Wizard**.

2 Click **Next**.

The **Setup Wizard - License** dialog box appears.



Setup Wizard - Licenses

Licenses

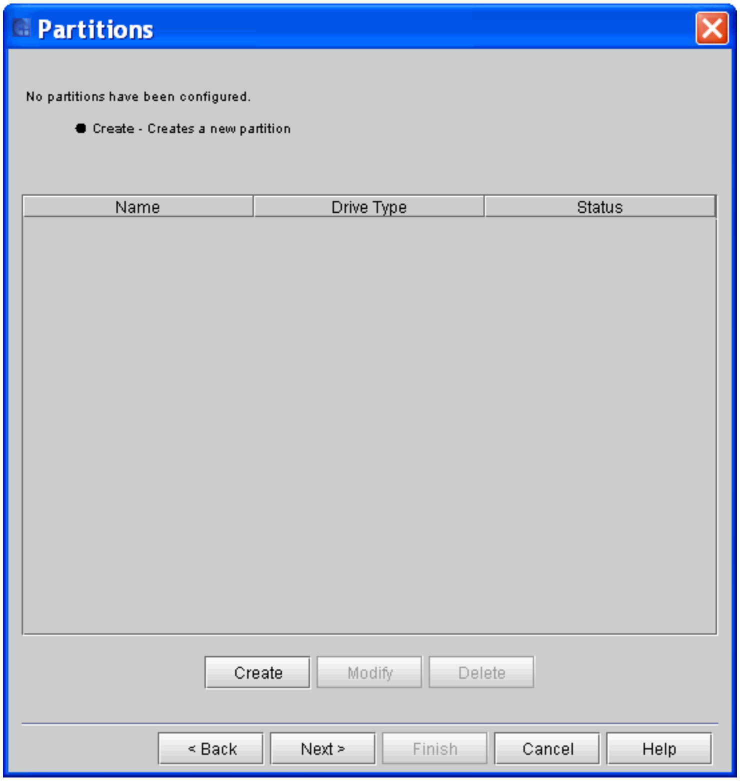
The following features are available for the library.
Enter the license key to enable the features.
Note: The license key is not case sensitive.

Name	Status	Expiration	Quantity
Advanced Reporting	Enabled	Permanent	1 License
Capacity On Demand	Enabled	Permanent	300 Slots
Encryption Key Management	Enabled	Permanent	12 Drives
Media Data Integrity Analysis	Enabled	Permanent	1 License
Partition	Enabled	Permanent	16 Partitions
Storage Networking	Enabled	Permanent	12 Licenses

Enter License Key:

3 Click **Next**.

The **Partitions** dialog box appears.



Partitions

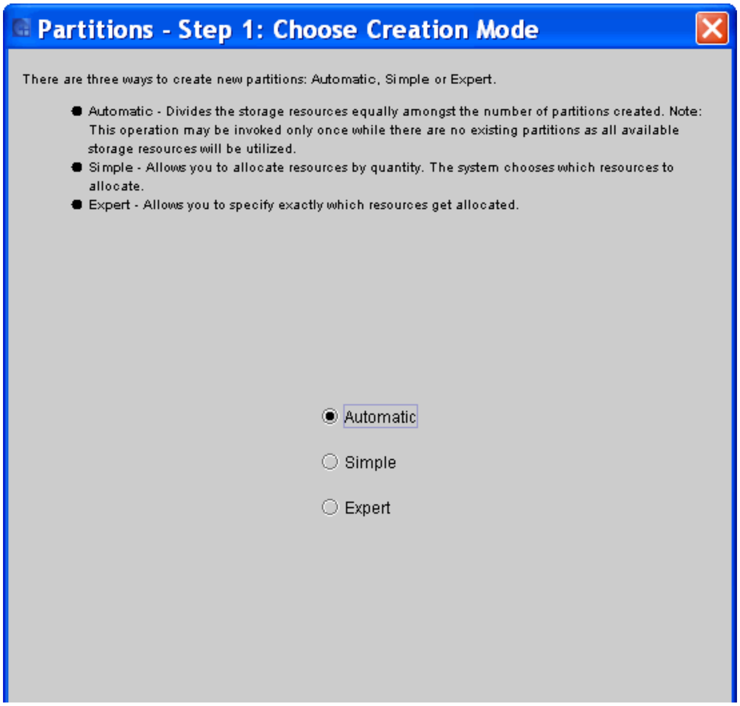
No partitions have been configured.

- Create - Creates a new partition

Name	Drive Type	Status

4 Click **Create.**

The **Partitions - Step 1: Choose Creation Mode dialog box** appears with **Automatic** selected by default.



There are three ways to create new partitions: Automatic, Simple or Expert.

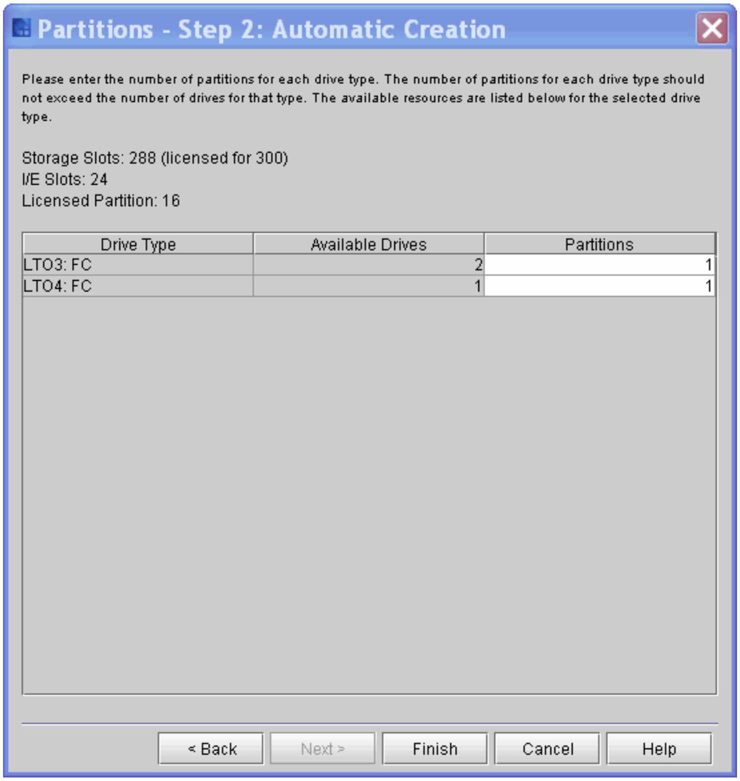
- Automatic - Divides the storage resources equally amongst the number of partitions created. Note: This operation may be invoked only once while there are no existing partitions as all available storage resources will be utilized.
- Simple - Allows you to allocate resources by quantity. The system chooses which resources to allocate.
- Expert - Allows you to specify exactly which resources get allocated.

● Automatic
○ Simple
○ Expert

Note The **Automatic** radio button will be disabled if there are partitions already configured.

5 Click **Next**.

The **Partitions - Step 2: Automatic Creation dialog box** appears.



Partitions - Step 2: Automatic Creation

Please enter the number of partitions for each drive type. The number of partitions for each drive type should not exceed the number of drives for that type. The available resources are listed below for the selected drive type.

Storage Slots: 288 (licensed for 300)
I/E Slots: 24
Licensed Partition: 16

Drive Type	Available Drives	Partitions
LTO3: FC	2	1
LTO4: FC	1	1

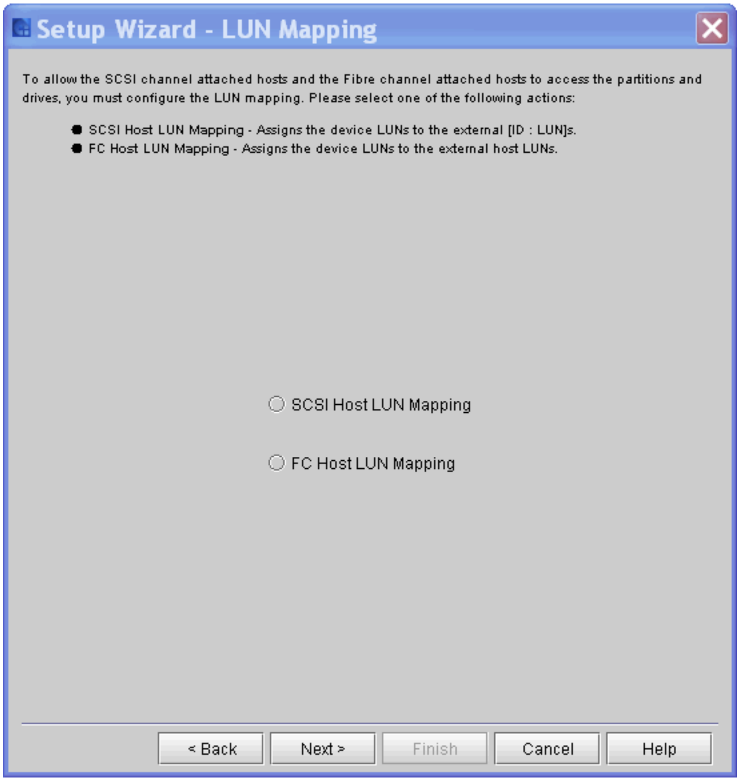
6 In the columns labeled **Partitions**, enter the number of partitions to create per media type.

7 Click **Finish.**

The partitions are created.

8 Click **Next.**

The **LUN Mapping** dialog box appears.



Setup Wizard - LUN Mapping

To allow the SCSI channel attached hosts and the Fibre channel attached hosts to access the partitions and drives, you must configure the LUN mapping. Please select one of the following actions:

- SCSI Host LUN Mapping - Assigns the device LUNs to the external [ID : LUN]s.
- FC Host LUN Mapping - Assigns the device LUNs to the external host LUNs.

○ SCSI Host LUN Mapping

○ FC Host LUN Mapping

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.
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 110.

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: **Simple** and **Expert** modes.

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.

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.

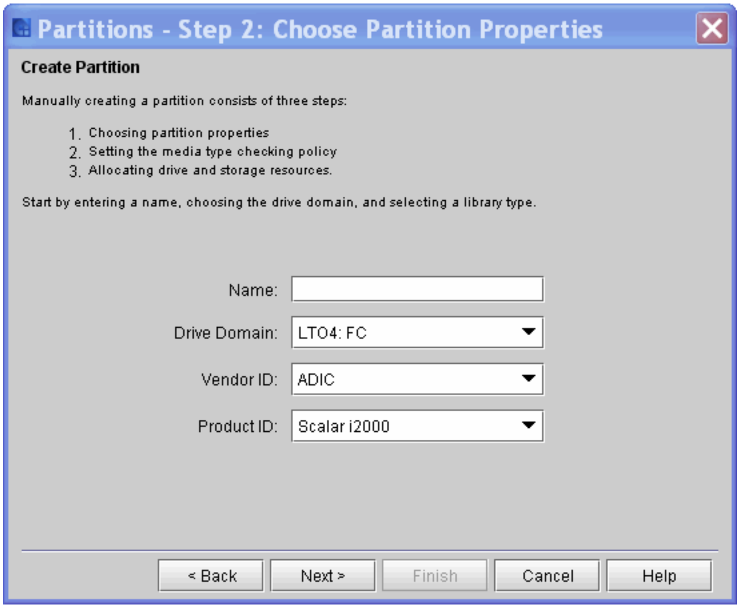
Note If you want to cancel the partition creation process, click **Close**. The **Close** button becomes unavailable after you click **Create** later in this procedure.

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.



Partitions - Step 2: Choose Partition Properties

Create Partition

Manually creating a partition consists of three steps:

1. Choosing partition properties
2. Setting the media type checking policy
3. Allocating drive and storage resources.

Start by entering a name, choosing the drive domain, and selecting a library type.

Name:

Drive Domain: LTO4: FC

Vendor ID: ADIC

Product ID: Scalar i2000

6 Configure the following settings:

- In the **Name** text box, type a name that describes the new partition.
- From the **Drive Domain** drop-down list, click the appropriate drive domain.
- From the **Vendor ID** list, select the vendor.
- 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.

7 To continue, click **Next**.

The **Partitions - Step 3: Choose Policy Settings** dialog box appears.

8 Configure 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.

⚠ 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 114.

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

  Enabling automatic drive cleaning allows the library to initiate drive cleaning each time a drive requests a cleaning operation. For automatic 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 214.

Note Automatic 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.

9 To continue, click **Next**.

The **Partitions - Step 4: Choose Resource Quantities** dialog box appears.

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

- Number of drives
- 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.

11 To continue, click **Next**.

The **Partitions - Summary Information** dialog box appears.

12 Verify that the parameters you set are correct.

13 To create the partition, click **Create**.

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

The **Partitions - Completed** dialog box appears.

14 Review the information to make sure it is correct.

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

16 Click **Finish**.

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

17 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.

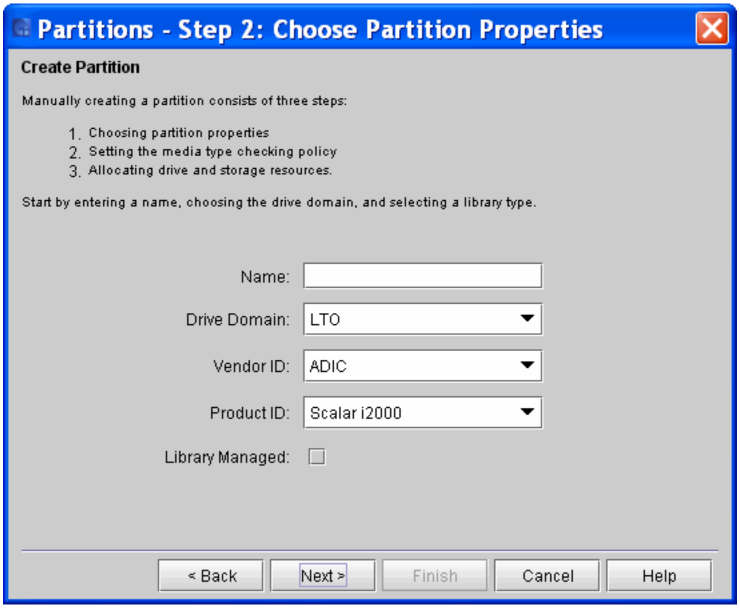
Note If you want to cancel the partition creation process, click **Close**. The **Close** button becomes unavailable after you click **Create** later in this procedure.

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.



Partitions - Step 2: Choose Partition Properties

Create Partition

Manually creating a partition consists of three steps:

1. Choosing partition properties
2. Setting the media type checking policy
3. Allocating drive and storage resources.

Start by entering a name, choosing the drive domain, and selecting a library type.

Name:

Drive Domain: LTO

Vendor ID: ADIC

Product ID: Scalar i2000

Library Managed: □

6 Configure the following settings:

- If you are creating a Library Managed Partition (LMP), do the following:

Note To create the LMP, you need to have completed the following tasks:

- Entered a Media Data Integrity Analysis license.
- Ensure that MeDIA enabled drives are installed in the library, and
- Ensure drives are connected to 7404 Fibre Channel Blade.

a Click the **Library Managed** check box.

The Name, Drive Domain, Vendor ID, and Product ID are greyed out, not allowing input. The Name field defaults to **Library Managed Partition**.

b Go to step 7.

- If you are not creating a LMP, do the following:

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

b From the **Drive Domain** drop-down list, click the appropriate drive type.

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

d 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.

7 To continue, click **Next**.

The **Partitions - Step 3: Choose Policy Settings** dialog box appears.

Note — If you are configuring the LMP, all fields are greyed out and do not allow input. Go to step 9.

8 Configure 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.

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 114

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

  Enabling automatic drive cleaning allows the library to initiate drive cleaning each time a drive requests a cleaning operation. For automatic 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 214.

Note Automatic 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.

9 To continue, click **Next**.

The **Partitions - Step 4: Select Drives** dialog box appears.

10 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.

11 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 288.

12 To continue, click **Next**.

The **Partitions - Step 5: Select Storage Slots** dialog box appears.

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

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

15 To continue, click **Next**.

The **Partitions - Step 6: Select I/E Slots** dialog box appears.

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

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

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

17 To continue, click **Next**.

Note Depending on whether Extended I/E is enabled, **Step 6: Select Extended I/E Slots** may appear. See the next step. If Extended I/E is not enabled, go to step 19.

To enable Extended I/E, go to **Setup > Physical Library**, and select the feature. For more information about Extended I/E, refer to Extended I/E Option on page 23

18 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.

The **Partitions - Summary Information** dialog box appears.

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

20 To create the partition, click **Create**.

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

The **Partitions - Completed** dialog box appears.

21 Review the information to make sure it is correct.

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

23 Click **Finish**.

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

24 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 and partition settings.

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**.

Note If the physical library is not offline, you receive a message that asks you whether you want to modify the partition, requiring the library to be taken offline. Click **Yes**. No host will be able to access the partition while the library is offline.

The **Partitions - Step 1: Choose Partition Properties** dialog box appears.

Note For LMP partitions, you can not modify these properties; all options will be 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 LMP partitions, you can not modify these properties; all options will be 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 114.

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

  Enabling automatic drive cleaning allows the library to initiate drive cleaning each time a drive requests a cleaning operation. For automatic 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 214.

Note Automatic 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.

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 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.

14 To continue, click **Next**.

The **Partitions - Step 5: Select I/E Slots** dialog box appears.

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

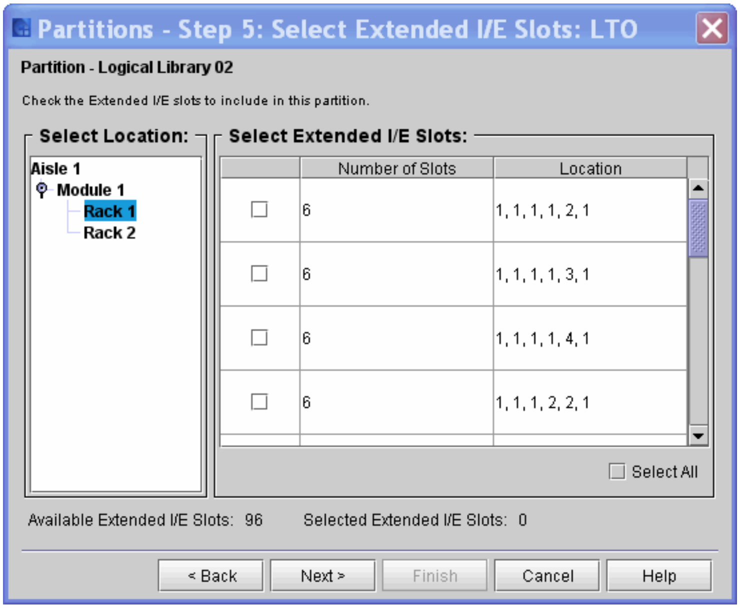
Make sure that you select the appropriate module because the library can have I/E stations in the control module and in expansion modules.

16 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.**

17 To continue, click **Next**.

If Extended I/E is configured, the **Extended I/E Slots** dialog box appears.



Partitions - Step 5: Select Extended I/E Slots: LTO

Partition - Logical Library 02

Check the Extended I/E slots to include in this partition.

Select Location:

- Aisle 1
  - Module 1
    - Rack 1
    - Rack 2

Select Extended I/E Slots:

	Number of Slots	Location
□	6	1, 1, 1, 1, 2, 1
□	6	1, 1, 1, 1, 3, 1
□	6	1, 1, 1, 1, 4, 1
□	6	1, 1, 1, 2, 2, 1

□ Select All

Available Extended I/E Slots: 96 Selected Extended I/E Slots: 0

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 library has I/O blades installed in it. If this dialog box does not appear, the **Partitions - Summary Information** dialog box appears instead. See Step 19.

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

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 I/O blade.

b 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 398, 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.

c 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 I/O blade can participate in drive firmware autoleveling operations. If you select drives that are not attached to I/O blades, they will not be updated during 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**.

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

The **Partitions - Completed** dialog box appears.

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.

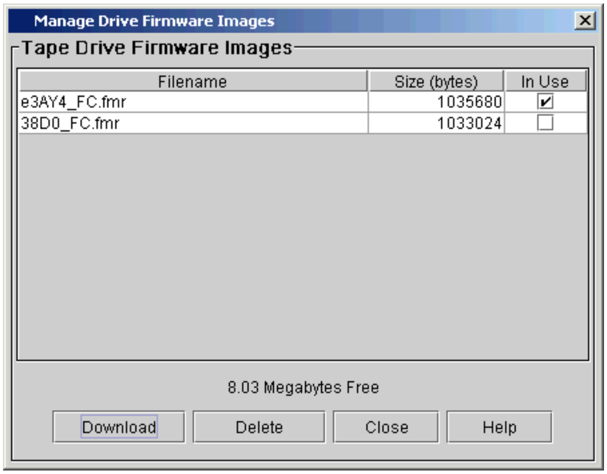
25 Click **Close**.

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.



Filename	Size (bytes)	In Use
e3AY4_FC.fmr	1035680	☑
38D0_FC.fmr	1033024	□

8.03 Megabytes Free

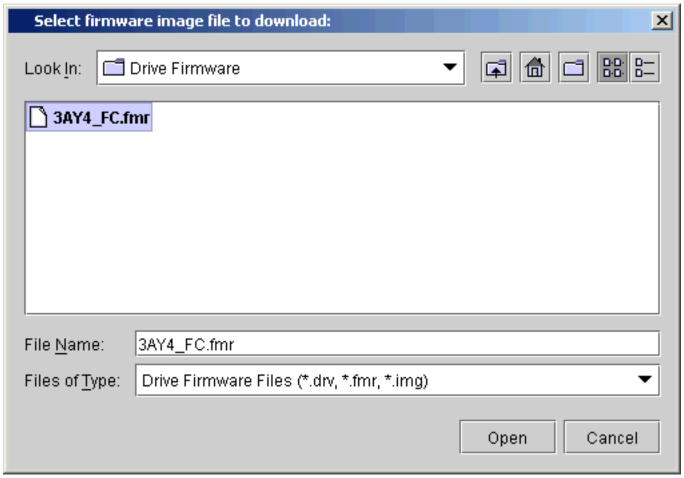
The library has enough space for 20 MB (with a maximum of 8 images) of drive firmware images. In this example, “8.03 Megabytes Free” indicates that 1.97 MB of space is currently unavailable. A check mark in the **In Use** column indicates one of the following conditions:

- 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.



Select firmware image file to download:

Look In: Drive Firmware

3AY4_FC.fmr

File Name: 3AY4_FC.fmr

Files of Type: Drive Firmware Files (*.drv, *.fmr, *.img)

3 Navigate to the location of the drive firmware image file (with either **a.drv**, **.fmr**, **.E**, or **.img** 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**.

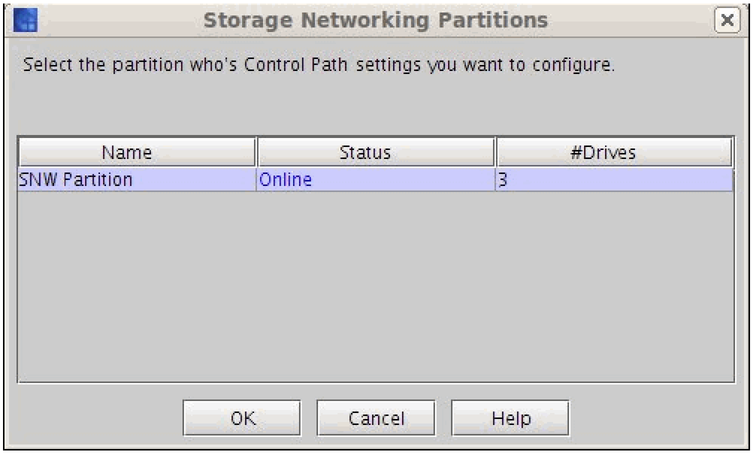
Selecting Storage Networking Partition for Configuration

Follow the steps below to select a partition and configure the control path.

1 Log on as an administrator.

2 From the main console, select **Setup > Partitions > Control Path**.

The **Storage Networking Partitions** dialog box appears.



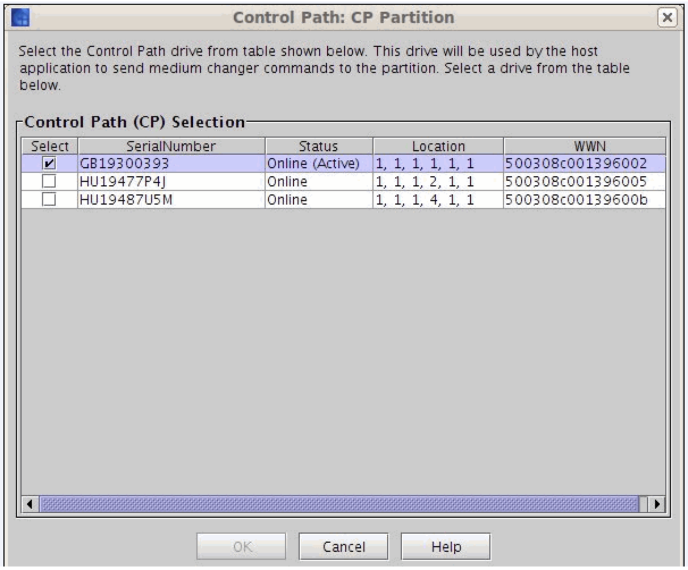
Storage Networking Partitions

Select the partition who's Control Path settings you want to configure.

Name	Status	#Drives
SNW Partition	Online	3

3 Highlight the partition you want to configure, and click **OK**.

The **Control Path** dialog box appears.



Control Path: CP Partition

Select the Control Path drive from table shown below. This drive will be used by the host application to send medium changer commands to the partition. Select a drive from the table below.

Control Path (CP) Selection

Select	SerialNumber	Status	Location	WWN
☑	GB19300393	Online (Active)	1, 1, 1, 1, 1, 1	500308c001396002
☐	HU19477P4J	Online	1, 1, 1, 2, 1, 1	500308c001396005
☐	HU19487U5M	Online	1, 1, 1, 4, 1, 1	500308c00139600b

4 Select the drive you want to configure as the control path.

The primary Control Path Drive you selected is highlighted in yellow.

5 Click **OK**.

Setting Up the Network Configuration

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

⚠ 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 159.

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 From the menu bar, click **Setup > Network Configuration**. Then, depending on whether IPv6 is enabled or disabled and the protocol of the network connection you want to configure:

- If IPv6 is disabled, the IPv4 **Network Configuration** dialog box appears.

  Proceed to Setting up IPv4 Network Configuration on page 146.

- If IPv6 is enabled, but you want to configure an IPv4 connection, click **IPv4 Configuration** on the Network Configuration submenu to display the IPv4 **Network Configuration** dialog.

  Proceed to Setting up IPv4 Network Configuration on page 146

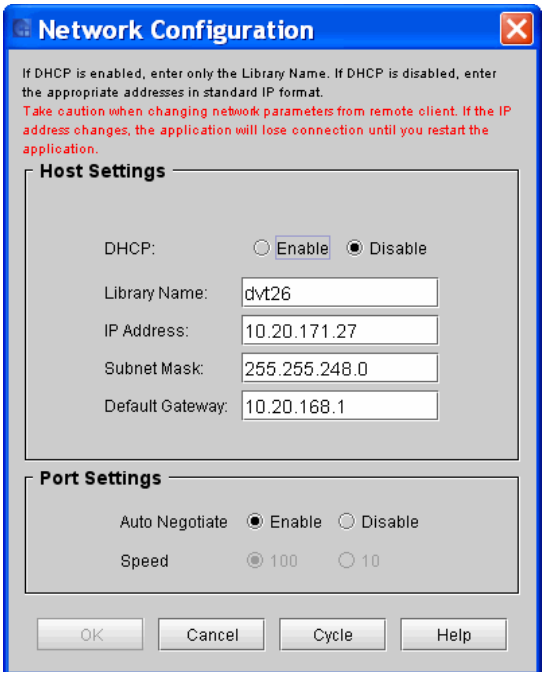
- If IPv6 is enabled and you want to configure an IPv6 connection, click **IPv6 Configuration** on the Network Configuration submenu to display the IPv6 **Network Configuration** dialog.

  Proceed to Setting up IPv6 Network Configuration on page 148.

Note The Network Configuration submenu only appears if you have enabled IPv6 for the physical library, as described in Setting Up Policies for the Physical Library on page 159.

Setting up IPv4 Network Configuration

After completing steps 1 through 3 of Setting Up the Network Configuration on page 145, the IPv4 **Network Configuration** dialog box appears.



Network Configuration

If DHCP is enabled, enter only the Library Name. If DHCP is disabled, enter the appropriate addresses in standard IP format.

Take caution when changing network parameters from remote client. If the IP address changes, the application will lose connection until you restart the application.

Host Settings

DHCP: ○ Enable ● Disable

Library Name: dvt26

IP Address: 10.20.171.27

Subnet Mask: 255.255.248.0

Default Gateway: 10.20.168.1

Port Settings

Auto Negotiate ● Enable ○ Disable

Speed ● 100 ○ 10

1 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, 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.
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 Mbps or 100 Mbps). **Speed** options are available only if **Auto Negotiate** is disabled.

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

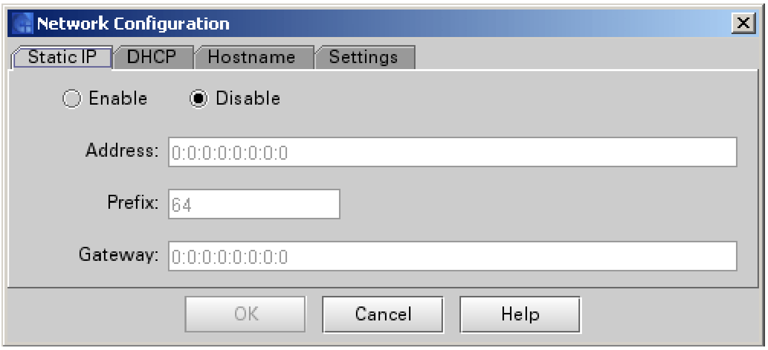
2 Make the appropriate network configuration changes, and then click **OK**.

A message appears that informs you that network connectivity will be lost temporarily, and asks whether you want to proceed.

3 Click **Yes**.

Setting up IPv6 Network Configuration

After completing steps 1 through 3 of Setting Up the Network Configuration on page 145, the **Static IP** tab of the IPv6 **Network Configuration** dialog box appears:



○ Enable ● Disable

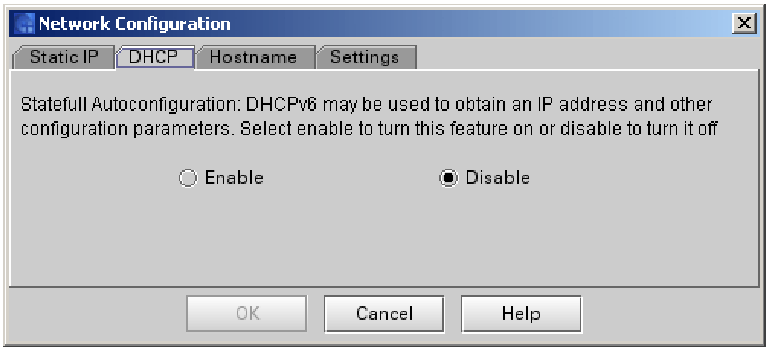
Address: 0:0:0:0:0:0:0:0

Prefix: 64

Gateway: 0:0:0:0:0:0:0:0

1 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.

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

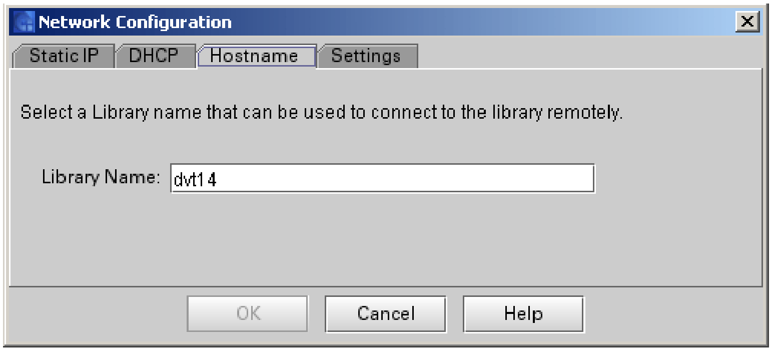


Statefull Autoconfiguration: DHCPv6 may be used to obtain an IP address and other configuration parameters. Select enable to turn this feature on or disable to turn it off

○ Enable ● Disable

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

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

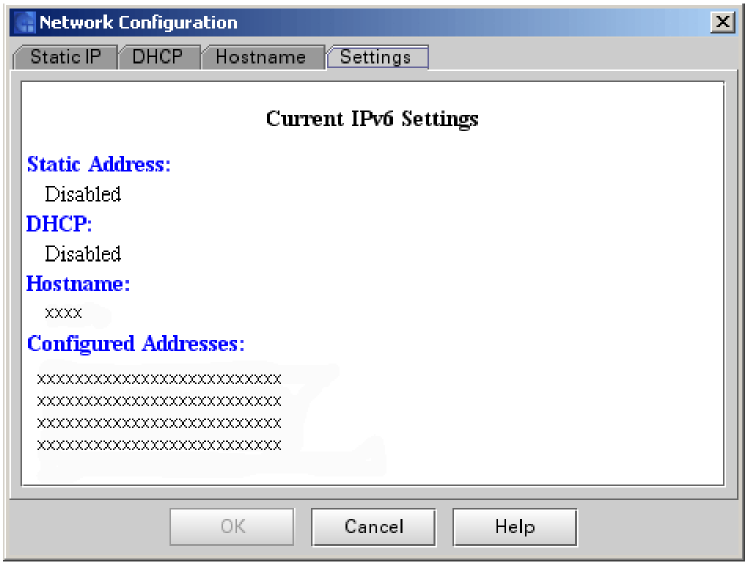


Select a Library name that can be used to connect to the library remotely.

Library Name: dvt14

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

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



Current IPv6 Settings

Static Address:
Disabled

DHCP:
Disabled

Hostname:
xxxx

Configured Addresses:
xxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxx

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

8 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.

9 Click **Yes**.

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 257.

Port Configuration

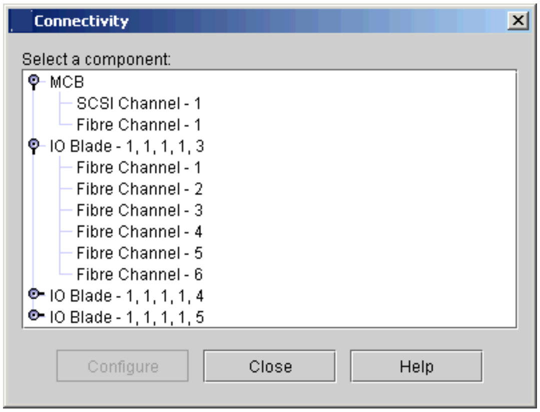
Use the **Port Configuration** command to view and configure connectivity parameters for FC ports. **Port Configuration** gives you access to the FC ports on the MCB and on the I/O blades.

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**→ **Connectivity**→ **Port Configuration**.

The **Connectivity** dialog box appears. All components that provide FC and SCSI ports appear in the dialog box if they are detected. You cannot configure settings for the SCSI port on the MCB.

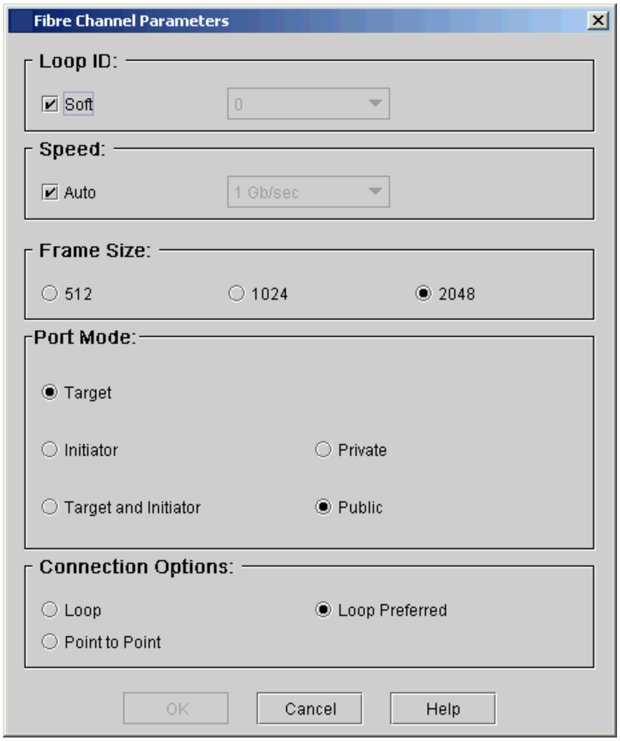


The example above shows expanded levels for “MCB” and “IO Blade - 1,1,1,1,3”.

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 either the MCB or an I/O blade, the **Fibre Channel Parameters** dialog box appears.



Fibre Channel Parameters

Loop ID:

☑ Soft 0

Speed:

☑ Auto 1 Gb/sec

Frame Size:

○ 512 ○ 1024 ● 2048

Port Mode:

● Target

○ Initiator ○ Private

○ Target and Initiator ● Public

Connection Options:

○ Loop ● Loop Preferred

○ Point to Point

You can configure two settings for an MCB connection and 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, clear the **Auto** check box and use a setting from the drop-down list. Because this setting is not configurable on the MCB, the **Speed** area does not appear on the **Fibre Channel Parameters** dialog box when configuring the MCB FC port. The MCB FC port speed is always 1 Gb/sec.

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 20 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 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. 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:

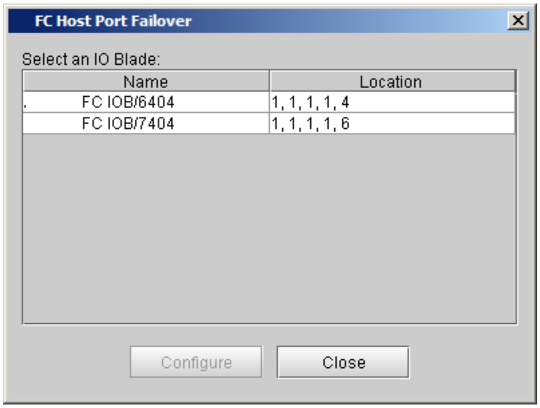
1 Log on as an administrator.

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 FC Host on page 184.

4 Click **Setup**→ **Connectivity**→ **FC Host Port Failover**.

The **FC Host Port Failover** dialog box appears, showing all the I/O blades found in the library. Each blade is identified by name and by location.

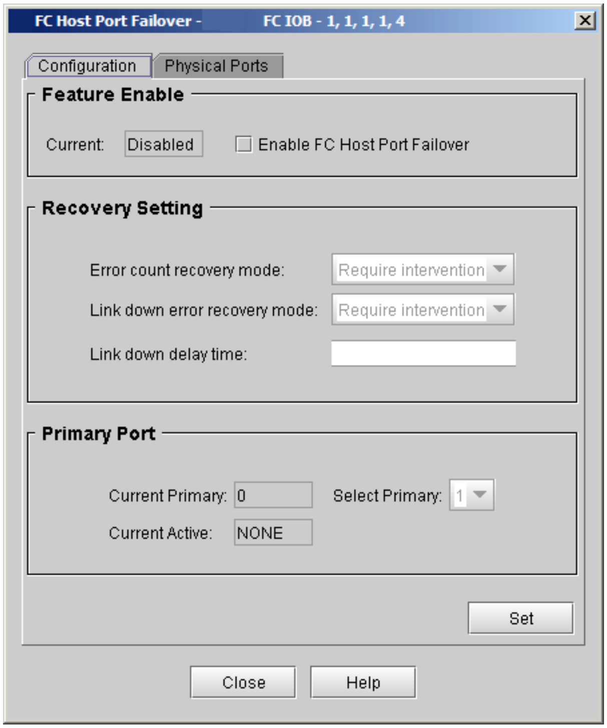


Select an IO Blade:

Name	Location
FC IOB/6404	1, 1, 1, 1, 4
FC IOB/7404	1, 1, 1, 1, 6

5 Click a blade to highlight it, and then click **Configure**.

The **FC Host Port Failover** dialog box appears



FC Host Port Failover - FC IOB - 1, 1, 1, 1, 4

Feature Enable

Current: Disabled

☐ Enable FC Host Port Failover

Recovery Setting

Error count recovery mode: Require intervention

Link down error recovery mode: Require intervention

Link down delay time:

Primary Port

Current Primary: 0

Select Primary: 1

Current Active: NONE

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**.

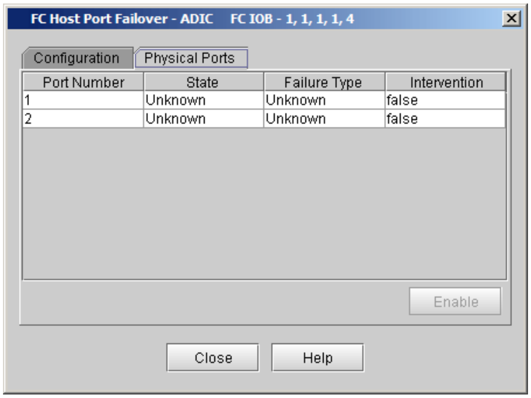
    If your configuration has errors, a warning message appears.

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.

1 On the **FC Host Port Failover** dialog box, click the **Physical Ports** tab.



Port Number	State	Failure Type	Intervention
1	Unknown	Unknown	false
2	Unknown	Unknown	false

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.

2 Click the port you want to enable.

3 Click **Enable**.

Note **Enable** is available only if the port is disabled.

4 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:

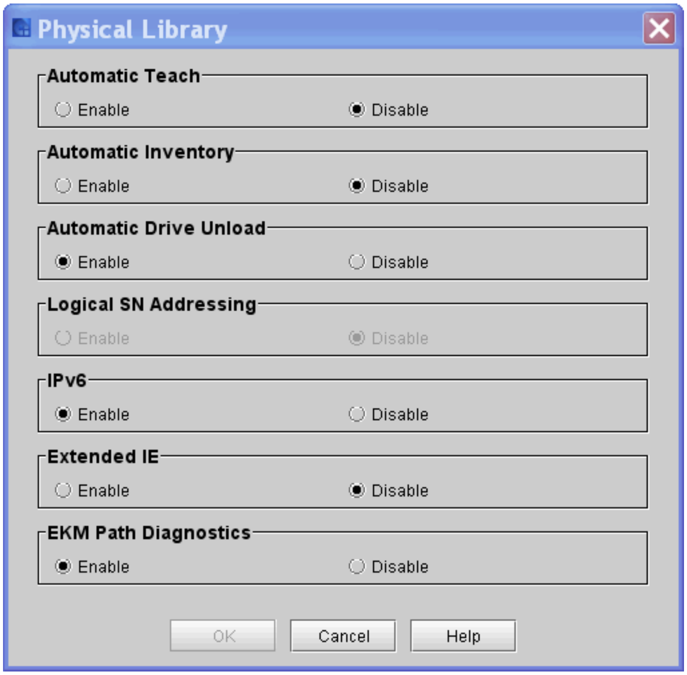
Enabling or disabling...	Specifies whether the library...
Automatic Teach	robotic assembly will be automatically calibrated and, if necessary, configured each time the power cycles off and on, or when the library door is opened and closed.
Automatic Inventory	will scan inventory automatically each time the power cycles off and on, or when the library door is opened and closed.
Automatic Drive Unload	will automatically eject cartridges from drives when a move media command is received from a data host.
Logical SN Addressing	will use logical serial number addressing for all drives in the library. Only CSEs can enable or disable logical serial number addressing.
IPv6	will support the configuration of IPv6 network settings.
Extended I/E	will enable extended import/export slot configurations. Extended I/E configurations increase the I/E slot count with storage slots that will be reported to hosts as I/E slots.
EKM Path Diagnostics	will enable EKM server connectivity diagnostics.

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**→ **Physical Library**.

The **Physical Library** dialog box appears.



Physical Library

Automatic Teach
○ Enable ● Disable

Automatic Inventory
○ Enable ● Disable

Automatic Drive Unload
● Enable ○ Disable

Logical SN Addressing
○ Enable ● Disable

IPv6
● Enable ○ Disable

Extended IE
○ Enable ● Disable

EKM Path Diagnostics
● Enable ○ Disable

4 Select **Enable** in the **Automatic Teach** area to schedule automatic calibration and configuration of the robotic assembly when the library powers up or when the library door is opened and closed.

Automatic Teach is disabled by default.

5 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.

Automatic Inventory is disabled by default.

6 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.

7 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 Enabling **IPv6** adds a submenu to the **Network Configuration** command on the **Setup** menu that you use to display the IPv4 or IPv6 **Network Configuration** dialog.

IPv6 is disabled by default.

8 Select **Enable** in the **Extended I/E** area to enable the Extended I/E feature.

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 Extended I/E Option on page 23

9 Select **Enable** in the **EKM Path Diagnostics** area to enable EKM background diagnostics.

Background EKM Path Diagnostics are disabled by default for Q-EKM configurations; Background EKM Path Diagnostics are enabled by default for SKM configurations.

Note: Enabling EKM Path Diagnostics activates regularly scheduled Encryption Key Server Path Diagnostics to inform of Key Server connectivity or operational issues. If SKM is configured, the background diagnostic should always be enabled as the library can hereby monitor SKM server status and report of issues as soon as they arise.

10 When finished, click **OK**.

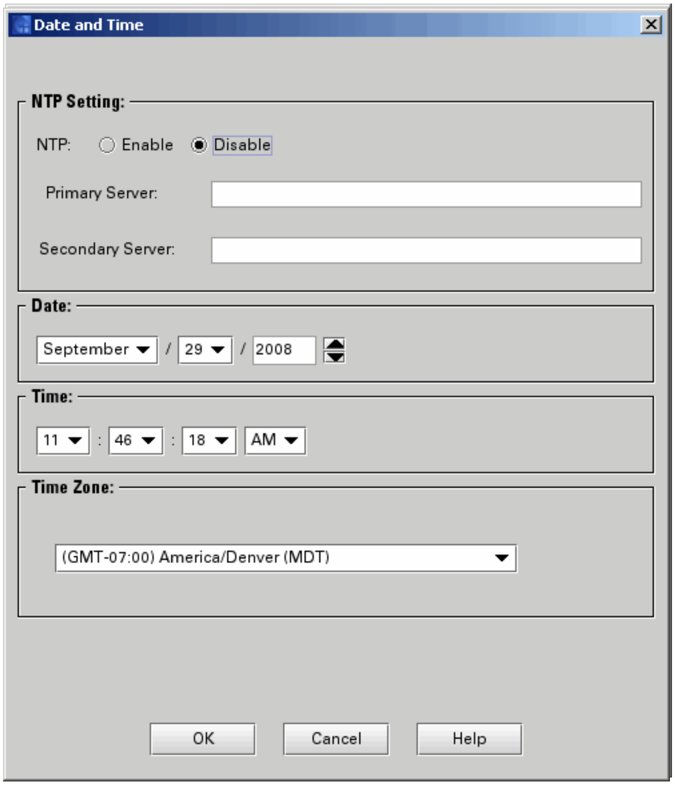
Specifying the Date and Time

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 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.



Date and Time

NTP Setting:

NTP: ○ Enable ● Disable

Primary Server:

Secondary Server:

Date:

September / 29 / 2008

Time:

11 : 46 : 18 AM

Time Zone:

(GMT-07:00) America/Denver (MDT)

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.**

  - 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). You have the option of using one or two IP addresses. Go to step 7.

    - If the DNS Server has been configured through the LMC (**Setup > DNS Configuration**), type the valid alpha/numeric IP Addresses that are accessible from the library. You have the option of using one or two IP addresses. 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.

Note 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.

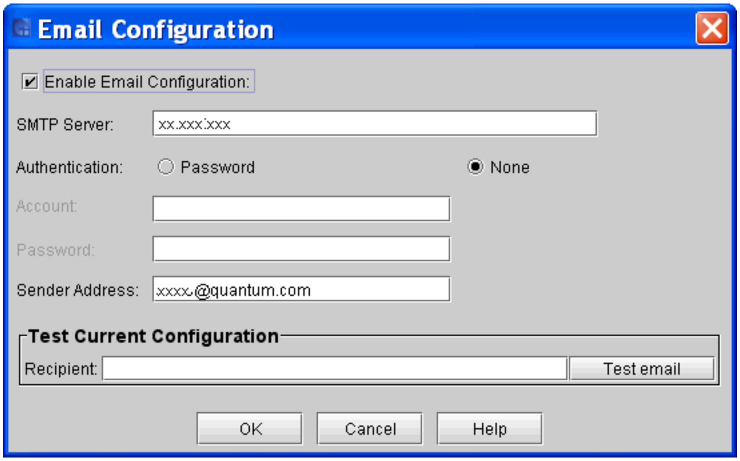
8 Click **OK**.

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
- Testing the Current E-Mail Configuration



Email Configuration

☑ Enable Email Configuration:

SMTP Server: xx.xxx.xxx

Authentication: ○ Password ● None

Account:

Password:

Sender Address: xxxx@quantum.com

Test Current Configuration

Recipient:

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. If you type, for example, "scalari6000", the library appends the domain information (for example, "@mycompany.com"). If you type, for example, "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 “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.
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 164.

Table 21 describes the severity levels for which the library can send notifications if e-mail addresses are set up appropriately to receive them.

Table 21 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.
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 Understanding E-mail Notifications on page 41.

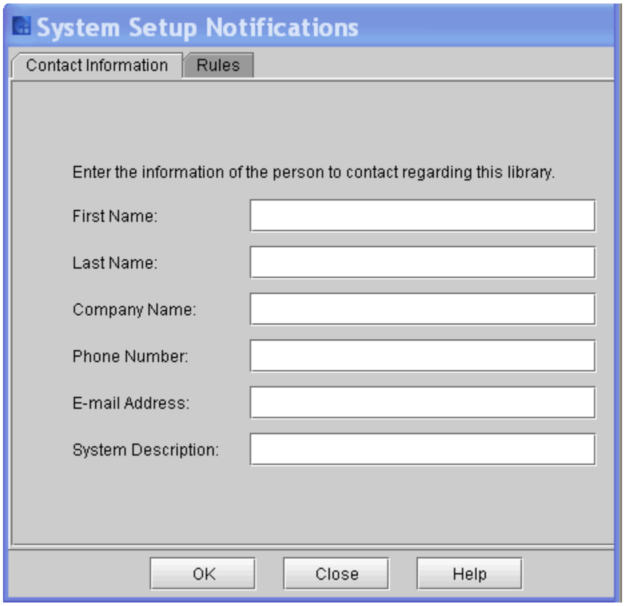
To set up e-mail recipients for notifications, perform the following steps:

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**→ **Notification**→ **System Setup**.

The **System Setup Notification** dialog box appears with the **Contact Information** tab displayed.



System Setup Notifications

Enter the information of the person to contact regarding this library.

First Name:

Last Name:

Company Name:

Phone Number:

E-mail Address:

System Description:

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.

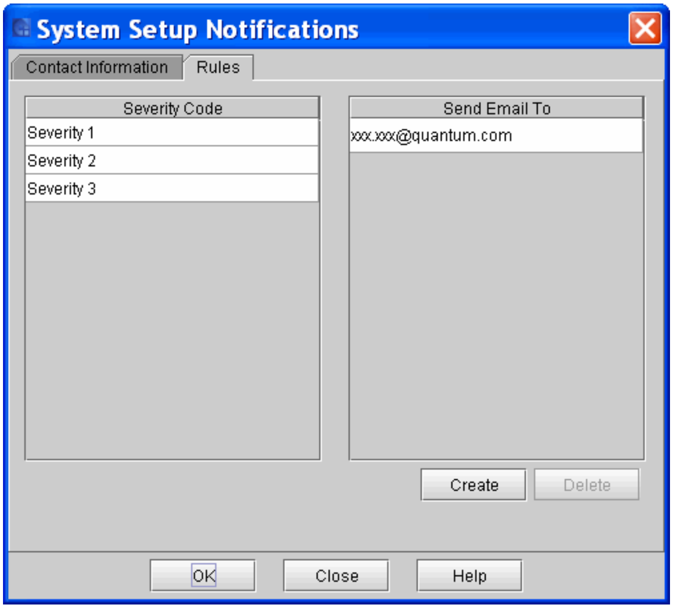
8 Click **Close**.

9 Setup 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.



Severity Code	Send Email To
Severity 1	xxx.xxx@quantum.com
Severity 2	
Severity 3	

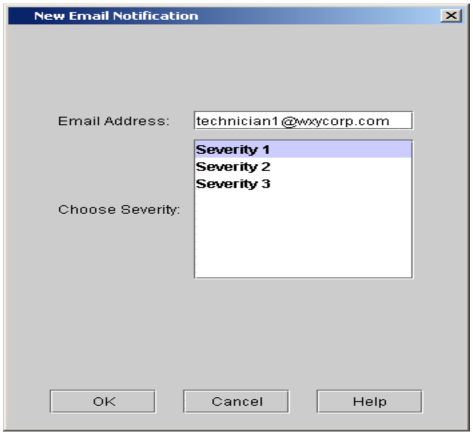
This dialog box shows all notification recipients that are set up currently in the LMC. By default, the only e-mail address to which the library sends e-mail notifications (severity level 1 [Failed] issues only) is techsup@quantum.com (Quantum technical support), as shown in this **Notification** dialog 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.
- 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.



Email Address: technician1@wxycorp.com

Choose Severity: Severity 1
Severity 2
Severity 3

11 In the **Email Address** text box, type the e-mail address that you want to receive 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 After you finish setting up all notifications, click **OK**.

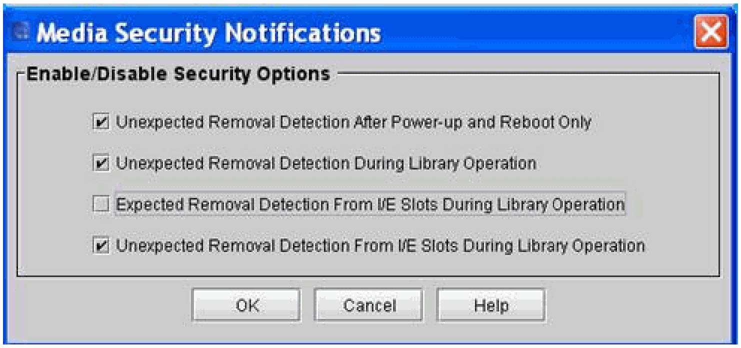
Setting Up Media Security Notifications

Once the Media Security Notification is set up and the physical library allows automatic inventory, you are notified when media is moved in or out of your library, either intentionally or unintentionally. Follow the steps below to set media security notification.

1 Logon as administrator.

2 Click **Setup > Notifications > Media Security**.

The **Media Security Notifications** dialog box appears.



Media Security Notifications

Enable/Disable Security Options

☑ Unexpected Removal Detection After Power-up and Reboot Only

☑ Unexpected Removal Detection During Library Operation

□ Expected Removal Detection From I/E Slots During Library Operation

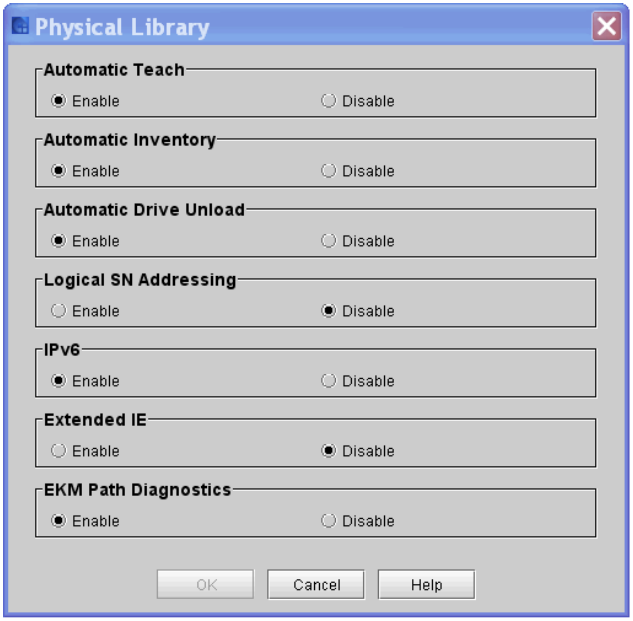
☑ Unexpected Removal Detection From I/E Slots During Library Operation

3 Check the box to the left of your media security notification choice.

4 Click **OK**.

5 From the main console, select **Setup > Physical Library**.

The **Physical Library** dialog box appears.



Automatic Teach
● Enable ○ Disable

Automatic Inventory
● Enable ○ Disable

Automatic Drive Unload
● Enable ○ Disable

Logical SN Addressing
○ Enable ● Disable

IPv6
● Enable ○ Disable

Extended IE
○ Enable ● Disable

EKM Path Diagnostics
● Enable ○ Disable

6 For **Automatic Inventory**, click **Enable**.

7 Click **OK**.

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→ Device→ IDs** command is available while viewing a partition. Use this command to set the SCSI ID for a SCSI-attached drive or the Loop ID for a Fibre-attached drive. All hosts that view the drive will see the same SCSI ID associated with the drive.

The **Setup→ Device→ Access** command gives you access to the **Channel Zoning**, **SCSI Host**, **FC Host**, **SNW Host**, **SNW Drives**, and **LUN Mapping Wizard** commands, which are available while viewing the physical library.

- Use the **Channel Zoning** command to restrict host access to particular I/O blade ports.
- Use the **SCSI Host** and **FC Host** commands to configure access to partition accessors and drives on a per-host basis. If you have connected your host to either the FC port or the SCSI port on the MCB, or to a port on one of the I/O blades, you must map the appropriate partitions by using either the **SCSI Host** command or 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 Host command to create, modify or delete access to the Storage Networking (SNW) drives configured in the library.
- Use the SNW Drives command to select the drives you want managed by the Storage Networking (SNW) feature. The drives selected can be configured so client hosts can be granted or denied access. Only HP LTO-5 generation or later drives are supported. Each drive selected will consume a SNW license.
- Use the LUN Mapping Wizard command to set up LUN Mapping for your fiber channel hosts

If you have not otherwise restricted access, **SCSI Host** has full control of all LUNs on all FC and SCSI channels, up to an overall system total of 2,048. SCSI hosts can configure access at the LUN-level for an overall system total of up to 2,048 LUNs.

If you have not otherwise restricted access, **FC Host** has full control of all LUNs on all FC and SCSI channels. Each FC host can be configured to access a maximum of 255 LUNs, up to an overall system total of 2,048.

Device IDs

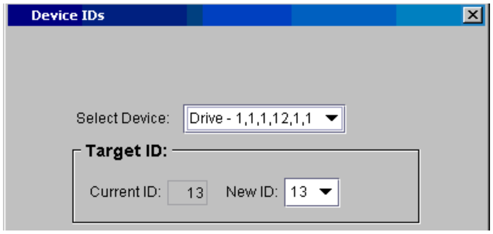
From a partition, you can change the SCSI ID for a SCSI-attached drive or the Loop ID for a Fibre-attached drive. For example, the default SCSI ID for a drive that you are installing might conflict with the assigned SCSI ID of an existing drive. You might be using an application that expects to communicate 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→ Device→ IDs**.

The **Device IDs** dialog box appears. (The following two examples show the SCSI version of the **Device IDs** dialog box, and then the FC version.)

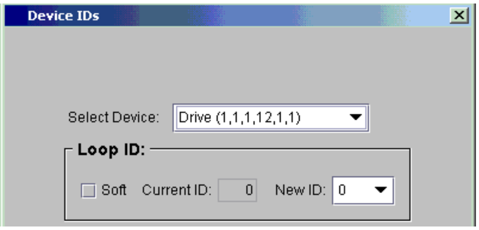


Device IDs

Select Device: Drive - 1,1,1,12,1,1

Target ID:

Current ID: 13 New ID: 13



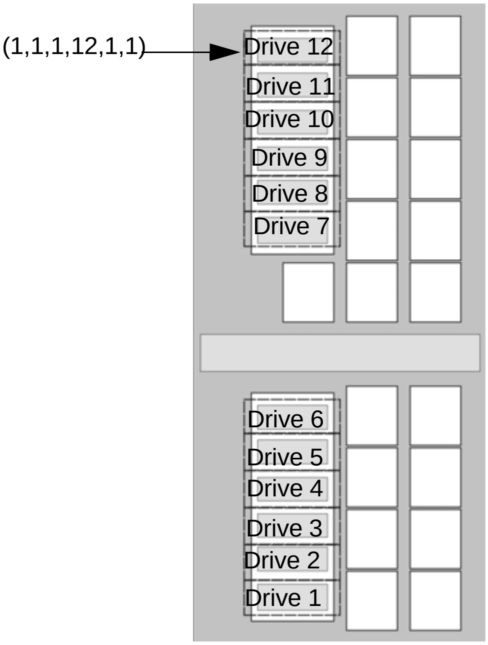
Device IDs

Select Device: Drive (1,1,1,12,1,1)

Loop ID:

□ Soft Current ID: 0 New ID: 0

The drive shown in both of these figures is in the topmost of the twelve drive bays in a control module. The following figure shows its location in the control module. For more information about location coordinates, see Understanding Location Coordinates on page 288.



4 To specify a particular ID for a drive, perform one of the following tasks:

   a For a FC drive, either click a new ID number from the **New ID** drop-down list or select the **Soft** check box to automatically assign an ID.

   b For a SCSI drive, click a new ID number from the **New ID** drop-down list.

5 Click **Set**.

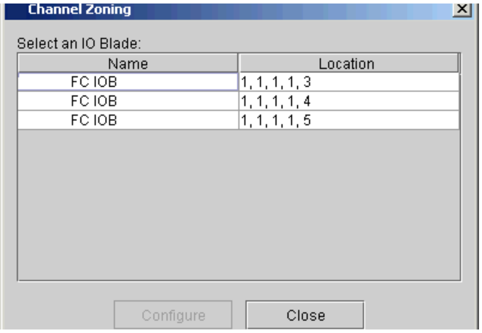
Channel Zoning

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**→ **Device**→ **Access**→ **Channel Zoning**.

   The **Channel Zoning** dialog box appears.



Channel Zoning

Select an IO Blade:

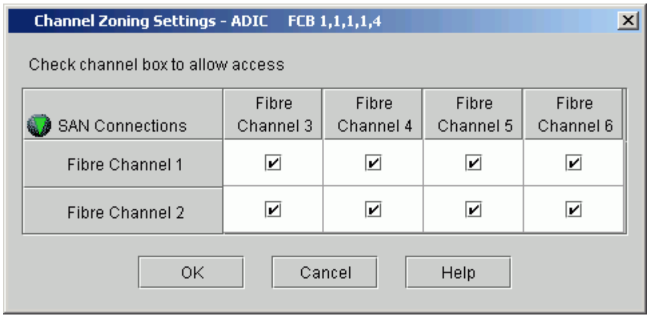
Name	Location
FC IOB	1, 1, 1, 1, 3
FC IOB	1, 1, 1, 1, 4
FC IOB	1, 1, 1, 1, 5

4. Click the I/O blade you want to configure to highlight it.

   The same I/O blade could 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.



Channel Zoning Settings - ADIC FCB 1,1,1,1,4

Check channel box to allow access

SAN Connections	Fibre Channel 3	Fibre Channel 4	Fibre Channel 5	Fibre Channel 6
Fibre Channel 1	☑	☑	☑	☑
Fibre Channel 2	☑	☑	☑	☑

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.

Note 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**.

SCSI Host

During device discovery, a particular partition or drive could map to a higher LUN space than is optimal for a particular application. The **SCSI Host** command enables you to create a virtual private remapping of available LUNs for a specific SCSI channel-attached host. Use this command to make devices appear to the host as if they were at lower LUNs in order to optimize system performance.

Note Use the **SCSI Host** command to map partitions when a SCSI channel host is connected to the MCB.

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 **SCSI 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 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.**

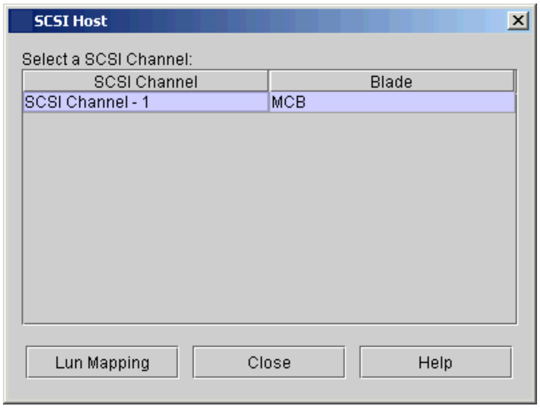
Creating SCSI Host LUN Mapping Assignments

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**→ **Device**→ **Access**→ **SCSI Host**.

The **SCSI Host** dialog box appears.



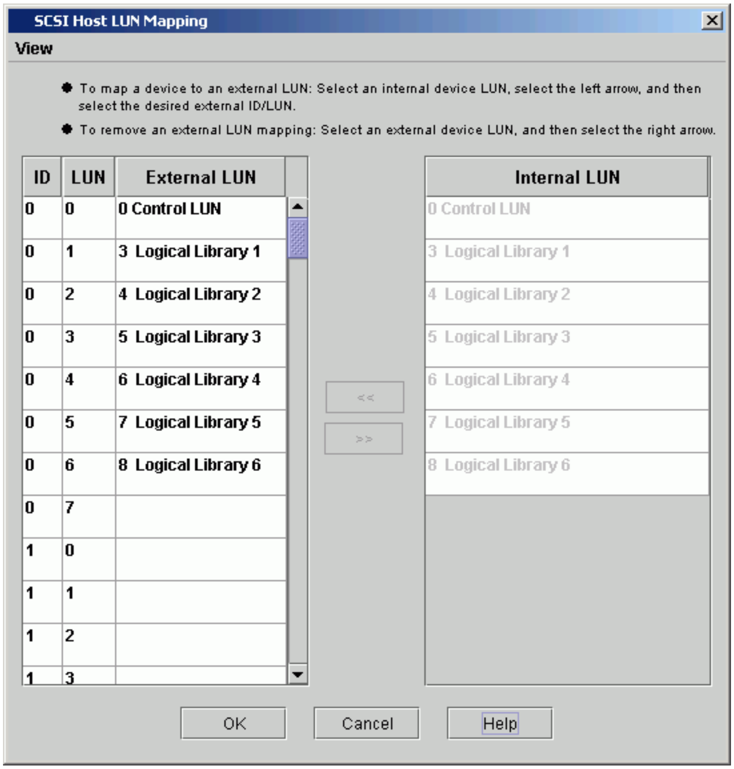
SCSI Channel	Blade
SCSI Channel - 1	MCB

4 Click a SCSI port that you want to configure to highlight it.

In the **SCSI Host** dialog box shown in the example, there is only one SCSI port available, and it is on the MCB.

5 With the port selected, click **LUN Mapping**.

The **SCSI Host LUN Mapping** dialog box appears in its default view.



SCSI Host LUN Mapping

View

- To map a device to an external LUN: Select an internal device LUN, select the left arrow, and then select the desired external ID/LUN.
- To remove an external LUN mapping: Select an external device LUN, and then select the right arrow.

ID	LUN	External LUN
0	0	0 Control LUN
0	1	3 Logical Library 1
0	2	4 Logical Library 2
0	3	5 Logical Library 3
0	4	6 Logical Library 4
0	5	7 Logical Library 5
0	6	8 Logical Library 6
0	7	
1	0	
1	1	
1	2	
1	3	

Internal LUN
0 Control LUN
3 Logical Library 1
4 Logical Library 2
5 Logical Library 3
6 Logical Library 4
7 Logical Library 5
8 Logical Library 6

In this figure, all devices have been manually mapped. The new map locations appear in heavy black type in the **ID/LUN/External LUN** column. The previous (default) device map position of a mapped device is shown in gray type in the **Internal LUN** column.

Note If you delete a partition that is currently displayed on the **SCSI Host LUN Mapping** dialog box, the internal LUN and any external LUN mappings for the partition will no longer appear on the dialog box.

6 Drag the partitions that you want the SCSI host to manage from the **Internal LUN** column to the **ID/LUN/External LUN** column.

In the default view, only partition names and the SCSI ID of the host connection are shown. In the **Show Details** view, partition name, product ID, vendor ID, and serial number of the host connection are shown.

Note 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 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.

To change the view, see Setting the View for the SCSI Host Device Column on page 184.

7 The right column of the SCSI host map dialog box, labeled **Internal LUN**, lists all available devices. The **ID/LUN/External LUN** column on the left provides map space for IDs 0-15 associated with the selected SCSI Channel, and LUNs 0-7 associated with each ID. Drag and drop devices from the **Internal LUN** column into the boxes associated with particular LUN assignments in the **ID/LUN/External LUN** column.

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 **ID/LUN/External LUN** column.

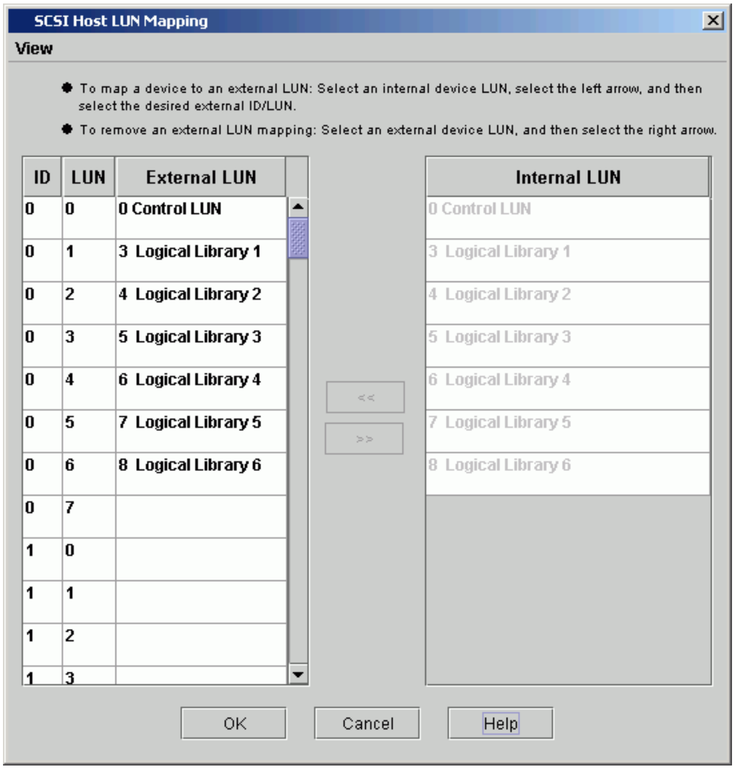
8 To save the mapping, click **OK**.

The SCSI host map is automatically saved as part of the configuration.

Modifying SCSI Host Mapping

When a device has been mapped, it is still listed, but unavailable, in the **Internal LUN** column.

In the following figure, no LUNs are currently available for mapping because they have been mapped into the **ID/LUN/External LUN** column already.



SCSI Host LUN Mapping

View

- To map a device to an external LUN: Select an internal device LUN, select the left arrow, and then select the desired external ID/LUN.
- To remove an external LUN mapping: Select an external device LUN, and then select the right arrow.

ID	LUN	External LUN
0	0	0 Control LUN
0	1	3 Logical Library 1
0	2	4 Logical Library 2
0	3	5 Logical Library 3
0	4	6 Logical Library 4
0	5	7 Logical Library 5
0	6	8 Logical Library 6
0	7	
1	0	
1	1	
1	2	
1	3	

Internal LUN
0 Control LUN
3 Logical Library 1
4 Logical Library 2
5 Logical Library 3
6 Logical Library 4
7 Logical Library 5
8 Logical Library 6

Drag the LUNs back into the **Device** column to make them 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 SCSI Host Device Column

Click **View** at the top of the **SCSI Host** 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.

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.

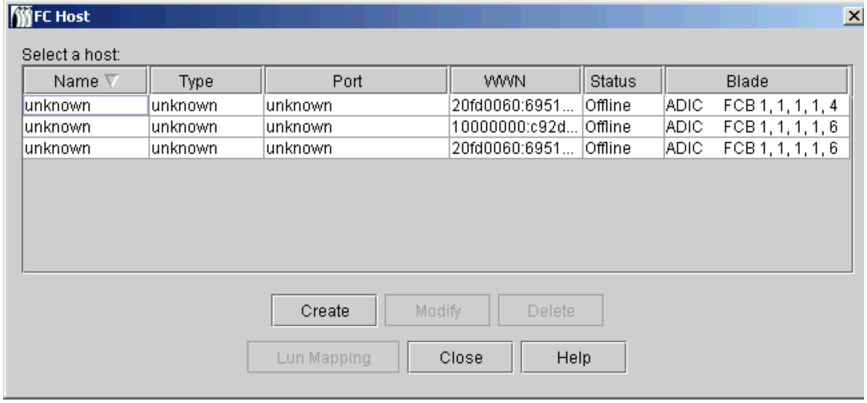
Depending on host operating system constraints, it might be necessary to reboot or reconfigure the host because of device map changes that result from using the **FC Host** command.

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.**

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**→ **Device**→ **Access**→ **FC Host**.

   The **FC Host** dialog box appears.



Select a host:

Name	Type	Port	WWN	Status	Blade
unknown	unknown	unknown	20fd0060:6951...	Offline	ADIC FCB 1, 1, 1, 1, 4
unknown	unknown	unknown	10000000:c92d...	Offline	ADIC FCB 1, 1, 1, 1, 6
unknown	unknown	unknown	20fd0060:6951...	Offline	ADIC FCB 1, 1, 1, 1, 6

Only the host's port, blade, and World Wide Name (WWN) appear.

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**→ **Device**→ **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.

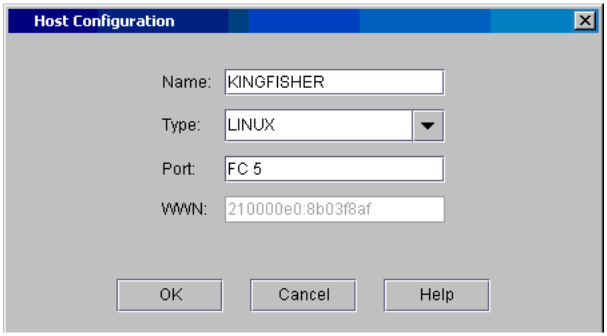
- In the **WWN** text box, type the host device World Wide Name (WWN).

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.



Name: KINGFISHER
Type: LINUX
Port: FC 5
WWN: 210000e0:8b03f8af

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**→ **Device**→ **Access**→ **FC Host**.

The **FC Host** dialog box appears.

Note FC hosts can be reconfigured without powering down the system.

4 Click the host from the list, and then click **Delete**.

Note The delete button is unavailable if the host is online.

A message appears that asks you whether you want to delete the host.

5 Click **Yes**.

A message appears that indicates a successful deletion.

6 Click **OK**.

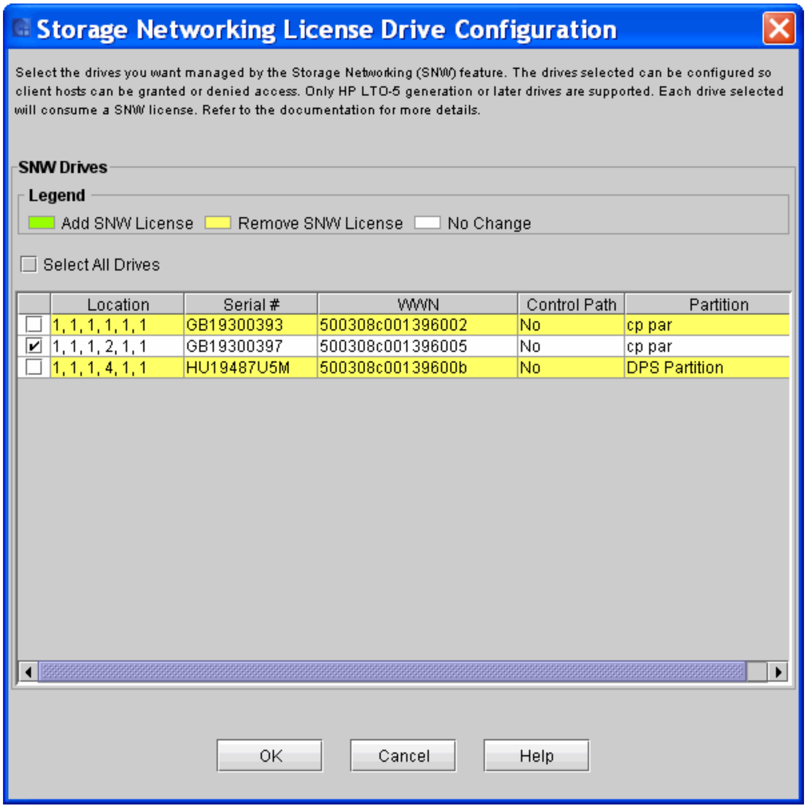
SNW (Storage Networking) Drives

The **SNW Drives** command enables you to select the drives you want managed by the Storage Networking (SNW) feature. The drives selected can be configured so client hosts can be granted or denied access. Only HP LTO-5 generation or later drives are supported. Each drive selected will consume a SNW license.

Selecting a Storage Networking Drive

1. Log on as an administrator.
2. If you are not already working from the physical library, select it. From the **View** menu, click the name of the physical library.
3. Click **Setup > Device > Access > SNW Drives**.

   The Storage Networking License Drive Configuration dialog box appears.



Storage Networking License Drive Configuration

Select the drives you want managed by the Storage Networking (SNW) feature. The drives selected can be configured so client hosts can be granted or denied access. Only HP LTO-5 generation or later drives are supported. Each drive selected will consume a SNW license. Refer to the documentation for more details.

SNW Drives

Legend

🟩 Add SNW License 🟨 Remove SNW License ⬜ No Change

□ Select All Drives

	Location	Serial #	WWN	Control Path	Partition
□	1, 1, 1, 1, 1, 1	GB19300393	500308c001396002	No	cp par
☑	1, 1, 1, 2, 1, 1	GB19300397	500308c001396005	No	cp par
□	1, 1, 1, 4, 1, 1	HU19487U5M	500308c00139600b	No	DPS Partition

4 To select all drives, click the check box next to **Select All Drives**.

5 To select an individual drive, click the check box in the left column for the appropriate row.

6 Click **OK**.

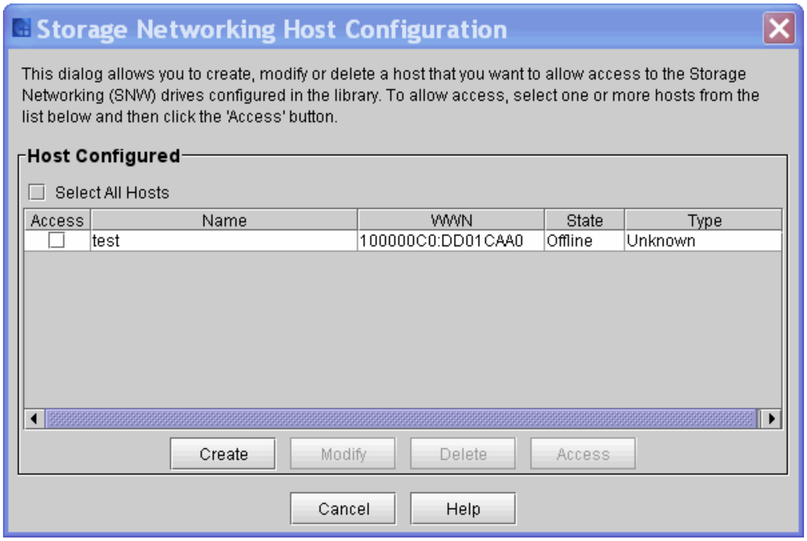
SNW (Storage Networking) Host

The **SNW Host** command enables you to create, modify or delete host access to the Storage Networking (SNW) drives configured in the library.

Accessing the SNW Host Device

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. From the main console, select **Setup > Device > Access > SNW Host**.

   The **Storage Networking Host Configuration** dialog box appears.



Storage Networking Host Configuration

This dialog allows you to create, modify or delete a host that you want to allow access to the Storage Networking (SNW) drives configured in the library. To allow access, select one or more hosts from the list below and then click the 'Access' button.

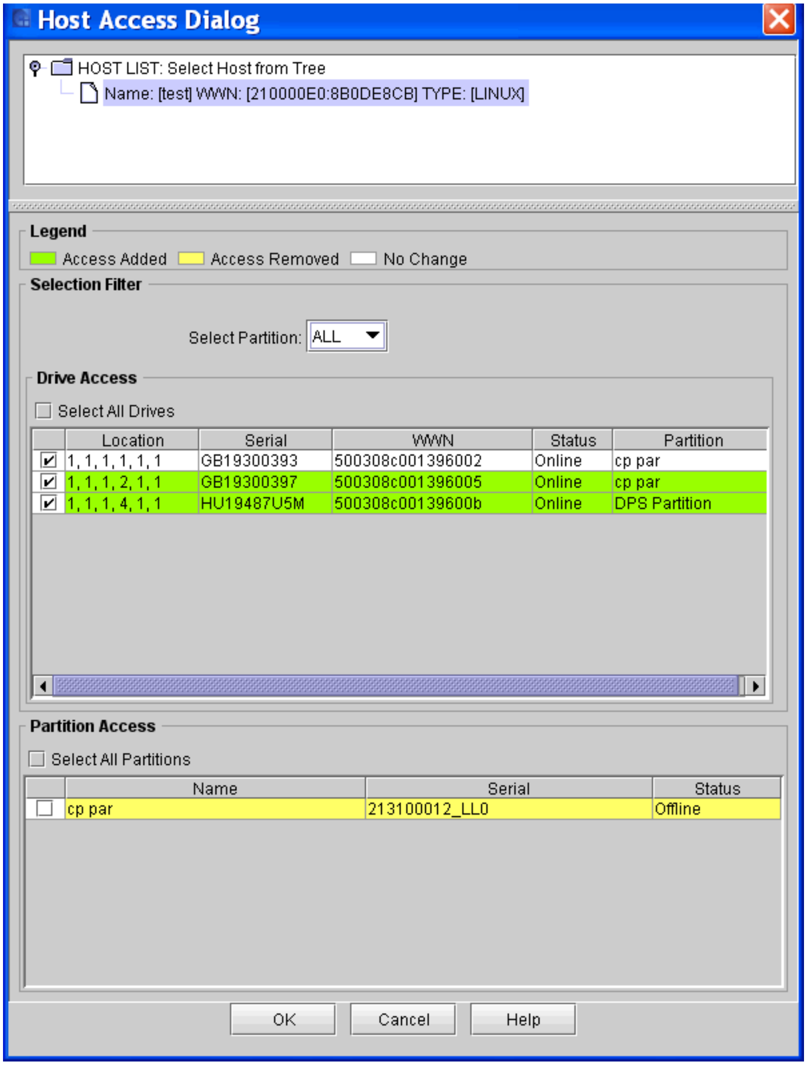
Host Configured

□ Select All Hosts

Access	Name	WWN	State	Type
□	test	100000C0:DD01CAA0	Offline	Unknown

4. Select the host(s) you want to access by clicking the check box from the Host Configured table.
5. Click **Access**.

The **Host Access** dialog box appears.



Host Access Dialog

HOST LIST: Select Host from Tree
Name: [test] WWN: [210000E0:8B0DE8CB] TYPE: [LINUX]

Legend

🟩 Access Added 🟨 Access Removed ⬜ No Change

Selection Filter

Select Partition: ALL

Drive Access

□ Select All Drives

	Location	Serial	WWN	Status	Partition
☑	1, 1, 1, 1, 1, 1	GB19300393	500308c001396002	Online	cp par
☑	1, 1, 1, 2, 1, 1	GB19300397	500308c001396005	Online	cp par
☑	1, 1, 1, 4, 1, 1	HU19487U5M	500308c00139600b	Online	DPS Partition

Partition Access

□ Select All Partitions

	Name	Serial	Status
□	cp par	213100012_LL0	Offline

6 On the top portion of the screen, expand the **HOST LIST** folder, and highlight the host you want to change.

7 From the **Select Partition** drop down menu, select the appropriate partition.

This action filters the drives in the **Drive Access** table and show only those drives that belong to the partition selected. By default all SNW drives will be displayed.

In the **Partition Access** section, the partitions are displayed.

8 Select drives.

To select all drives in the **Drive Access** table, click the **Select All Drives** check box; to select individual drives, select the check box for each drive.

When a drive check box is selected/unselected the color of the row in the table will change to indicated the change to the current drive configuration. The colors have the following meaning GREEN (access will be granted to the host selected in the HOST LIST), YELLOW (access will be denied to the host selected in the HOST LIST) and WHITE (no change has been made).

The drives that are presented in the **Drive Access** table have the following characteristics:

- They have a SNW license.
- They are HP LTO-5 fibre drives.
- They are connected to a Ethernet Expansion Blade.

9 Select partitions.

To select all partitions in the **Partition Access** table, click the **Select All Partitions** check box; to select individual partition, select the check box for each partition. When a partition is selected/unselected the table row color will change indicating the new configuration requested. The colors have the same meaning as the drive table described above.

The partitions that are presented in the **Partition Access** table have the following characteristics:

- They contain one or more SNW licensed drives.
- They have a Control Path drive configured.

10 To make changes to a number of hosts, follow steps 6 through 9 for each host.

11 Click **OK** to apply the changes.

The Host is configured.

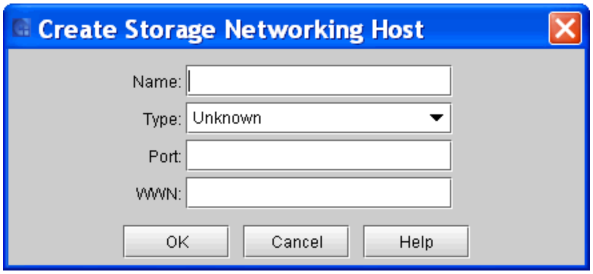
Creating SNW (Storage Networking) Host

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. From the main console, select **Setup > Device > Access > SNW Host.**

   The **Storage Networking Host Configuration** dialog box appears.

   This dialog allows the user to Create, Delete or Modify hosts that will access the Storage Networking (SNW) drives configured in you library. The SNW drives must be licensed before access can be granted/denied.
4. To create a host click the **Create** button.

   The **Create Storage Networking Host** dialog box appears.



5. Using the fields provided, provide the following required information:

   a. In the **Name** text box, type a host device name.

      There are no character restrictions for this field There is a length restriction of 40 characters.

   b. From the **Type** drop-down list, click the appropriate host type by operating system.

   c. In the **Port** text box, type the host device port.

      The **Port** field can remain blank.

Note You can use this free-form text field to describe the connectivity or logical visibility, for example. This field has no configuration functionality.

d In the **WWN** text box, type the host device World Wide Name (WWN).

6 Click **OK**.

The **Host Configured** portion of the dialog box displays the host that you created.

7 To close the dialog box, click **Cancel**.

Modifying SNW Host

Note SNW hosts can be reconfigured without powering down the system.

1 Log on as an administrator.

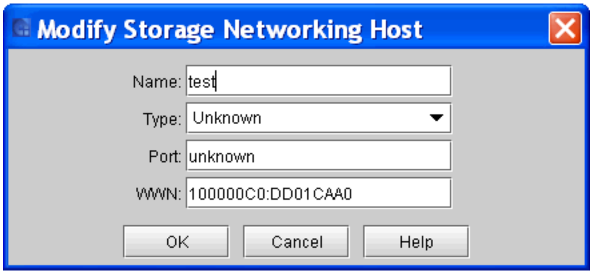
2 To ensure you are working from the physical library, from the main console, select **View** and click the name of the physical library.

3 Click **Setup > Device > Access > SNW Host**.

The **Storage Networking Host Configuration** dialog box appears.

4 Select a check box for the appropriate host from the Host Configured table then click on the **Modify** button. Only one host can be selected for this operation.

The **Modify Storage Networking Host** dialog box appears.



Modify Storage Networking Host

Name: test

Type: Unknown

Port: unknown

WWN: 100000C0:DD01CAA0

5. Change the **Name**, **Type**, or **Port**. You can not change the WWN.
6. Click **OK**.

   The **Host Configured** portion of the dialog box displays the host that you modified.
7. To close the dialog box, click **Cancel.**

Deleting SNW Host

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 > Device > Access > SNW Host**.

   The **Storage Networking Host Configuration** dialog box appears.
4. Select a check box for the appropriate host from the Host Configuration table then click **Delete**.

   Only one host can be selected for this operation.

Note The delete button is unavailable if the host is online.

FC Host LUN Mapping

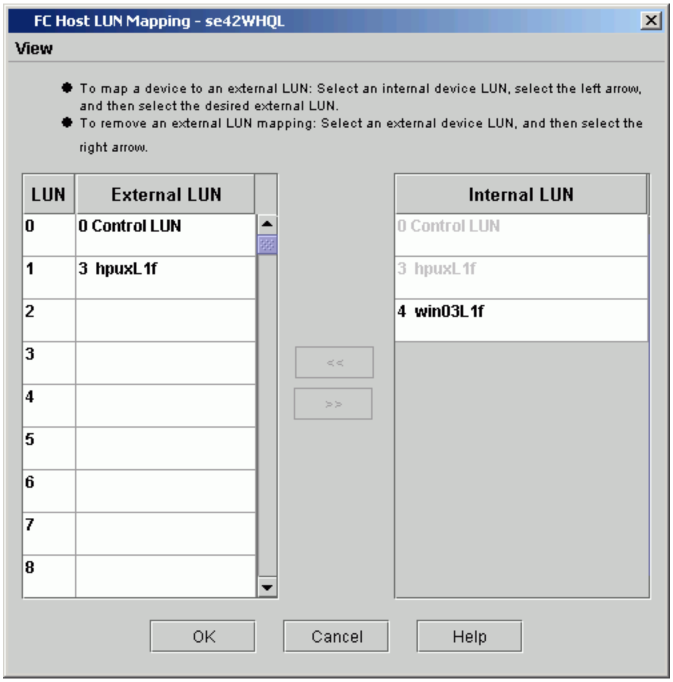
Use the **FC Host LUN Mapping** dialog box to give a selected host access to partitions and drives.

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 > Device > Access > FC Host**.

   The **FC Host** dialog box appears.
4. With a host selected on the **FC Host** dialog box, click **LUN Mapping**.

The **FC Host LUN Mapping** dialog box appears in its default view.



FC Host LUN Mapping - se42WHQL

View

- To map a device to an external LUN: Select an internal device LUN, select the left arrow, and then select the desired external LUN.
- To remove an external LUN mapping: Select an external device LUN, and then select the right arrow.

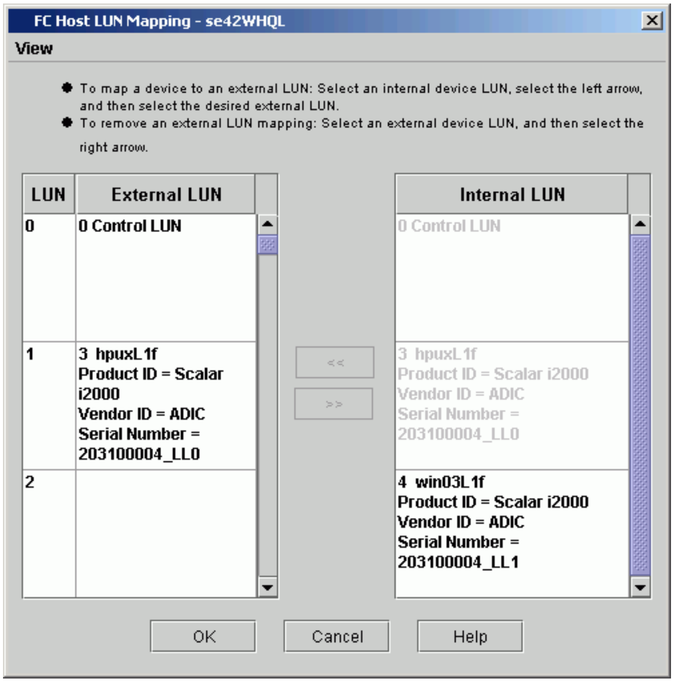
LUN	External LUN
0	0 Control LUN
1	3 hpuxL1f
2	
3	
4	
5	
6	
7	
8	

Internal LUN
0 Control LUN
3 hpuxL1f
4 win03L1f

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.

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 SCSI Host Device Column on page 184.



- To map a device to an external LUN: Select an internal device LUN, select the left arrow, and then select the desired external LUN.
- To remove an external LUN mapping: Select an external device LUN, and then select the right arrow.

LUN	External LUN
0	0 Control LUN
1	3 hpuxL1f Product ID = Scalar i2000 Vendor ID = ADIC Serial Number = 203100004_LL0
2	

Internal LUN
0 Control LUN
3 hpuxL1f Product ID = Scalar i2000 Vendor ID = ADIC Serial Number = 203100004_LL0
4 win03L1f Product ID = Scalar i2000 Vendor ID = ADIC Serial Number = 203100004_LL1

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 22 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 24, Scalar i500, Scalar 100, 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.
Vendor ID	ADIC or Quantum.
Serial Number	Partition ID, as shown by **System**→ **Monitor**.

The following table describes the descriptors that appear in the **Show Details** view for drives.

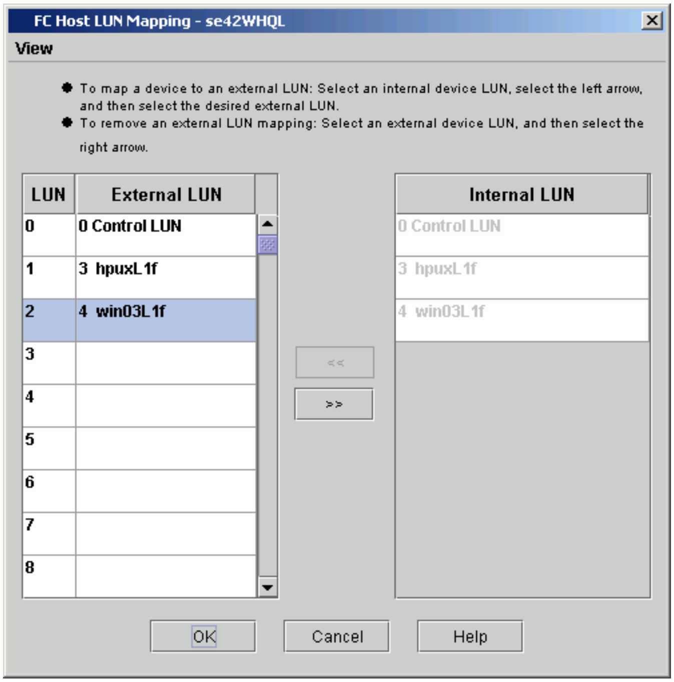
Table 23 Descriptors

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.



FC Host LUN Mapping - se42WHQL

View

- To map a device to an external LUN: Select an internal device LUN, select the left arrow, and then select the desired external LUN.
- To remove an external LUN mapping: Select an external device LUN, and then select the right arrow.

LUN	External LUN
0	0 Control LUN
1	3 hpuxL1f
2	4 win03L1f
3	
4	
5	
6	
7	
8	

Internal LUN
0 Control LUN
3 hpuxL1f
4 win03L1f

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.

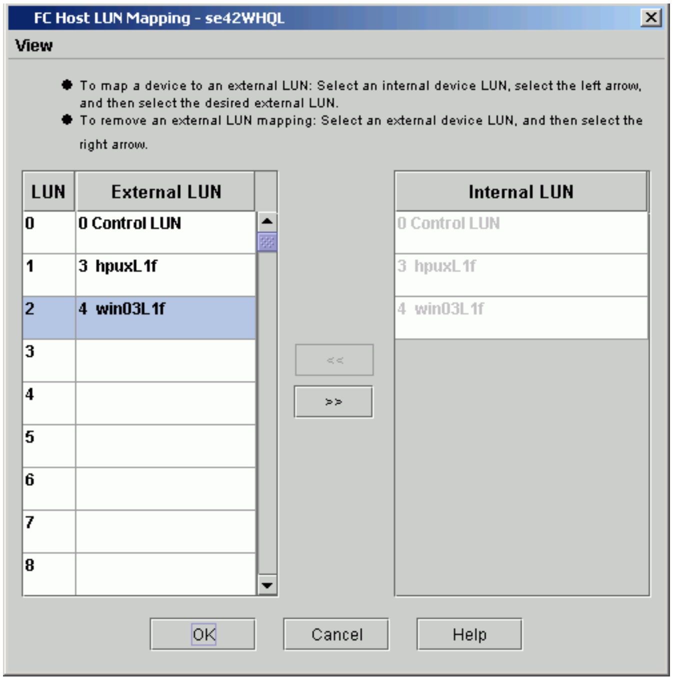
7 To save the mapping, click **OK**.

The FC host map is automatically saved as part of the configuration. For more information about device numbering in a SAN context, see the *ADIC Management Console User's Guide* or 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.



- To map a device to an external LUN: Select an internal device LUN, select the left arrow, and then select the desired external LUN.
- To remove an external LUN mapping: Select an external device LUN, and then select the right arrow.

LUN	External LUN
0	0 Control LUN
1	3 hpuxL1f
2	4 win03L1f
3	
4	
5	
6	
7	
8	

Internal LUN
0 Control LUN
3 hpuxL1f
4 win03L1f

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.

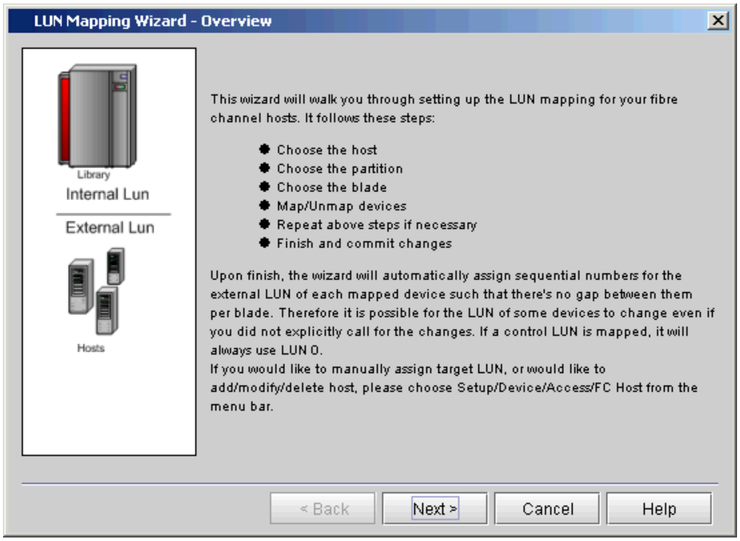
Note — If you want to manually assign a target LUN, or want to add/modify/delete the host, select **Setup**→ **Device**→ **Access**→ **FC Host** on the menu bar. For more information, see FC Host on page 184.

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**→ **Device**→ **Access**→ **LUN Mapping Wizard**.

The **LUN Mapping Wizard – Overview** dialog box appears.



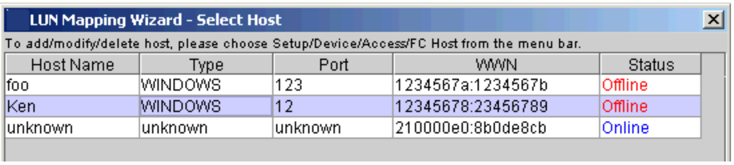
This wizard will walk you through setting up the LUN mapping for your fibre channel hosts. It follows these steps:

- Choose the host
- Choose the partition
- Choose the blade
- Map/Unmap devices
- Repeat above steps if necessary
- Finish and commit changes

Upon finish, the wizard will automatically assign sequential numbers for the external LUN of each mapped device such that there's no gap between them per blade. Therefore it is possible for the LUN of some devices to change even if you did not explicitly call for the changes. If a control LUN is mapped, it will always use LUN 0.
If you would like to manually assign target LUN, or would like to add/modify/delete host, please choose Setup/Device/Access/FC Host from the menu bar.

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.

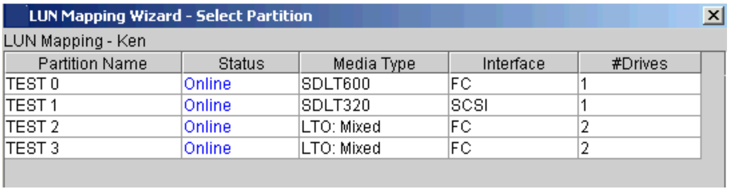


To add/modify/delete host, please choose Setup/Device/Access/FC Host from the menu bar.

Host Name	Type	Port	WWN	Status
foo	WINDOWS	123	1234567a:1234567b	Offline
Ken	WINDOWS	12	12345678:23456789	Offline
unknown	unknown	unknown	210000e0:8b0de8cb	Online

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.

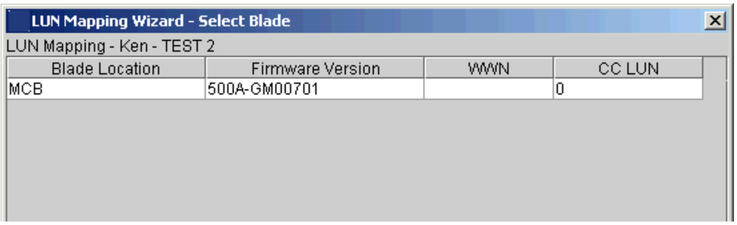


LUN Mapping - Ken

Partition Name	Status	Media Type	Interface	#Drives
TEST 0	Online	SDLT600	FC	1
TEST 1	Online	SDLT320	SCSI	1
TEST 2	Online	LTO: Mixed	FC	2
TEST 3	Online	LTO: Mixed	FC	2

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.

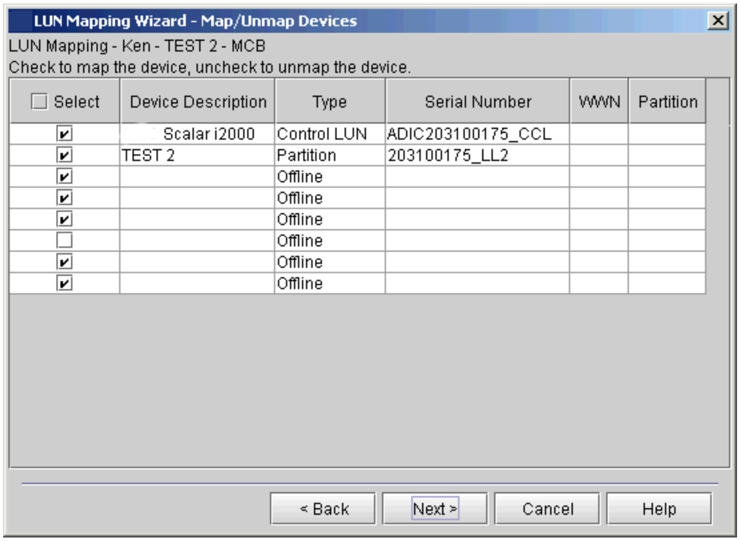


LUN Mapping - Ken - TEST 2

Blade Location	Firmware Version	WWN	CC LUN
MCB	500A-GM00701		0

5 Select a blade to configure and then click **Next** to continue.

The **LUN Mapping Wizard – Map/Unmap Devices** dialog box appears.

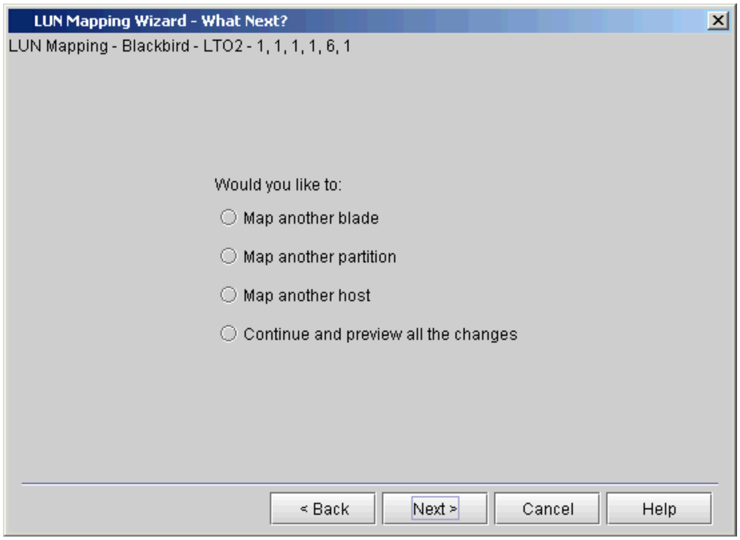


LUN Mapping - Ken - TEST 2 - MCB
Check to map the device, uncheck to unmap the device.

☐ Select	Device Description	Type	Serial Number	WWN	Partition
☑	Scalar i2000	Control LUN	ADIC203100175_CCL		
☑	TEST 2	Partition	203100175_LL2		
☑		Offline			
☑		Offline			
☑		Offline			
☐		Offline			
☑		Offline			
☑		Offline			

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.



LUN Mapping - Blackbird - LTO2 - 1, 1, 1, 1, 6, 1

Would you like to:

○ Map another blade

○ Map another partition

○ Map another host

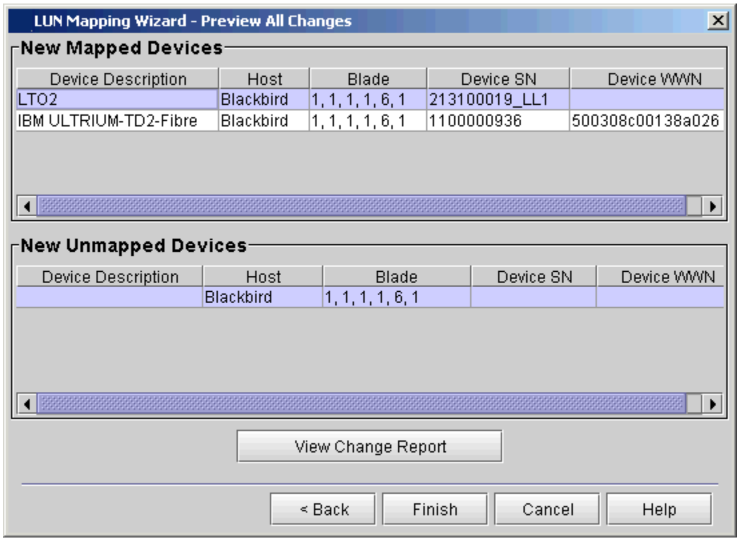
○ Continue and preview all the changes

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.

If your configurations are complete, select **Continue and preview all changes**.

The **LUN Mapping Wizard – Preview All Changes** dialog box appears.



LUN Mapping Wizard - Preview All Changes

New Mapped Devices

Device Description	Host	Blade	Device SN	Device WWN
LTO2	Blackbird	1, 1, 1, 1, 6, 1	213100019_LL1	
IBM ULTRIUM-TD2-Fibre	Blackbird	1, 1, 1, 1, 6, 1	1100000936	500308c00138a026

New Unmapped Devices

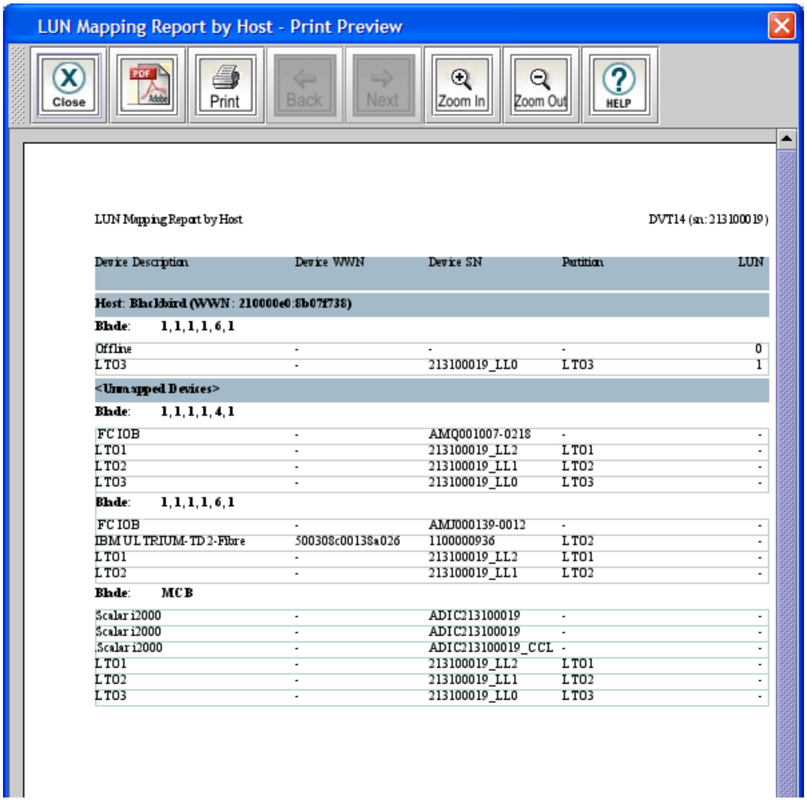
Device Description	Host	Blade	Device SN	Device WWN
	Blackbird	1, 1, 1, 1, 6, 1		

8 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.



LUN Mapping Report by Host DVT14 (sn: 213100019)

Device Description	Device WWN	Device SN	Partition	LUN
Host: Blackbird (WWN: 210000e0:8b07f738)				
Blade: 1, 1, 1, 1, 6, 1				
Offline	-	-	-	0
LTO3	-	213100019_LL0	LTO3	1
<Unmapped Devices>				
Blade: 1, 1, 1, 1, 4, 1				
FC IOB	-	AMQ001007-0218	-	-
LTO1	-	213100019_LL2	LTO1	-
LTO2	-	213100019_LL1	LTO2	-
LTO3	-	213100019_LL0	LTO3	-
Blade: 1, 1, 1, 1, 6, 1				
FC IOB	-	AMJ000139-0012	-	-
IBM ULTRIUM-TD2-Fibre	500308c00138a026	1100000936	LTO2	-
LTO1	-	213100019_LL2	LTO1	-
LTO2	-	213100019_LL1	LTO2	-
Blade: MCB				
Scalar i2000	-	ADIC213100019	-	-
Scalar i2000	-	ADIC213100019	-	-
.Scalar i2000	-	ADIC213100019_CCL	-	-
LTO1	-	213100019_LL2	LTO1	-
LTO2	-	213100019_LL1	LTO2	-
LTO3	-	213100019_LL0	LTO3	-

The changes on the report include:

- Added Mapping – (**A**)
- Removed Mapping – (**R**)
- LUN Modified – (**M**)

9 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.**

10 After you have reviewed the **LUN Mapping Change Preview Report**, click **Close** to return to the **LUN Mapping Wizard – Preview All Changes** dialog box.

11 If you are satisfied with your LUN mapping changes and want to complete the wizard process, click **Finish**.

Your LUN mapping changes are finalized, and then you have the option of viewing the LUN 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.

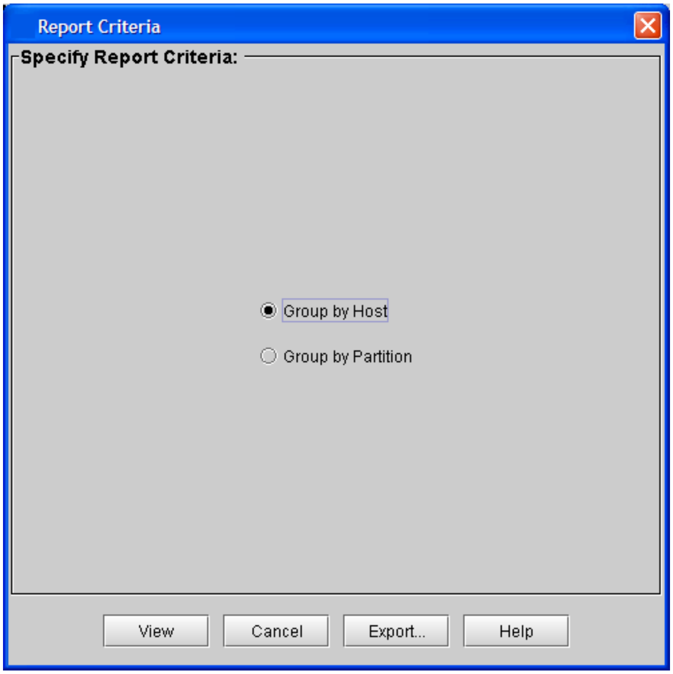
When generating the LUN Mapping Report, you can choose to group devices by the associated host or by the associated partition.

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.



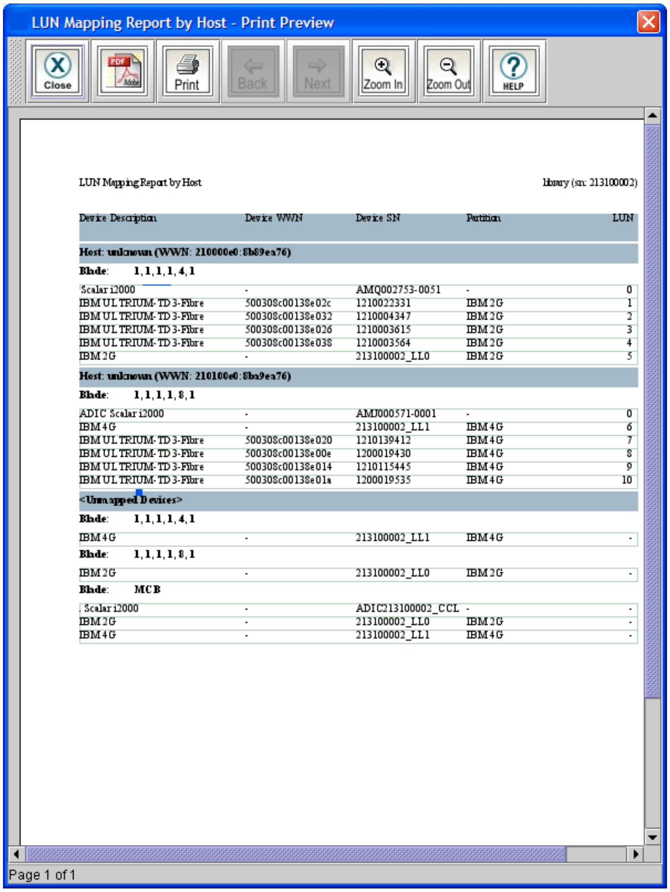
2 Under **Specify Report Criteria**, click a grouping option.

- **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.

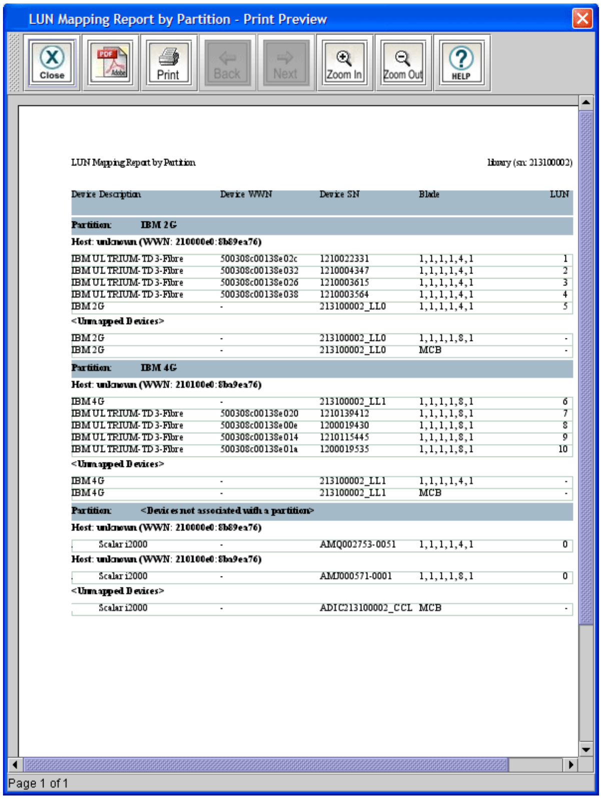
The following figure shows an example of a **LUN Mapping Report grouped by host.**



LUN Mapping Report by Host — library (sn: 213100002)

Device Description	Device WWN	Device SN	Partition	LUN
Host: unknown (WWN: 210000e0:8b89ea76)				
Blade: 1, 1, 1, 1, 4, 1				
Scalar i2000	-	AMQ002753-0051	-	0
IBM UL TRIUM-TD3-Fibre	500308c00138e02c	1210022331	IBM 2G	1
IBM UL TRIUM-TD3-Fibre	500308c00138e032	1210004347	IBM 2G	2
IBM UL TRIUM-TD3-Fibre	500308c00138e026	1210003615	IBM 2G	3
IBM UL TRIUM-TD3-Fibre	500308c00138e038	1210003564	IBM 2G	4
IBM 2G	-	213100002_LL0	IBM 2G	5
Host: unknown (WWN: 210100e0:8ba9ea76)				
Blade: 1, 1, 1, 1, 8, 1				
ADIC Scalar i2000	-	AMJ000571-0001	-	0
IBM 4G	-	213100002_LL1	IBM 4G	6
IBM UL TRIUM-TD3-Fibre	500308c00138e020	1210139412	IBM 4G	7
IBM UL TRIUM-TD3-Fibre	500308c00138e00e	1200019430	IBM 4G	8
IBM UL TRIUM-TD3-Fibre	500308c00138e014	1210115445	IBM 4G	9
IBM UL TRIUM-TD3-Fibre	500308c00138e01a	1200019535	IBM 4G	10
<Unmapped Devices>				
Blade: 1, 1, 1, 1, 4, 1				
IBM 4G	-	213100002_LL1	IBM 4G	-
Blade: 1, 1, 1, 1, 8, 1				
IBM 2G	-	213100002_LL0	IBM 2G	-
Blade: MCB				
Scalar i2000	-	ADIC213100002_CCL	-	-
IBM 2G	-	213100002_LL0	IBM 2G	-
IBM 4G	-	213100002_LL1	IBM 4G	-

The following figure shows an example of a **LUN Mapping Report grouped by partition**.



LUN Mapping Report by Partition — library (sn: 213100002)

Device Description	Device WWN	Device SN	Blade	LUN
Partition: IBM 2G				
Host: unknown (WWN: 210000e0:8b89ea76)				
IBM ULTRIUM-TD3-Fibre	500308c00138e02c	1210022331	1,1,1,1,4,1	1
IBM ULTRIUM-TD3-Fibre	500308c00138e032	1210004347	1,1,1,1,4,1	2
IBM ULTRIUM-TD3-Fibre	500308c00138e026	1210003615	1,1,1,1,4,1	3
IBM ULTRIUM-TD3-Fibre	500308c00138e038	1210003564	1,1,1,1,4,1	4
IBM 2G	-	213100002_LL0	1,1,1,1,4,1	5
<Unmapped Devices>				
IBM 2G	-	213100002_LL0	1,1,1,1,8,1	-
IBM 2G	-	213100002_LL0	MCB	-
Partition: IBM 4G				
Host: unknown (WWN: 210100e0:8ba9ea76)				
IBM 4G	-	213100002_LL1	1,1,1,1,8,1	6
IBM ULTRIUM-TD3-Fibre	500308c00138e020	1210139412	1,1,1,1,8,1	7
IBM ULTRIUM-TD3-Fibre	500308c00138e00e	1200019430	1,1,1,1,8,1	8
IBM ULTRIUM-TD3-Fibre	500308c00138e014	1210115445	1,1,1,1,8,1	9
IBM ULTRIUM-TD3-Fibre	500308c00138e01a	1200019535	1,1,1,1,8,1	10
<Unmapped Devices>				
IBM 4G	-	213100002_LL1	1,1,1,1,4,1	-
IBM 4G	-	213100002_LL1	MCB	-
Partition: <Devices not associated with a partition>				
Host: unknown (WWN: 210000e0:8b89ea76)				
Scalar i2000	-	AMQ002753-0051	1,1,1,1,4,1	0
Host: unknown (WWN: 210100e0:8ba9ea76)				
Scalar i2000	-	AMJ000571-0001	1,1,1,1,8,1	0
<Unmapped Devices>				
Scalar i2000	-	ADIC213100002_CCL	MCB	-

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

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

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 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**.

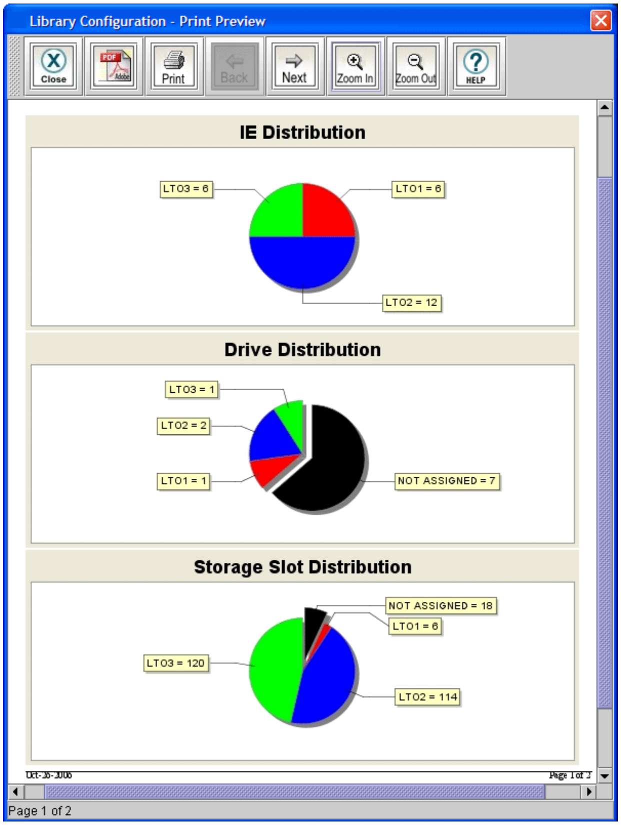
5 To close the **Report Criteria** dialog box, click **Cancel**.

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**.

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

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

Configuring Drive Cleaning

When you create or modify a partition, you can specify that tape drives in that partition be automatically cleaned each time the drive requests a cleaning operation.

For automatic drive cleaning to function, you must configure drive cleaning 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 Automatic 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.

For more information about enabling automatic drive cleaning for a partition, see Working With Partitions on page 112 on page 171. For more information about manually cleaning drives, see Cleaning a Drive on page 374.

Assigning Cleaning Magazines and Importing Cleaning Media

To configure the library for drive cleaning, first assign one or more magazines as cleaning magazines, and then import cleaning media.

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.

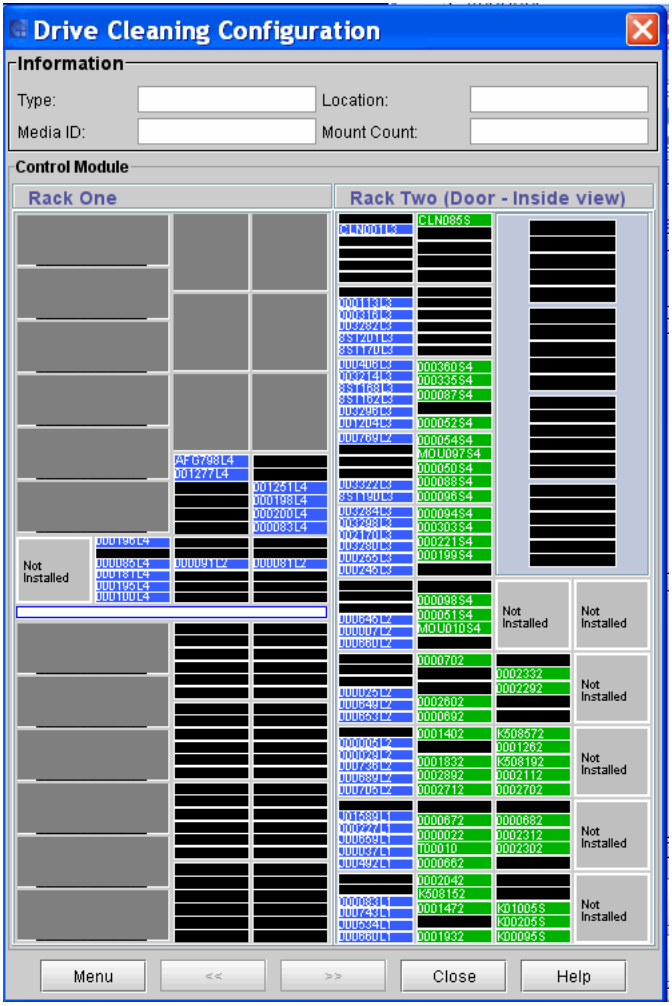
1. Insert one or more pieces of cleaning media into the I/E station and close the I/E station door.

   Use a standard barcode label for cleaning media. Barcode numbers do not require a specific prefix or suffix.

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

3. On the menu bar, click **Setup**→ **Drive Cleaning.**

The **Drive Cleaning Configuration** dialog box appears.



4 Click a magazine slot or a piece of media 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.

5 If the library has more than one module, click the arrow buttons to display the next or previous module.

6 To assign a magazine for cleaning, click any slot in the magazine to select it. Click **Menu**, and then click **Assign magazine for cleaning**.

The magazine is assigned for cleaning.

7 Repeat this step to assign additional cleaning magazines.

8 To import cleaning media, click the cleaning media in the I/E station to select it, and then do one of the following:

- To import only the selected piece of media, click **Menu**, and then click **Import <barcode number> as cleaning media**.
- To import all media in the selected I/E station magazine, click **Menu**, and then click **Import all tapes in magazine as cleaning media**.

The cleaning media is moved to an available cleaning magazine, and can be used for automatic or manual cleaning.

9 Click **Close** to close the **Drive Cleaning Configuration** dialog box.

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.

ExportingCleaningMedia

Cleaning media can be used a limited number of times. If a piece of media is expired, export it and remove it from the library

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 **Setup**→ **Drive Cleaning.**

The **Drive Cleaning Configuration** dialog box appears. If the library has more than one module, click the arrow buttons to display the next or previous module.

To determine if a piece of cleaning media has been used the maximum number of times, 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 is moved to an available I/E station magazine.

4 Click **Close** to close the **Drive Cleaning Configuration** dialog box.

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, click the name of the physical library.

2 On the menu bar, click **Setup**→ **Drive Cleaning.**

The **Drive Cleaning 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 217.

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.

6 Click **Close** to close the **Drive Cleaning Configuration** dialog box.

Note If you try to unassign a cleaning magazine that contains cleaning media, a message appears asking if you are sure you want to continue. If you click **Yes**, any media in the magazine is not accessible until you add the magazine to a partition or assign it again as a 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.

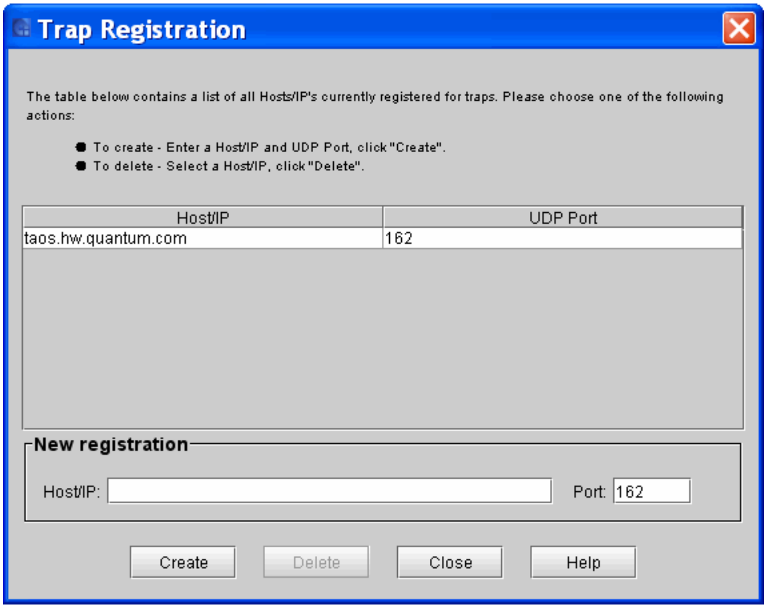
Registering an Application

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**→ **Trap Registration**.

The **Trap Registration** dialog box appears.



Trap Registration

The table below contains a list of all Hosts/IP's currently registered for traps. Please choose one of the following actions:

- To create - Enter a Host/IP and UDP Port, click "Create".
- To delete - Select a Host/IP, click "Delete".

Host/IP	UDP Port
taos.hw.quantum.com	162

New registration

Host/IP: Port: 162

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**→ **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.

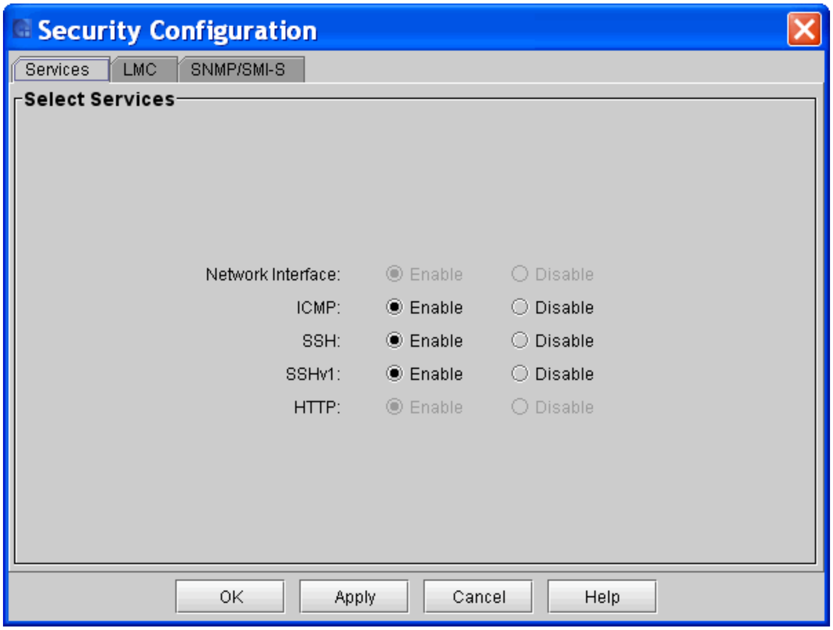
1. Log on as an admin user.
2. Click **Setup**→ **Security**.

   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.



Security Configuration

Services | LMC | SNMP/SMI-S

Select Services

Network Interface: ● Enable ○ Disable
ICMP: ● Enable ○ Disable
SSH: ● Enable ○ Disable
SSHv1: ● Enable ○ Disable
HTTP: ● Enable ○ Disable

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.
- **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**.

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.)

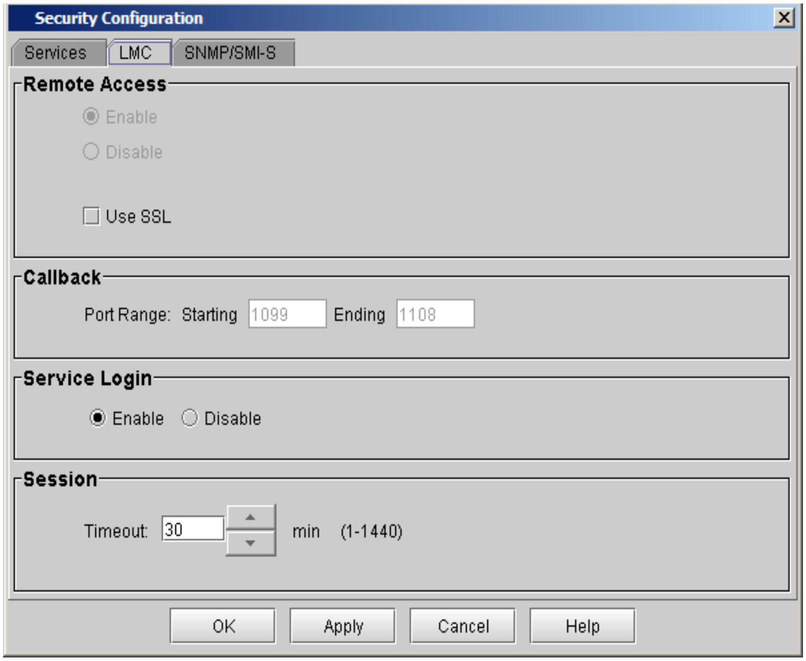
3 If you want to apply the changes, but you do not want to close the dialog box, click **Apply**. Otherwise, click **OK** to apply the changes and close the dialog box.

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.


Security Configuration

Services | LMC | SNMP/SMI-S

Remote Access
● Enable
○ Disable

□ Use SSL

Callback
Port Range: Starting 1099 Ending 1108

Service Login
● Enable ○ Disable

Session
Timeout: 30 min (1-1440)

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 i6000.

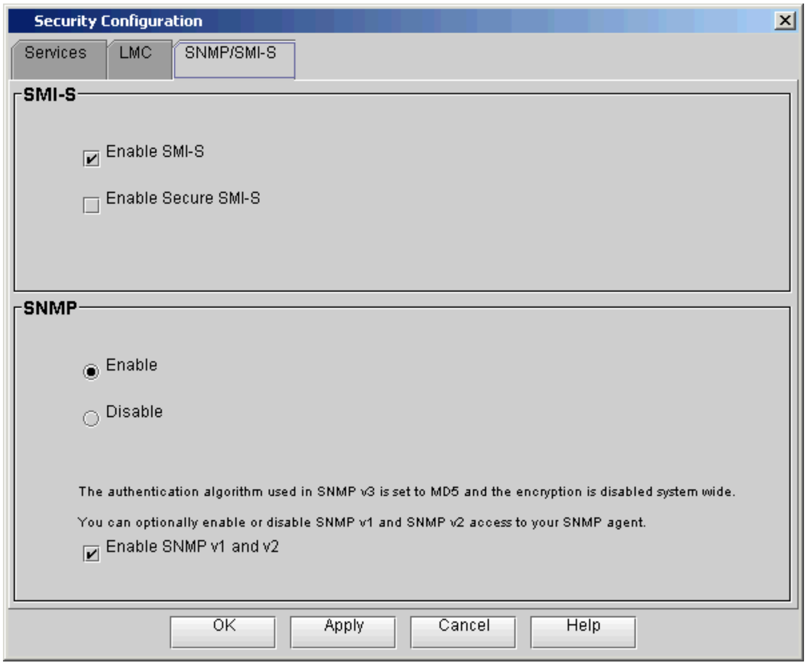
- **Session** — To configure the length of the session's timeout, type or use the arrow buttons to specify the length of a session before it times out. Valid session timeouts are 1-1440 minutes (1 minute - 24 hours), where the default is 30 minutes.

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.



☑ Enable SMI-S

☐ Enable Secure SMI-S

● Enable

○ Disable

The authentication algorithm used in SNMP v3 is set to MD5 and the encryption is disabled system wide.

You can optionally enable or disable SNMP v1 and SNMP v2 access to your SNMP agent.

☑ Enable SNMP v1 and v2

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.

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**→ **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 219.

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. This library supports the Microsoft® Active Directory® LDAP server and user account information in the schema defined by RFC 2307. User password schemes must be encrypted using UNIX® crypt.

Note The Scalar i6.5 release provided enhancements to the Lightweight Directory Access Protocol (LDAP) features.
For maximum ease of use of this feature, Quantum strongly recommends that you are running version i6.5 or greater.

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.

CAUTION **Any LDAP configurations from i6.3.1 and earlier will not import into the i6.5 LDAP configuration. You must reconfigure LDAP for the i6.5 update.**

LDAP Server Guidelines

LDAP is the industry standard Internet protocol that provides centralized user account management subsystem. User account information is centralized and shared by different applications, simplifying user account management tasks. Administrative users can add, delete, and modify only local user account information.

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. Users without administrator privileges must be assigned to these groups on the LDAP server to have access to the corresponding partitions on the library. LDAP accounts with administrative 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

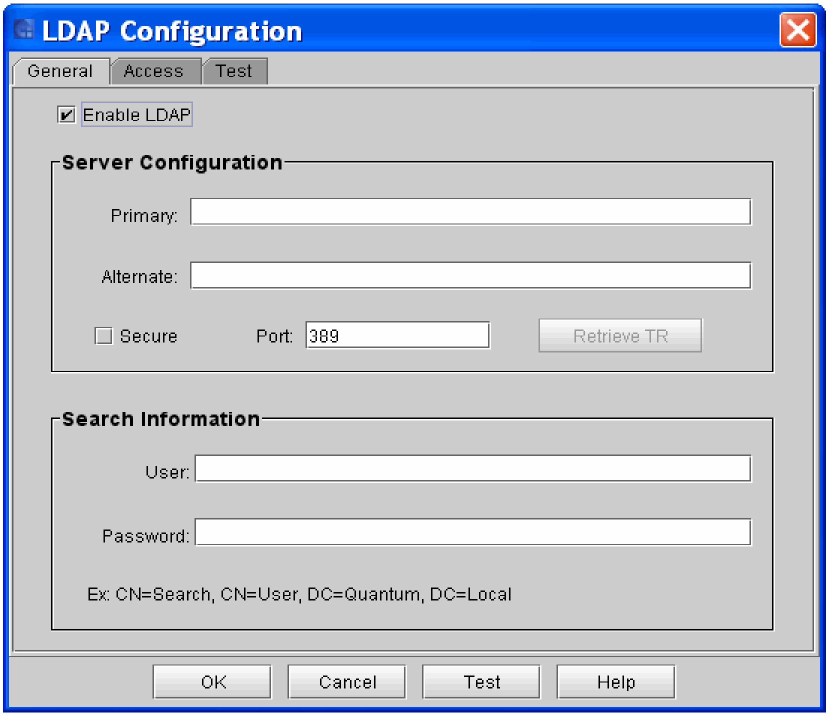
You must install and run OpenLDAP 2.4 or later. The supported Objects in OpenLDAP 2.4 and above are of type “Person” or derived objects, and the group Objects must be of type “GroupOfNames”.

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-memberof” command.

Configuring LDAP

1 From the Setup menu, click **LDAP**.

The **LDAP Configuration** dialog box displays with the **General** tab displayed.



2 In the **General** tab, you can enable or disable LDAP functionality:

- 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.

3 To configure or modify LDAP, use the appropriate tabs and set the following configurations:

General tab

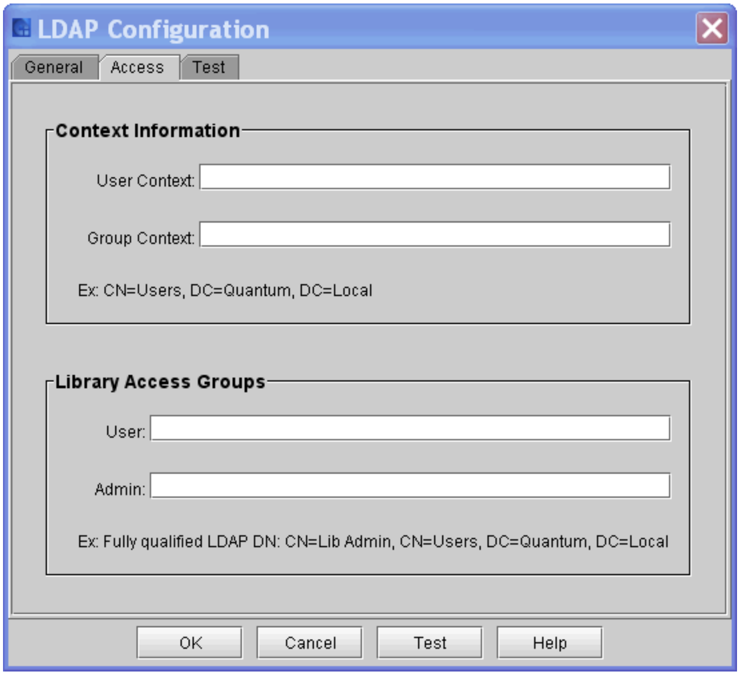
- **Server Configuration** section
  - **Primary:** You must provide a primary IP address or DNS name.
  - **Alternate**: An alternate IP address or DNS name is optional.
  - **Secure**
    Use this check box to enable the setup options to access a secure LDAP server, which can be done using any port except 389. The default secure port is 636. If you enable this option, you must retrieve the Trusted Root Certificate from the server by clicking **Retrieve TR**.
  - **Port:** Enter the appropriate port in this field. The default port for non secure connection is 389 – and 636 for secure (SSL) based LDAP connections. The port setting can be changed.
  - **Retrieve TR:** Use this function to retrieve the Trusted Root Certificate from the LDAP server. A dialog box displays basic Trust Root certificate information, for example, subject name, MD5, and SHA 1 hashes. It is recommended that you verify this information independently on the LDAP server.

CAUTION 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.

- **Search Information** section
  The Search Information section allows you to enter on the LDAP server a user name and password for a user who has sufficient privileges to search for user names. The user name is specified in distinguished name format. To use this feature administrative user rights are not required, but you must have the right to search user names in the LDAP directory.

4 Click the **Access** tab.

Use this tab to configure LDAP authentication.



LDAP Configuration

Context Information

User Context:

Group Context:

Ex: CN=Users, DC=Quantum, DC=Local

Library Access Groups

User:

Admin:

Ex: Fully qualified LDAP DN: CN=Lib Admin, CN=Users, DC=Quantum, DC=Local

- **Context Information** section
  - **User Context**: This is a path in distinguished name format to the location used to search for the login users. You can search for a user in the context specified and all contexts below it.
  - **Group Context**: This is a path in distinguished name format to the location used to search for the groups to which a user belongs. Only groups which are in the Group context or below are considered for library access.

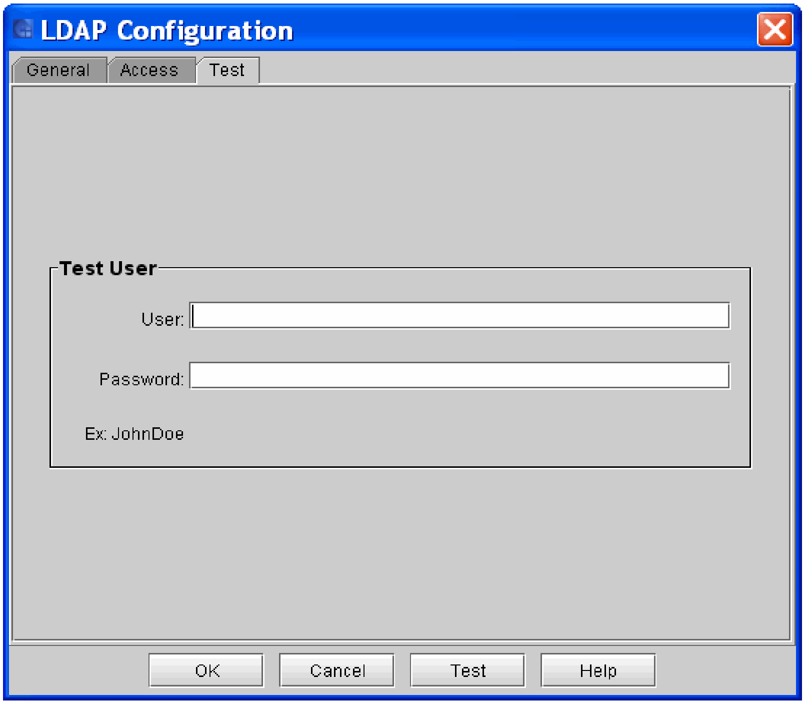
- **Library Access Groups** section
  - **User**: This field contains a fully distinguished name of the groups to which all the library non-admin users belong.
  - **Admin**: This field contains a fully distinguished name of the group to which all admin users belong.

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 needn't 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.

5 To validate your configuration, click **OK** or **Test**.

6 Click the **Test** tab.

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.



Test User

User:

Password:

Ex: JohnDoe

Test User section

- **User**: Type the appropriate User name.
- **Password**: Type the user password.

7 To initiate the library authentication process to the LDAP server, click **Test** after providing the user name and password.

A dialog box appears displaying what level of access the user is assigned, and to which library partition(s) the user has access.

8 After you have entered the LDAP configurations, click **Test** to verify the LDAP connection.

A connection with the LDAP server(s) is established and the library determines whether the LDAP Distinguished Names specified in the Access tab are valid.

A message box appears indicating that 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 was successful, in the message box, click **OK** and continue.

9 To accept and save the library configuration, in the LDAP Configuration dialog box, click **OK**.

10 To validate your configuration, click **OK** or **Test**.

EKM Management Solutions

The Scalar i6000 supports two encryption key management solutions:

- Quantum Encryption Key Manager (Q-EKM) - For IBM LTO-4 Fibre Channel tape drives, IBM LTO-4 SAS tape drives, and IBM LTO-5 Fibre Channel tape drives; and LTO-4 and LTO-5 tape cartridges only.
- Scalar Key Manager (SKM) - For HP LTO-4 and HP LTO-5 Fibre Channel and SAS tape drives and LTO-4 and LTO-5 tape cartridges only. For more information, refer to Running MeDIA Test Reports on page 487

Note These two key management solutions are not interoperable. The Scalar library does not support using both Q-EKM and SKM in the same partition.

The encryption key management solutions generate, protect, store, and manage encryption keys. These keys are used by their respective tape drives to encrypt information being written to, and decrypt information being read from, tape media. Q-EKM and SKM are installed on a server.

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 110 or Step 1: Enabling the EKM License Key below.

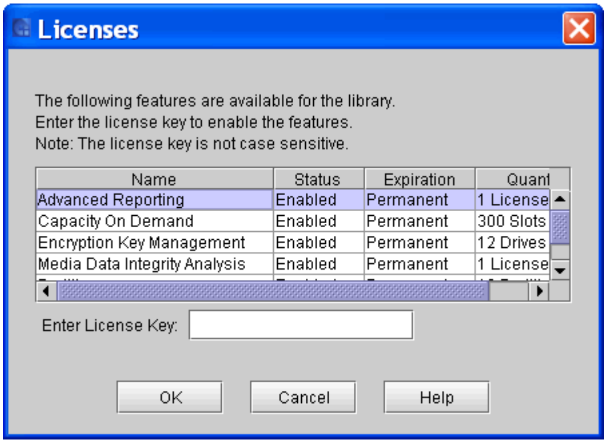
Setting Up EKM on the Scalar i6000

Setting up EKM on the Scalar i6000 consists of the following steps:

Step 1: Enabling the EKM License Key

1 From the menu bar, click **Setup > Licenses**.

The **Licenses** dialog box appears.



Licenses

The following features are available for the library.
Enter the license key to enable the features.
Note: The license key is not case sensitive.

Name	Status	Expiration	Quant
Advanced Reporting	Enabled	Permanent	1 License
Capacity On Demand	Enabled	Permanent	300 Slots
Encryption Key Management	Enabled	Permanent	12 Drives
Media Data Integrity Analysis	Enabled	Permanent	1 License

Enter License Key:

This dialog box lists the licensed features for your library, including their status, expiration date, and quantity.

2 To enable a license key, in the **Enter License Key** box, type the appropriate license key.

You do not need to highlight the feature before you enter a license key. License keys are not case sensitive and all inclusive. For example, J2BGL-22622-52C22 can be entered as j2bgl-22622-52c22.

3 Click **OK**.

Step 2: Configuring the SKM Server

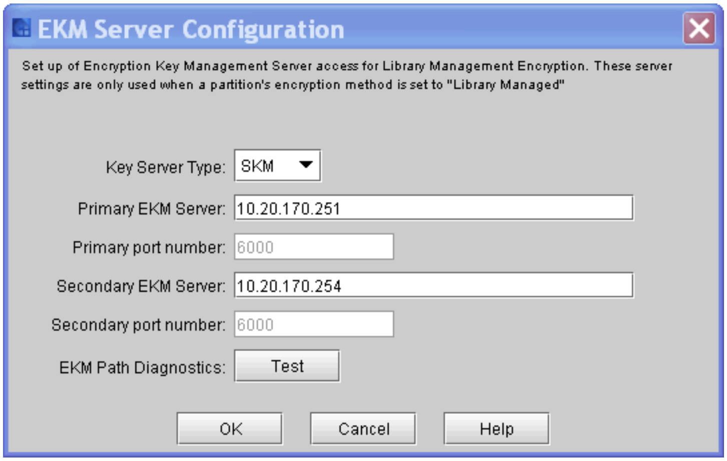
Server settings are only used when a partition's encryption method is set to "Enable Library Managed." For more information on partitions, see Working With Partitions on page 112.

Note In order to synchronize properly, the TCP/IP and SSL ports on the primary and secondary SKM servers must be set to the same values. Synchronization causes the entire configuration properties files of the primary server to overwrite the configuration files on the secondary server. Because the TCP/IP and SSL ports are listed in the configuration properties files, the primary and secondary servers must use the same TCP/IP and SSL port settings.

1 From the menu bar, click **Setup > Encryption > Server Configuration**.

The **SKM Server Configuration** dialog box appears.

Note SKM server settings are used only when a partition's encryption method is set to "Library Managed.



EKM Server Configuration

Set up of Encryption Key Management Server access for Library Management Encryption. These server settings are only used when a partition's encryption method is set to "Library Managed"

Key Server Type: SKM

Primary EKM Server: 10.20.170.251

Primary port number: 6000

Secondary EKM Server: 10.20.170.254

Secondary port number: 6000

EKM Path Diagnostics: Test

2 At the **Key Server Type** drop-down list, select the server type (such as Q-EKM or SKM).

3 In the **Primary SKM Server** text box, type the appropriate host IP address. You can use an iPv4 address or an iPv6 address.

4 In the **Primary port number** text box, accept the displayed default value for the primary SKM server. The port for SKM is 6000, and this value cannot be changed.

5 Optionally, in the **Secondary SKM Server** text box, you can provide the IP address of a secondary SKM server. You can use an iPv4 address or an iPv6 address.

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 SKM Server** text box, or you may leave this text box blank.

6 In the Secondary port number text box, if you configured a secondary server, accept the displayed default value for the secondary server. The port for SKM is 6000, and this value cannot be changed.

7 To test the configuration, click **Test**.

The **Path Diagnostic Results** dialog box appears.

8 Click **Close**. 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.

Step 3: Configuring Partitions for Encryption

You can use the Partition Configuration screen to change the encryption method used by a partition.

Encryption on the Scalar Enterprise library is enabled by partition only. You cannot select individual drives for encryption; you must select an entire partition to be encrypted. Only partitions that are encryption-capable are displayed.

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 modify only one partition at a time.

Encryption Methods, Details, and Restrictions

The following encryption methods are available on the library:

Enable Library Managed — Enables library managed encryption support via a connected key manager server— either Scalar Key Manager (SKM) or Quantum Encryption Key Manager (Q-EKM) — for all tape drives and encryption-capable media assigned to the partition.

- **SKM** supports encryption on LTO-4 data cartridges using HP LTO-4 or newer 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 HP LTO-4 or newer or LTO-5 Fibre Channel tape drives.

  Generating Encryption Keys for SKM: The library automatically generates keys as soon as you set up the servers. Note that you cannot change a partition to Library Managed Encryption until after key generation is complete.

- **Q-EKM** supports encryption on LTO-4 data cartridges using IBM LTO-4 or newer 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 either IBM LTO-4 or newer or LTO-5 Fibre Channel tape drives.

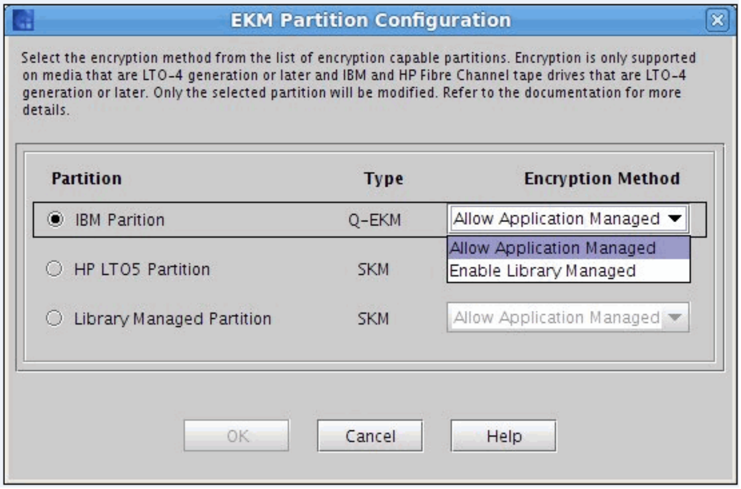
- **If you are using both SKM and Q-EKM**, you must separate the tape drives among the partitions so that each partition only contains tape drives supported by either SKM or Q-EKM. The library will assign the correct servers (SKM or Q-EKM) depending on the drive type in the partition.
- Only LTO-4 or higher tape cartridges will be encrypted in Library Managed Encryption partitions (the partition may can contain LTO-2 and LTO-3 media, but they will not be encrypted).
- In order 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.
- You must have an LME license installed on the library (see Step 1: Enabling the EKM License Key on page 236) before you can select this option.
- Your SKM or Q-EKM servers must be installed, configured on the library, and be operational before you can select this option.

Allow Application Managed — 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.

To change the encryption method

1. Log on as an administrator.
2. If you are not already working from the physical library, select it. From the **View** menu, click the name of the physical library.
3. Click **Setup > Encryption > Partition Configuration**.

The **Partition Configuration** screen appears. Each partition's current encryption method is listed under **Encryption Method**.



EKM Partition Configuration

Select the encryption method from the list of encryption capable partitions. Encryption is only supported on media that are LTO-4 generation or later and IBM and HP Fibre Channel tape drives that are LTO-4 generation or later. Only the selected partition will be modified. Refer to the documentation for more details.

Partition	Type	Encryption Method
● IBM Parition	Q-EKM	Allow Application Managed
○ HP LTO5 Partition	SKM	
○ Library Managed Partition	SKM	Allow Application Managed

4 If you want to change the encryption method on a partition, make sure that no tape drives in that partition have cartridges in them. If there are cartridges in the tape drives, you cannot change the encryption method.

5 For any library partition, change the encryption method by selecting from the **Encryption Method** drop-down list:

- Enable Library Managed
- Allow Application Managed

Note When you change a partition from Enable Library Managed to Allow Application Managed, the 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 Click **OK**.

A warning message is displayed.

7 To take the partition offline, click **Yes**.

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 that occurred during the process.

8 In the **EKM** drop-down list, select the appropriate encryption option. The encryption method that you select will apply to all encryption-capable tape drives and media in that partition.

Encryption Method	Description
Not Supported	Means that no tape drives in that partition support encryption. If "Unsupported" is shown, it is greyed out and you are unable to change the selection.
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 Q-EKM server. This option allows an external backup application to provide encryption support to all encryption-capable tape drives and media within the partition. The library will not communicate with the Q-EKM server(s) (IBM LTO4/5 drives) or SKM servers (HP LTO4/5 drives) for this 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 a connected Q- EKM server for all encryption-capable tape drives and media assigned to the partition.

9 If there are no other changes to your partition, click **Next.**
For more information on partitions, see the online Help or Working With Partitions on page 112.

Encryption and Using Q-EKM on the Scalar i6000

Supporting Encryption

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* (6-01847-01).

The Scalar i6000 library supports encrypting LTO-4 or greater tape media using IBM LTO-4 or greater Fibre Channel drives only. All IBM LTO-4 or greater FC drives are encryption-capable, but to use the Q-EKM software application, you must purchase a Q-EKM 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 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). 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.

Configuring Encryption Settings

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.

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 381 and Updating Drive Firmware on page 398

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 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.

SKM Management

Sharing Encrypted Tape Cartridges

If you are using SKM, you can share 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 249).
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 248).
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 251.

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 Communication Certificates

Transport Layer Security (TLS) certificates are unique certificates that must be installed on the library in order for the library to communicate with the SKM servers.

Normally you only need to install them once, when you initially set up SKM. The Communication Certification Import window allows you to install root, admin, and client certifications, or use the existing TLS bundle provided by Quantum.

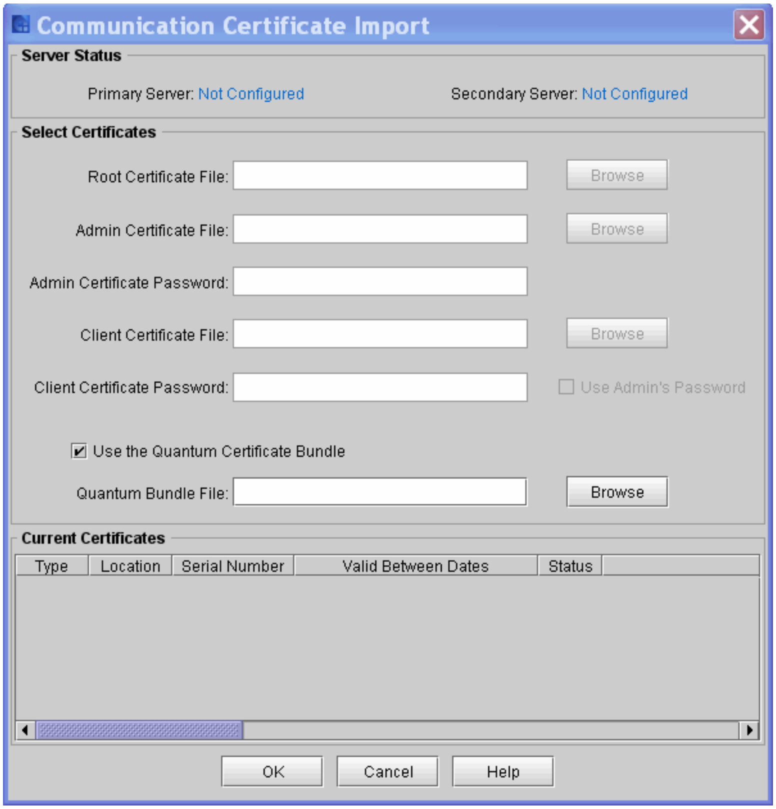
Note You should only need to upload TLS Certificates when upgrading a system up to i8 or above.

You received a CD which contains the TLS certificates bundled in a single file.

1 Insert the CD into the CD ROM drive of your computer. 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.

2 From the **Tools** menu, select **EKM Management > Import Communication Certificates**.

The **Communication Certificate Import** dialog box appears.



Communication Certificate Import

Server Status

Primary Server: Not Configured   Secondary Server: Not Configured

Select Certificates

Root Certificate File:

Admin Certificate File:

Admin Certificate Password:

Client Certificate File:

Client Certificate Password:

□ Use Admin's Password

☑ Use the Quantum Certificate Bundle

Quantum Bundle File:

Current Certificates

Type	Location	Serial Number	Valid Between Dates	Status

Under **Server Status**, the status of the primary and secondary servers appear.

3 Click **Browse** to retrieve the **Root Certificate File**.

4 Click **Browse** to retrieve the **Admin Certificate File.**

5 In the **Admin Certificate Password** field, type the password used when you generated the certificate files.

6 Click **Browse** to retrieve the **Client Certificate File**.

7 In the **Client Certificate Password** field, type the password used when you generated the certificate files.

8 If you choose to use the **Quantum Certificate Bundle**, click the check box, and then click **Browse** to locate the Quantum Bundle File.

Note If you have current certificates, they are listed in the **Current Certificates** section

9 Click **OK**.

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.

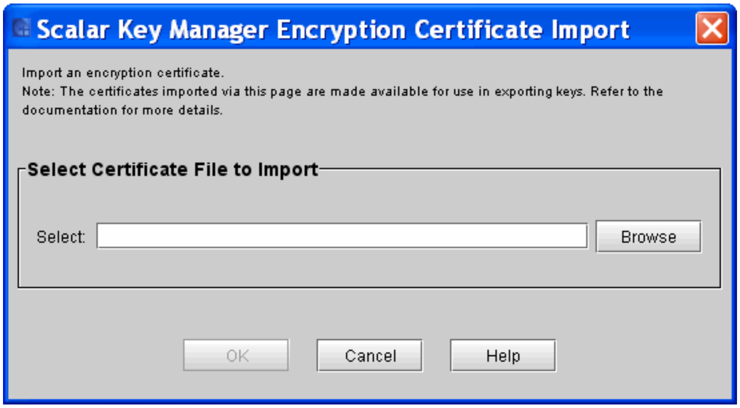
Before starting this process, read and follow the sequence of steps outlined in Sharing Encryption Tape Cartridges—page 248.

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.

.



Import an encryption certificate.
Note: The certificates imported via this page are made available for use in exporting keys. Refer to the documentation for more details.

Select Certificate File to Import

Select:

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.

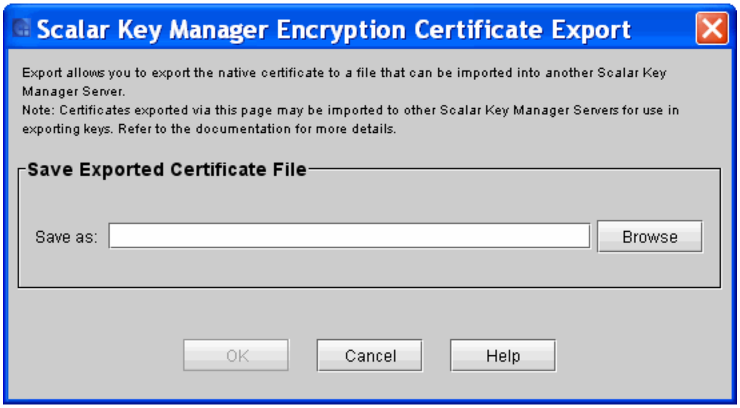
NOTE: This function is available to users with Administrator-level privileges and only applies to SKM servers. Both SKM servers must be connected and operational in order to export encryption key certificates.

To export an encryption key certificate:

1 Before starting this process, read and follow the sequence of steps outlined in Sharing Encrypted Tape Cartridges—page 248.

2 From the Tools menu, select **EKM Management > Encryption Certificate > Export.**

The **SKM Certificate Export** dialog box appears.



Scalar Key Manager Encryption Certificate Export

Export allows you to export the native certificate to a file that can be imported into another Scalar Key Manager Server.
Note: Certificates exported via this page may be imported to other Scalar Key Manager Servers for use in exporting keys. Refer to the documentation for more details.

Save Exported Certificate File

Save as:

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 CartridgesSharing Encrypted Tape Cartridges on page 245.
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.

   The dialog box closes and you are returned to the main console.

Exporting Encryption Keys

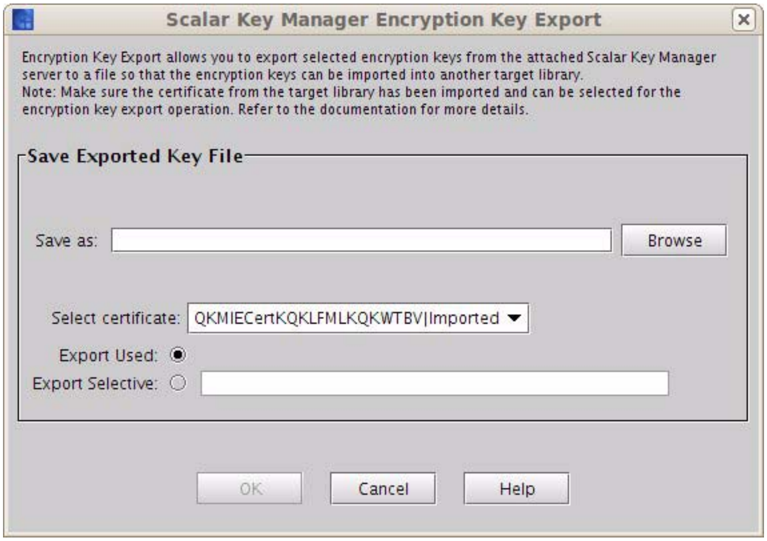
Each SKM server provides a unique encryption key for each tape cartridge that is encrypted. In order for another (i.e., destination) SKM server to read tapes encrypted by your SKM server, you need to export the encryption keys used to encrypt those tapes and send them to the destination server.

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—page 248.
2 From the **Tools** menu, select **EKM Management > Encryption Key > Export**.

The **Scalar Key Manager Encryption Key Expor**t screen appears.


Scalar Key Manager Encryption Key Export

Encryption Key Export allows you to export selected encryption keys from the attached Scalar Key Manager server to a file so that the encryption keys can be imported into another target library.
Note: Make sure the certificate from the target library has been imported and can be selected for the encryption key export operation. Refer to the documentation for more details.

Save Exported Key File

Save as: [Browse]

Select certificate: QKMIECertKQKLFMLKQKWTBV|Imported

Export Used: ●

Export Selective: ○

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—page 248). 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 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

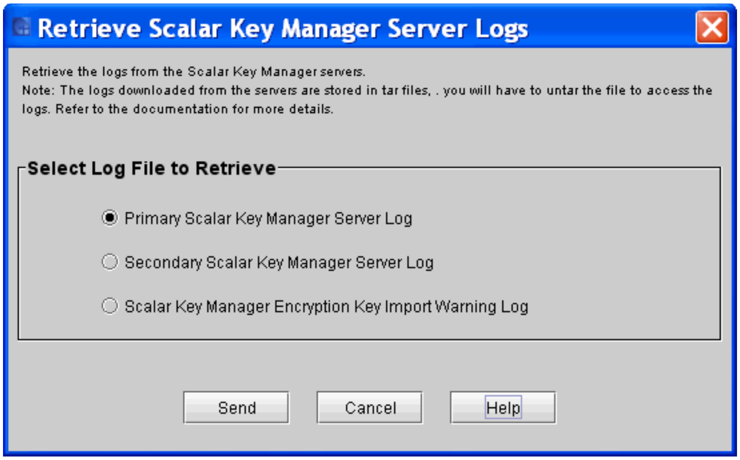
The SKM Server Logs contain information on activity that has occurred on the SKM servers. You can save the logs to a location on a computer, or e-mail the logs to a recipient. The logs downloaded from the servers are stored in the form of tar files.

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.**



Retrieve the logs from the Scalar Key Manager servers.
Note: The logs downloaded from the servers are stored in tar files, . you will have to untar the file to access the logs. Refer to the documentation for more details.

Select Log File to Retrieve

● Primary Scalar Key Manager Server Log

○ Secondary Scalar Key Manager Server Log

○ Scalar Key Manager Encryption Key Import Warning Log

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.

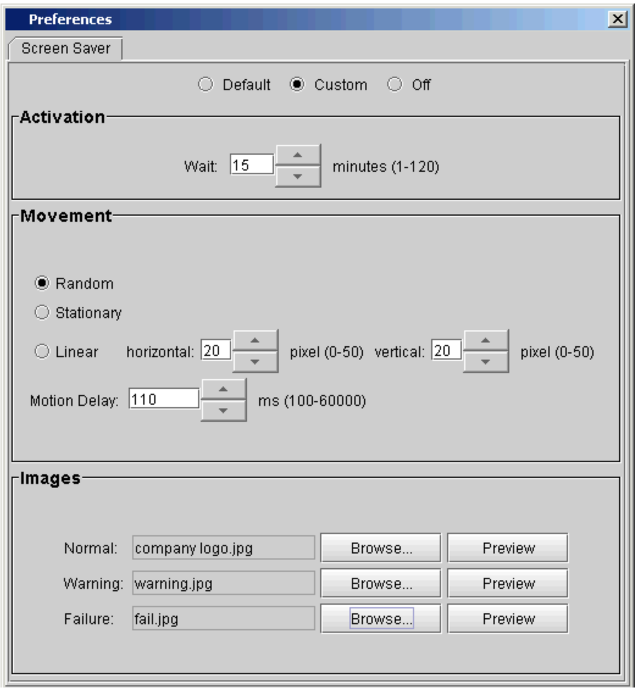
Configuring Screen Saver Preferences

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**→ **Preferences**.

The **Preferences** dialog box appears with the **Screen Saver** tab displayed.



Preferences

Screen Saver

○ Default ● Custom ○ Off

Activation

Wait: 15 minutes (1-120)

Movement

● Random

○ Stationary

○ Linear horizontal: 20 pixel (0-50) vertical: 20 pixel (0-50)

Motion Delay: 110 ms (100-60000)

Images

Normal:	company logo.jpg	Browse...	Preview
Warning:	warning.jpg	Browse...	Preview
Failure:	fail.jpg	Browse...	Preview

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 411.

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 enables 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).

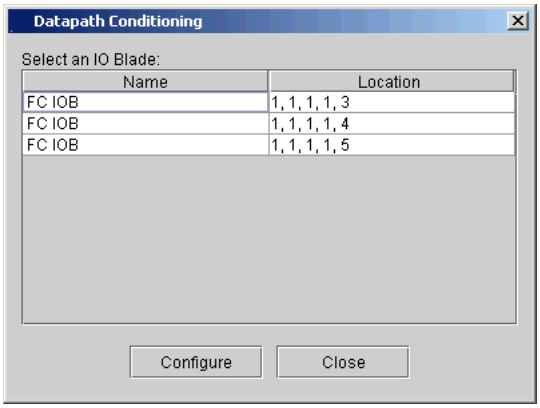
Note I/O blades must be present to access the **Datapath Conditioning** dialog box.

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**→ **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.



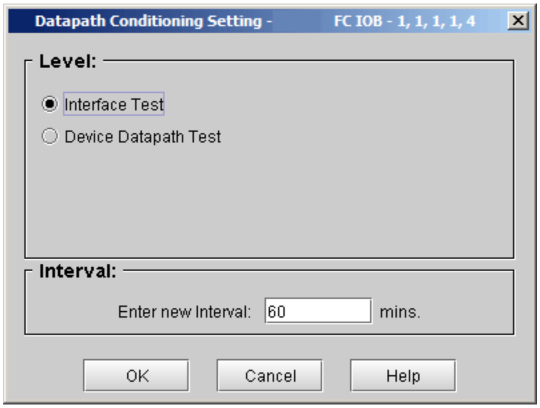
Datapath Conditioning

Select an IO Blade:

Name	Location
FC IOB	1, 1, 1, 1, 3
FC IOB	1, 1, 1, 1, 4
FC IOB	1, 1, 1, 1, 5

4 Click a blade to highlight it, and then click **Configure**.

The **Datapath Conditioning Setting** dialog box appears.



Datapath Conditioning Setting - FC IOB - 1, 1, 1, 1, 4

Level:

● Interface Test

○ Device Datapath Test

Interval:

Enter new Interval: 60 mins.

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 164.

For instructions on how to e-mail or save the configuration record, see Mailing or Saving the Configuration Record on page 356.

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 > Aisle Light Settings**.

   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.

For the time limited settings, if the lights were on before the operation, the timer starts over when the lights are automatically turned on.

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.

The default setting is **Always Off.**

Chapter 5

Running Your Library

This chapter includes the following sections, which explain how to access and operate your library:

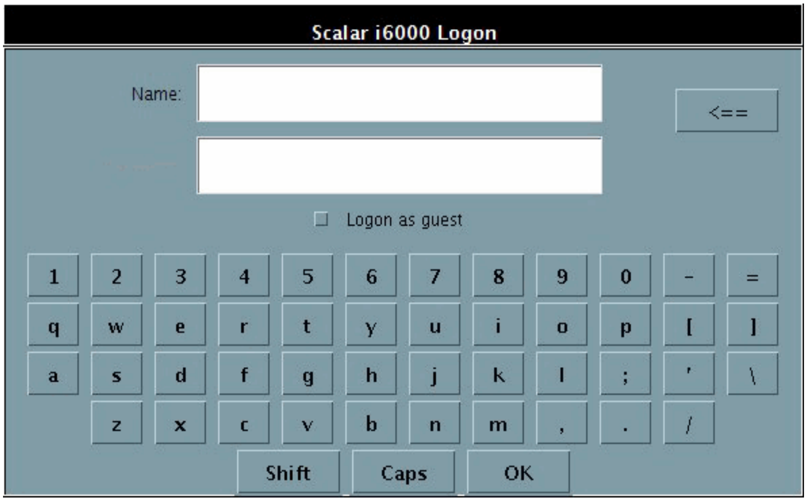
Logging On and Off

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 to access the LMC applet on a host computer.

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.

Only one administrator at any given time can be logged on to the library.

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.

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.

2 A message appears that asks you whether you are sure that you want to log off. Select **Yes**.

The **Scalar i6000 Logon** dialog box appears.

Logging On From the LMC Applet (Web Browser)

The LMC Java applet lets you access all features of the LMC from a host computer using a standard web browser. To use the LMC applet, 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 LMC applet, make sure the host computer meets the following software requirements:

- **Web Browser** – Microsoft Internet Explorer 6.0 or higher, 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 LMC Applet

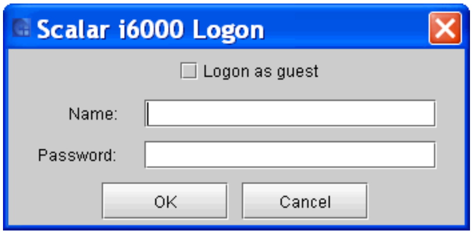
After verifying that the host computer meets the software requirements and has network access to the library, access the LMC applet and log on.

1. On the host computer, point your web browser to the IP address of the library.

   The first time you access the LMC applet it 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.
- Only one administrator at any given time can be logged on to the library.
- 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.

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 From the LMC Applet (Web Browser)

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.

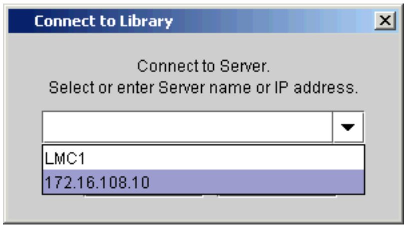
3 To close the LMC applet, click **Cancel**.

Connecting to Multiple Libraries

This feature allows you log in to multiple libraries, and switch from one library console to another without logging off.

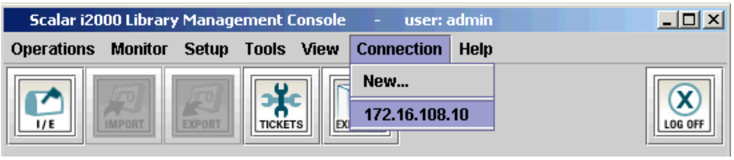
1 From the LMC menu, click **Connection** > **New.**

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.



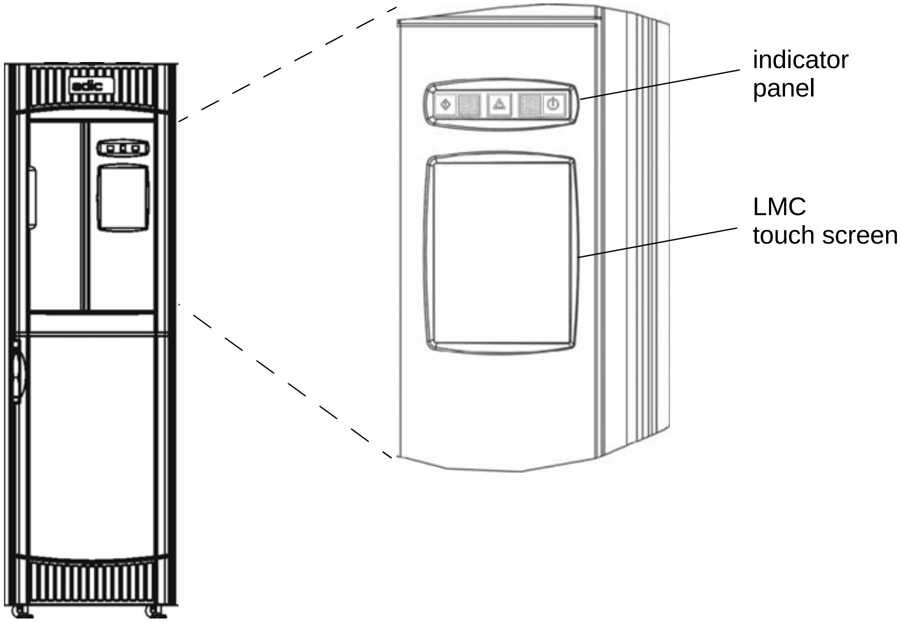
Note

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 Library Op Panel on page 269.

Figure 23 Library Op Panel

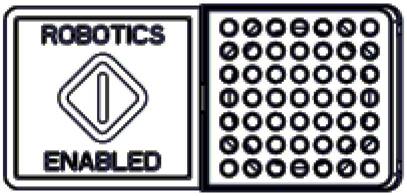


The indicator panel includes a **Robotics Enabled** button with its associated indicator, a **Status** indicator, and a **Power** button with its associated indicator. The Library Management Console (LMC) appears on the touch screen. For more information about indicator panel functions, see table 5 on page 270. For a brief overview of the LMC, see Library Management Console (LMC) on page 271.

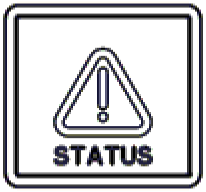
Indicator Panel

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.

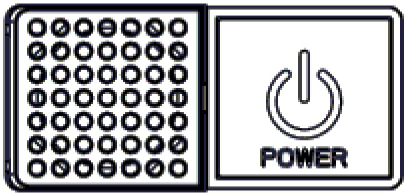
Note — The enabled state does not mean that robotics are communicating with the host. It means that the robotics are communicating with the library controller.



Robotics Enabled indicator and button



Status indicator



Power button and indicator

The following tables describe the indicators in detail.

Table 24 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 25 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 26 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 the LMC Applet (Web Browser) on page 265.

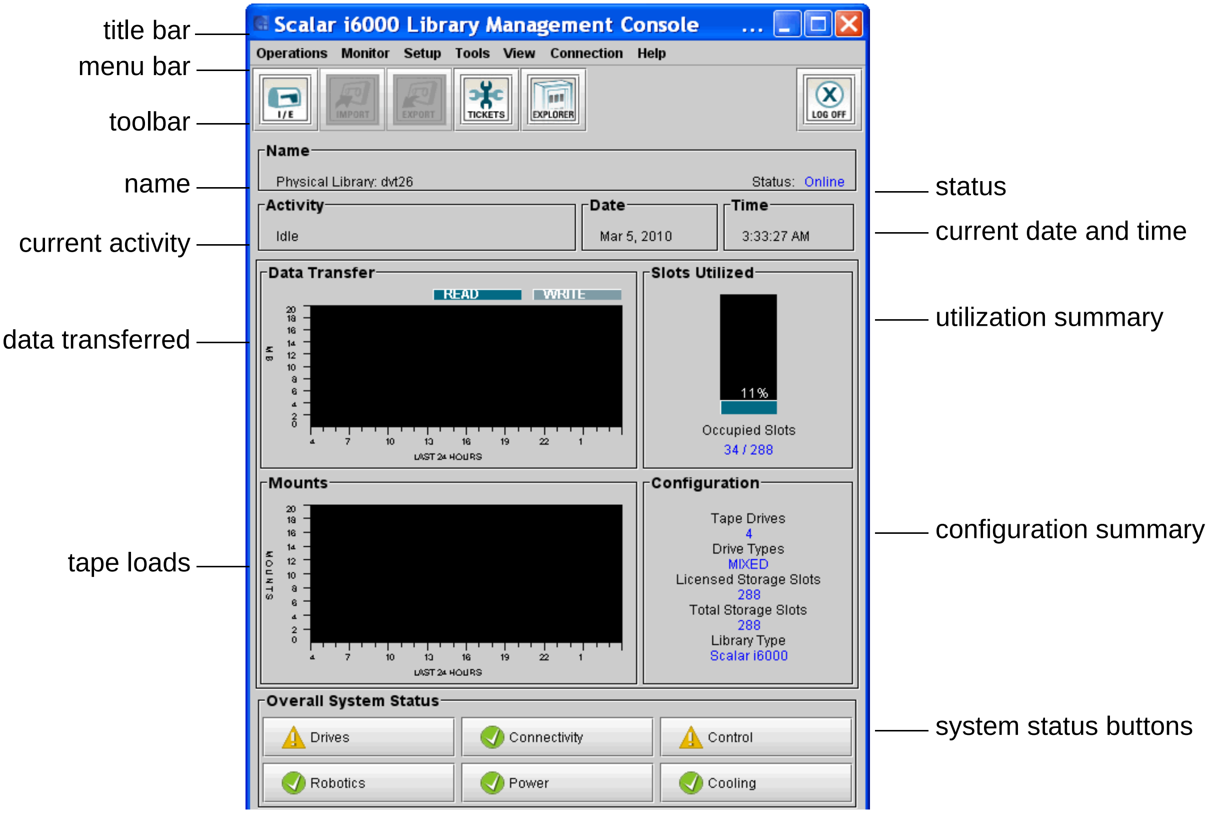
Note To manage your library from a remote client, you must set up the library's initial network configuration from the touch screen. For more information, see Setting Up the Network Configuration on page 145.

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 different on the remote client view of the LMC. Compare figure 24 to figure 25.

- 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 24 LMC (Local Touch Screen - Physical Library View)



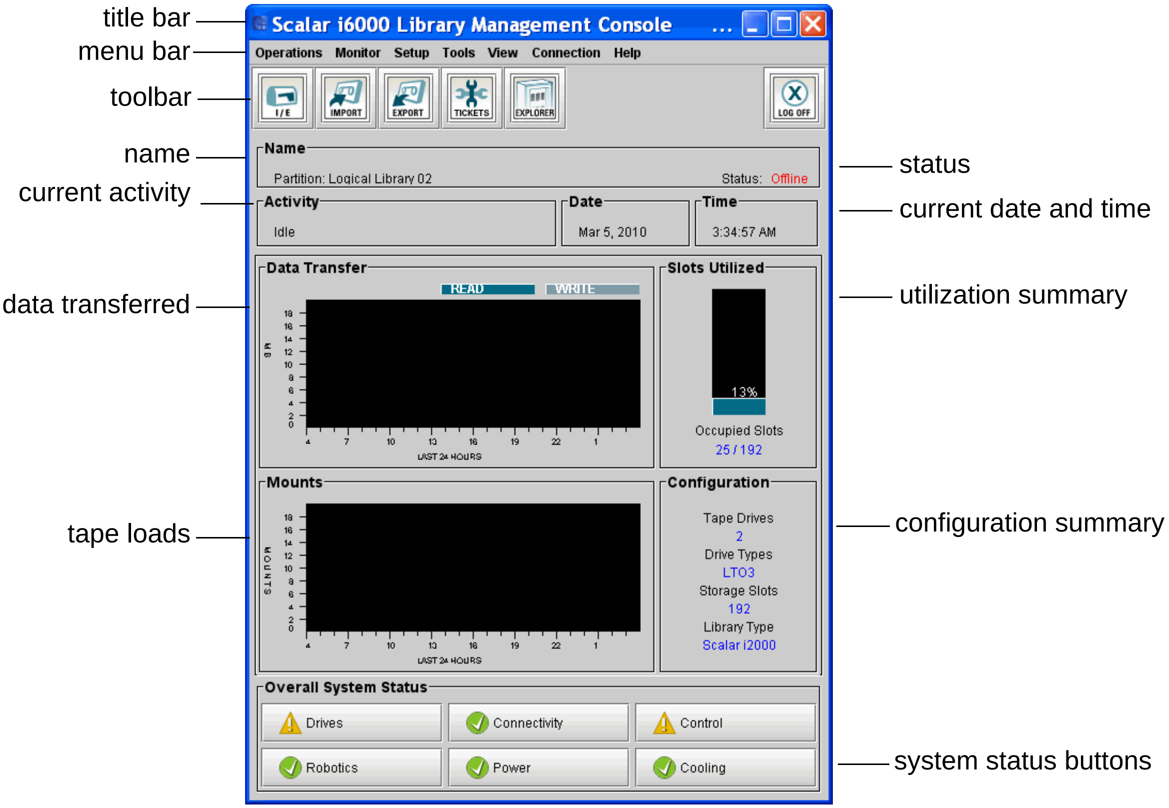
Physical Library: dvt26
Status: Online

Activity: Idle
Date: Mar 5, 2010
Time: 3:33:27 AM

Occupied Slots
34 / 288

Tape Drives
4
Drive Types
MIXED
Licensed Storage Slots
288
Total Storage Slots
288
Library Type
Scalar i6000

Figure 25 LMC (Remote Client With Partition View Shown)



Name

Partition: Logical Library 02

Status: Offline

Activity: Idle

Date: Mar 5, 2010

Time: 3:34:57 AM

Occupied Slots 25 / 192

Configuration

Tape Drives 2

Drive Types LTO3

Storage Slots 192

Library Type Scalar i2000

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 27 on page 275 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 27 Menu Commands: Privileges and Environments

Menu Command	Privilege Level	Physical Library View	Partition View	Touch Screen	Remote
On the 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
On the 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

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 in it. 11 Guest can view the main LMC display, but cannot obtain more details or perform operations.

Table 27 Menu Commands: Privileges and Environments

Menu Command (Continued)	Privilege Level	Physical Library View	Partition View	Touch Screen	Remote
IO Blade	Admin, User[1]	X		X	X
SCSI Channel	Admin, User[1]	X		X	X
Fibre Channel	Admin, User[1]	X		X	X
Ethernet Blade	Admin, User	X		X	X
IE Station	Admin, User[1]	X		X	X
Extended IE Slots	Admin, User	X	X	X	X
Slots	Admin, User[1]	X	X	X	X
Media	Admin, User[1]	X	X	X	X
Sensor	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	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 in it. 11 Guest can view the main LMC display, but cannot obtain more details or perform operations.

Table 27 Menu Commands: Privileges and Environments

Menu Command (Continued)	Privilege Level	Physical Library View	Partition View	Touch Screen	Remote
On the 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
Device	Admin, User[1]	X	X	X	X
IDs[4]	Admin, User[1]		X	X	X
Access	Admin	X		X	X
Channel Zoning	Admin	X		X	X
SCSI Host	Admin	X		X	X
FC Host	Admin	X		X	X
SNW Host	Admin	X		X	X
SNW Drives	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

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 in it. 11 Guest can view the main LMC display, but cannot obtain more details or perform operations.

Table 27 Menu Commands: Privileges and Environments

Menu Command (Continued)	Privilege Level	Physical Library View	Partition View	Touch Screen	Remote
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
Physical Library	Admin	X		X	X
Local Users	Admin	X		X	X
Notification	Admin	X		X	X
System Setup	Admin	X		X	X
Media Security	Admin	X		X	X
Date and Time	Admin	X		X	X
Licenses	Admin	X		X	X
Email Configuration	Admin	X		X	X
Trap Registration	Admin	X		X	X
Security[8]	Admin	X		X	
LDAP	Admin	X		X	X
Drive Cleaning	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 in it. 11 Guest can view the main LMC display, but cannot obtain more details or perform operations.

Table 27 Menu Commands: Privileges and Environments

Menu Command (Continued)	Privilege Level	Physical Library View	Partition View	Touch Screen	Remote
Encryption	Admin	X		X	X
Server Configuration	Admin	X		X	X
Partition Configuration	Admin	X		X	X
Preferences	Admin	X		X	X
Aisle Light Settings	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 in it. 11 Guest can view the main LMC display, but cannot obtain more details or perform operations.					

Table 27 Menu Commands: Privileges and Environments

Menu Command (Continued)	Privilege Level	Physical Library View	Partition View	Touch Screen	Remote
On the 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
Update Drive Firmware	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
Media	Admin	X			X
Integrity Analysis	Admin	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 in it. 11 Guest can view the main LMC display, but cannot obtain more details or perform operations.

Table 27 Menu Commands: Privileges and Environments

Menu Command (Continued)	Privilege Level	Physical Library View	Partition View	Touch Screen	Remote
Usage	Admin	X			X
Security	Admin	X			X
Library Configuration		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
Retrieve SKM Logs	Admin	X	X	X	X
MeDIA	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 in it. 11 Guest can view the main LMC display, but cannot obtain more details or perform operations.

Table 27 Menu Commands: Privileges and Environments

Menu Command (Continued)	Privilege Level	Physical Library View	Partition View	Touch Screen	Remote
Test Selection...	Admin	X		X	X
Test Reports...	Admin	X		X	X
Sift Sort	Admin	X	X	X	X
Export...	Admin	X	X	X	X
Capture Report...	Admin	X	X	X	X
On the 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
On the Connection menu:					
New	Admin, User, Guest	X	X		X
[library IP address]	Admin, User, Guest	X	X		X
On the Help menu:					
Content	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 in it. 11 Guest can view the main LMC display, but cannot obtain more details or perform operations.

Table 27 Menu Commands: Privileges and Environments

Menu Command (Continued)	Privilege Level	Physical Library View	Partition View	Touch Screen	Remote
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 in it. 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 338.

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 511.

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 513.

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 37.

The **Library 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 **Log Off** button logs off the current user after confirming the logoff request. You also can log off by clicking **Operations**→ **Log Off**. For more information, see Logging On and Off on page 263.

Reading the Library Information Panel

The library information panel, shown in Figure 26, occupies the central portion of the main LMC display. It provides you with a significant amount of dynamically updated status information.

Figure 26 LMC (Remote Client With Partition View Shown)

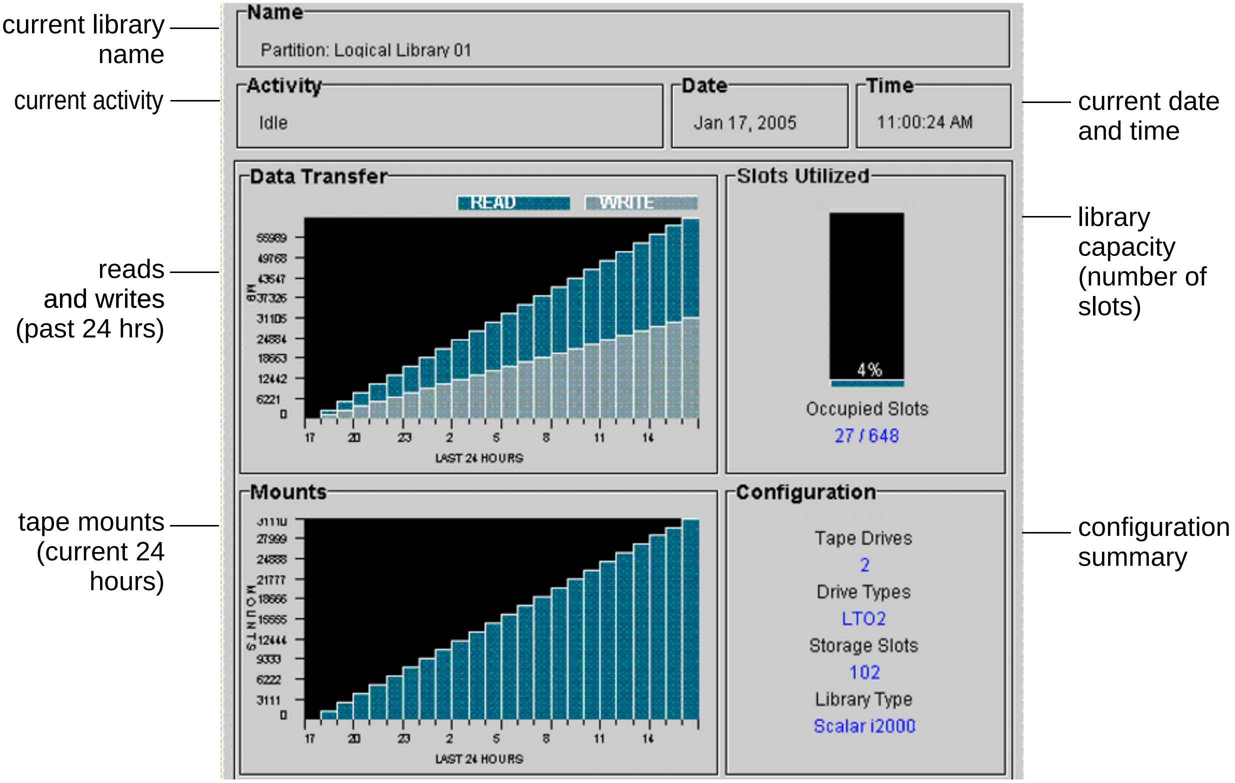

Name
Partition: Logical Library 01
Activity
Idle
Date
Jan 17, 2005
Time
11:00:24 AM
Slots Utilized
Occupied Slots
27 / 648
Configuration
Tape Drives
2
Drive Types
LTO2
Storage Slots
102
Library Type
Scalar i2000

Table 28 describes the areas on the library information panel.

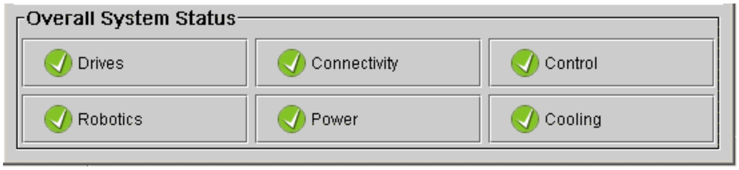
Table 28 Areas on the Library Information Panel

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.
Activity	The current activity for the current library.
Date	The current date. The date that appears reflects user settings, but the system operates according to Greenwich Mean Time (GMT).
Time	The current user enabled time. 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.
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

System Status Buttons

System status buttons are located in the **Overall System Status** area at the bottom of the LMC (see figure 27).

Figure 27 System Status Buttons in Good Status



Each button represents a subsystem. Table 29 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 29 Subsystems and Their Components

Subsystem	Components
Drives	Drives and media, such as brick firmware, drive bricks, drive sleds, cartridges, and magazines
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, 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

Table 29 Subsystems and Their Components (Continued)

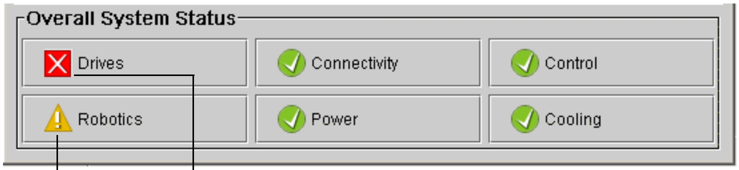
Subsystem	Components
Cooling	Cooling system components, such as fans for the library management module (LMM) and the I/O management unit

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 27 indicate that all subsystems are functioning normally (Good), while those shown in figure 28 indicate that issues exist in the Drives and Robotics subsystems.

Figure 28 Status Buttons - Drives and Robotics Issues



indicates Failed status

indicates Warning or Degraded status

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 47.

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 360.

Cartridge Locations

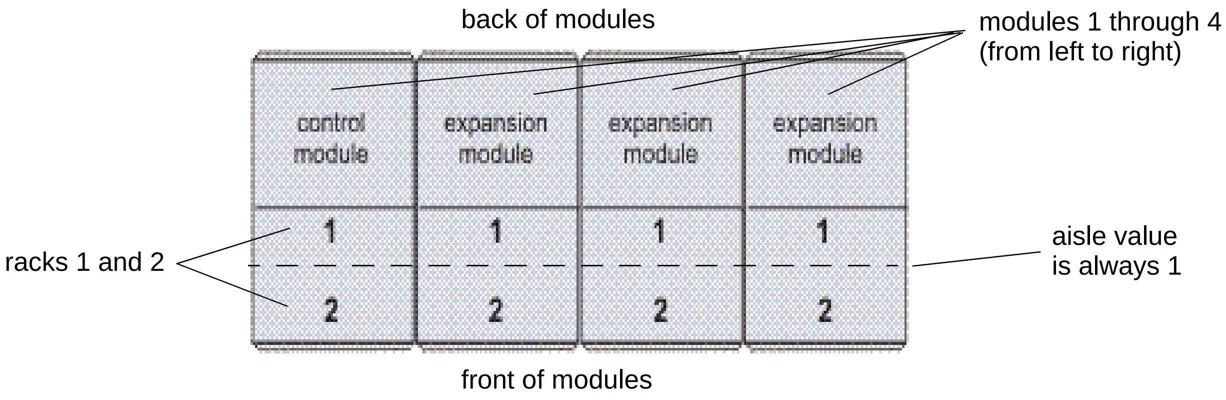
The library uses a coordinate addressing system that indicates the location of cartridges using six coordinates. The coordinates are represented by the library in a comma separated list. For example:

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 will always be 1.
- **Module** — there are from one to twelve modules (the control module and up to seven expansion modules). The value will be between 1 and 12.
- **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.

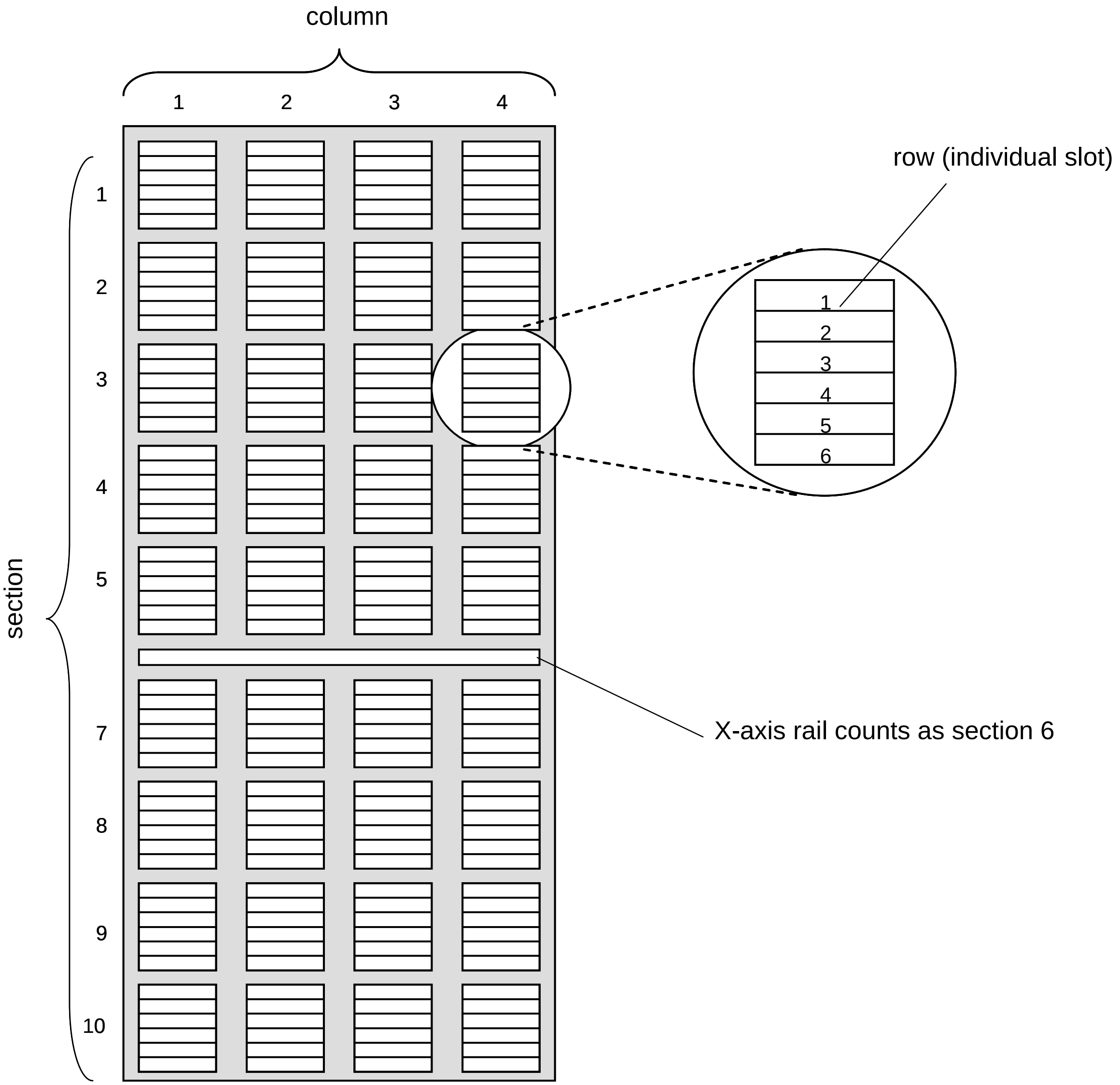
Figure 29 Aisle, Module, and Rack Numbering Locations



- **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.
- **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 and between 1 and 5 for DLT cartridges.

Figure 29 shows the section, column and row numbering for rack 1 of a library that contains LTO cartridges. See figure 30 on page 290 to review rack numbering.

Figure 30 Section, Column, and Row Numbering for Rack 1 - LTO Cartridges



Note

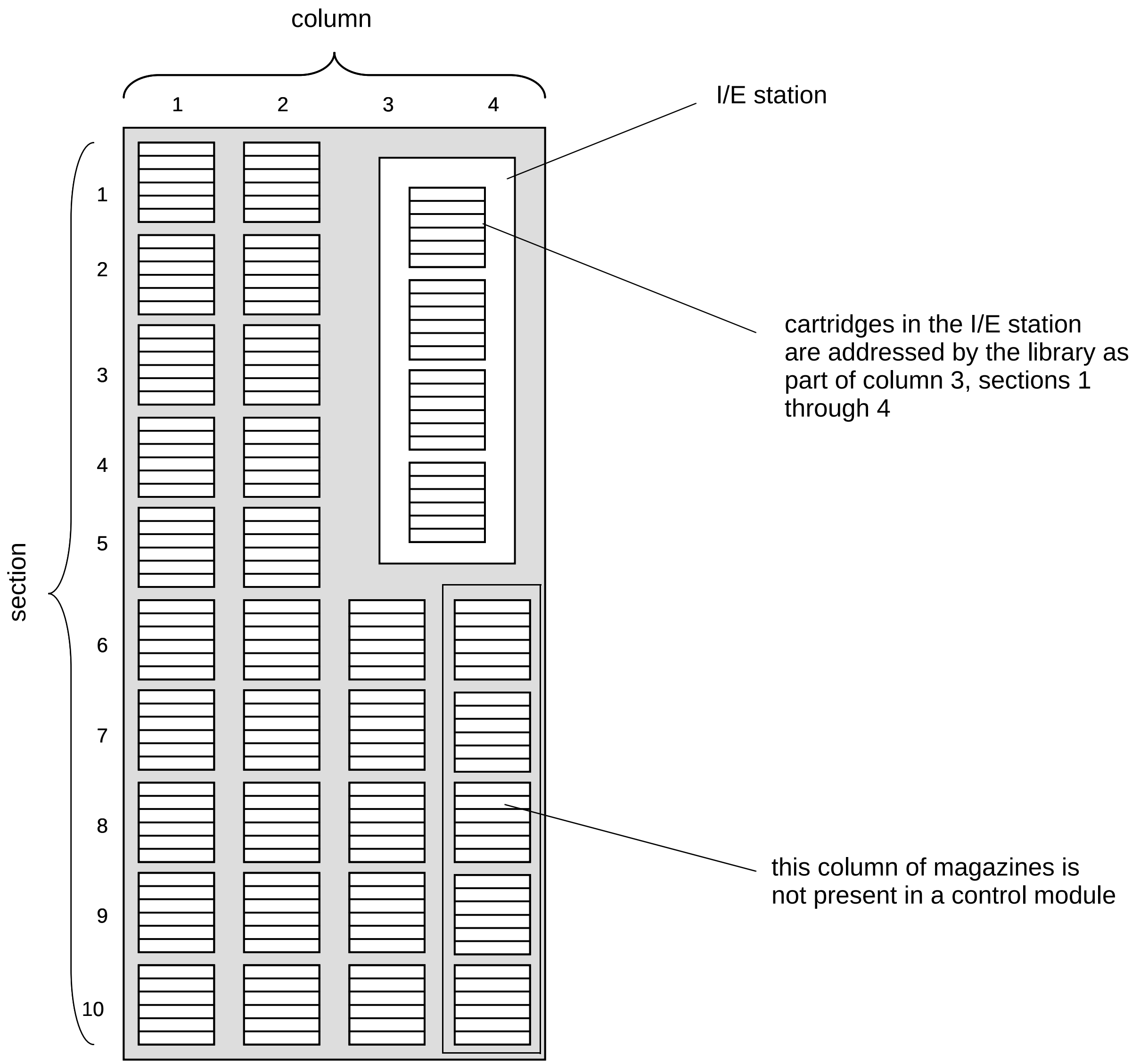
- Tape drives that are installed in rack 1 of a control module or an expansion module replace storage in columns 1 and 2. Because drives are installed from the bottom to the top, you lose the storage starting in section 10 first. You do not lose the magazine in columns 1 and 2 of section 5.
- Column 1 never contains storage in the control module.

Figure 31 on page 292 shows the section, column, and row numbering for rack 2 of a library that contains LTO cartridges. See figure 29 on page 289 to review rack numbering.

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 31 on page 292.

Figure 31 Section, Column, and Row Numbering for Rack 2 - LTO Cartridges



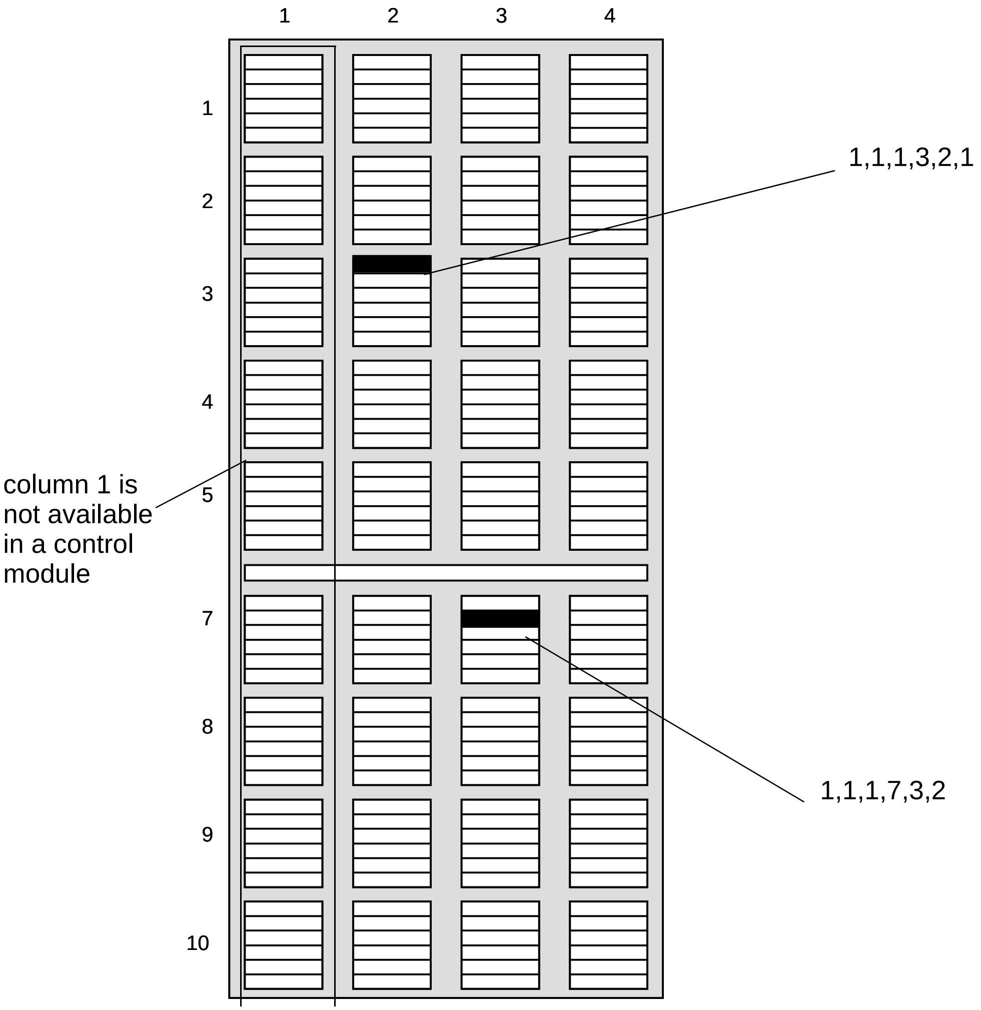
cartridges in the I/E station are addressed by the library as part of column 3, sections 1 through 4

this column of magazines is not present in a control module

Note In figure 31 on page 292, the five magazines shown in column 4, sections 6-10 do not exist in a control module. However, these magazines exist in expansion modules.

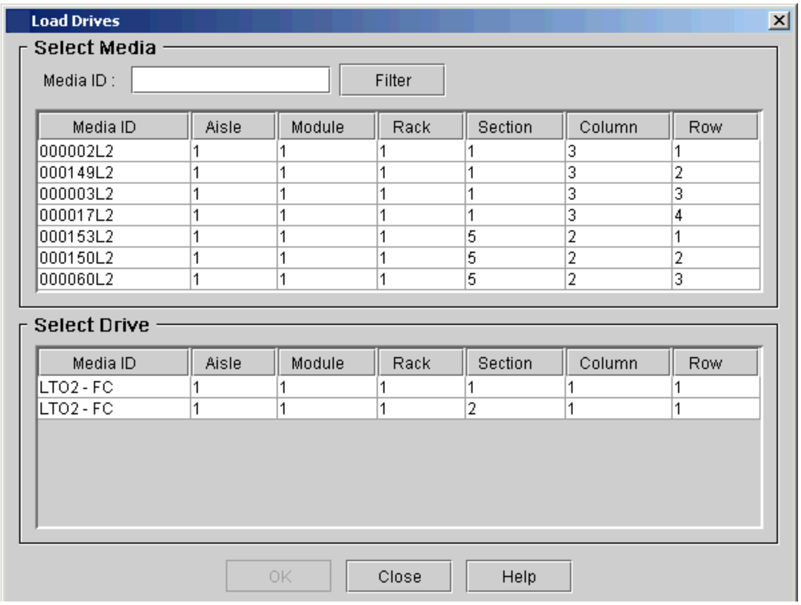
Figure 32 on page 294 shows examples of location coordinates. These examples assume that the linear storage is located in aisle 1, module 1, and rack 1. That is why the first three numbers in the comma separated list are 1,1,1. The last three numbers represent the address on the linear storage assembly.

Figure 32 Example Location Coordinates



The LMC uses dialog boxes, like the one shown in figure 33, 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 33 Coordinates in Load Drives Dialog



Media ID	Aisle	Module	Rack	Section	Column	Row
000002L2	1	1	1	1	3	1
000149L2	1	1	1	1	3	2
000003L2	1	1	1	1	3	3
000017L2	1	1	1	1	3	4
000153L2	1	1	1	5	2	1
000150L2	1	1	1	5	2	2
000060L2	1	1	1	5	2	3

Media ID	Aisle	Module	Rack	Section	Column	Row
LTO2 - FC	1	1	1	1	1	1
LTO2 - FC	1	1	1	2	1	1

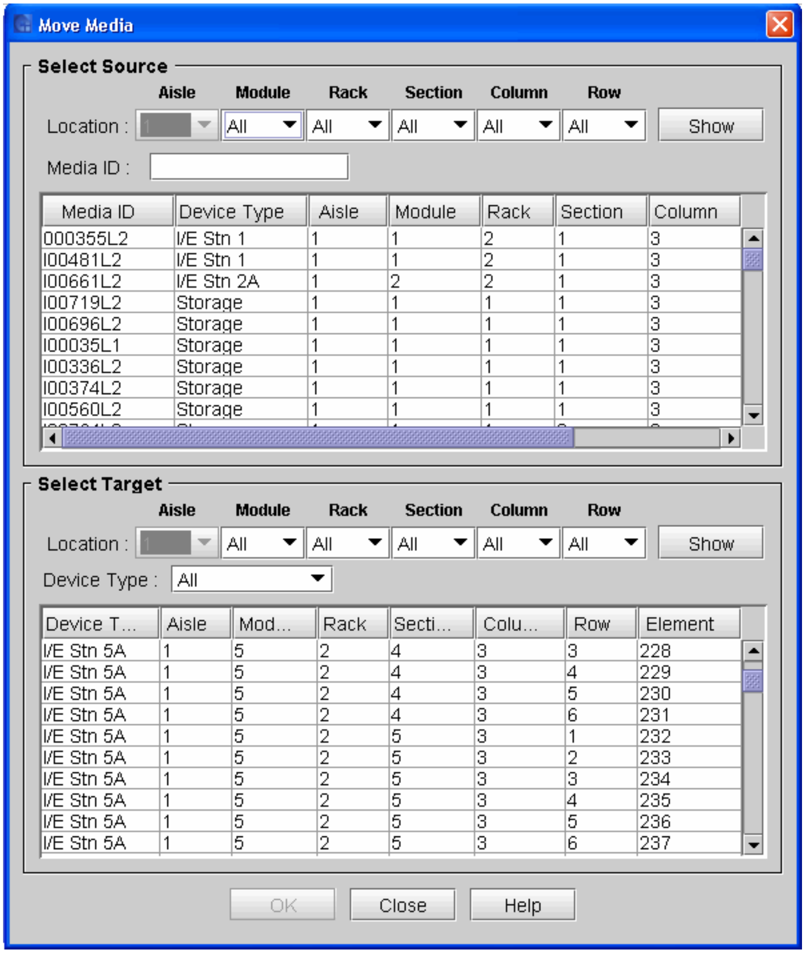
Tape Drive Locations

The location coordinates of a drive is based on the position of the drive in the module and section.

- Tape drives are always in rack 1, column 1, of a particular module.
- Columns are read from left to right as you face the rack.
- 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 with each drive cluster containing up to six drives.

- Drive number 1 is in the lowest section of the lower drive cluster. Drives are numbered from bottom to top. Figure 35 on page 298 shows the physical location of drive 9, which is the last drive listed in the **Move Media** dialog box shown in figure 34. Compare with table 30.

Figure 34 Location Coordinates for Drives



Select Source

Location : Aisle 1, Module All, Rack All, Section All, Column All, Row All

Media ID :

Media ID	Device Type	Aisle	Module	Rack	Section	Column
000355L2	I/E Stn 1	1	1	2	1	3
I00481L2	I/E Stn 1	1	1	2	1	3
I00661L2	I/E Stn 2A	1	2	2	1	3
I00719L2	Storage	1	1	1	1	3
I00696L2	Storage	1	1	1	1	3
I00035L1	Storage	1	1	1	1	3
I00336L2	Storage	1	1	1	1	3
I00374L2	Storage	1	1	1	1	3
I00560L2	Storage	1	1	1	1	3

Select Target

Location : Aisle 1, Module All, Rack All, Section All, Column All, Row All

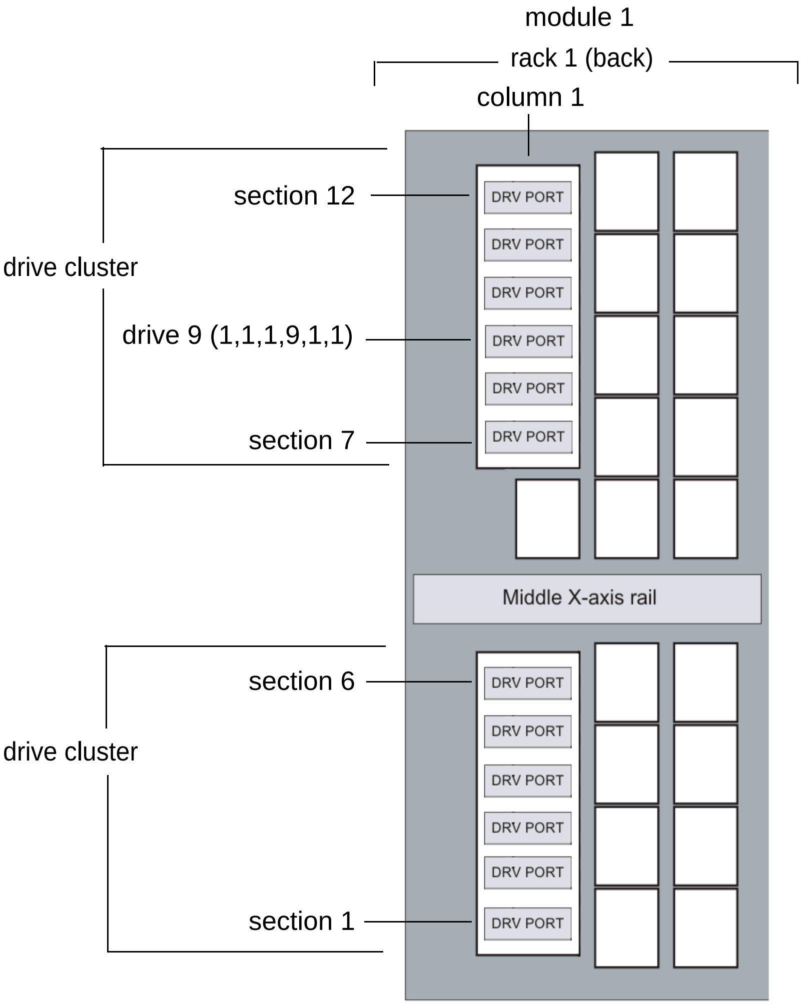
Device Type : All

Device T...	Aisle	Mod...	Rack	Secti...	Colu...	Row	Element
I/E Stn 5A	1	5	2	4	3	3	228
I/E Stn 5A	1	5	2	4	3	4	229
I/E Stn 5A	1	5	2	4	3	5	230
I/E Stn 5A	1	5	2	4	3	6	231
I/E Stn 5A	1	5	2	5	3	1	232
I/E Stn 5A	1	5	2	5	3	2	233
I/E Stn 5A	1	5	2	5	3	3	234
I/E Stn 5A	1	5	2	5	3	4	235
I/E Stn 5A	1	5	2	5	3	5	236
I/E Stn 5A	1	5	2	5	3	6	237

Table 30 Drive Location Coordinates

1	**1-8**	**1**	**1-12**	**1**	**1**
Aisle	Module	Rack	Section	Column	Row

Figure 35 Drive-side Location Coordinates



I/O Blade Locations

The LMC displays I/O blade locations in parenthetical format. For example, see the **Connectivity** dialog box in figure 36. The location for the first I/O blade listed in the **Connectivity** dialog box is reported as (1,1,1,1,3). The location coordinates see aisle, module, rack, cluster, and bay. By reading the numbers backwards, you can determine that the location of the I/O blade is in bay 3 of the control module’s I/O management unit. In figure 37 on page 300, its bay (1,1,1,1,3) is shaded gray. This figure shows the numbering sequence and the bay positions in the I/O management unit.

Figure 36 I/O Blade Location Coordinates

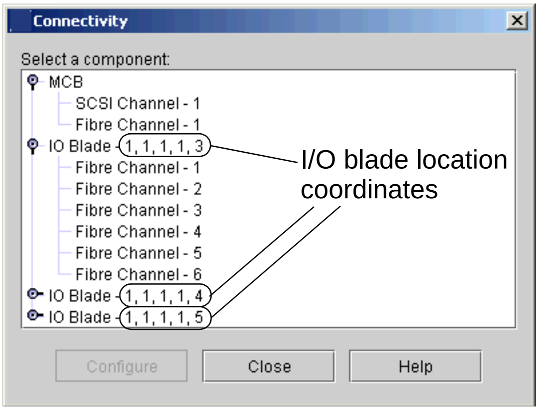
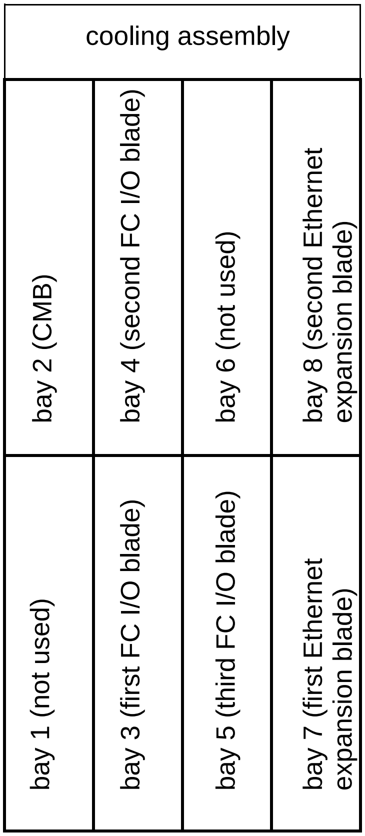


Figure 37 I/O Management Unit Bay Numbering


cooling assembly
bay 2 (CMB)
bay 4 (second FC I/O blade)
bay 6 (not used)
bay 8 (second Ethernet expansion blade)
bay 1 (not used)
bay 3 (first FC I/O blade)
bay 5 (third FC I/O blade)
bay 7 (first Ethernet expansion blade)

Note Bay 2 is used as the control management blade. Bay 1 is not used.

The definitions for aisle, module, and rack are the same for I/O blades as they are for other library components. For more information, see Cartridge Locations on page 288.

The key to interpreting the last two blade location coordinates follows:

- **Cluster** — the cluster designation for the I/O management unit is always 1.
- **Bay** — there are eight bays in the I/O management unit. If you look at the I/O management unit from the back of a library module, bay 1 is the bay on the lower left. Bay 1 is not populated. Bay 2 always contains a management control blade (MCB). No I/O blades can be installed in bays 1 or 2. Bays 3 through 5 can contain I/O blades.

Table 31 Blade Location Coordinates

1	1-8	1	1	3-8
Aisle	Module	Rack	Cluster	Bay

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.

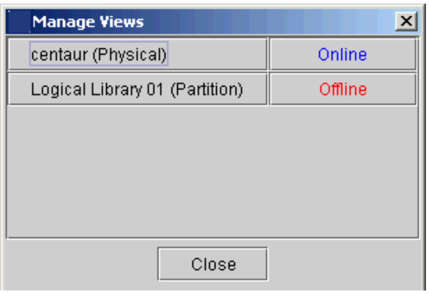
After you select a library view, the library information panel area of the main LMC display shows status information and statistical details about the physical library or partition.

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.



Manage Views

centaur (Physical)	Online
Logical Library 01 (Partition)	Offline

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.

3 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.

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.

The **Change Library Mode** dialog box appears.

For more information about using this dialog box to change online or offline mode, see Changing the Library's State on page 303.

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.

Note 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 316.

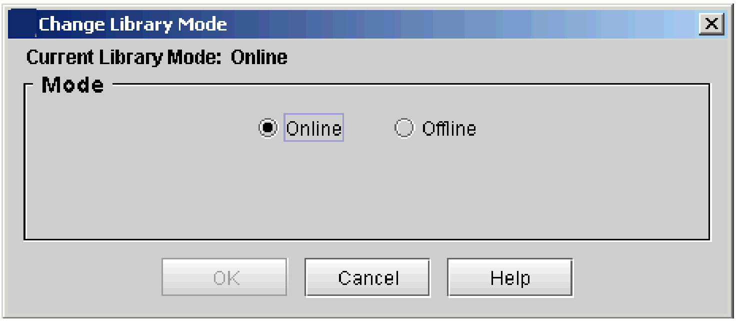
Taking the Physical Library or a Partition Online or Offline

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.



Change Library Mode

Current Library Mode: Online

Mode

● Online ○ Offline

- 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 32 on page 305 summarizes the library functions that require the physical library or partitions to be either online or offline.

Table 32 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 27 on page 275.

For information on user accounts that reside on a Lightweight Directory Access Protocol (LDAP) server, see Using LDAP on page 228.

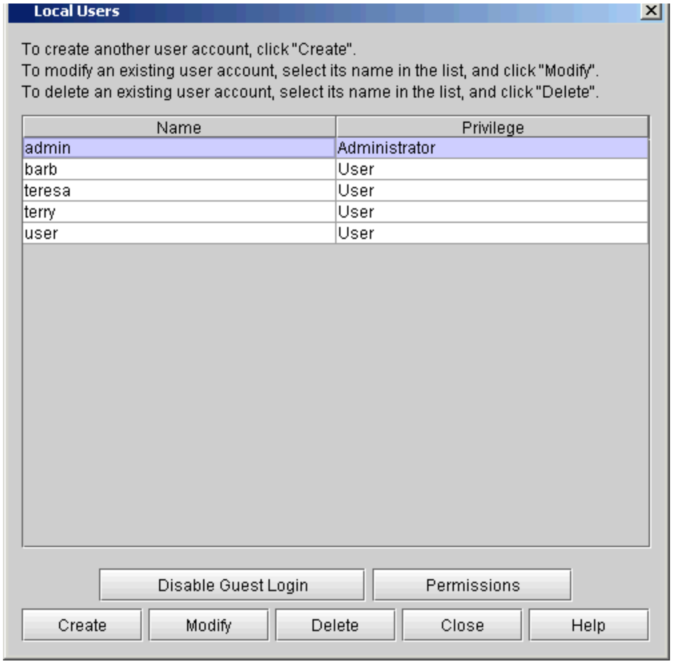
Creating Local User Accounts

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** > **Local Users**.

The **Local Users** dialog box appears.



Local Users

To create another user account, click "Create".
To modify an existing user account, select its name in the list, and click "Modify".
To delete an existing user account, select its name in the list, and click "Delete".

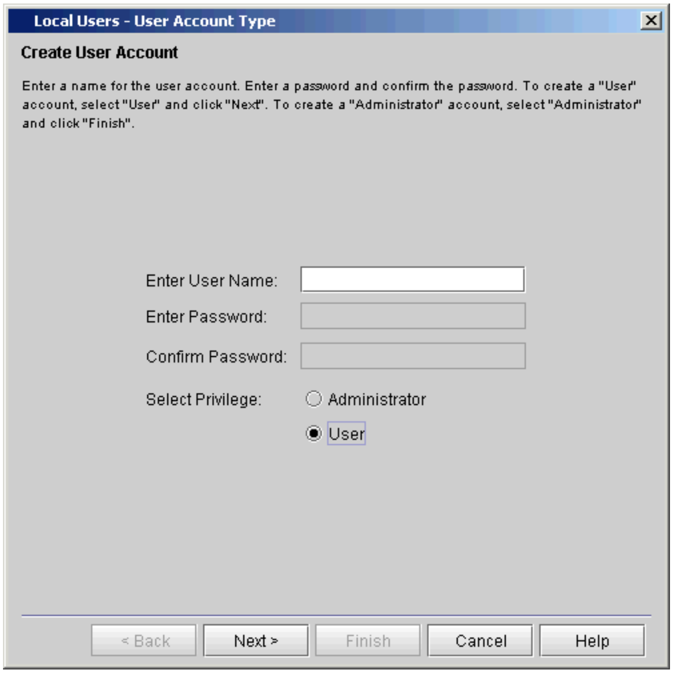
Name	Privilege
admin	Administrator
barb	User
teresa	User
terry	User
user	User

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 27 on page 275.

5 To create a user account, click **Create**.

The **Local Users - User Account Type** dialog box appears.



Local Users - User Account Type

Create User Account

Enter a name for the user account. Enter a password and confirm the password. To create a "User" account, select "User" and click "Next". To create a "Administrator" account, select "Administrator" and click "Finish".

Enter User Name:

Enter Password:

Confirm Password:

Select Privilege: ○ Administrator
● User

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.

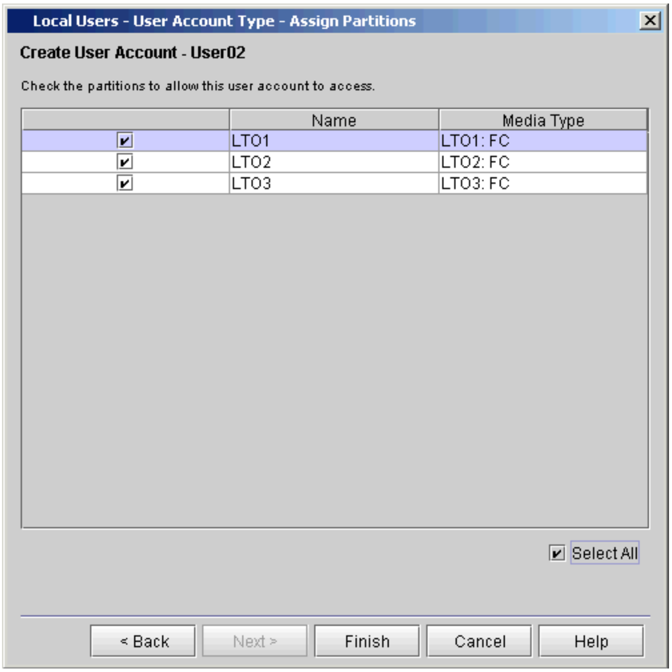
9 For **Select Privilege**, select a privilege level (**Administrator** or **User**).

Note For a list of commands that are available to administrators and users, see table 27 on page 275.

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.



Local Users - User Account Type - Assign Partitions

Create User Account - User02

Check the partitions to allow this user account to access.

	Name	Media Type
☑	LTO1	LTO1: FC
☑	LTO2	LTO2: FC
☑	LTO3	LTO3: FC

☑ Select All

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.

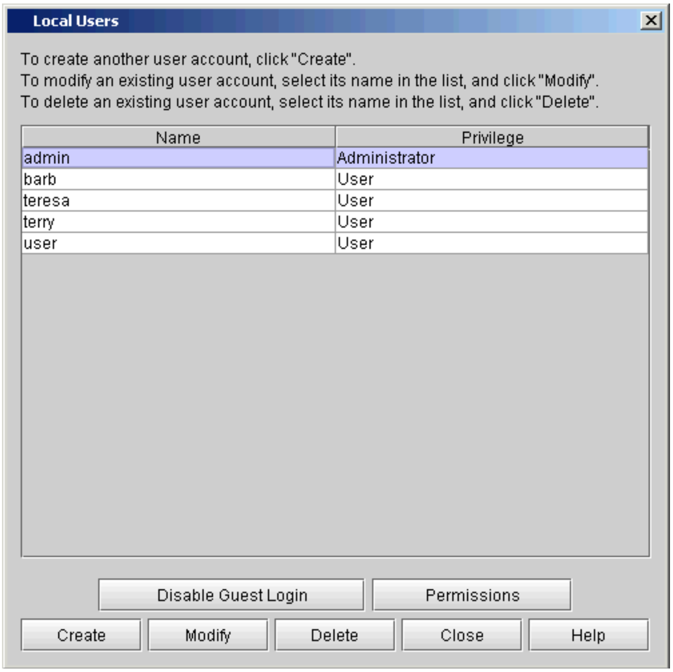
Modifying Local User Accounts

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**→ **Local Users**.

The **Local Users** dialog box appears.



Local Users

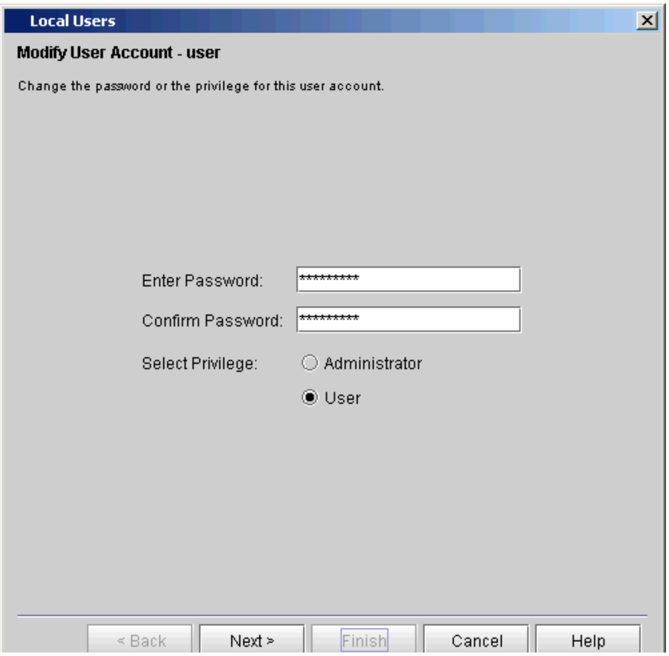
To create another user account, click "Create".
To modify an existing user account, select its name in the list, and click "Modify".
To delete an existing user account, select its name in the list, and click "Delete".

Name	Privilege
admin	Administrator
barb	User
teresa	User
terry	User
user	User

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 27 on page 275.

4 Click the name of the account that you want to modify to highlight it, and then click **Modify**.

The following dialog box appears.


Local Users

Modify User Account - user

Change the password or the privilege for this user account.

Enter Password: **********

Confirm Password: **********

Select Privilege: ○ Administrator ● User

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.

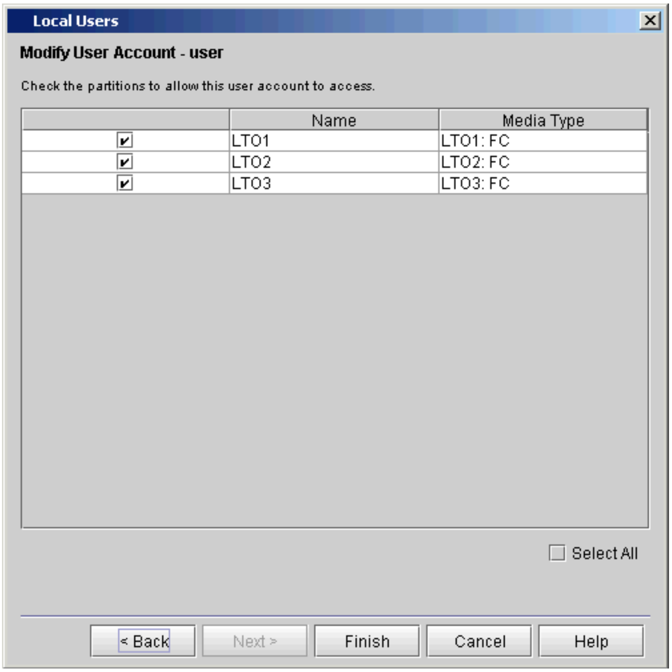
6 If you want to change the privilege level of this user account, select the appropriate privilege level (**Administrator** or **User**). Otherwise, proceed to the next step.

Note For a list of commands that are available to administrators and users, see table 27 on page 275.

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.



Local Users

Modify User Account - user

Check the partitions to allow this user account to access.

	Name	Media Type
☑	LTO1	LTO1: FC
☑	LTO2	LTO2: FC
☑	LTO3	LTO3: FC

☐ Select All

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**→ **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.

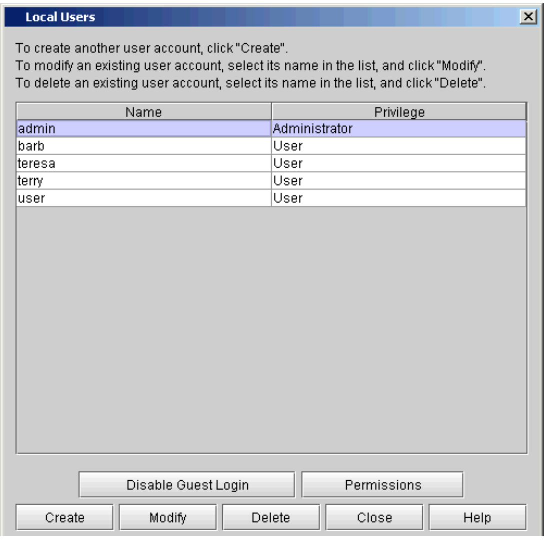
Viewing Local User Account Permissions

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**→ **Local Users**.

The **Local Users** dialog box appears.



Local Users

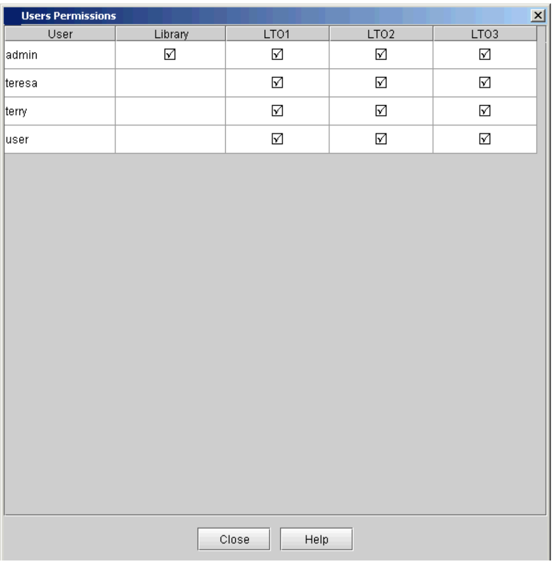
To create another user account, click "Create".
To modify an existing user account, select its name in the list, and click "Modify".
To delete an existing user account, select its name in the list, and click "Delete".

Name	Privilege
admin	Administrator
barb	User
teresa	User
terry	User
user	User

4 To view the permissions for all users, click **Permissions**.

The **Users Permissions** dialog box appears.

.



Users Permissions

User	Library	LTO1	LTO2	LTO3
admin	☑	☑	☑	☑
teresa		☑	☑	☑
terry		☑	☑	☑
user		☑	☑	☑

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.

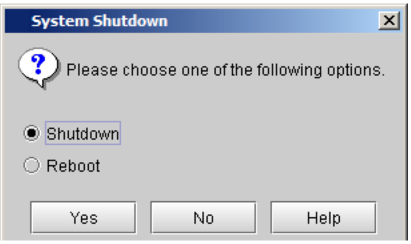
Reboot shuts down and restarts the library's operating system and firmware. When performing a reboot, the library finishes all active commands received from the host application and does not process any new commands. The library shuts down all partitions and restarts them during the reboot. In addition, 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 159.

⚠ 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.



System Shutdown

Please choose one of the following options.

● Shutdown
○ Reboot

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**.

Note To recover from library shutdown, you must cycle power on the library (power it off and then power it on). SeePowering Off the Library and Powering On the Library on page 318.

When the shutdown process completes, the LMC display turns dark. The library is now ready to be powered off.

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 316.**

1 After starting the shutdown process, wait for the LMC display to turn dark.

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 5 minutes after powering off the library before you power it on.

⚠ **CAUTION** **Waiting 5 minutes is important because the power supply discharges for several 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.

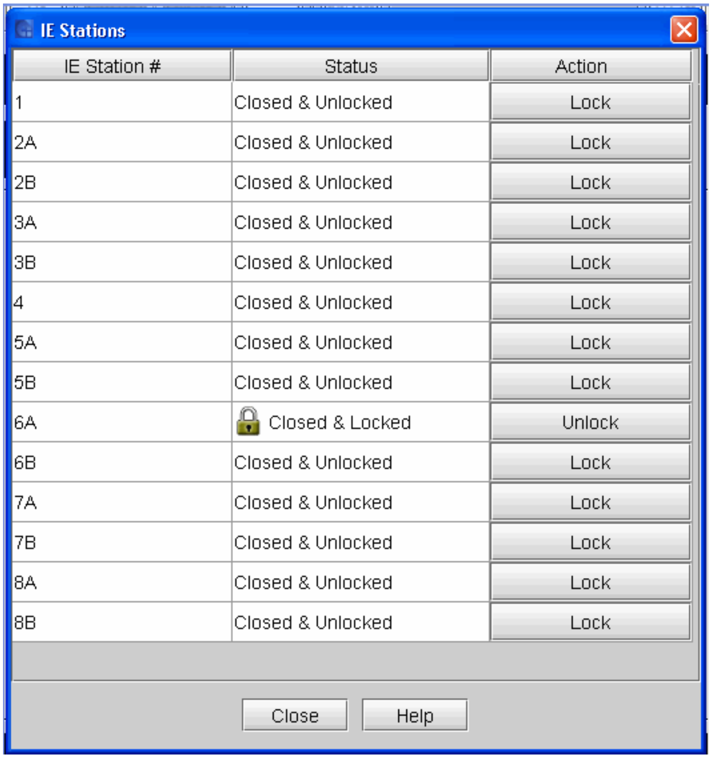
There are two reasons the I/E station door locks:

- 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.



IE Stations

IE Station #	Status	Action
1	Closed & Unlocked	Lock
2A	Closed & Unlocked	Lock
2B	Closed & Unlocked	Lock
3A	Closed & Unlocked	Lock
3B	Closed & Unlocked	Lock
4	Closed & Unlocked	Lock
5A	Closed & Unlocked	Lock
5B	Closed & Unlocked	Lock
6A	🔒 Closed & Locked	Unlock
6B	Closed & Unlocked	Lock
7A	Closed & Unlocked	Lock
7B	Closed & Unlocked	Lock
8A	Closed & Unlocked	Lock
8B	Closed & Unlocked	Lock

Note I/E Station # column lists the I/E station number for each door. 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.

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.

Figure 25 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 33 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	
Monitor→ Connectivity→ Fibre Channel	X	
Monitor→ IE Station	X	
Monitor→ Slot	X	
Monitor→ Media	X	
Monitor→ Sensor	X	
Monitor→ Users	X	
Setup→ Setup Wizard	X	
Setup→ Partitions	X	
Setup→ Device→ IDs	X	
Setup→ Device→ Access→ Channel Zoning	X	
Setup→ Device→ Access→ SCSI Host	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

Table 33 Menu Commands When Robotics Are Disabled

Available Menu Commands When Robotics Become Disabled	After Discovery	Before Discovery
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
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

Chapter 6

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 37.

This chapter consists of the following sections:

  - Using Library Explorer on page 360
  - Configuring and Testing Drives on page 365
  - Working With Connectivity on page 376
  - Capturing Snapshots on page 378
  - Updating Library Software on page 381
  - Updating Drive Firmware on page 398
  - Teaching the Library (Configuration and Calibration) on page 408
  - Saving and Restoring Library Configuration on page 411
  - Viewing the Drive Resource Utilization Reports on page 420
  - Setting Up Advanced Reporting Options on page 424
  - Working With Verification Tests on page 430
  - Using the Partitions Defragmentation Tool on page 482
  - Removing Lodged Cartridges on page 486
- Running MeDIA Test Reports on page 487
- Using Sift Sort on page 492
- Maintaining Air Filters on page 498

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:

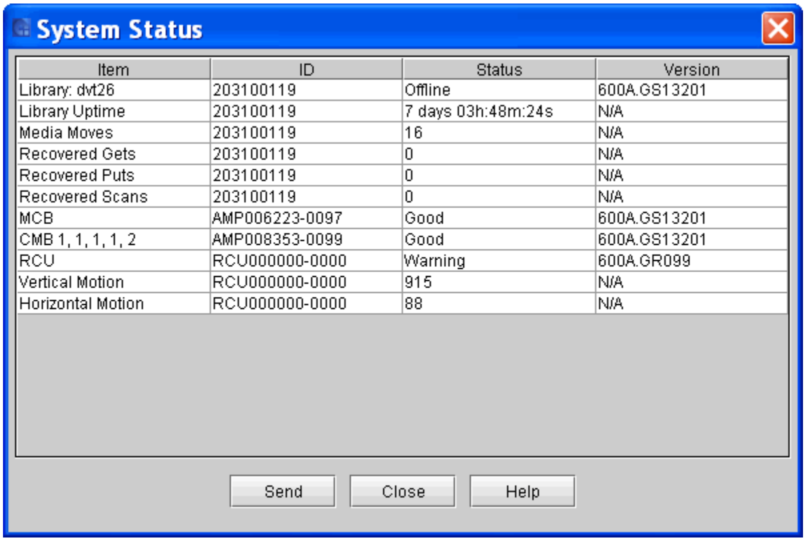
- System
- Drives
- Connectivity
- I/E stations
- Extended I/E Slots
- Slots
- Media
- Sensors
- Email Configuration Record
- Users
- Partitions
- EKM Servers

MonitoringSystemStatus

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**.

The **System Status** dialog box appears.



Item	ID	Status	Version
Library: dvt26	203100119	Offline	600A.GS13201
Library Uptime	203100119	7 days 03h:48m:24s	N/A
Media Moves	203100119	16	N/A
Recovered Gets	203100119	0	N/A
Recovered Puts	203100119	0	N/A
Recovered Scans	203100119	0	N/A
MCB	AMP006223-0097	Good	600A.GS13201
CMB 1, 1, 1, 1, 2	AMP008353-0099	Good	600A.GS13201
RCU	RCU000000-0000	Warning	600A.GR099
Vertical Motion	RCU000000-0000	915	N/A
Horizontal Motion	RCU000000-0000	88	N/A

The following table describes the elements on the **System Status** dialog box.

Element	Description
Item	A system item for which status information is available (hardware or system metric).
ID	If applicable or available, the serial number or other identifying number of the system item.
Status	Status information for the system item.

The following table describes the items that can appear in the status list.

.

Item	ID	Status Description
Library	The library serial number	The status of the library (Online or Offline).
Library Uptime	The library serial number	The amount of time that the library has been up (in days, hours, minutes, and seconds).
Media Moves	The library serial number	The number of media moves during the library's history.
Recovered Gets	The library serial number	The number of recovered gets during the library's history.
Recovered Puts	The library serial number	The number of recovered puts during the library's history.
Recovered Scans	The library serial number	The number of recovered scans during the library's history.
MCB	The MCB serial number	The current status of the MCB (Good, Degraded, or Failed).
CMB	The CMB serial number	For each CMB that is present, the current status of the CMB (Good, Degraded, or Failed).
RCU	The RCU serial number	The current status of the RCU (Good, Degraded, or Failed).
Vertical Motion	The RCU serial number	The number of meters vertically traveled during the library's history.
Horizontal Motion	The RCU serial number	The number of meters horizontally traveled during the library's history.

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.

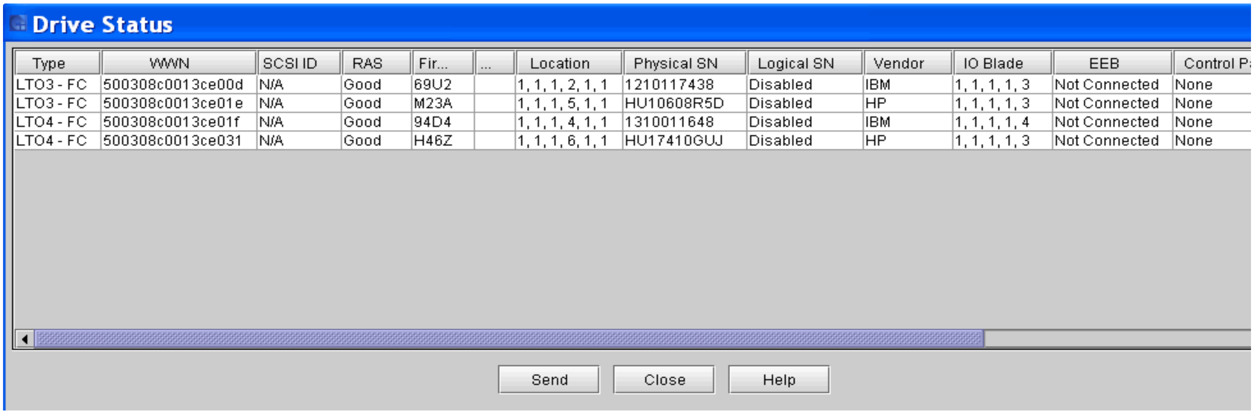
- Mail, save, or print status information by using the Send button (see Mailing, Saving, and Printing Status Information on page 354).

Monitoring Drive Status

The **Drive Status** dialog box displays status information for tape drives in the currently selected partition. If you are working in 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.



Drive Status

Type	WWN	SCSI ID	RAS	Fir...	...	Location	Physical SN	Logical SN	Vendor	IO Blade	EEB	Control P:
LTO3 - FC	500308c0013ce00d	N/A	Good	69U2		1, 1, 1, 2, 1, 1	1210117438	Disabled	IBM	1, 1, 1, 1, 3	Not Connected	None
LTO3 - FC	500308c0013ce01e	N/A	Good	M23A		1, 1, 1, 5, 1, 1	HU10608R5D	Disabled	HP	1, 1, 1, 1, 3	Not Connected	None
LTO4 - FC	500308c0013ce01f	N/A	Good	94D4		1, 1, 1, 4, 1, 1	1310011648	Disabled	IBM	1, 1, 1, 1, 4	Not Connected	None
LTO4 - FC	500308c0013ce031	N/A	Good	H46Z		1, 1, 1, 6, 1, 1	HU17410GUJ	Disabled	HP	1, 1, 1, 1, 3	Not Connected	None

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.
SCSI ID	For a SCSI drive only, the SCSI ID of the drive.

Element	Description
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.
Location	The location of the drive by means of a coordinate system. For information about location coordinates, see Understanding Location Coordinates on page 288.
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 288.
Encryption	The Encryption type currently used by the drive; the values are 'Application Managed', 'Library Managed' or 'Unsupported if the drive does not support encryption.
EEB	Reports if a drive is connected to an Ethernet Expansion Blade. The values are Connected, or Not Connected.
Control Path	Reports if a drive is a Control Path (Primary). The values are Primary or None. It also reports which drive is currently the active drive by Display "(Active)", example "Primary (Active)"
Partition Name	The name of the partition to which the drive is assigned.
Usage Type	Indicates if the drive is specialised for use in Library Managed Partitions (MeDIA) or is for use in regular partitions (Standard).

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 354).

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** command does not appear on the menu.

- The **SCSI Channel Status** dialog box displays information about the SCSI connection on the MCB.
- 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 whether or not the EEB is connected.

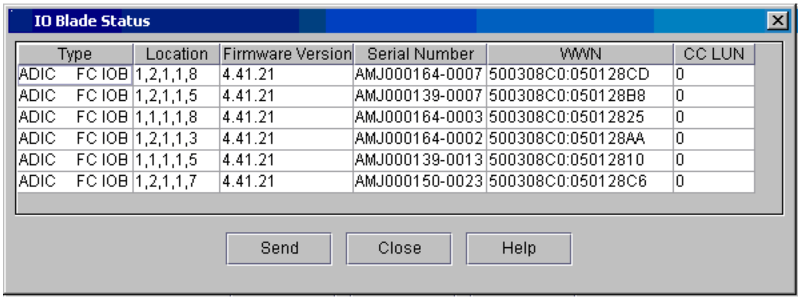
You must perform the following procedures while viewing the physical library.

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.



Type	Location	Firmware Version	Serial Number	WWN	CC LUN
ADIC FC IOB	1,2,1,1,8	4.41.21	AMJ000164-0007	500308C0:050128CD	0
ADIC FC IOB	1,2,1,1,5	4.41.21	AMJ000139-0007	500308C0:050128B8	0
ADIC FC IOB	1,1,1,1,8	4.41.21	AMJ000164-0003	500308C0:05012825	0
ADIC FC IOB	1,2,1,1,3	4.41.21	AMJ000164-0002	500308C0:050128AA	0
ADIC FC IOB	1,1,1,1,5	4.41.21	AMJ000139-0013	500308C0:05012810	0
ADIC FC IOB	1,2,1,1,7	4.41.21	AMJ000150-0023	500308C0:050128C6	0

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 299).
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:

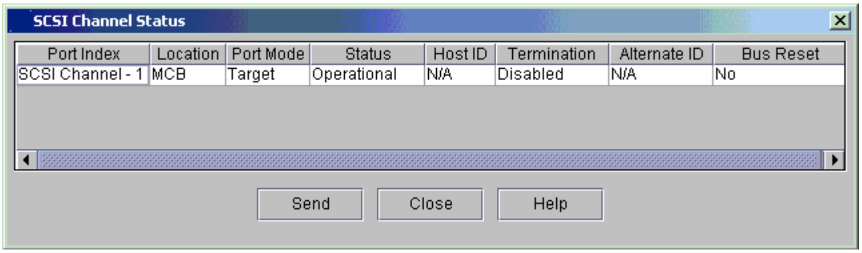
- Change the sorting of I/O blades in the status list (for example, by type or location) by clicking the column heading by which you want the I/O blades sorted. Repeatedly clicking a column heading toggles between ascending and descending order.
- Mail, save, or print status information by using the **Send** button (see Mailing, Saving, and Printing Status Information on page 354.

Viewing SCSI 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**→ **SCSI Channel**.

The **SCSI Channel Status** dialog box appears.



Port Index	Location	Port Mode	Status	Host ID	Termination	Alternate ID	Bus Reset
SCSI Channel - 1	MCB	Target	Operational	N/A	Disabled	N/A	No

The following table describes the elements on the **SCSI 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 SCSI Channel (Operational or Lost Sync).
Host ID	The SCSI ID.
Termination	Terminated or Not Terminated.
Alternate ID	The alternate SCSI ID.
Bus Reset	Indicates whether the bus is configured to reset when library power is turned on (Yes or No).

3 From the **IO Blade Status** dialog box, you can perform the following tasks:

- Change the sorting of SCSI 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.

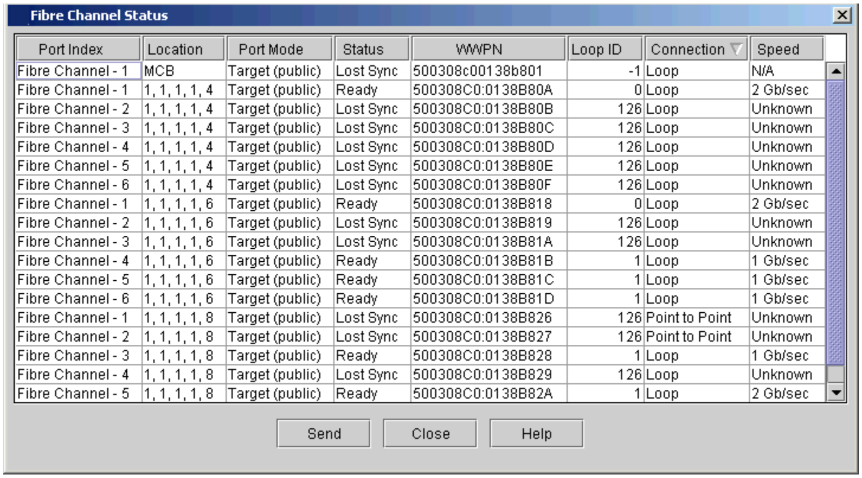
- Mail, save, or print status information by using the **Send** button (see Mailing, Saving, and Printing Status Information on page 354).

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.



Fibre Channel Status

Port Index	Location	Port Mode	Status	WWPN	Loop ID	Connection	Speed
Fibre Channel - 1	MCB	Target (public)	Lost Sync	500308c00138b801	-1	Loop	N/A
Fibre Channel - 1	1, 1, 1, 1, 4	Target (public)	Ready	500308C0:0138B80A	0	Loop	2 Gb/sec
Fibre Channel - 2	1, 1, 1, 1, 4	Target (public)	Lost Sync	500308C0:0138B80B	126	Loop	Unknown
Fibre Channel - 3	1, 1, 1, 1, 4	Target (public)	Lost Sync	500308C0:0138B80C	126	Loop	Unknown
Fibre Channel - 4	1, 1, 1, 1, 4	Target (public)	Lost Sync	500308C0:0138B80D	126	Loop	Unknown
Fibre Channel - 5	1, 1, 1, 1, 4	Target (public)	Lost Sync	500308C0:0138B80E	126	Loop	Unknown
Fibre Channel - 6	1, 1, 1, 1, 4	Target (public)	Lost Sync	500308C0:0138B80F	126	Loop	Unknown
Fibre Channel - 1	1, 1, 1, 1, 6	Target (public)	Ready	500308C0:0138B818	0	Loop	2 Gb/sec
Fibre Channel - 2	1, 1, 1, 1, 6	Target (public)	Lost Sync	500308C0:0138B819	126	Loop	Unknown
Fibre Channel - 3	1, 1, 1, 1, 6	Target (public)	Lost Sync	500308C0:0138B81A	126	Loop	Unknown
Fibre Channel - 4	1, 1, 1, 1, 6	Target (public)	Ready	500308C0:0138B81B	1	Loop	1 Gb/sec
Fibre Channel - 5	1, 1, 1, 1, 6	Target (public)	Ready	500308C0:0138B81C	1	Loop	1 Gb/sec
Fibre Channel - 6	1, 1, 1, 1, 6	Target (public)	Ready	500308C0:0138B81D	1	Loop	1 Gb/sec
Fibre Channel - 1	1, 1, 1, 1, 8	Target (public)	Lost Sync	500308C0:0138B826	126	Point to Point	Unknown
Fibre Channel - 2	1, 1, 1, 1, 8	Target (public)	Lost Sync	500308C0:0138B827	126	Point to Point	Unknown
Fibre Channel - 3	1, 1, 1, 1, 8	Target (public)	Ready	500308C0:0138B828	1	Loop	1 Gb/sec
Fibre Channel - 4	1, 1, 1, 1, 8	Target (public)	Lost Sync	500308C0:0138B829	126	Loop	Unknown
Fibre Channel - 5	1, 1, 1, 1, 8	Target (public)	Ready	500308C0:0138B82A	1	Loop	2 Gb/sec

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).

Element	Description
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 150).
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:

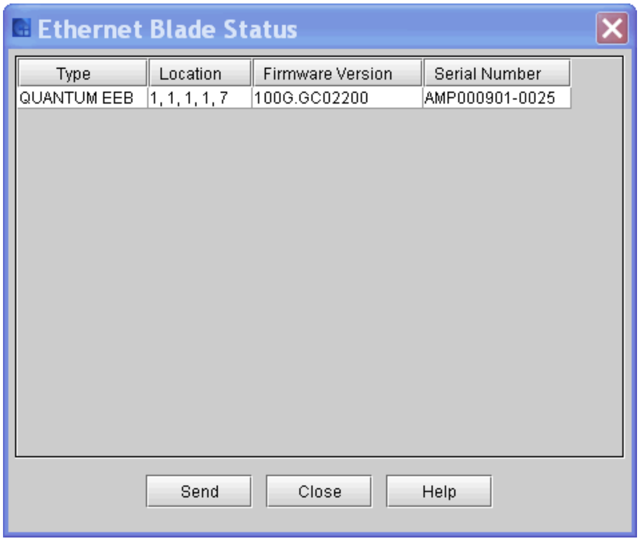
- Change the sorting of Fibre Channel connections in the status list (for example, by type or location) by clicking the column heading by which you want the connections sorted. Repeatedly clicking a column heading toggles between ascending and descending order.
- Mail, save, or print status information by using the **Send** button (see Mailing, Saving, and Printing Status Information on page 354).

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.



Ethernet Blade Status

Type	Location	Firmware Version	Serial Number
QUANTUM EEB	1, 1, 1, 1, 7	100G.GC02200	AMP000901-0025

See the following table for descriptions of the elements on the **Ethernet Blade Status** dialog box.

Element	Description
Type	The type of drive.
Location	The location of the drive by means of a coordinate system. For information about location coordinates, see Understanding Location Coordinates on page 288.
Firmware Version	The firmware level of the drive.
Serial Number	The serial number of the blade.

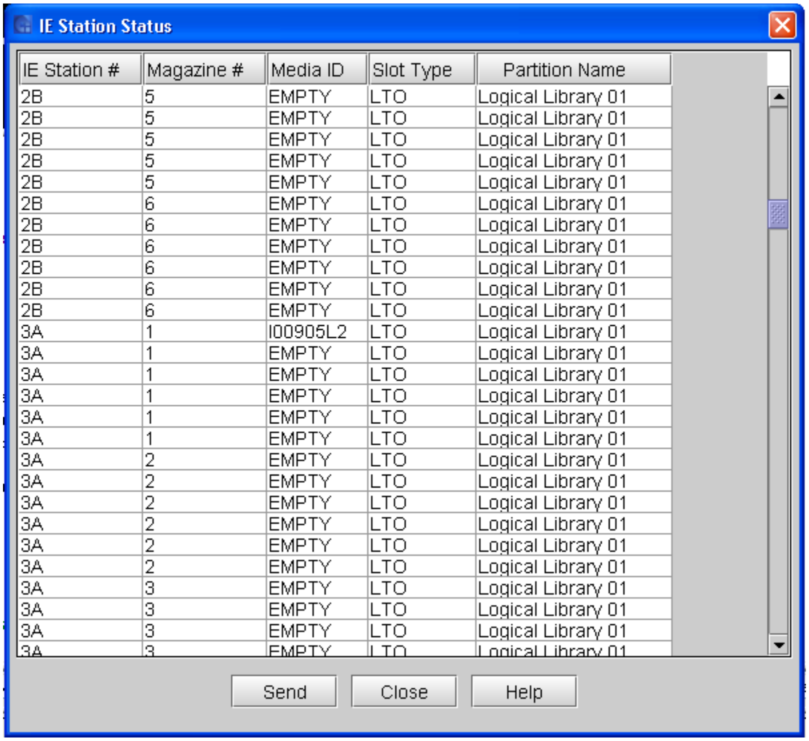
3 From the **Ethernet Blade Status** dialog box, you can Mail, save, or print status information by using the **Send** button (see Mailing, Saving, and Printing Status Information on page 354.

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.



IE Station #	Magazine #	Media ID	Slot Type	Partition Name
2B	5	EMPTY	LTO	Logical Library 01
2B	5	EMPTY	LTO	Logical Library 01
2B	5	EMPTY	LTO	Logical Library 01
2B	5	EMPTY	LTO	Logical Library 01
2B	5	EMPTY	LTO	Logical Library 01
2B	6	EMPTY	LTO	Logical Library 01
2B	6	EMPTY	LTO	Logical Library 01
2B	6	EMPTY	LTO	Logical Library 01
2B	6	EMPTY	LTO	Logical Library 01
2B	6	EMPTY	LTO	Logical Library 01
2B	6	EMPTY	LTO	Logical Library 01
3A	1	I00905L2	LTO	Logical Library 01
3A	1	EMPTY	LTO	Logical Library 01
3A	1	EMPTY	LTO	Logical Library 01
3A	1	EMPTY	LTO	Logical Library 01
3A	1	EMPTY	LTO	Logical Library 01
3A	1	EMPTY	LTO	Logical Library 01
3A	2	EMPTY	LTO	Logical Library 01
3A	2	EMPTY	LTO	Logical Library 01
3A	2	EMPTY	LTO	Logical Library 01
3A	2	EMPTY	LTO	Logical Library 01
3A	2	EMPTY	LTO	Logical Library 01
3A	2	EMPTY	LTO	Logical Library 01
3A	3	EMPTY	LTO	Logical Library 01
3A	3	EMPTY	LTO	Logical Library 01
3A	3	EMPTY	LTO	Logical Library 01
3A	3	EMPTY	LTO	Logical Library 01

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 (1-8), 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 354).

Monitoring Slot and Extended I/E Slot Status

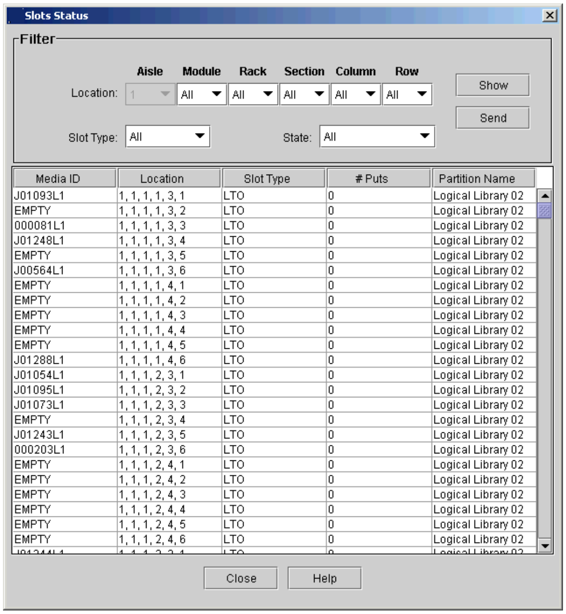
Note To view slot status for Extended I/E slots, use the procedure below.

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**.

Note For Extended I/E, click **Monitor > Extended I/E Slots**.

The **Slots Status** dialog box appears.



Location: 1, All, All, All, All, All

Slot Type: All

State: All

Media ID	Location	Slot Type	# Puts	Partition Name
J01093L1	1, 1, 1, 1, 3, 1	LTO	0	Logical Library 02
EMPTY	1, 1, 1, 1, 3, 2	LTO	0	Logical Library 02
000081L1	1, 1, 1, 1, 3, 3	LTO	0	Logical Library 02
J01248L1	1, 1, 1, 1, 3, 4	LTO	0	Logical Library 02
EMPTY	1, 1, 1, 1, 3, 5	LTO	0	Logical Library 02
J00564L1	1, 1, 1, 1, 3, 6	LTO	0	Logical Library 02
EMPTY	1, 1, 1, 1, 4, 1	LTO	0	Logical Library 02
EMPTY	1, 1, 1, 1, 4, 2	LTO	0	Logical Library 02
EMPTY	1, 1, 1, 1, 4, 3	LTO	0	Logical Library 02
EMPTY	1, 1, 1, 1, 4, 4	LTO	0	Logical Library 02
EMPTY	1, 1, 1, 1, 4, 5	LTO	0	Logical Library 02
J01288L1	1, 1, 1, 1, 4, 6	LTO	0	Logical Library 02
J01054L1	1, 1, 1, 2, 3, 1	LTO	0	Logical Library 02
J01095L1	1, 1, 1, 2, 3, 2	LTO	0	Logical Library 02
J01073L1	1, 1, 1, 2, 3, 3	LTO	0	Logical Library 02
EMPTY	1, 1, 1, 2, 3, 4	LTO	0	Logical Library 02
J01243L1	1, 1, 1, 2, 3, 5	LTO	0	Logical Library 02
000203L1	1, 1, 1, 2, 3, 6	LTO	0	Logical Library 02
EMPTY	1, 1, 1, 2, 4, 1	LTO	0	Logical Library 02
EMPTY	1, 1, 1, 2, 4, 2	LTO	0	Logical Library 02
EMPTY	1, 1, 1, 2, 4, 3	LTO	0	Logical Library 02
EMPTY	1, 1, 1, 2, 4, 4	LTO	0	Logical Library 02
EMPTY	1, 1, 1, 2, 4, 5	LTO	0	Logical Library 02
EMPTY	1, 1, 1, 2, 4, 6	LTO	0	Logical Library 02

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.
In the status list area:	
Media ID	The slot barcode.
Location	The location of the slot (see Understanding Location Coordinates on page 288).
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 342).

- Mail, save, or print status information by using the **Send** button (see Mailing, Saving, and Printing Status Information on page 354).

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 288.

   - 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**.

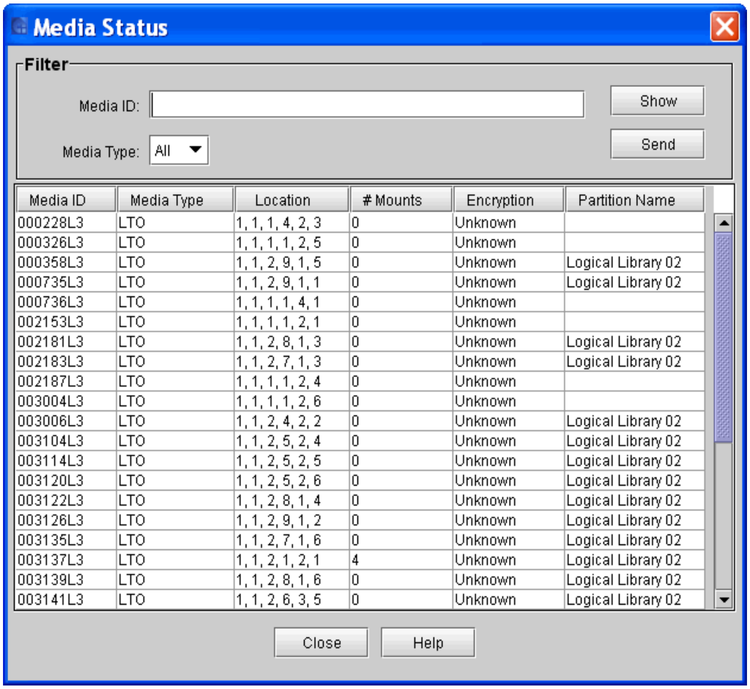
2. Click **Show**.

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.



Media ID:

Media Type: All

Media ID	Media Type	Location	# Mounts	Encryption	Partition Name
000228L3	LTO	1, 1, 1, 4, 2, 3	0	Unknown	
000326L3	LTO	1, 1, 1, 1, 2, 5	0	Unknown	
000358L3	LTO	1, 1, 2, 9, 1, 5	0	Unknown	Logical Library 02
000735L3	LTO	1, 1, 2, 9, 1, 1	0	Unknown	Logical Library 02
000736L3	LTO	1, 1, 1, 1, 4, 1	0	Unknown	
002153L3	LTO	1, 1, 1, 1, 2, 1	0	Unknown	
002181L3	LTO	1, 1, 2, 8, 1, 3	0	Unknown	Logical Library 02
002183L3	LTO	1, 1, 2, 7, 1, 3	0	Unknown	Logical Library 02
002187L3	LTO	1, 1, 1, 1, 2, 4	0	Unknown	
003004L3	LTO	1, 1, 1, 1, 2, 6	0	Unknown	
003006L3	LTO	1, 1, 2, 4, 2, 2	0	Unknown	Logical Library 02
003104L3	LTO	1, 1, 2, 5, 2, 4	0	Unknown	Logical Library 02
003114L3	LTO	1, 1, 2, 5, 2, 5	0	Unknown	Logical Library 02
003120L3	LTO	1, 1, 2, 5, 2, 6	0	Unknown	Logical Library 02
003122L3	LTO	1, 1, 2, 8, 1, 4	0	Unknown	Logical Library 02
003126L3	LTO	1, 1, 2, 9, 1, 2	0	Unknown	Logical Library 02
003135L3	LTO	1, 1, 2, 7, 1, 6	0	Unknown	Logical Library 02
003137L3	LTO	1, 1, 2, 1, 2, 1	4	Unknown	Logical Library 02
003139L3	LTO	1, 1, 2, 8, 1, 6	0	Unknown	Logical Library 02
003141L3	LTO	1, 1, 2, 6, 3, 5	0	Unknown	Logical Library 02

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 288).
# 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.

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 345).
- Mail, save, or print status information by using the **Send** button (see Mailing, Saving, and Printing Status Information on page 354).

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 wildcard 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.

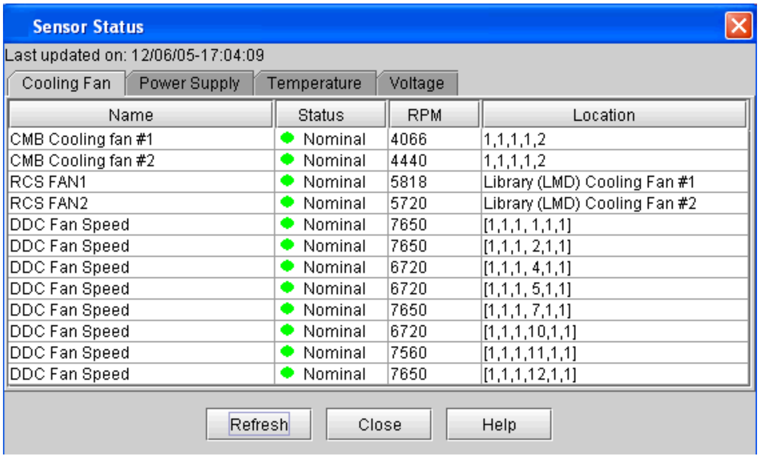
Accessing the Sensor Status Dialog Box

Click **Monitor**→ **Sensor**.

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.



Last updated on: 12/06/05-17:04:09

Name	Status	RPM	Location
CMB Cooling fan #1	● Nominal	4066	1,1,1,1,2
CMB Cooling fan #2	● Nominal	4440	1,1,1,1,2
RCS FAN1	● Nominal	5818	Library (LMD) Cooling Fan #1
RCS FAN2	● Nominal	5720	Library (LMD) Cooling Fan #2
DDC Fan Speed	● Nominal	7650	[1,1,1, 1,1,1]
DDC Fan Speed	● Nominal	7650	[1,1,1, 2,1,1]
DDC Fan Speed	● Nominal	6720	[1,1,1, 4,1,1]
DDC Fan Speed	● Nominal	6720	[1,1,1, 5,1,1]
DDC Fan Speed	● Nominal	7650	[1,1,1, 7,1,1]
DDC Fan Speed	● Nominal	6720	[1,1,1,10,1,1]
DDC Fan Speed	● Nominal	7560	[1,1,1,11,1,1]
DDC Fan Speed	● Nominal	7650	[1,1,1,12,1,1]

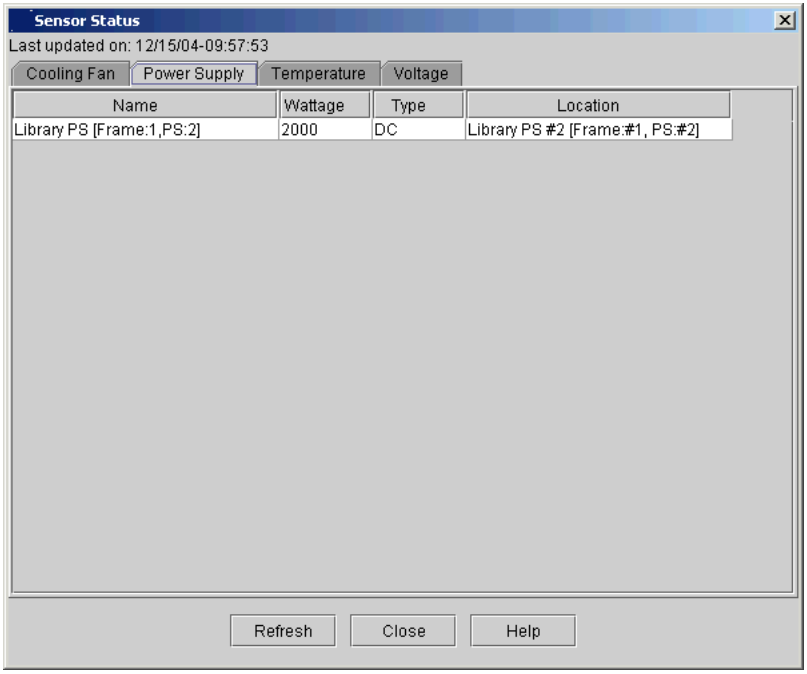
The following table describes the elements on the **Cooling Fan** tab.

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 288.

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.



Last updated on: 12/15/04-09:57:53

Name	Wattage	Type	Location
Library PS [Frame:1,PS:2]	2000	DC	Library PS #2 [Frame:#1, PS:#2]

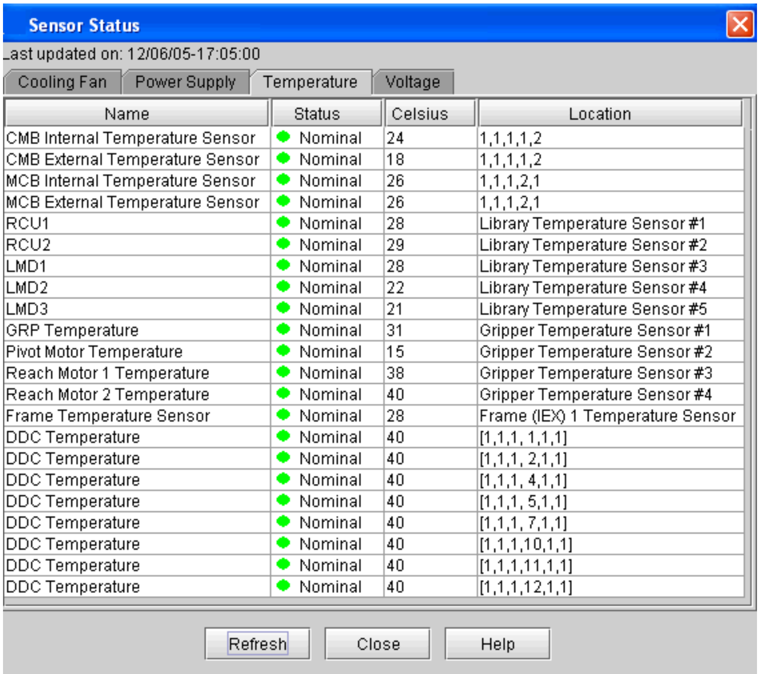
The following table describes the elements on the **Power Supply** tab.

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.



Last updated on: 12/06/05-17:05:00

Name	Status	Celsius	Location
CMB Internal Temperature Sensor	● Nominal	24	1,1,1,1,2
CMB External Temperature Sensor	● Nominal	18	1,1,1,1,2
MCB Internal Temperature Sensor	● Nominal	26	1,1,1,2,1
MCB External Temperature Sensor	● Nominal	26	1,1,1,2,1
RCU1	● Nominal	28	Library Temperature Sensor #1
RCU2	● Nominal	29	Library Temperature Sensor #2
LMD1	● Nominal	28	Library Temperature Sensor #3
LMD2	● Nominal	22	Library Temperature Sensor #4
LMD3	● Nominal	21	Library Temperature Sensor #5
GRP Temperature	● Nominal	31	Gripper Temperature Sensor #1
Pivot Motor Temperature	● Nominal	15	Gripper Temperature Sensor #2
Reach Motor 1 Temperature	● Nominal	38	Gripper Temperature Sensor #3
Reach Motor 2 Temperature	● Nominal	40	Gripper Temperature Sensor #4
Frame Temperature Sensor	● Nominal	28	Frame (IEX) 1 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, 4,1,1]
DDC Temperature	● Nominal	40	[1,1,1, 5,1,1]
DDC Temperature	● Nominal	40	[1,1,1, 7,1,1]
DDC Temperature	● Nominal	40	[1,1,1,10,1,1]
DDC Temperature	● Nominal	40	[1,1,1,11,1,1]
DDC Temperature	● Nominal	40	[1,1,1,12,1,1]

The following table describes the elements on the **Temperature** tab.

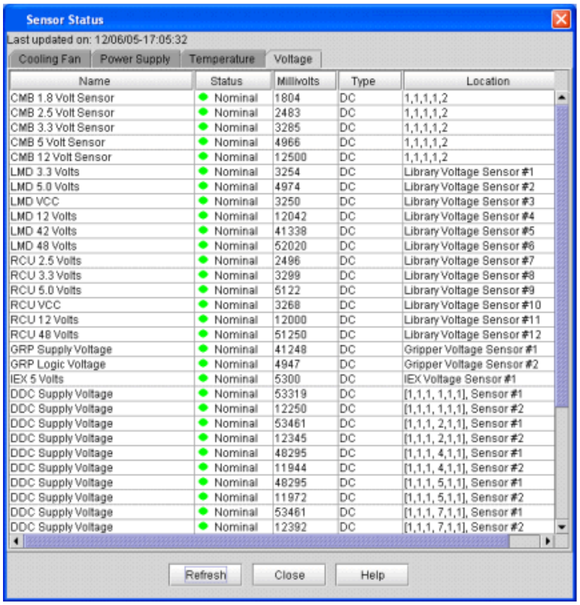
Element	**Description**
Name	The name of the temperature sensor.
Status	The temperature status in the vicinity of the sensor. If the temperature is within normal operational limits, the status is nominal. Otherwise, a warning or alarm is indicated.
Celsius	The sensor’s temperature reading in degrees Celsius.

Element	Description
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 288.

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.



Last updated on: 12/06/05-17:05:32

Name	Status	Millivolts	Type	Location
CMB 1.8 Volt Sensor	● Nominal	1804	DC	1,1,1,1,2
CMB 2.5 Volt Sensor	● Nominal	2483	DC	1,1,1,1,2
CMB 3.3 Volt Sensor	● Nominal	3285	DC	1,1,1,1,2
CMB 5 Volt Sensor	● Nominal	4966	DC	1,1,1,1,2
CMB 12 Volt Sensor	● Nominal	12500	DC	1,1,1,1,2
LMD 3.3 Volts	● Nominal	3254	DC	Library Voltage Sensor #1
LMD 5.0 Volts	● Nominal	4974	DC	Library Voltage Sensor #2
LMD VCC	● Nominal	3250	DC	Library Voltage Sensor #3
LMD 12 Volts	● Nominal	12042	DC	Library Voltage Sensor #4
LMD 42 Volts	● Nominal	41338	DC	Library Voltage Sensor #5
LMD 48 Volts	● Nominal	52020	DC	Library Voltage Sensor #6
RCU 2.5 Volts	● Nominal	2496	DC	Library Voltage Sensor #7
RCU 3.3 Volts	● Nominal	3299	DC	Library Voltage Sensor #8
RCU 5.0 Volts	● Nominal	5122	DC	Library Voltage Sensor #9
RCU VCC	● Nominal	3268	DC	Library Voltage Sensor #10
RCU 12 Volts	● Nominal	12000	DC	Library Voltage Sensor #11
RCU 48 Volts	● Nominal	51250	DC	Library Voltage Sensor #12
GRP Supply Voltage	● Nominal	41248	DC	Gripper Voltage Sensor #1
GRP Logic Voltage	● Nominal	4947	DC	Gripper Voltage Sensor #2
IEX 5 Volts	● Nominal	5300	DC	IEX Voltage Sensor #1
DDC Supply Voltage	● Nominal	53319	DC	[1,1,1, 1,1,1], Sensor #1
DDC Supply Voltage	● Nominal	12250	DC	[1,1,1, 1,1,1], Sensor #2
DDC Supply Voltage	● Nominal	53461	DC	[1,1,1, 2,1,1], Sensor #1
DDC Supply Voltage	● Nominal	12345	DC	[1,1,1, 2,1,1], Sensor #2
DDC Supply Voltage	● Nominal	48295	DC	[1,1,1, 4,1,1], Sensor #1
DDC Supply Voltage	● Nominal	11944	DC	[1,1,1, 4,1,1], Sensor #2
DDC Supply Voltage	● Nominal	48295	DC	[1,1,1, 5,1,1], Sensor #1
DDC Supply Voltage	● Nominal	11972	DC	[1,1,1, 5,1,1], Sensor #2
DDC Supply Voltage	● Nominal	53461	DC	[1,1,1, 7,1,1], Sensor #1
DDC Supply Voltage	● Nominal	12392	DC	[1,1,1, 7,1,1], Sensor #2

The following table describes the elements on the **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 288.

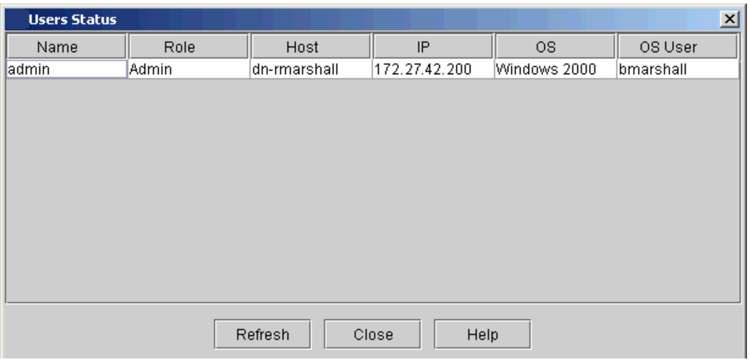
2 To view current information, click **Refresh**.

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.



Users Status

Name	Role	Host	IP	OS	OS User
admin	Admin	dn-rmarshall	172.27.42.200	Windows 2000	bmarshall

The following table describes the elements on the **Users Status** dialog box.

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**.

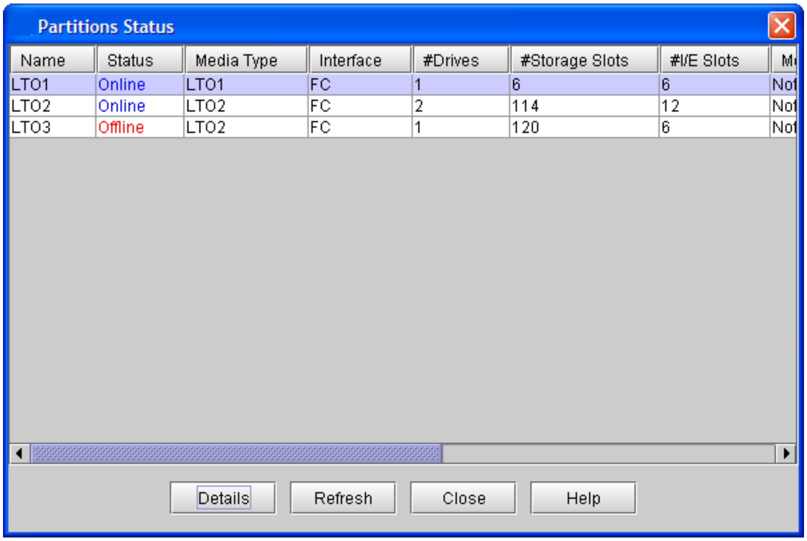
Monitoring Partitions Status

If you want to see settings and information for a partition but do not need to make changes, view partition details. Unlike modifying a partition, viewing 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.**

The **Partitions Status** dialog box appears with a list of all logical partitions in the library and information about each partition.



Name	Status	Media Type	Interface	#Drives	#Storage Slots	#I/E Slots	Mi
LTO1	Online	LTO1	FC	1	6	6	Not
LTO2	Online	LTO2	FC	2	114	12	Not
LTO3	Offline	LTO2	FC	1	120	6	Not

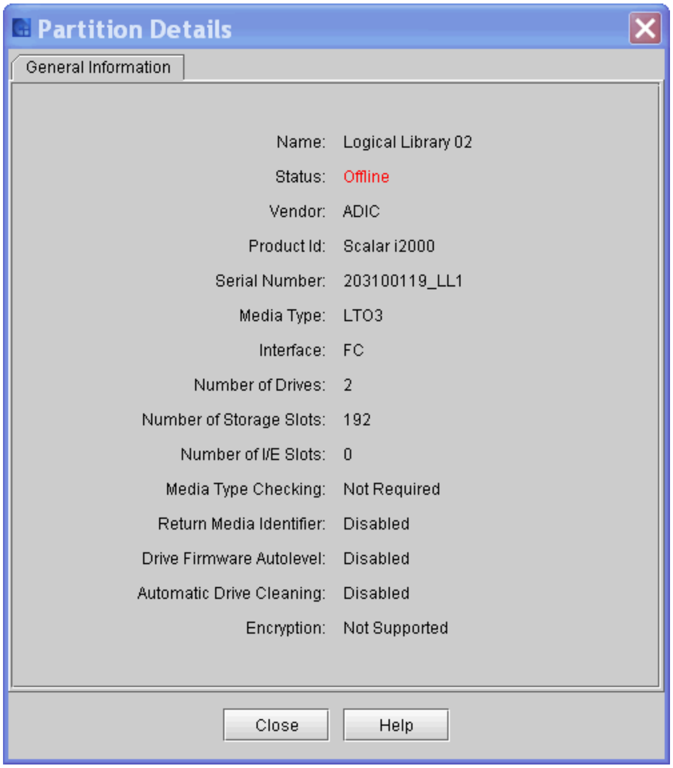
The following table describes the elements on the **Partitions Status** dialog box.

Element	Description
Name	The name of the partition.
Status	The status of the partition (Online or Offline).

Element (Continued)	Description
Media Type	The type of media used in the partition (LTO-1, LTO-2, LTO-3, LTO-4, LTO-5, or DLT).
Interface	The type of interface used to connect to the host (FCor SCSI).
#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).
Encryption	Reports whether the media is encrypted. The values are Not Supported, Application Managed, or Library Managed.

3 To see additional details for a partition, click the partition in the list, and then click **Details**.

The **Partition Details** dialog box appears. This windows shows additional information about the partition, such as vendor, product ID, and serial number.



Name: Logical Library 02
Status: Offline
Vendor: ADIC
Product Id: Scalar i2000
Serial Number: 203100119_LL1
Media Type: LTO3
Interface: FC
Number of Drives: 2
Number of Storage Slots: 192
Number of I/E Slots: 0
Media Type Checking: Not Required
Return Media Identifier: Disabled
Drive Firmware Autolevel: Disabled
Automatic Drive Cleaning: Disabled
Encryption: Not Supported

4 Click **Close** to close the **Partition Details** dialog box.

5 Click **Close** to return to the **Partitions Status** dialog box.

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.

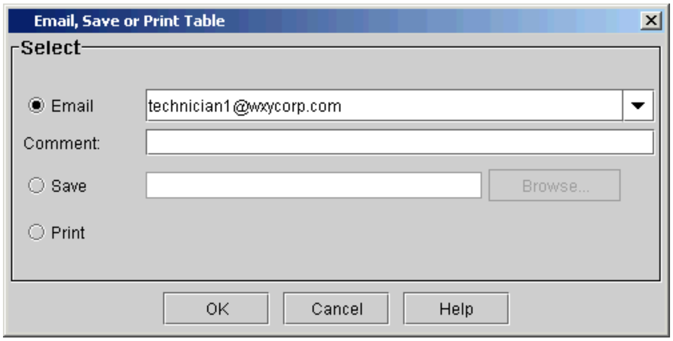
The information that is sent will be the same as what the status dialog box appears at the time that you click **Send**.

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 164.

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.



Email, Save or Print Table

Select

● Email: technician1@wxycorp.com

Comment:

○ Save

○ Print

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 259.

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 164.

Note Only users with administrative privileges can e-mail or save the configuration record.

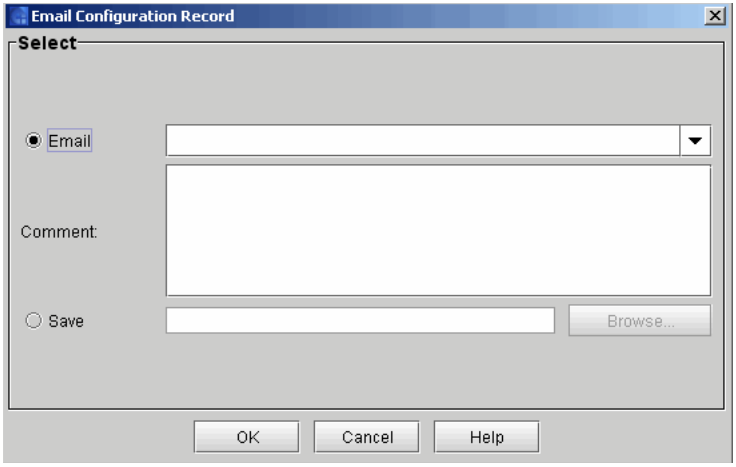
Mailing the Configuration Record

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.



Email Configuration Record

Select

● Email

Comment:

○ Save

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.

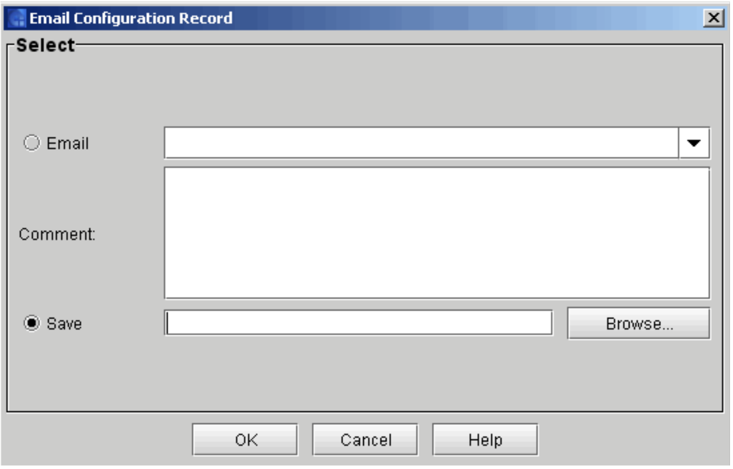
The e-mail message includes both the configuration record information and your comments as embedded text with “Library Configuration Information” as the subject.

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 37. For a summary of user privileges defined by physical library, partition, and command menu, see table 27 on page 275.

Is the Access Door Closed?

Library operations are taken offline 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 module to eight modules, and one drive up to the maximum number of 96 drives.

You can access the Library Explorer from both the physical and partition views, but the functionality in the physical view is limited. If you are in a partition view, Library Explorer displays slots and drives pertaining to that particular partition.

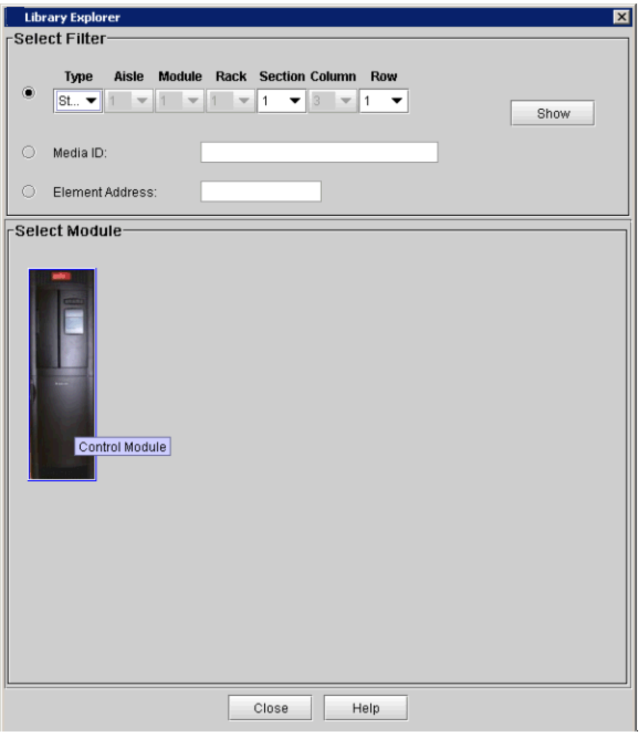
The **Library Explorer** features are available to administrator and service users, along with non-administrative users who have limited access to library functions. Users who do not have administrative privileges can perform all Operations options available to non-administrative users directly from 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

1 From the **Tools** menu, click **Library Explorer**.

The **Library Explorer** dialog box appears.



Type	Aisle	Module	Rack	Section	Column	Row
St...	1	1	1	1	3	1

2 You can display library data using either the **Select Filter** options or clicking on a particular module in the **Select Module** area.

- 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 **DeviceType** 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.

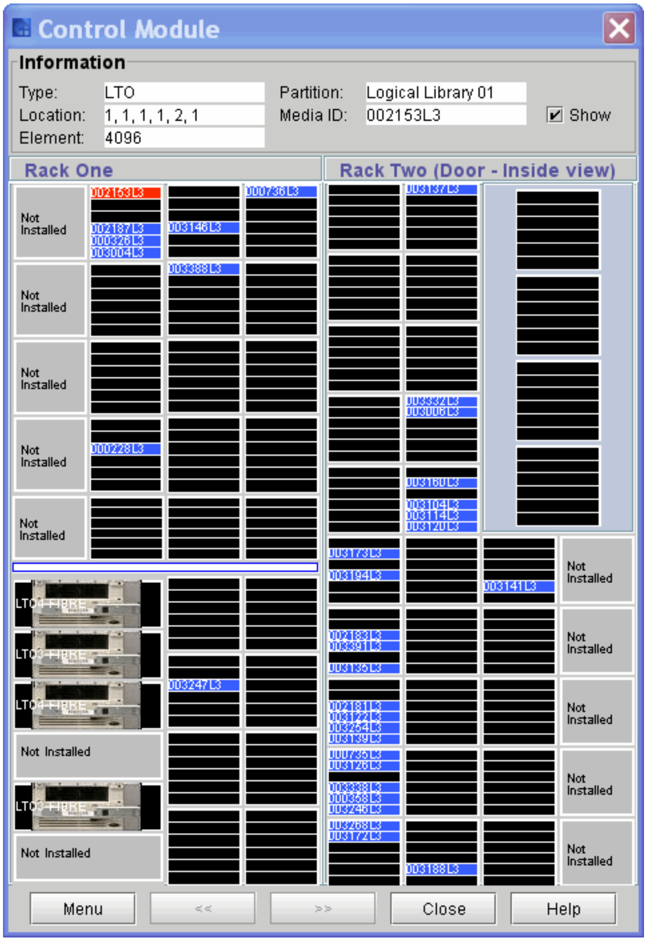
  - To search for a specific cartridge according to the cartridge's barcode, select the **Media ID** filter, type the barcode in the **Media ID** field, and then click **Show**.

    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.

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.



Control Module

Information

Type: LTO
Location: 1, 1, 1, 1, 2, 1
Element: 4096
Partition: Logical Library 01
Media ID: 002153L3
☑ Show

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, but the functionality in the physical view is limited. 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, uncheck 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

Configuring and Testing Drives

The **Drives** dialog box enables you to do the following:

- Set speed and connection parameters
- Reset drives
- Cycle power to drives
- Take drives online or offline
- Identify drives
- Run a pass/fail test for LTO-type drives
- Eject tape cartridges from drives
- Send the logs by e-mail or save drive logs
- Clean drives

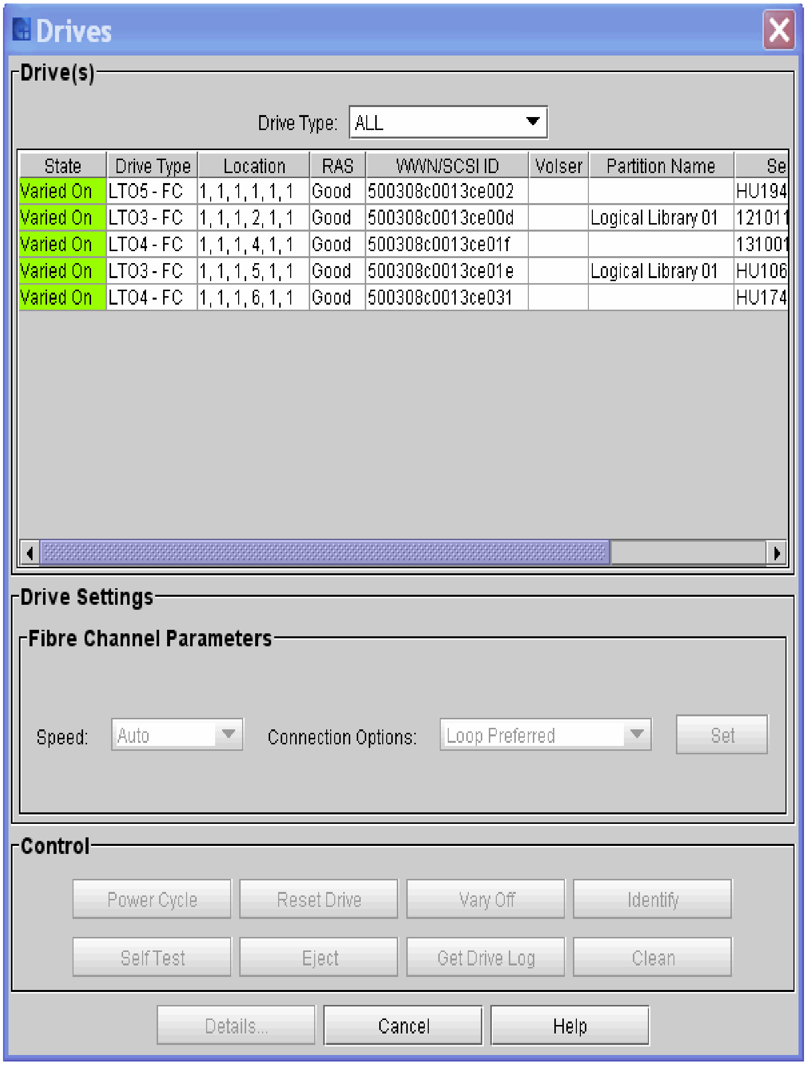
Drive information on this dialog box is automatically refreshed whenever a drive is added or removed.

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.



Drives

Drive(s)

Drive Type: ALL

State	Drive Type	Location	RAS	WWN/SCSI ID	Volser	Partition Name	Se
Varied On	LTO5 - FC	1, 1, 1, 1, 1, 1	Good	500308c0013ce002			HU194
Varied On	LTO3 - FC	1, 1, 1, 2, 1, 1	Good	500308c0013ce00d		Logical Library 01	121011
Varied On	LTO4 - FC	1, 1, 1, 4, 1, 1	Good	500308c0013ce01f			131001
Varied On	LTO3 - FC	1, 1, 1, 5, 1, 1	Good	500308c0013ce01e		Logical Library 01	HU106
Varied On	LTO4 - FC	1, 1, 1, 6, 1, 1	Good	500308c0013ce031			HU174

Drive Settings

Fibre Channel Parameters

Speed: Auto

Connection Options: Loop Preferred

Control

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 or Varied Off).
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 288.
RAS	The status of the drive as reported by the RAS system (for example, Good or Failed).
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.

Element	Description
In the Drive Settings: **Fibre Channel Parameters** area:	
Speed drop-down list	Configures the speed of the specified drive. Possible speed settings are: • Auto (default) • 1-Gb/s • 2-Gb/s • 4-Gb/s For LTO-5, possible settings are: • Auto (default) • 2-Gb/s • 4-Gb/s • 8-Gb/s
Connection Options drop-down list	Configures the type of connection for the specified drive. This setting is not available for libraries in advanced configuration. Possible connection types are: • Loop Preferred • Point to Point • Loop
Set button	Applies the selections you made in the **Fibre Channel Parameters** area to the specified drive.
In the **Control** area:	
Power Cycle button	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 button	Resets the specified drive without cycling the power.
Vary Off or Vary On button	Varies off or varies on the specified drive. The label of the button toggles between **Vary Off** and **Vary On**. Each use of this button updates the drive information in the **Drive(s)** area. Use this button when you hot swap drives.

Element	Description
Identify button	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 button	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 button	Ejects any currently loaded tape from the specified drive.
Get Drive Log button	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 467). 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.
Clean	Enables the drive cleaning process (see Cleaning a Drive on page 374).

The **Details** button displays the **Drive Details** dialog box. For more information, see Viewing Drive Details on page 369.

4 In the **Drive(s)** area, click the appropriate drive row to highlight it.

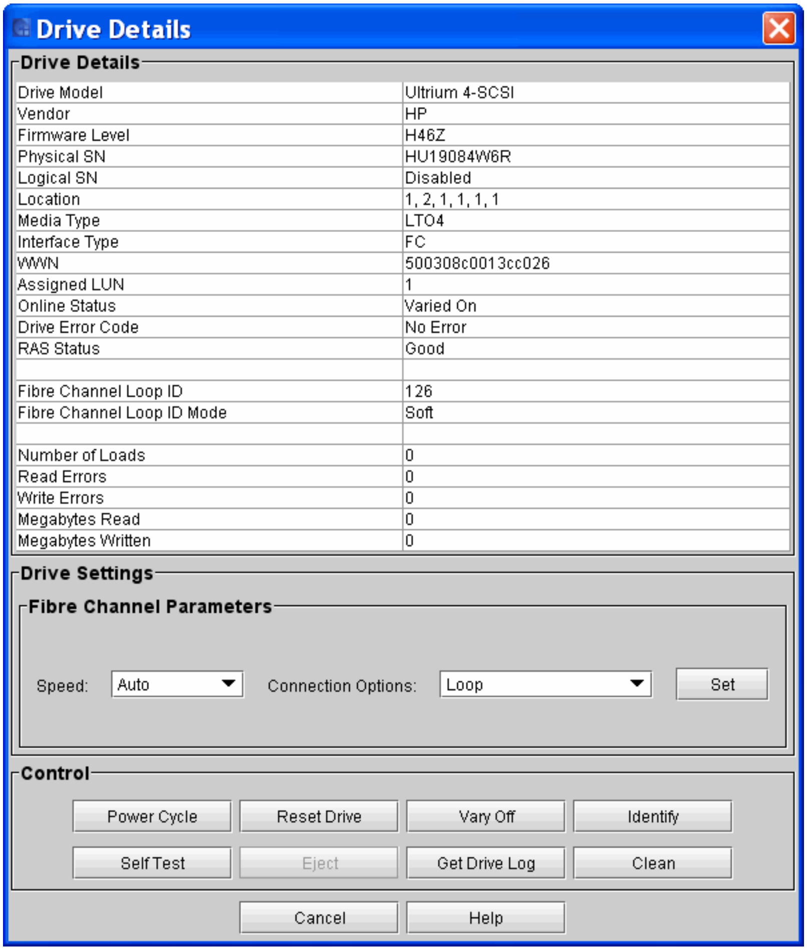
5 Perform operations in either the **Fibre Channel Parameters** area or the **Control** area of the **Drives** dialog box.

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.



Drive Details

Drive Details

Drive Model	Ultrium 4-SCSI
Vendor	HP
Firmware Level	H46Z
Physical SN	HU19084W6R
Logical SN	Disabled
Location	1, 2, 1, 1, 1, 1
Media Type	LTO4
Interface Type	FC
WWN	500308c0013cc026
Assigned LUN	1
Online Status	Varied On
Drive Error Code	No Error
RAS Status	Good
Fibre Channel Loop ID	126
Fibre Channel Loop ID Mode	Soft
Number of Loads	0
Read Errors	0
Write Errors	0
Megabytes Read	0
Megabytes Written	0

Drive Settings

Fibre Channel Parameters

Speed: Auto

Connection Options: Loop

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 Configuring and Testing Drives on page 365.

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.
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. For information about location coordinates, see the *Scalar i6000 User's Guide*.
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.
SCSI ID	For SCSI drives only, the SCSI ID of the drive. This field does not appear for Fibre drives.
Assigned LUN	The assigned logical unit number.
Volser	If a cartridge is loaded in the specified drive, the volume serial number of the cartridge.
Online Status	The status of the drive (Varied On or Varied Off).
Drive Error Code	For LTO drives only, the drive brick error code. This field does not appear for Fibre drives. If the drive currently has no errors, “No Error” appears in this field. If the library is unable to acquire a drive error code, such as when the robotics are disabled, “Unavailable” appears in this field.

Element	Description
RAS Status	The status of the drive as reported by the RAS 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 in this library.
Read Errors	The number of read errors that have occurred during the drive’s history in this library.
Write Errors	The number of write errors that have occurred during the drive’s history in this library.
Megabytes Read	The amount of data in megabytes that the drive has read during its history in this library.
Megabytes Written	The amount of data in megabytes that the drive has written during its history in this library.

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.

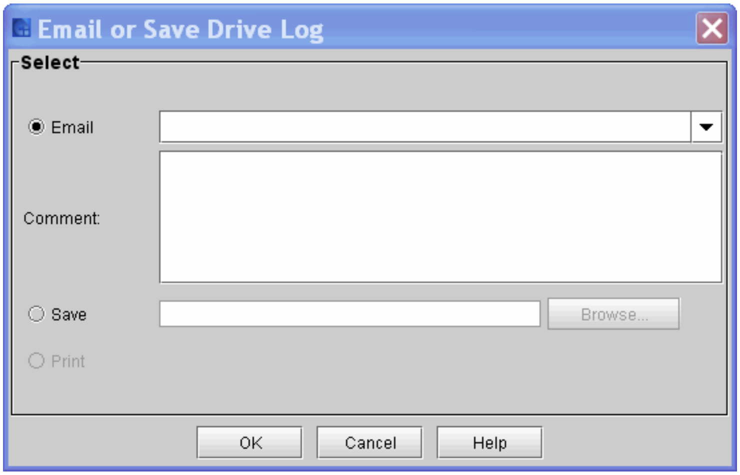
Note

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 164.

1 From the **Drives** dialog box, click **Get Drive Log**.

The **Email or Save Drive Log** dialog box appears.



● Email
○ Save
○ Print

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 automatic 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, for example, LTO or DLT.)

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.

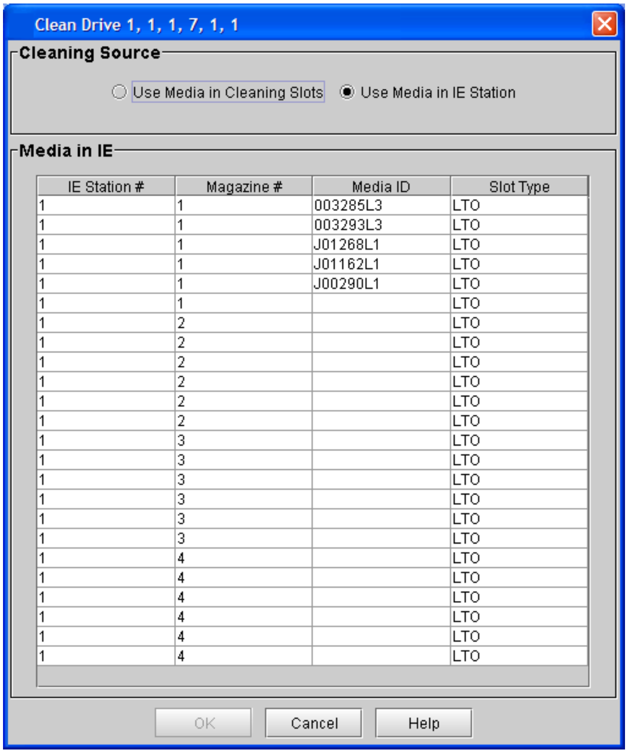
- Configure drive cleaning by assigning cleaning magazines and importing cleaning media. (For more information on configuring drive cleaning, see Configuring Drive Cleaning on page 214.)

After adding cleaning media to the library, manually initiate a drive cleaning operation.

1 On the menu bar, click **Tools**→ **Drives** to display the **Drives** dialog box.

2 Click a drive in the list, and then click **Clean**.

The **Clean Drive** dialog box appears.



Cleaning Source

○ Use Media in Cleaning Slots ● Use Media in IE Station

Media in IE

IE Station #	Magazine #	Media ID	Slot Type
1	1	003285L3	LTO
1	1	003293L3	LTO
1	1	J01268L1	LTO
1	1	J01162L1	LTO
1	1	J00290L1	LTO
1	1		LTO
1	2		LTO
1	2		LTO
1	2		LTO
1	2		LTO
1	2		LTO
1	2		LTO
1	3		LTO
1	3		LTO
1	3		LTO
1	3		LTO
1	3		LTO
1	3		LTO
1	4		LTO
1	4		LTO
1	4		LTO
1	4		LTO
1	4		LTO
1	4		LTO

3 Under **Cleaning Source**, click 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.

Working With Connectivity

The **Connectivity** dialog box enables you to do the following:

- Reset an I/O blade
- Reset the Fibre Channel port on the MCB or a Fibre Channel port on an I/O blade
- Power cycle an I/O blade
- Visually locate a specific I/O blade in the library

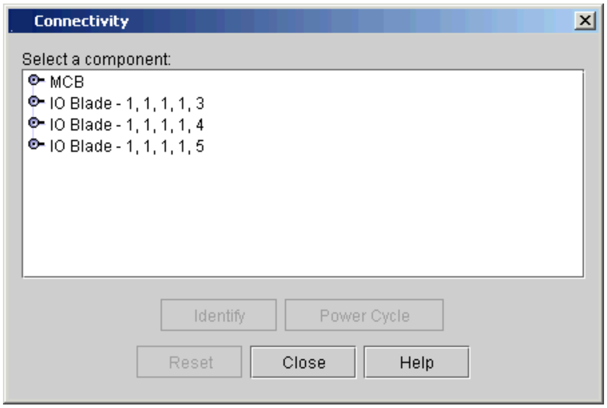
1 Log on as an administrator.

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**.

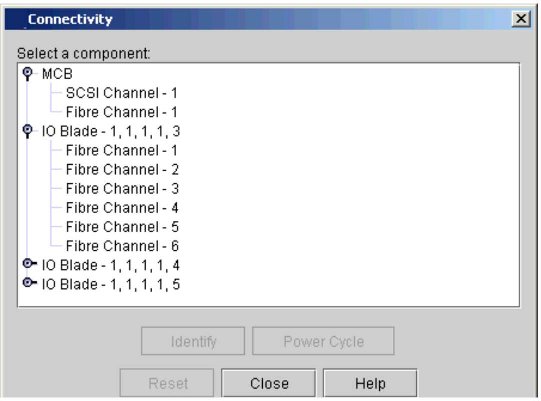
Note If the physical library is not offline, you receive a message that asks you whether you want to take it offline. Click **Yes**.

The **Connectivity** dialog box appears with the MCB and all I/O blades in the library listed.



4 To display the ports for a specific blade, click the name of the blade (MCB or one of the I/O blades).

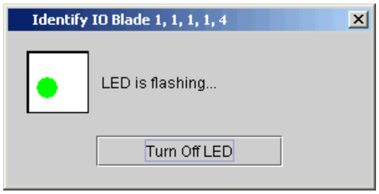
The following example shows the ports for the MCB and the I/O blade at location 1,1,1,1,4. (For information about location coordinates, see Understanding Location Coordinates on page 288.)



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 the Fibre Channel port on the MCB, click the I/O blade or the port to highlight it, and then click **Reset**.
- To cycle the power for an I/O blade, click the I/O blade to highlight it, and then click **Power Cycle**.
- To cause the LEDs on an I/O blade to blink rapidly so that you can easily find it in the library, click the I/O blade to highlight it, and then click **Identify**.

  When you click **Identify**, the following dialog box appears.



Identify IO Blade 1, 1, 1, 1, 4

LED is flashing...

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.

Note

- 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.
- You can mail or save snapshots from a remote client. However, you cannot save snapshots from the library's touch screen. 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 164.

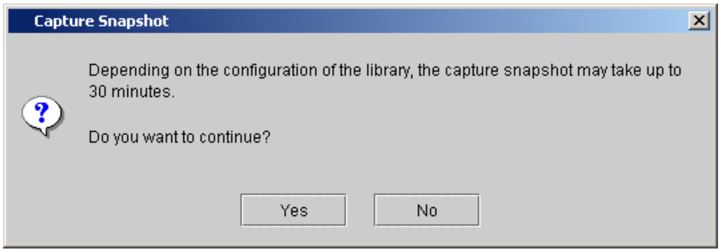
1 Log on as an administrator.

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.



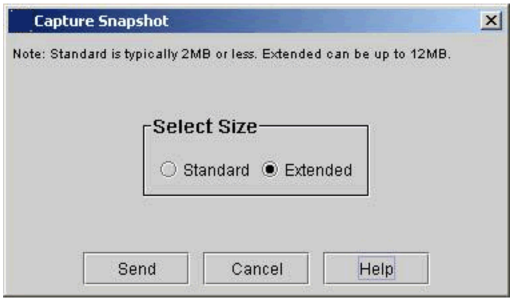
Capture Snapshot

Depending on the configuration of the library, the capture snapshot may take up to 30 minutes.

Do you want to continue?

5 If you want to continue, click **Yes**.

The **Capture Snapshot** dialog box appears.



Capture Snapshot

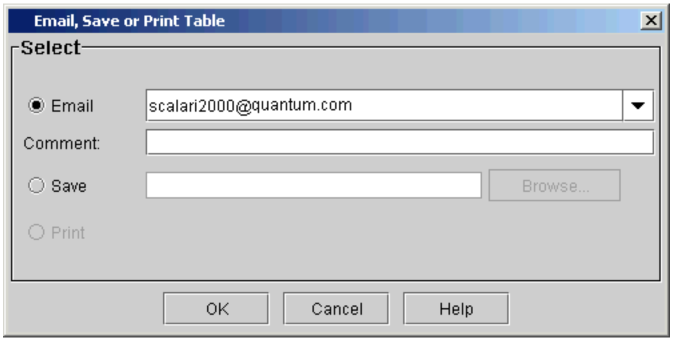
Note: Standard is typically 2MB or less. Extended can be up to 12MB.

Select Size: ○ Standard ● Extended

The **Standard** option captures information about all library components. The **Extended** option captures a greater amount of detailed information.

6 Select **Standard** or **Extended**, and then click **Send**.

The **Email, Save or Print Table** dialog box appears.



Email, Save or Print Table

Select

● Email: scalari2000@quantum.com

Comment:

○ Save

○ Print

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 should send the snapshot to Quantum technical support (www.quantum.com/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)
- 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 form 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 reinstallation process completes. The reinstallation procedure should be run only under specific circumstances. For more information, see Rolling Back to the Previous Build Package on page 395.

Note Rollback and reinstallation of current package options are viable recovery steps during a failed firmware upgrade, however these features should not be used as troubleshooting tools.

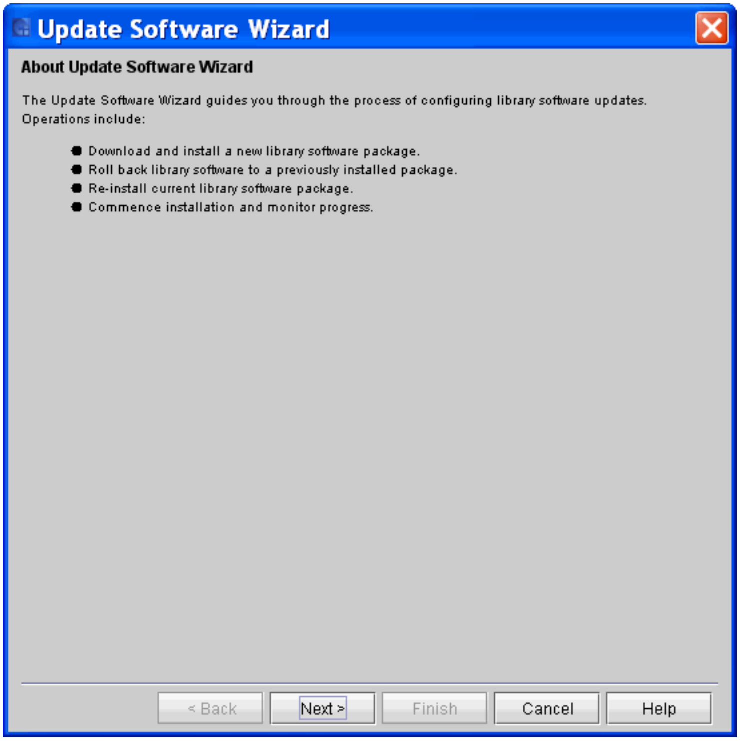
Accessing the Update Software Wizard

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.
3. Click **Tools** > **Update Software**.

The **Update Software Wizard** dialog box appears.



About Update Software Wizard

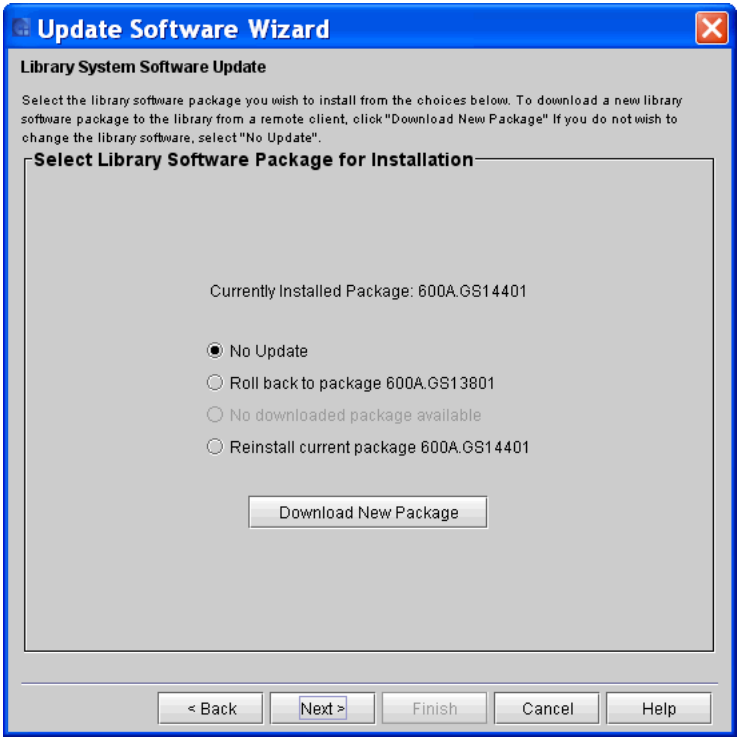
The Update Software Wizard guides you through the process of configuring library software updates. Operations include:

- Download and install a new library software package.
- Roll back library software to a previously installed package.
- Re-install current library software package.
- Commence installation and monitor progress.

This dialog box explains the operations you can perform by using the **Update Software Wizard**.

4 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.



Library System Software Update

Select the library software package you wish to install from the choices below. To download a new library software package to the library from a remote client, click "Download New Package" If you do not wish to change the library software, select "No Update".

Select Library Software Package for Installation

Currently Installed Package: 600A.GS14401

● No Update
○ Roll back to package 600A.GS13801
○ No downloaded package available
○ Reinstall current package 600A.GS14401

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 Some upgrades will not be download upgrades but instead CF (compact flash) swap upgrades.

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.

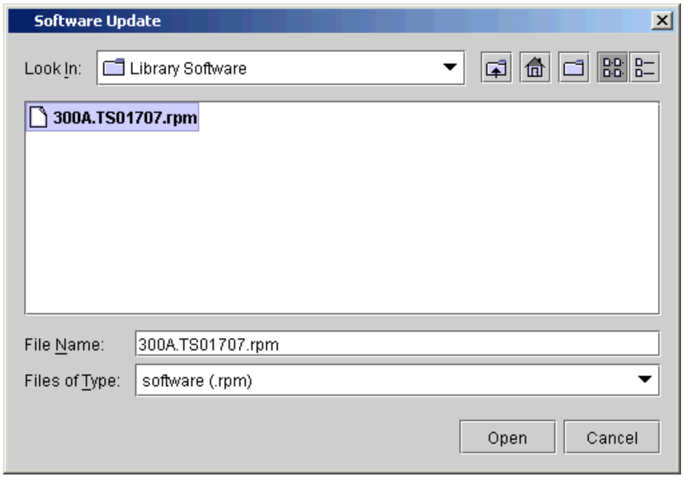
Downloading a New Library Software Package

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.

1 On the **Library System Software Update** dialog box, click **Download New Package**.

The **Software Update** dialog box appears.



Software Update

Look In: Library Software

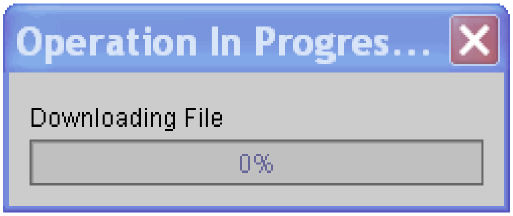
300A.TS01707.rpm

File Name: 300A.TS01707.rpm

Files of Type: software (.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.

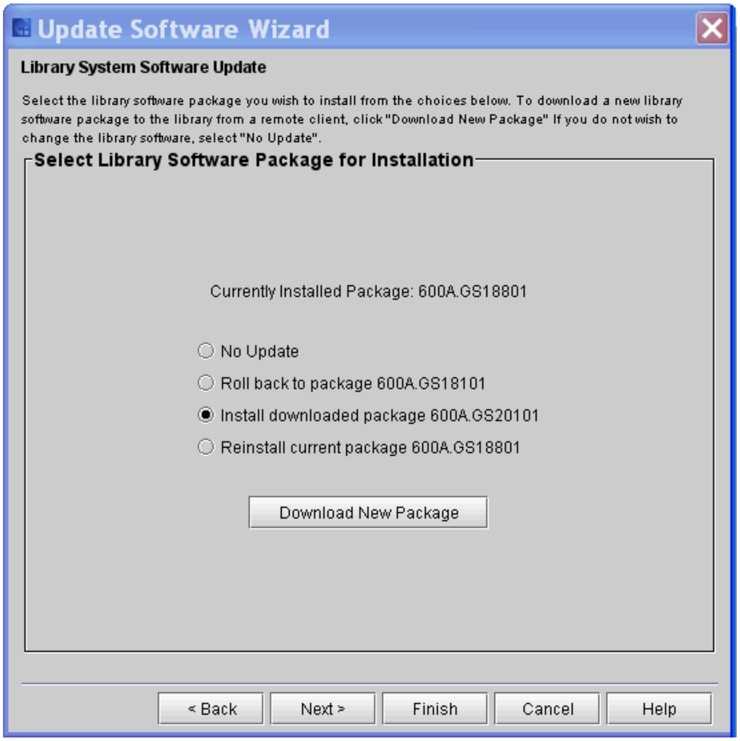


Operation In Progres...

Downloading File

0%

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.



Update Software Wizard

Library System Software Update

Select the library software package you wish to install from the choices below. To download a new library software package to the library from a remote client, click "Download New Package" If you do not wish to change the library software, select "No Update".

Select Library Software Package for Installation

Currently Installed Package: 600A.GS18801

○ No Update
○ Roll back to package 600A.GS18101
● Install downloaded package 600A.GS20101
○ Reinstall current package 600A.GS18801

The version number of the software package appears at the end of the **Install downloaded package** option.

Installing a New Library Software Package

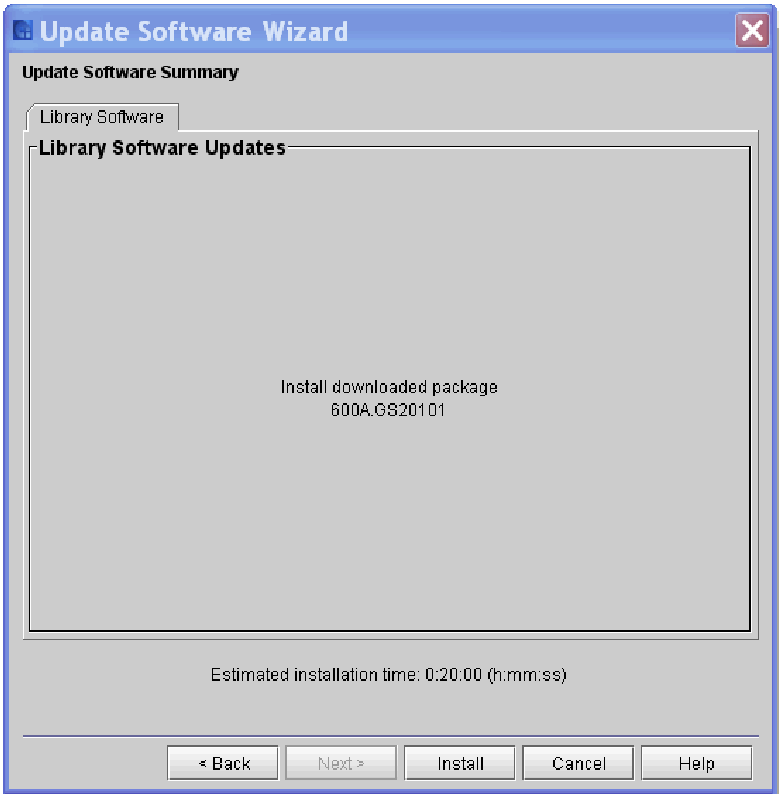
After you download the new library software package, you are ready to install it from either the library’s touch screen or a remote client. This procedure assumes that you are working from a remote client.

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.



Install downloaded package
600A.GS20101

Estimated installation time: 0:20:00 (h:mm:ss)

3 Click **Install.**

A warning message appears asking you to take the library offline.

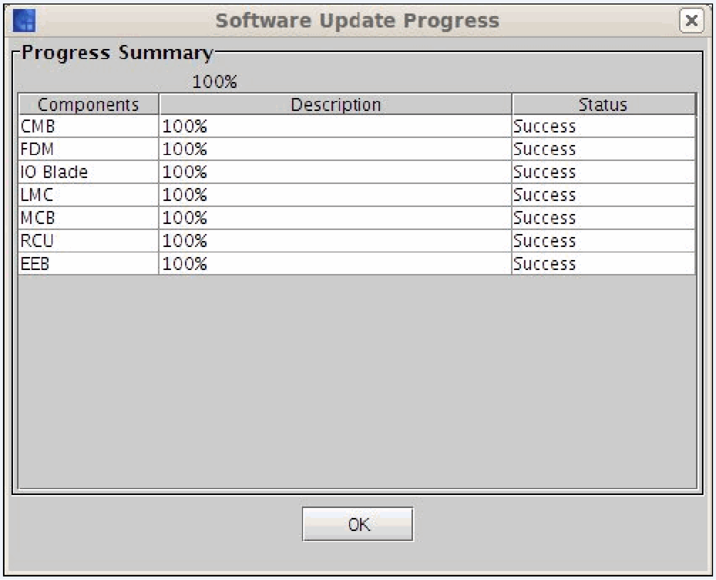
4 Click **Yes**.

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.



100%

Components	Description	Status
CMB	100%	Success
FDM	100%	Success
IO Blade	100%	Success
LMC	100%	Success
MCB	100%	Success
RCU	100%	Success
EEB	100%	Success

Real-time progress information appears under **Progress Summary** in the **Description** and **Status** columns.

Note During the update, the **Abort** button appears dimmed and is unavailable. Do not interrupt the update process before it is completed. Interrupting the update process might cause the library to become unusable until its software is restored.

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 the remote browser and log in again once the library has completed its reboot process.

9 Click **Help > About**. Validate that the components reflect the correct firmware version.

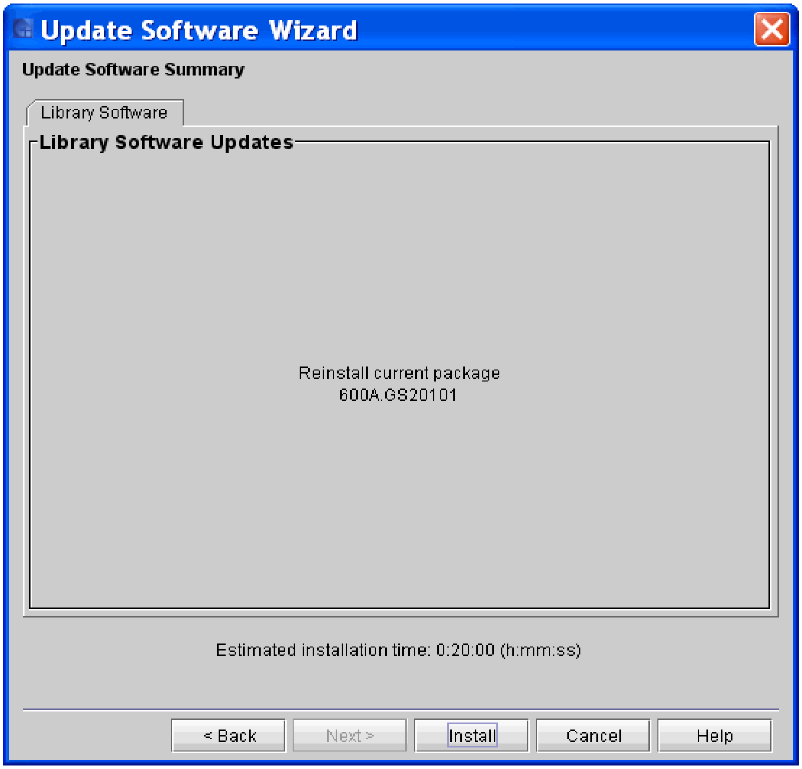
Reinstalling Current Library Software

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 either of the following situations has occurred:

- The compact flash on the MCB has been replaced, the library software on it is now at a different level, and you want to invoke the level that is on the MCB compact flash
- 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.



Reinstall current package
600A.GS20101

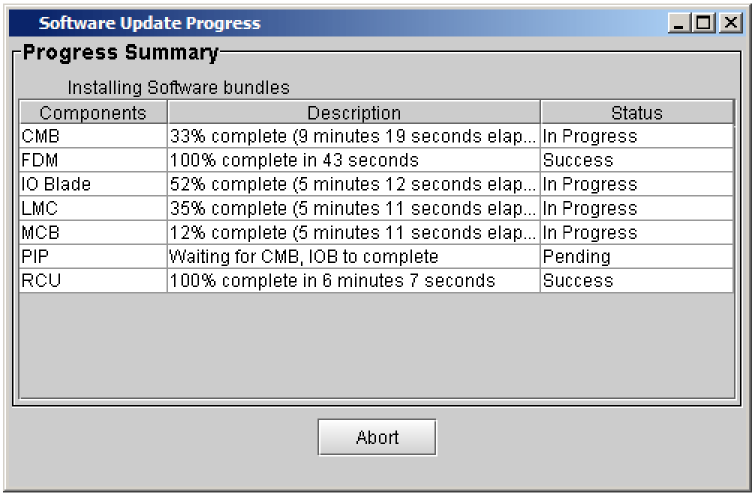
Estimated installation time: 0:20:00 (h:mm:ss)

3 Click **Install**.

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.

The **Software Update Progress** dialog box appears.



Software Update Progress

Progress Summary

Installing Software bundles

Components	Description	Status
CMB	33% complete (9 minutes 19 seconds elap...	In Progress
FDM	100% complete in 43 seconds	Success
IO Blade	52% complete (5 minutes 12 seconds elap...	In Progress
LMC	35% complete (5 minutes 11 seconds elap...	In Progress
MCB	12% complete (5 minutes 11 seconds elap...	In Progress
PIP	Waiting for CMB, IOB to complete	Pending
RCU	100% complete in 6 minutes 7 seconds	Success

Real-time progress information appears under **Progress Summary** in the **Description** and **Status** columns.

CAUTION **During the update, the Abort button appears dimmed and is unavailable. Do not interrupt the update process before it is completed. Interrupting the update process might cause the library to become unusable until its software is restored.**

Note The components that already have the correct version loaded will transition to a “Success” status quickly during the reinstall process.

4 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.

5 Bring the physical library online.

   a From the LMC, click **Operations** > **Change Mode**.

   b Select **Online**, and then click **OK**.

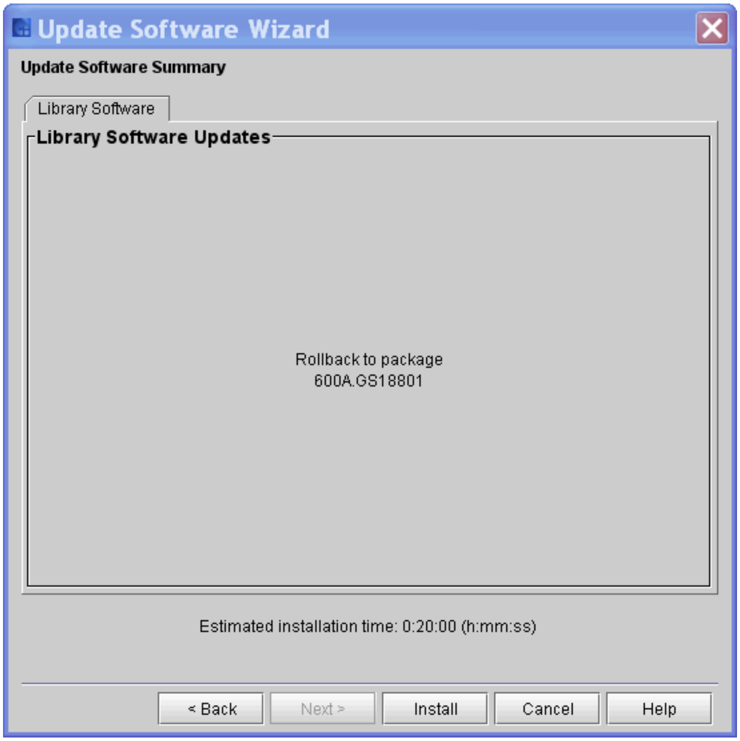
6 Click **Help > About**. Validate that the components reflect the correct firmware version.

Rolling Back to the Previous Build Package

1 On the **Library System Software Update** dialog box, select **Rollback to package.**

2 Click **Next.**

The **Update Software Wizard** dialog box appears.



Update Software Summary

Library Software Updates

Rollback to package
600A.GS18801

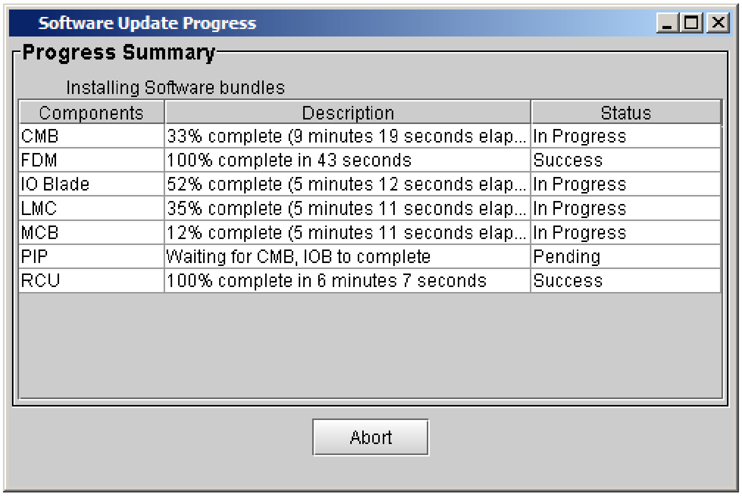
Estimated installation time: 0:20:00 (h:mm:ss)

3 Click **Install.**

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.

The **Software Update Progress** dialog box appears.



Installing Software bundles

Components	Description	Status
CMB	33% complete (9 minutes 19 seconds elap...	In Progress
FDM	100% complete in 43 seconds	Success
IO Blade	52% complete (5 minutes 12 seconds elap...	In Progress
LMC	35% complete (5 minutes 11 seconds elap...	In Progress
MCB	12% complete (5 minutes 11 seconds elap...	In Progress
PIP	Waiting for CMB, IOB to complete	Pending
RCU	100% complete in 6 minutes 7 seconds	Success

Real-time progress information appears under **Progress Summary** in the **Description** and **Status** columns.

CAUTION **During the update, the Abort button appears dimmed and is unavailable. Do not interrupt the update process before it is completed. Interrupting the update process might cause the library to become unusable until its software is restor**ed.

4 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.**

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 Ether 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.

You can use the **Update Drive Firmware** command from the **Tools** menu 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:

- Accessing the Update Drive Firmware Dialog Box on page 399.
- Downloading New Drive Firmware on page 401
- Updating Drive Firmware Using Firmware Images on page 403
- Updating Drive Firmware Using Update Tapes on page 406

Accessing the Update Drive Firmware Dialog Box

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.

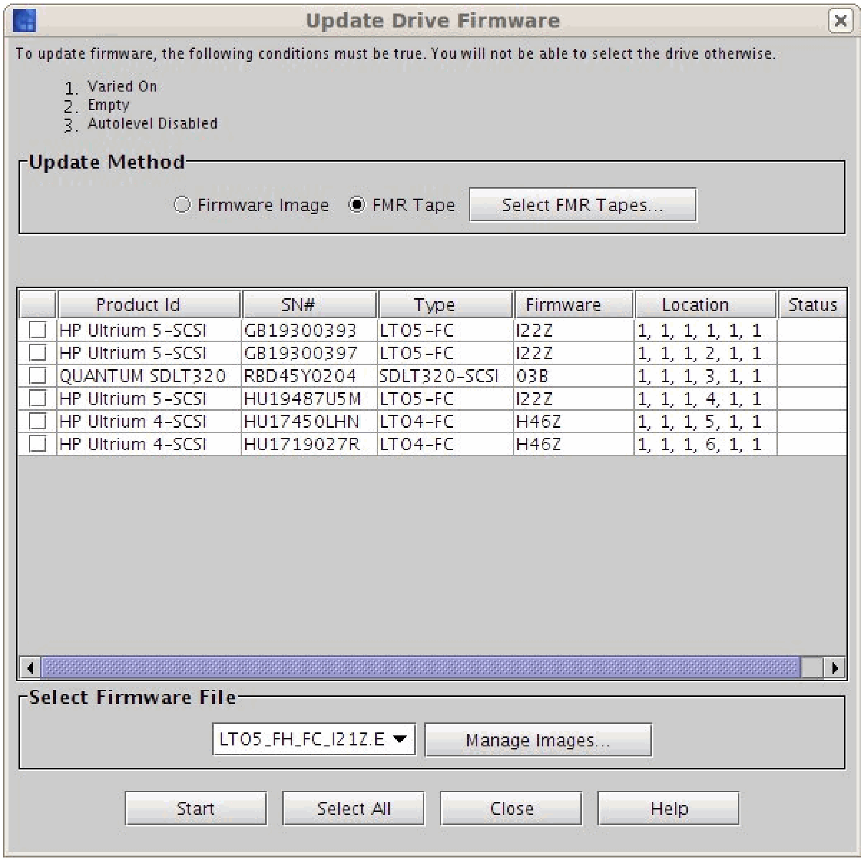
⚠ CAUTION **If you are viewing a partition, drive firmware update operations affect drives that are within the partition only.**

3 Click **Tools** > **Update Drive Firmware**.

If the physical library or the partition you are viewing is not offline, you receive a message that asks you whether you want to take it offline.

4 Click **Yes**.

The **Update Drive Firmware** dialog box appears.



Update Drive Firmware

To update firmware, the following conditions must be true. You will not be able to select the drive otherwise.

1. Varied On
2. Empty
3. Autolevel Disabled

Update Method

○ Firmware Image ● FMR Tape [Select FMR Tapes...]

	Product Id	SN#	Type	Firmware	Location	Status
□	HP Ultrium 5-SCSI	GB19300393	LTO5-FC	I22Z	1, 1, 1, 1, 1, 1	
□	HP Ultrium 5-SCSI	GB19300397	LTO5-FC	I22Z	1, 1, 1, 2, 1, 1	
□	QUANTUM SDLT320	RBD45Y0204	SDLT320-SCSI	03B	1, 1, 1, 3, 1, 1	
□	HP Ultrium 5-SCSI	HU19487U5M	LTO5-FC	I22Z	1, 1, 1, 4, 1, 1	
□	HP Ultrium 4-SCSI	HU17450LHN	LTO4-FC	H46Z	1, 1, 1, 5, 1, 1	
□	HP Ultrium 4-SCSI	HU1719027R	LTO4-FC	H46Z	1, 1, 1, 6, 1, 1	

Select Firmware File

LTO5_FH_FC_I21Z.E ▼ [Manage Images...]

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.

To update drive firmware by using downloaded firmware images, proceed to Updating Drive Firmware Using Firmware Images on page 403 below. To update drive firmware by using update tapes, proceed to Updating Drive Firmware Using Update Tapes on page 406.

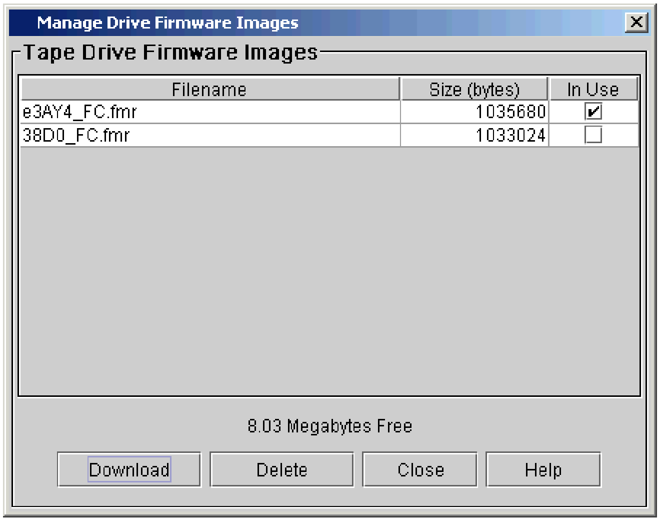
Downloading New Drive Firmware

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.

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.

1 On the **Update Drive Firmware** dialog box, click **Manage Images**.

The **Manage Drive Firmware Images** dialog box appears.



Manage Drive Firmware Images

Tape Drive Firmware Images

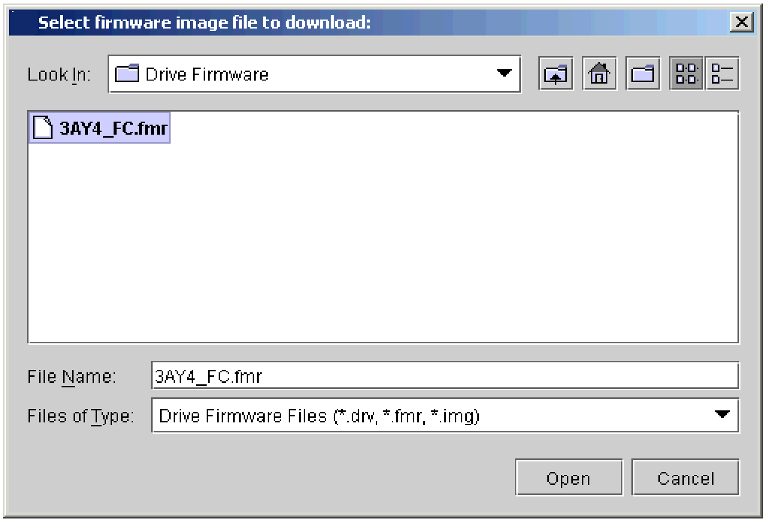
Filename	Size (bytes)	In Use
e3AY4_FC.fmr	1035680	☑
38D0_FC.fmr	1033024	□

8.03 Megabytes Free

The library has enough space for 20 MB (with a maximum of 8 images) of drive firmware images. 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.



File Name: 3AY4_FC.fmr
Files of Type: Drive Firmware Files (*.drv, *.fmr, *.img)

3 Navigate to the location of the drive firmware image file (with either a **.drv**, **.fmr**, **.E**, or **.img** 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. After the download process finishes, the drive firmware image file is added to the list on the **Manage Drive Firmware Images** dialog box.

5 On the **Manage Drive Firmware Images** dialog box, click **Close**.

The **Update Drive Firmware** dialog box appears again.

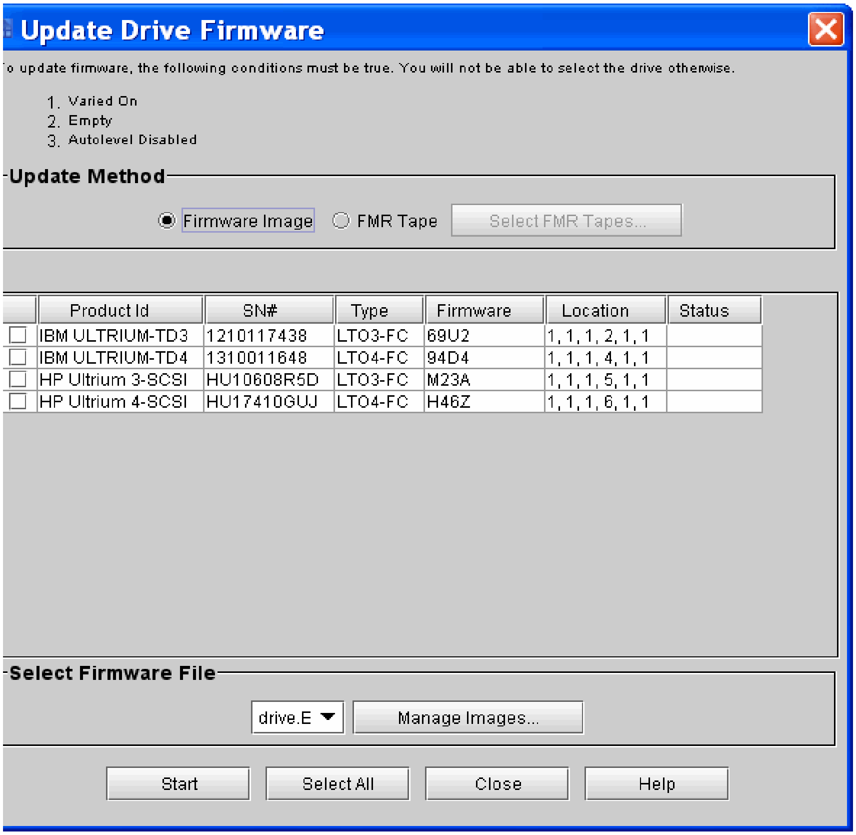
Updating Drive Firmware Using Firmware Images

⚠ **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, remove prior to initiating drive code changes.**

1 On the **Update Drive Firmware** dialog box, select **Firmware Image**.



Update Drive Firmware

o update firmware, the following conditions must be true. You will not be able to select the drive otherwise.

1. Varied On
2. Empty
3. Autolevel Disabled

Update Method

● Firmware Image ○ FMR Tape

	Product Id	SN#	Type	Firmware	Location	Status
□	IBM ULTRIUM-TD3	1210117438	LTO3-FC	69U2	1, 1, 1, 2, 1, 1	
□	IBM ULTRIUM-TD4	1310011648	LTO4-FC	94D4	1, 1, 1, 4, 1, 1	
□	HP Ultrium 3-SCSI	HU10608R5D	LTO3-FC	M23A	1, 1, 1, 5, 1, 1	
□	HP Ultrium 4-SCSI	HU17410GUJ	LTO4-FC	H46Z	1, 1, 1, 6, 1, 1	

Select Firmware File

drive.E

Note Drives that are not connected to I/O Blades 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 406.

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, like HP or IBM for example, 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**.

Note The library automatically logs off other users so that they cannot perform library operations while the drive firmware update operation is in progress.

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.

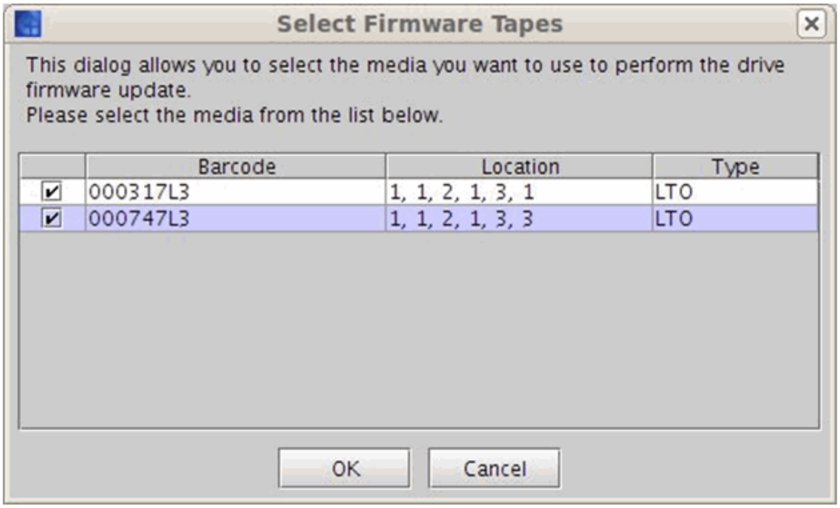
1 Write down the Barcode number on the tape before inserting it into the I/E Station.

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.



Select Firmware Tapes

This dialog allows you to select the media you want to use to perform the drive firmware update.
Please select the media from the list below.

	Barcode	Location	Type
☑	000317L3	1, 1, 2, 1, 3, 1	LTO
☑	000747L3	1, 1, 2, 1, 3, 3	LTO

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.

CAUTION **Do not power cycle the drive.**

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.

You can configure the library to automatically perform the full teach routine (configuration and calibration) whenever the library's power is cycled. For more information, see Setting Up Policies for the Physical Library on page 159.

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 The library automatically performs an inventory after it completes the configuration teach process.

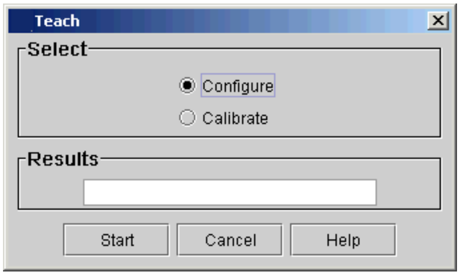
1 Log on as an administrator.

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**.

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 **Teach** dialog box appears.



Select

● Configure

○ Calibrate

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. If the configuration teach process completes successfully, the **Teach** dialog box could close automatically.

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 two special magazines in each drive-side and door-side storage rack. 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.

Note When the library reaches 20,000 moves after the last calibration occurred, and if then the library is rebooted or an access door is closed, the library automatically recalibrates itself.

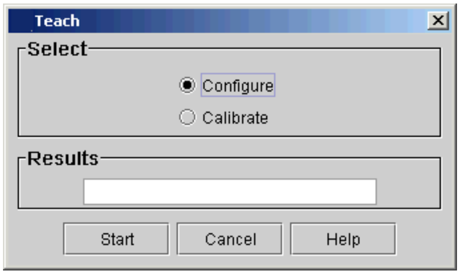
1 Log on as an administrator.

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**.

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 **Teach** dialog box appears with **Configure** selected by default.



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. If the calibration teach process completes successfully, the **Teach** dialog box could close automatically.

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, seeSetting Up Policies for the Physical Library on page 159.

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.

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 compact flash memory on 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. You also have the option to save the rescue image when you save the remote restore image.
- The revert image is automatically created and stored locally as the first step of any restore or rescue operation. The **Revert** command is available from both the remote client and the local touch screen.

When to Save the Library Configuration

Even though you can choose to save the library configuration at any time, the library prompts you to save in certain situations. Specifically, the library prompts you to save whenever you change configuration settings in the following areas:

- User accounts
- RAS event notifications
- E-mail setup

Other configuration changes that the library detects cause the library to generate warning tickets for the Control subsystem. This causes a warning icon to appear on the **Control** system status button. Be aware that if a more serious unresolved ticket already exists in that status group, the warning ticket is generated, but no notification is sent until the more serious problem ticket is resolved or closed.

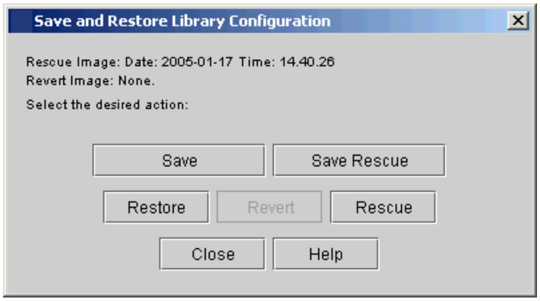
CAUTION **Changes to hardware, such as removing drives or I/O blades, do not prompt you to save, either by means of messages or warning tickets. Therefore, it is important to save the configuration image after a hardware configuration change.**

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.
2. Make sure that you are viewing the physical library. From the **View** menu, click the name of the physical library.
3. Click **Tools** > **Save/Restore**.

   The **Save and Restore Library Configuration** dialog box appears.



Save and Restore Library Configuration

Rescue Image: Date: 2005-01-17 Time: 14.40.26
Revert Image: None.
Select the desired action:

4. Click **Save**.
5. 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.
6. To proceed, click **Open**.

   The library prompts you to decide whether you want to write over the current rescue image that is stored locally on the library.

7 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.

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

3 Click **Tools** > **Save/Restore**.

The **Save and Restore Library Configuration** dialog box appears.

4 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.

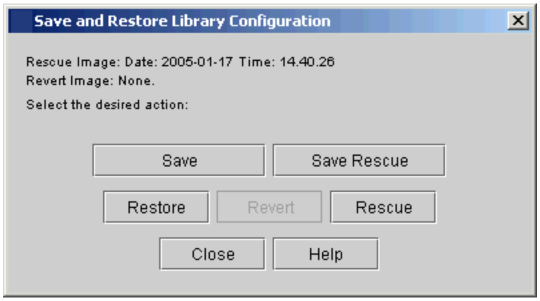
CAUTION **Be cautious if you plan to use a saved library configuration image that is out of date. You might restore configuration information that you do not want, such as former passwords, partitions, mappings, and hardware configurations.**

1 Log on as an administrator from the remote client. The **Restore** command is not available from the library's touch screen.

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

3 Click **Tools** > **Save/Restore**.

The **Save and Restore Library Configuration** dialog box appears.



Save and Restore Library Configuration

Rescue Image: Date: 2005-01-17 Time: 14.40.26
Revert Image: None.
Select the desired action:

4 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**.

5 Using the file chooser dialog box, locate the restore image file on the remote file system.

6 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.

7 After the restore operation has completed on the library, close and restart the remote client.

8 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.

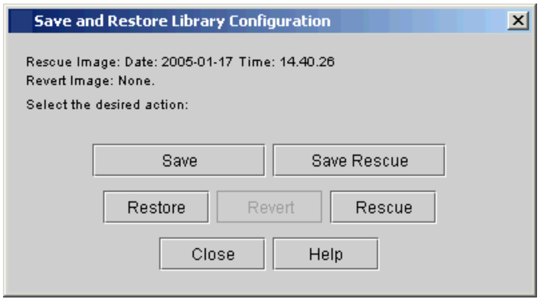
If library configuration has occurred since the last time the image was saved, those changes will be lost when the older configuration is restored. The restore operation will succeed, but you will then need to reconfigure the library, including the partitions and mappings. Therefore, it is important 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.

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

3 Click **Tools** > **Save/Restore**.

The **Save and Restore Library Configuration** dialog box appears.



Save and Restore Library Configuration

Rescue Image: Date: 2005-01-17 Time: 14.40.26
Revert Image: None.
Select the desired action:

4 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**.

5 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.

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 recommence.

Reverting Library Configuration

In the event that either a restore or rescue operation fails before completion and the library becomes unstable, the **Revert** command provides a way to roll back any library configuration changes that might have occurred during the operation. The **Revert** command is unavailable if no revert image is saved. On a new library, no revert image exists until a restore or rescue operation is attempted for the first time.

1 Log on as an administrator from the remote client or from the library’s touch screen.

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

3 Click **Tools** > **Save/Restore**.

   The **Save and Restore Library Configuration** dialog box appears.

4 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**.

5 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.

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 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, seeEnabling Licenses on page 110.

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.

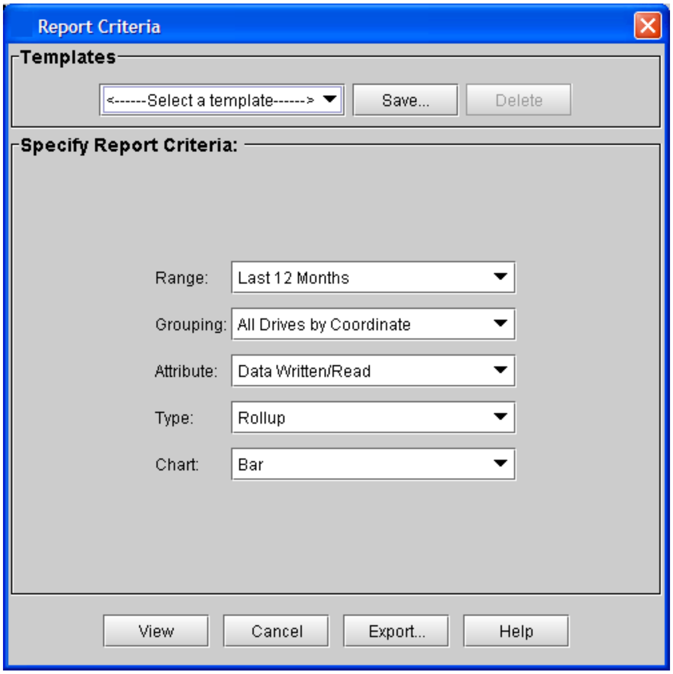
Note You can e-mail, save, or print reports from a remote client. However, you cannot save or print reports from the library's touch screen.

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 **Report Criteria** dialog box appears.



Range: Last 12 Months

Grouping: All Drives by Coordinate

Attribute: Data Written/Read

Type: Rollup

Chart: Bar

4 In the **Report Criteria** dialog box, 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.
- Attribute
    - Data Written/Read
    - Mount Count
    - Media Motion Hours
    - 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

5 Choose from the following charts to visually display your data:

    - Bar
    - Bar 3D
    - Line
    - Stacked Area
    - Stacked Bar
    - Stacked Bar 3D

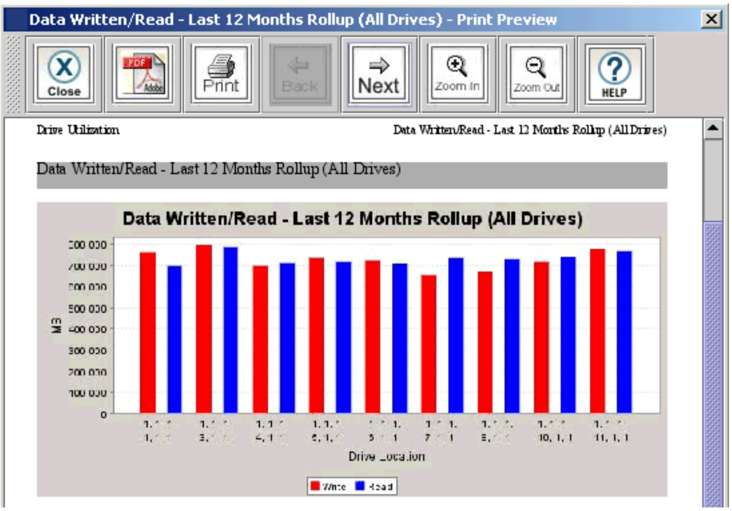
6 To directly send or save the data, click **Export**.

- 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.

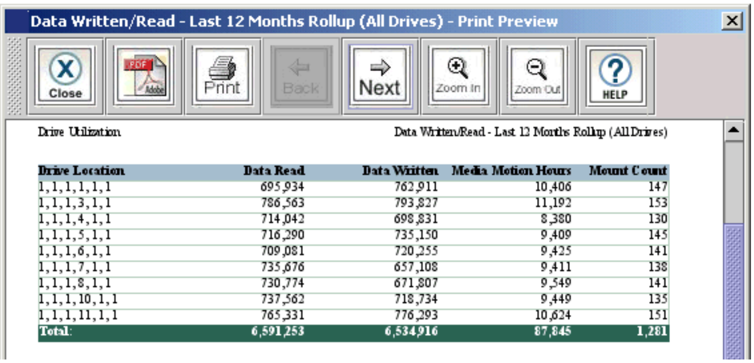
7 Click **OK**.

8 To view a report according to the criteria selected, click **View**.

The report appears graphically according to the type of chart you selected.


Data Written/Read - Last 12 Months Rollup (All Drives) - Print Preview
Close
PDF Adobe
Print
Back
Next
Zoom In
Zoom Out
HELP
Drive Utilization
Data Written/Read - Last 12 Months Rollup (All Drives)
Data Written/Read - Last 12 Months Rollup (All Drives)
Data Written/Read - Last 12 Months Rollup (All Drives)
800 000
700 000
600 000
500 000
400 000
300 000
200 000
100 000
0
MB
10, 1, 1
11, 1, 1
Drive Location
Write
Read

9 To view the next page of the report, click the **Next** icon on the toolbar.


Data Written/Read - Last 12 Months Rollup (All Drives) - Print Preview
Close
PDF Adobe
Print
Back
Next
Zoom In
Zoom Out
HELP

Drive Utilization

Data Written/Read - Last 12 Months Rollup (All Drives)

Drive Location	Data Read	Data Written	Media Motion Hours	Mount Count
1,1,1,1,1,1	695,934	762,911	10,406	147
1,1,1,3,1,1	786,563	793,827	11,192	153
1,1,1,4,1,1	714,042	698,831	8,380	130
1,1,1,5,1,1	716,290	735,150	9,409	145
1,1,1,6,1,1	709,081	720,255	9,425	141
1,1,1,7,1,1	735,676	657,108	9,411	138
1,1,1,8,1,1	730,774	671,807	9,549	141
1,1,1,10,1,1	737,562	718,734	9,449	135
1,1,1,11,1,1	765,331	776,293	10,624	151
Total:	**6,591,253**	**6,534,916**	**87,845**	**1,281**

10 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 **Report Criteria** dialog box appears.

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

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**.

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
- Media Integrity Analysis 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 164.

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, or Media (Integrity Analysis, Usage, or Security)**.

   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 report.

For more information about choosing report criteria, seGenerating Media Integrity Analysis Reports on page 65, Generating the Tickets Report on page 76, or Viewing the Drive Resource Utilization Reports on page 420.

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

4 Type a name for the template, and then click **OK**.

The template appears in the list under **Templates**.

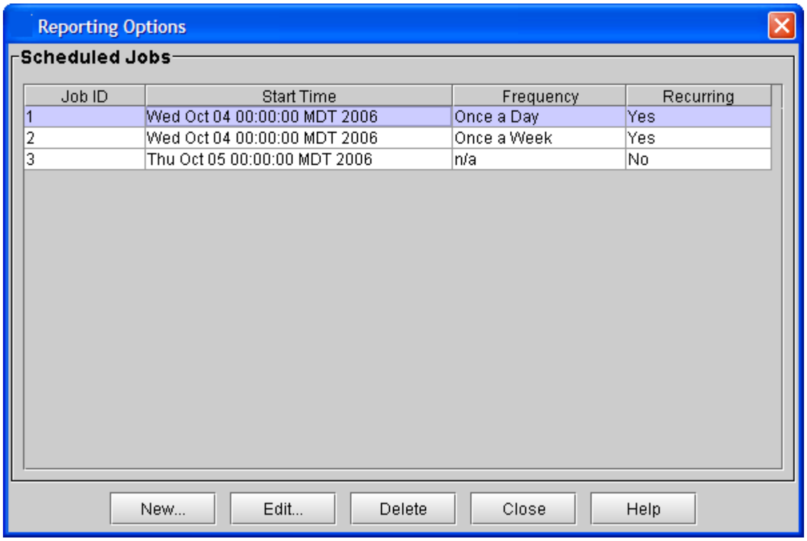
5 To close the **Report Criteria** dialog box, click **Cancel**.

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.



Reporting Options

Scheduled Jobs

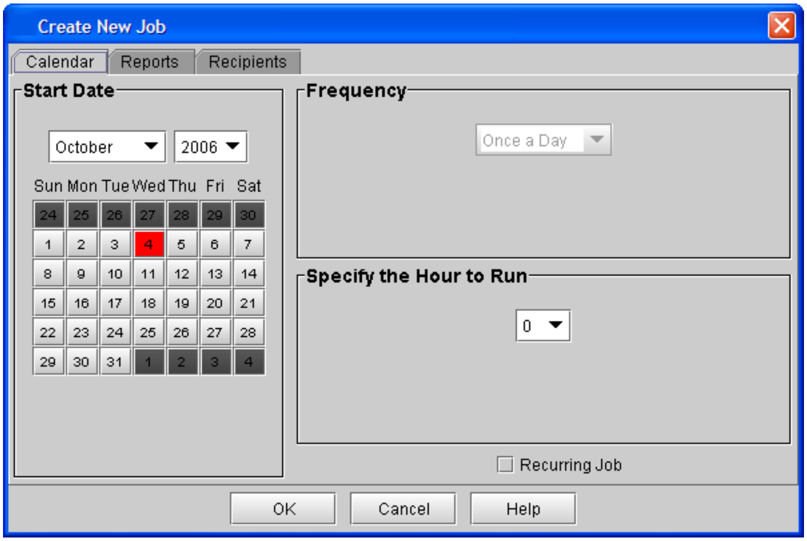
Job ID	Start Time	Frequency	Recurring
1	Wed Oct 04 00:00:00 MDT 2006	Once a Day	Yes
2	Wed Oct 04 00:00:00 MDT 2006	Once a Week	Yes
3	Thu Oct 05 00:00:00 MDT 2006	n/a	No

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.



Start Date

October 2006

Sun	Mon	Tue	Wed	Thu	Fri	Sat
24	25	26	27	28	29	30
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	1	2	3	4

Frequency: Once a Day

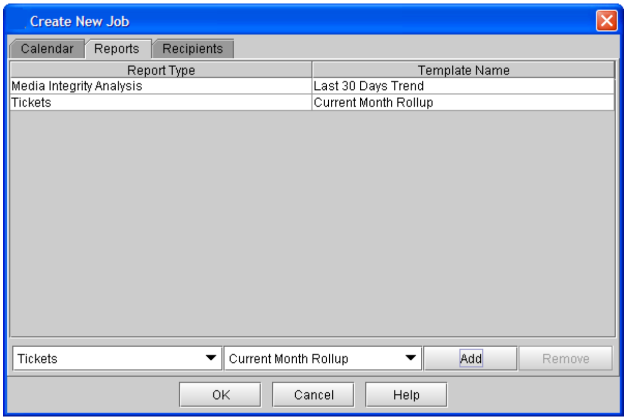
Specify the Hour to Run: 0

☐ Recurring Job

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, seeSaving Report Criteria Templates on page 425.



Create New Job

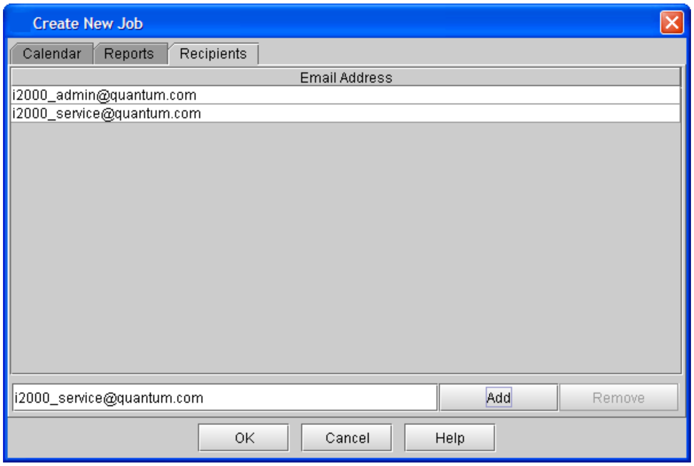
Calendar | Reports | Recipients

Report Type	Template Name
Media Integrity Analysis	Last 30 Days Trend
Tickets	Current Month Rollup

Tickets ▼ | Current Month Rollup ▼

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**.



Create New Job

Calendar | Reports | Recipients

Email Address
i2000_admin@quantum.com
i2000_service@quantum.com

i2000_service@quantum.com

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 429.

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 three types of verification test that help diagnose problems with the library:

- Installation verification test
- Partial system tests
- FRU operation tests

The verification tests provide the following:

- Fully automated tests
- Tests to determine marginality of installation
- Detailed problem analysis

- Full system tests or individual field replaceable unit (FRU) tests
- Logs of installation and configuration tests
- Graphical reports showing passed, marginal, 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 that are available.

Installation Verification Test

The installation verification test enables you to verify that the library's installation and configuration is complete and functioning correctly. The installation verification test runs the following individual tests:

- Library alignment test
- Picker assembly test
- I/E station assembly test
- Get/Put test
- Scanner fiducial test

The smaller library configuration will require about 1 hour and the larger configurations will require as long as 6 hours to run the installation verification test. The time to complete individual tests on an eight-frame configuration is approximately:

- Library alignment test - 30 minutes
- Picker assembly test - 1 minute
- I/E station assembly test - 5 minutes for each 24 slot I/E station
- Get/Put test - 120 minutes
- Scanner fiducial test - 75 minutes

Note These times do not include debug or repair time.

Partial System Tests

The partial system tests perform the selected subtests to test an area or range of the library configuration. The selectable tests include:

- Frame test - This test includes the same individual tests as the installation verification 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 Operational Tests

The FRU operational tests enable you to verify the replacement of a FRU. When the FRU test is selected, you can select any of the following individual tests:

- Accessor assembly
- Picker assembly
- Drive sled assembly
- I/E station assembly
- Scan barcode

When one of the subtests 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.

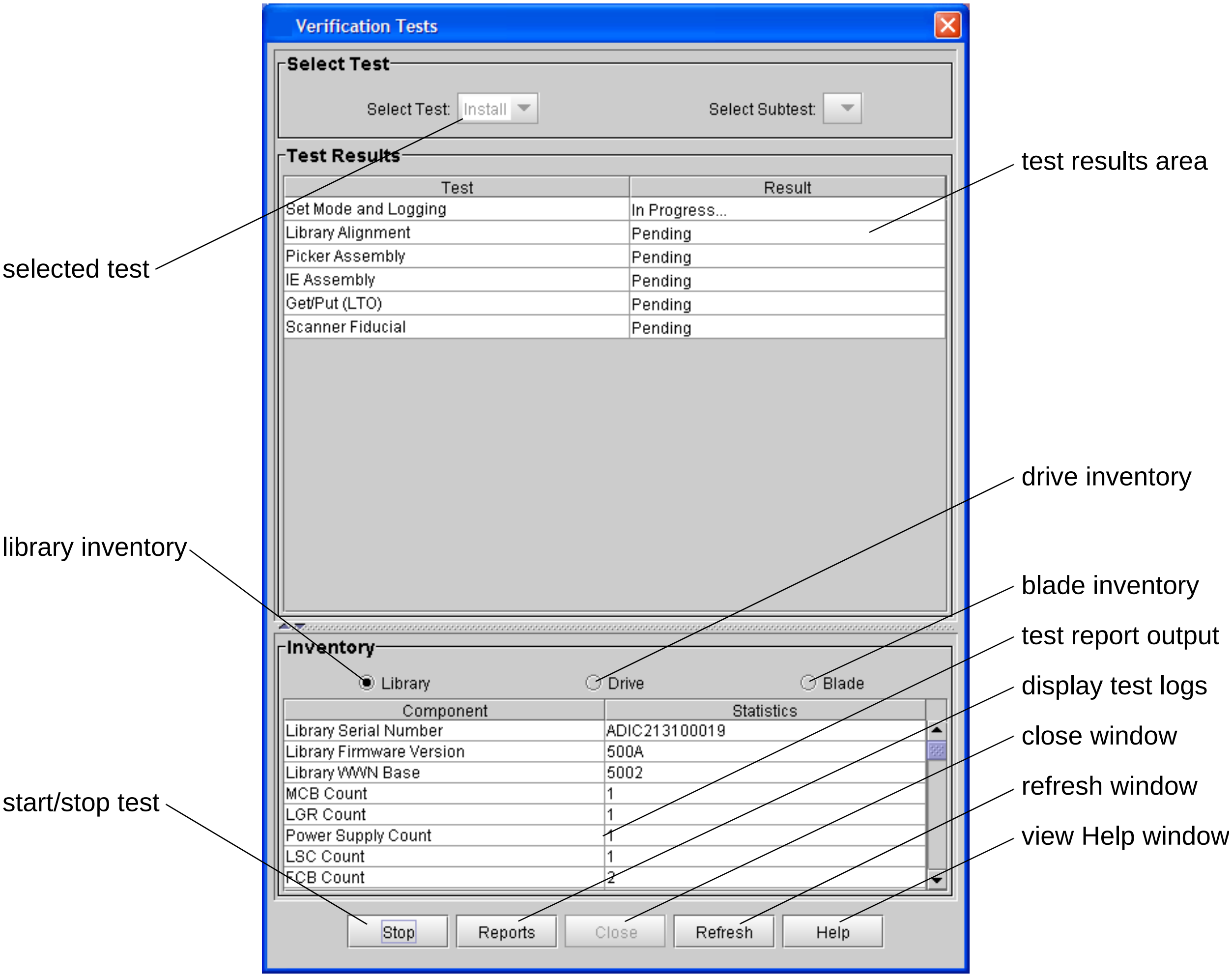
Custom Library Alignment Tests

The custom tests enable you to run a sub-test that is normally part of the larger tests that call multiple sub-tests (such as Installation, Partial, etc.). Please refer to the **Verification Test Functions** section for more specific information about each sub-test.

Verification Test Functions

Use the **Verification Tests** dialog box to run tests and view results. Figure 38 shows the parts of the **Verification Tests** dialog box. To display the dialog box, click **Tools** > **Verification Tests**.

Figure 38 Verification Tests Dialog Box



Verification Tests

Select Test

Select Test: Install

Select Subtest:

Test Results

Test	Result
Set Mode and Logging	In Progress...
Library Alignment	Pending
Picker Assembly	Pending
IE Assembly	Pending
Get/Put (LTO)	Pending
Scanner Fiducial	Pending

Inventory

● Library ○ Drive ○ Blade

Component	Statistics
Library Serial Number	ADIC213100019
Library Firmware Version	500A
Library WWN Base	5002
MCB Count	1
LGR Count	1
Power Supply Count	1
LSC Count	1
FCB Count	2

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 marginal and 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 statistical information:

- Frame card serial numbers
- Power supply serial numbers
- Number of cartridges in the library
- Controller serial number and firmware information for the following:
  - Management control blade
  - Control management blade
  - Robotic control unit or RCU
  - Picker
  - I/E stations

Drive Inventory

This inventory list provides the following information about each drive:

- Drive sled locations
- Drive sled controller serial numbers
- Drive sled controller boot and application firmware versions
- Drive brick serial numbers and firmware versions
- Drive logical serial number if the library is configured for logical serial number addressing

Blade Inventory

This inventory list provides the following information about each Fibre Channel I/O blade:

- Location of each blade
- Serial number of the blades

Test Results

The results of all subtests appear on the Verification Tests dialog box after each individual test is completed. See table 34 for an explanation of test results.

Table 34 Test Results

Test Results	Explanation
PASSED	Completed the test without reported errors.
MARGINAL	Completed the test, but the system had to retry or had to skip part of the test. A MARGINAL result is considered PASSED, but the log should be checked to see if the marginality can be corrected.
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 marginal or failed results again.

Verification Test Graphical Reports

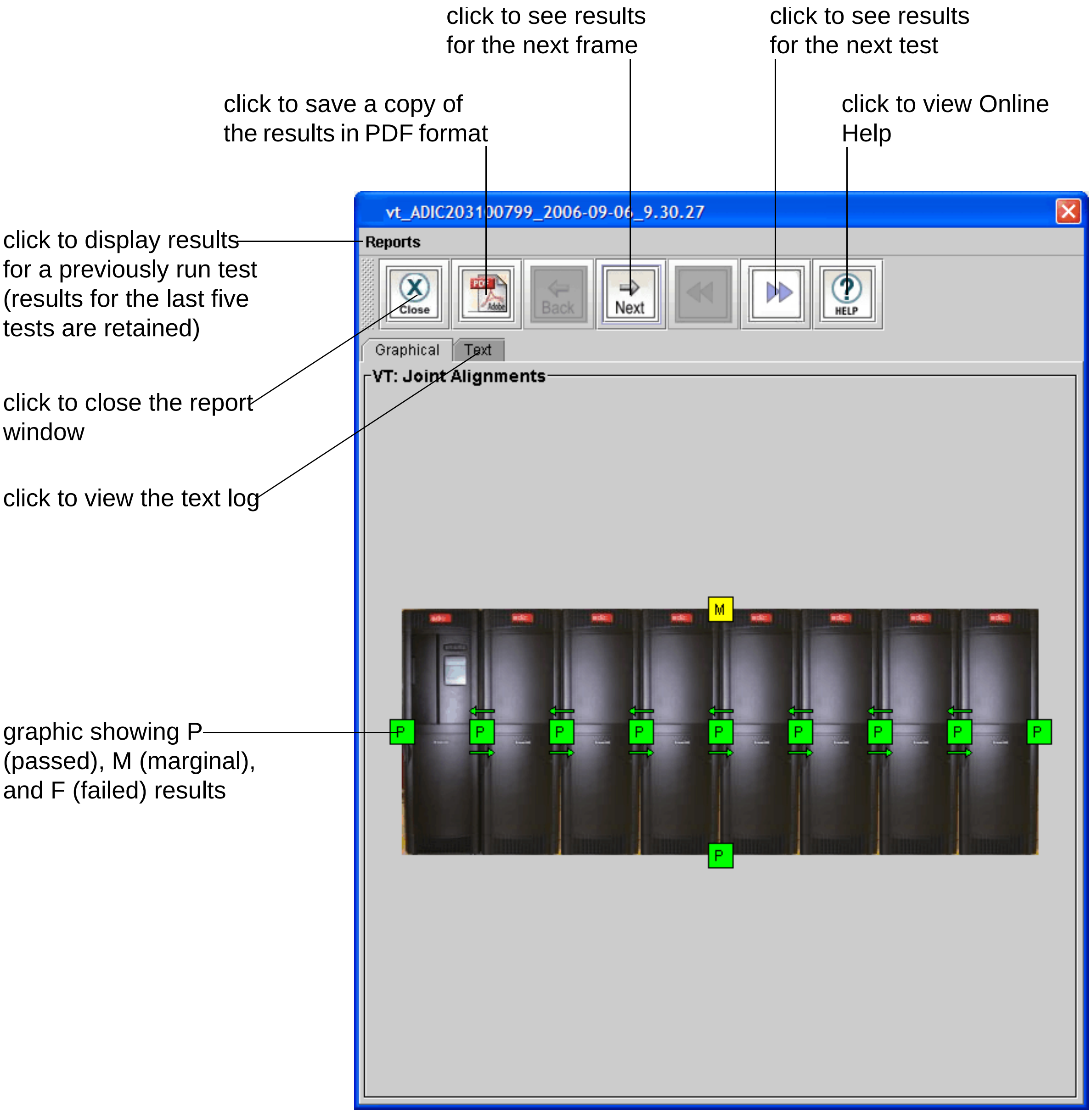
Some verification tests produce graphical reports that let you easily see if the test generated passed, marginal, or failed results. Each result is shown in a different color:

- P - passed (green)
- M - marginal (yellow)
- 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 marginal or failed result.

To view the graphical reports for a test, click **Reports** on the **Verification Tests** dialog box. Figure 39 on page 439 shows the parts of the report window.

Figure 39 Report Window



click to see results for the next frame

click to see results for the next test

click to save a copy of the results in PDF format

click to view Online Help

click to display results for a previously run test (results for the last five tests are retained)

click to close the report window

click to view the text log

graphic showing P (passed), M (marginal), and F (failed) results

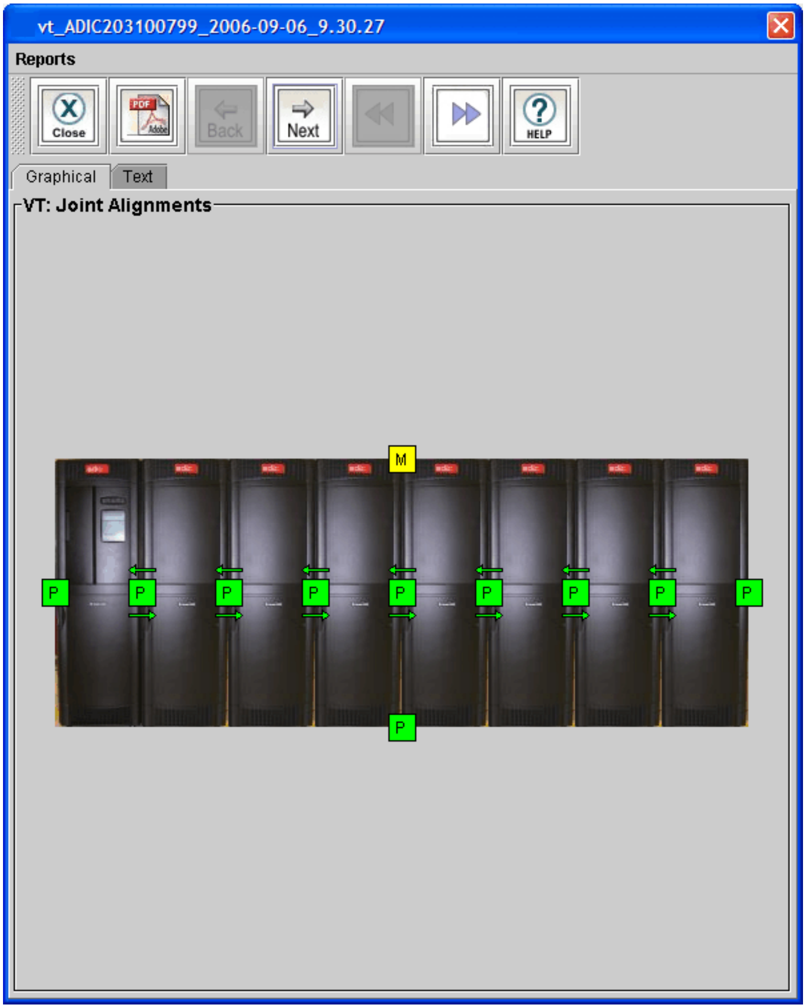
Joint Alignments

The joint alignment 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 40 on page 441.

Figure 40 Joint Alignments Graphical Report



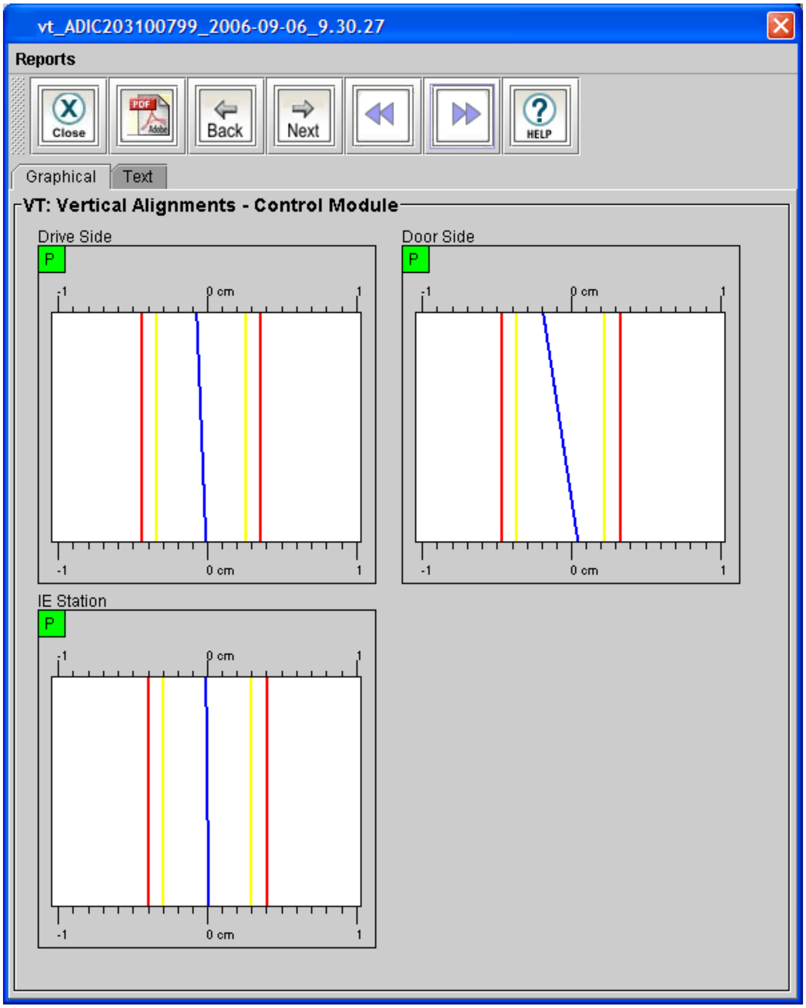
Vertical Alignments

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 41 on page 443.

Figure 41 Vertical Alignments Graphical Report



Horizontal Alignments

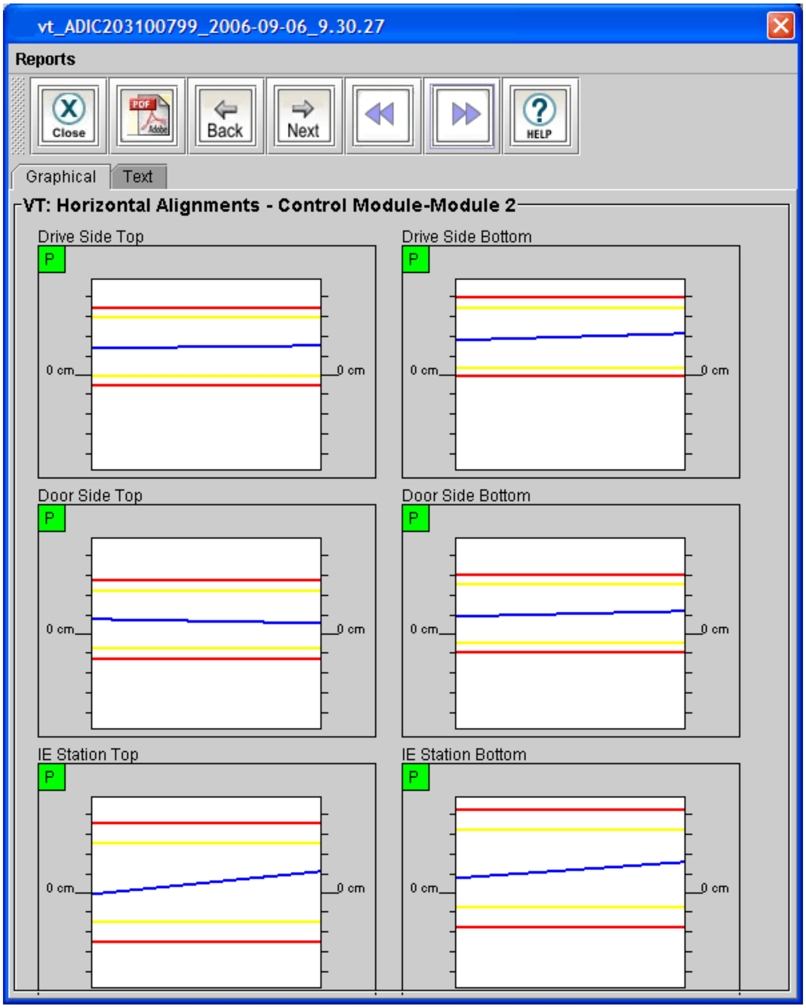
The horizontal alignments graphical report shows the results for tests of horizontal alignment of tape magazines on the drive-side and door-side across frames, and for horizontal alignment of I/E stations across frames.

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 42 on page 445.

Figure 42 Horizontal Alignments Graphical Report



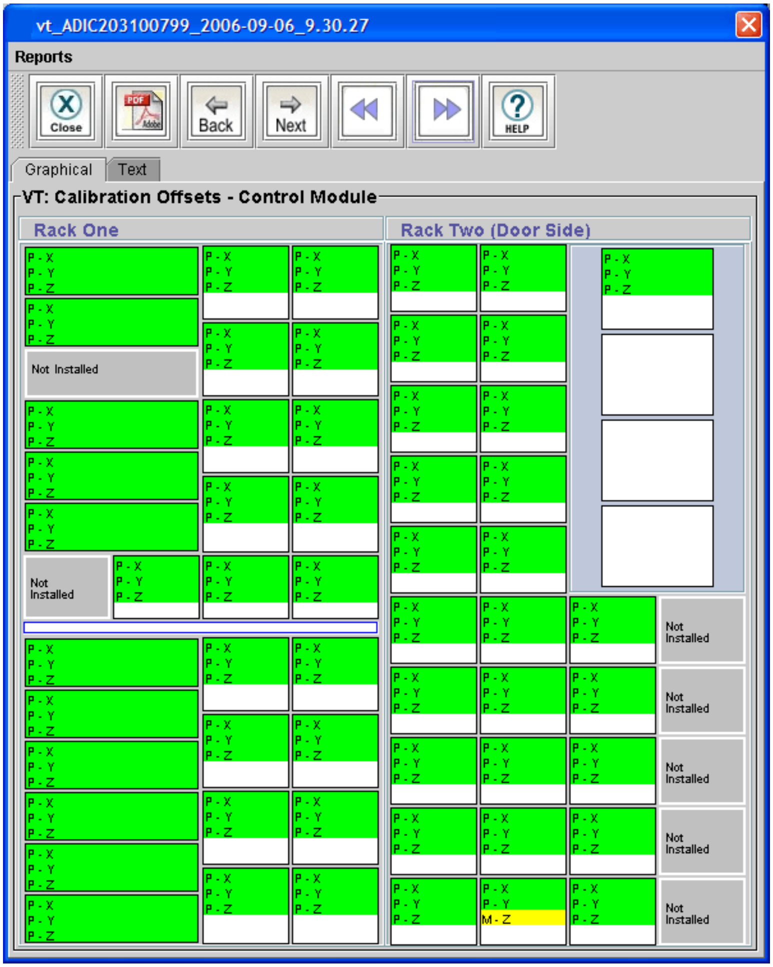
Calibration Offsets

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 43 on page 447.

Figure 43 Calibration Offsets Graphical Report



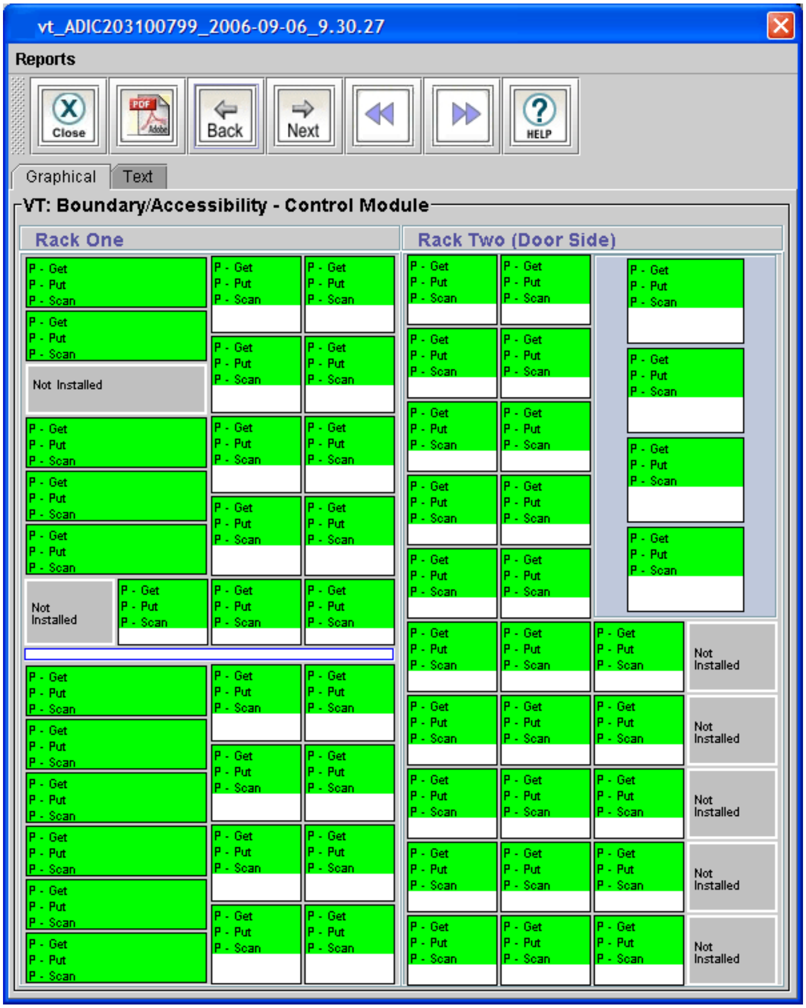
Boundary/Accessibility

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 44 on page 449.

Figure 44 Boundary/ Accessibility Graphical Report



vt_ADIC203100799_2006-09-06_9.30.27

Reports

Graphical | Text

VT: Boundary/Accessibility - Control Module

Rack One

P - Get P - Put P - Scan	P - Get P - Put P - Scan	P - Get P - Put P - Scan
P - Get P - Put P - Scan	P - Get P - Put P - Scan	P - Get P - Put P - Scan
Not Installed	P - Get P - Put P - Scan	P - Get P - Put P - Scan
P - Get P - Put P - Scan	P - Get P - Put P - Scan	P - Get P - Put P - Scan
P - Get P - Put P - Scan	P - Get P - Put P - Scan	P - Get P - Put P - Scan
P - Get P - Put P - Scan	P - Get P - Put P - Scan	P - Get P - Put P - Scan
Not Installed	P - Get P - Put P - Scan	P - Get P - Put P - Scan
P - Get P - Put P - Scan	P - Get P - Put P - Scan	P - Get P - Put P - Scan
P - Get P - Put P - Scan	P - Get P - Put P - Scan	P - Get P - Put P - Scan
P - Get P - Put P - Scan		
P - Get P - Put P - Scan		
P - Get P - Put P - Scan		
P - Get P - Put P - Scan		
P - Get P - Put P - Scan		
P - Get P - Put P - Scan		

Rack Two (Door Side)

P - Get P - Put P - Scan	P - Get P - Put P - Scan	P - Get P - Put P - Scan	
P - Get P - Put P - Scan	P - Get P - Put P - Scan	P - Get P - Put P - Scan	
P - Get P - Put P - Scan	P - Get P - Put P - Scan	P - Get P - Put P - Scan	
P - Get P - Put P - Scan	P - Get P - Put P - Scan	P - Get P - Put P - Scan	
P - Get P - Put P - Scan	P - Get P - Put P - Scan		
P - Get P - Put P - Scan	P - Get P - Put P - Scan	P - Get P - Put P - Scan	Not Installed
P - Get P - Put P - Scan	P - Get P - Put P - Scan	P - Get P - Put P - Scan	Not Installed
P - Get P - Put P - Scan	P - Get P - Put P - Scan	P - Get P - Put P - Scan	Not Installed
P - Get P - Put P - Scan	P - Get P - Put P - Scan	P - Get P - Put P - Scan	Not Installed
P - Get P - Put P - Scan	P - Get P - Put P - Scan	P - Get P - Put P - Scan	Not Installed

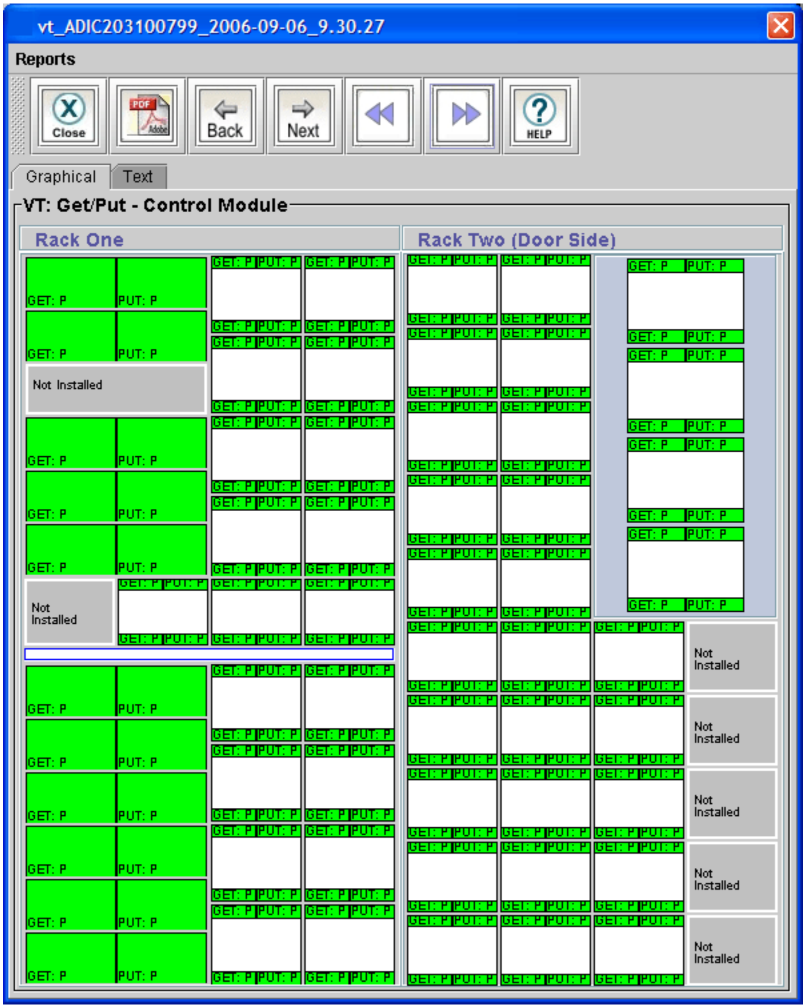
Get/Put

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 marginal 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 45 on page 451.

Figure 45 Get/Put Graphical Report



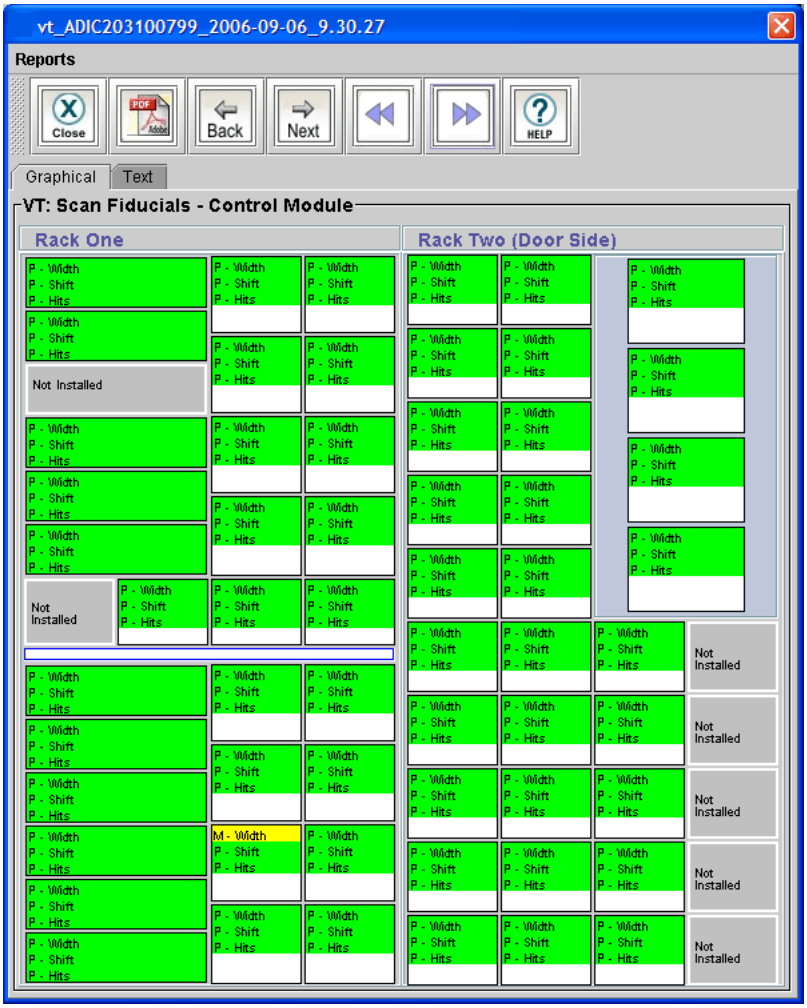
Scan Fiducials

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 marginal or 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 marginal or failed results, the scanner should be inspected and replaced if necessary.

See figure 46 on page 453.

Figure 46 Scan Fiducials Graphical Report


vt_ADIC203100799_2006-09-06_9.30.27
Reports
Close
PDF
Adobe
Back
Next
HELP
Graphical
Text
VT: Scan Fiducials - Control Module
Rack One
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
Not Installed
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
Not Installed
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
M - Width P - Shift P - Hits
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
Rack Two (Door Side)
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
P - Width P - Shift P - Hits
Not Installed
Not Installed
Not Installed
Not Installed
Not Installed

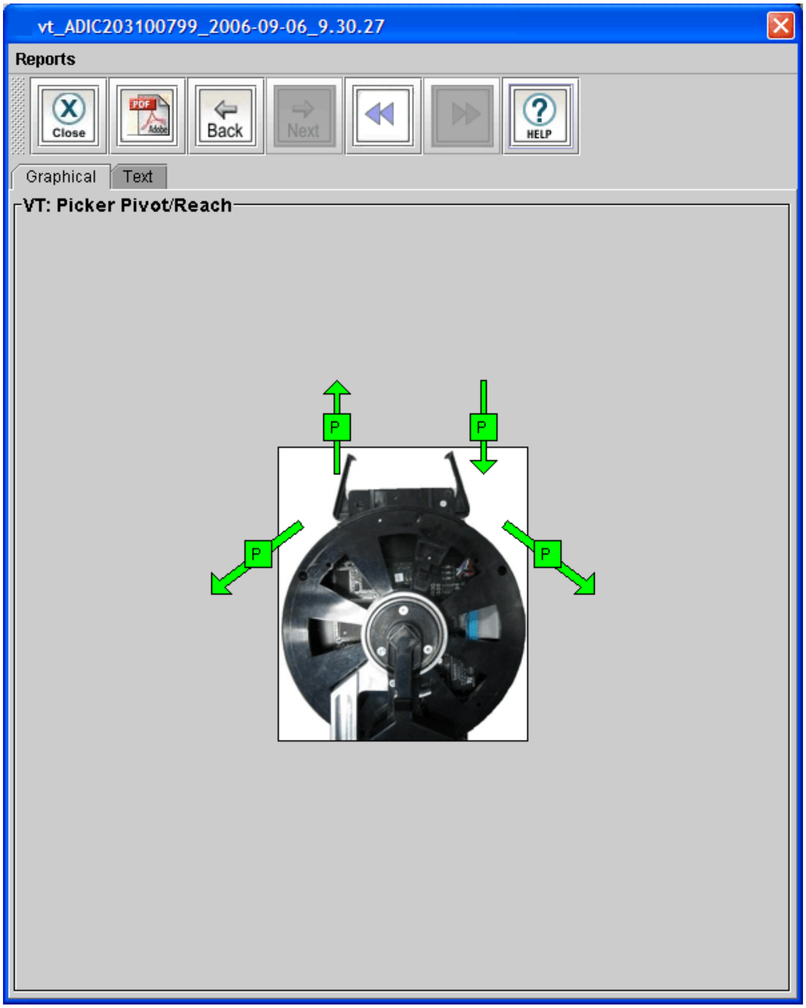
Picker Pivot/Reach

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 marginal or 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 47 on page 455.

Figure 47 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.

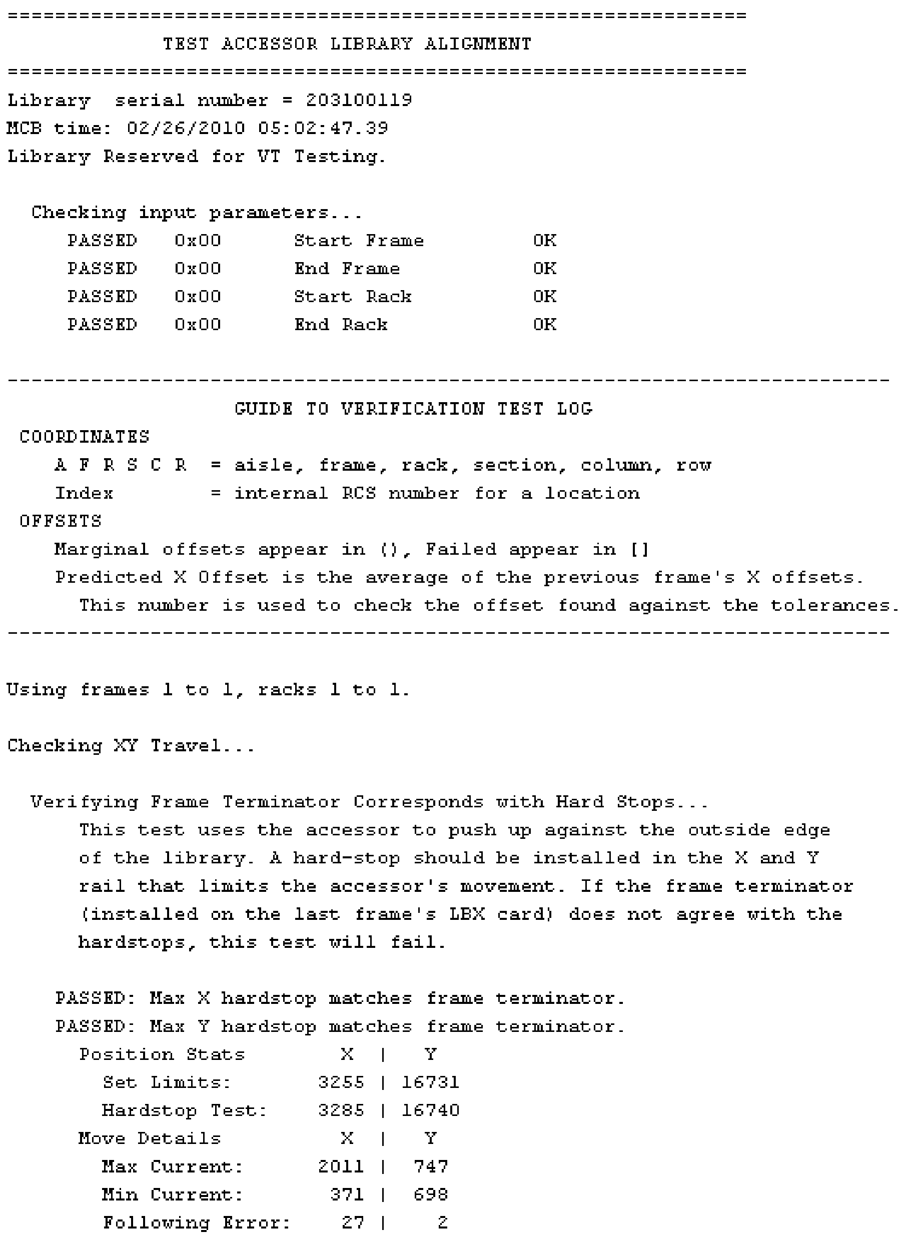
This log file is appended with data as each test finishes. You can repeat the test if any problems are found and fixed. If the **Verification Tests** dialog box was not closed during the retesting, all results are contained in one log file.

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 48 on page 457 shows an example of a test log. It provides the following information:

- The test output is from the library alignment test.
- 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. MARGINAL output is placed between parentheses, and 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 48 on page 457.

Figure 48 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
```

Running the Verification Tests

This section provides instructions for starting the installation verification test, partial tests, and FRU operational tests.

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.

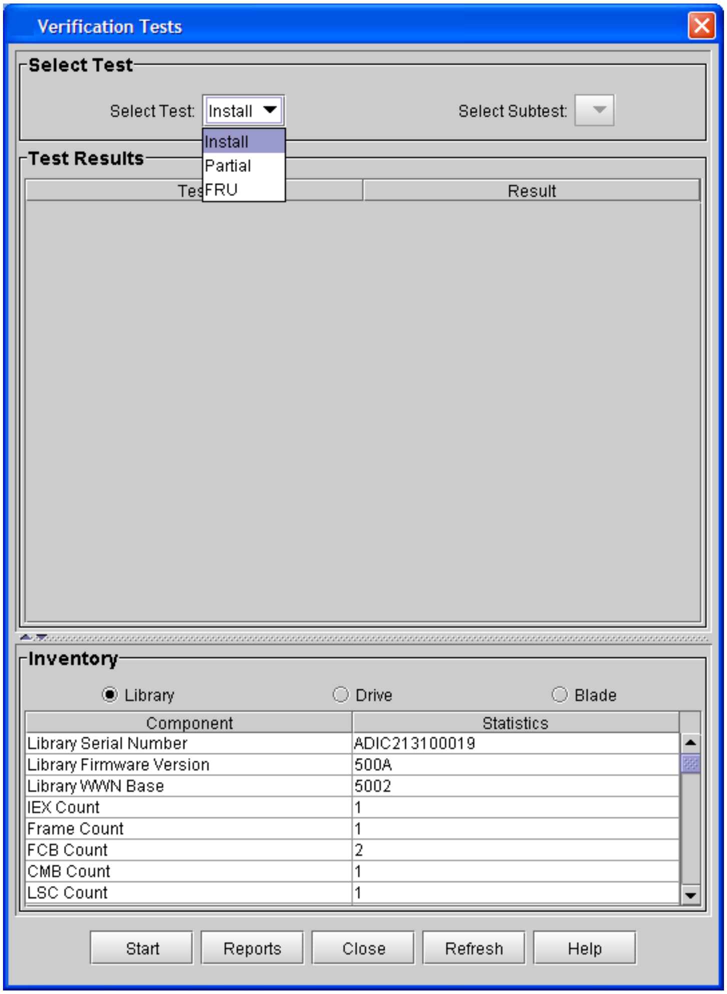
If a typical user logs on while an administrator is logged on and running a verification test, testing will continue unaffected. Only one administrator can be logged on at any given time.

Installation Verification Test

When the installation 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.



Select Test: Install

Select Subtest:

Inventory: ● Library ○ Drive ○ Blade

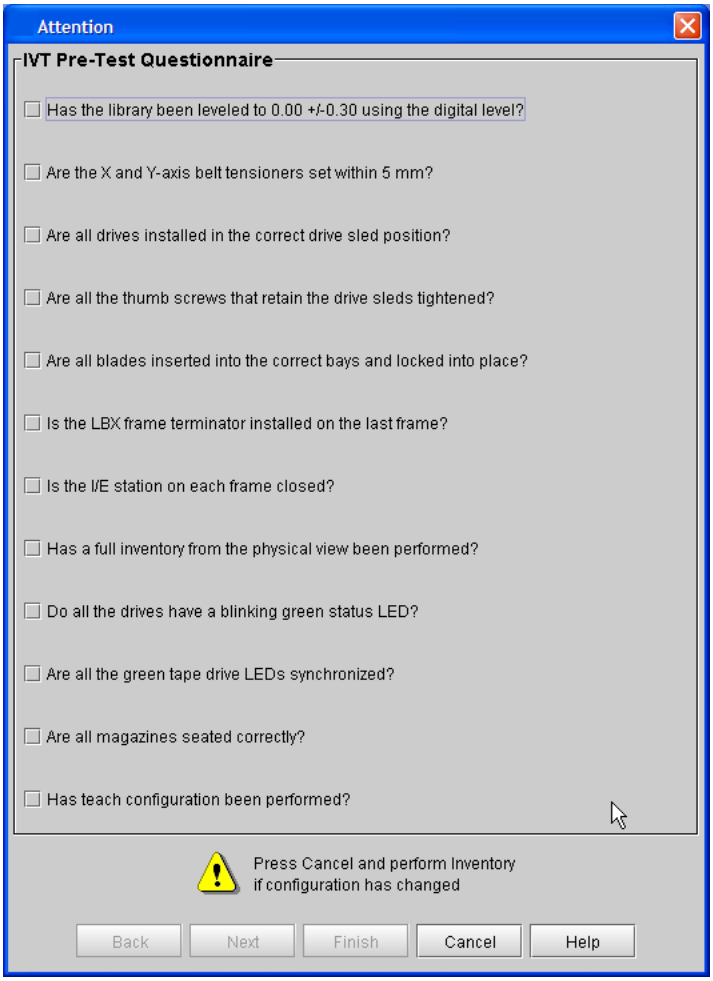
Component	Statistics
Library Serial Number	ADIC213100019
Library Firmware Version	500A
Library WWN Base	5002
IEX Count	1
Frame Count	1
FCB Count	2
CMB Count	1
LSC Count	1

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.



Attention

IVT Pre-Test Questionnaire

□ Has the library been leveled to 0.00 +/-0.30 using the digital level?

□ Are the X and Y-axis belt tensioners set within 5 mm?

□ Are all drives installed in the correct drive sled position?

□ Are all the thumb screws that retain the drive sleds tightened?

□ Are all blades inserted into the correct bays and locked into place?

□ Is the LBX frame terminator installed on the last frame?

□ Is the I/E station on each frame closed?

□ Has a full inventory from the physical view been performed?

□ Do all the drives have a blinking green status LED?

□ Are all the green tape drive LEDs synchronized?

□ Are all magazines seated correctly?

□ Has teach configuration been performed?

Press Cancel and perform Inventory
if configuration has changed

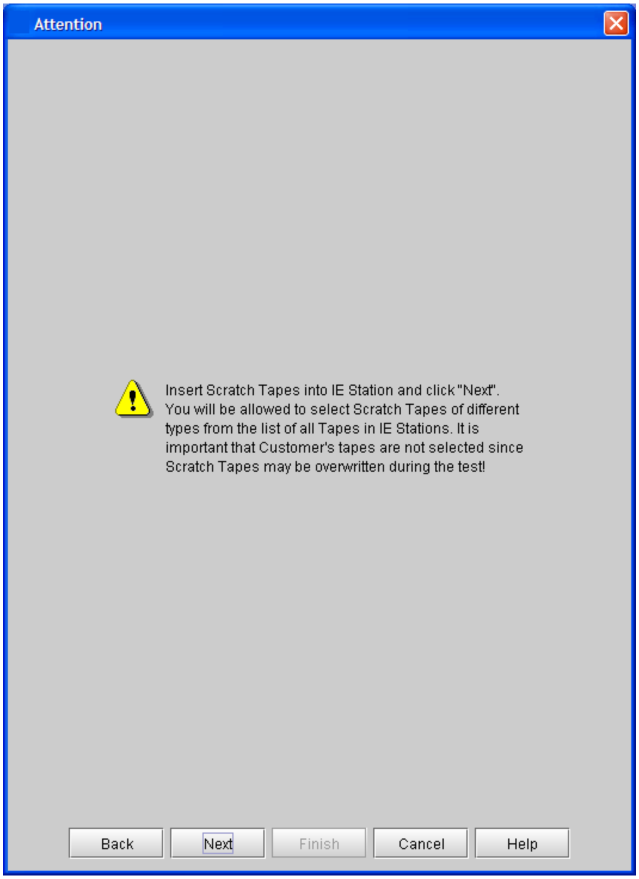
7 Complete the pre-test questionnaire by clicking inside the box next to the questions.

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.



Insert Scratch Tapes into IE Station and click "Next". You will be allowed to select Scratch Tapes of different types from the list of all Tapes in IE Stations. It is important that Customer's tapes are not selected since Scratch Tapes may be overwritten during the test!

9 Insert a “scratch” cartridge into the I/E station, and then click **Next**.

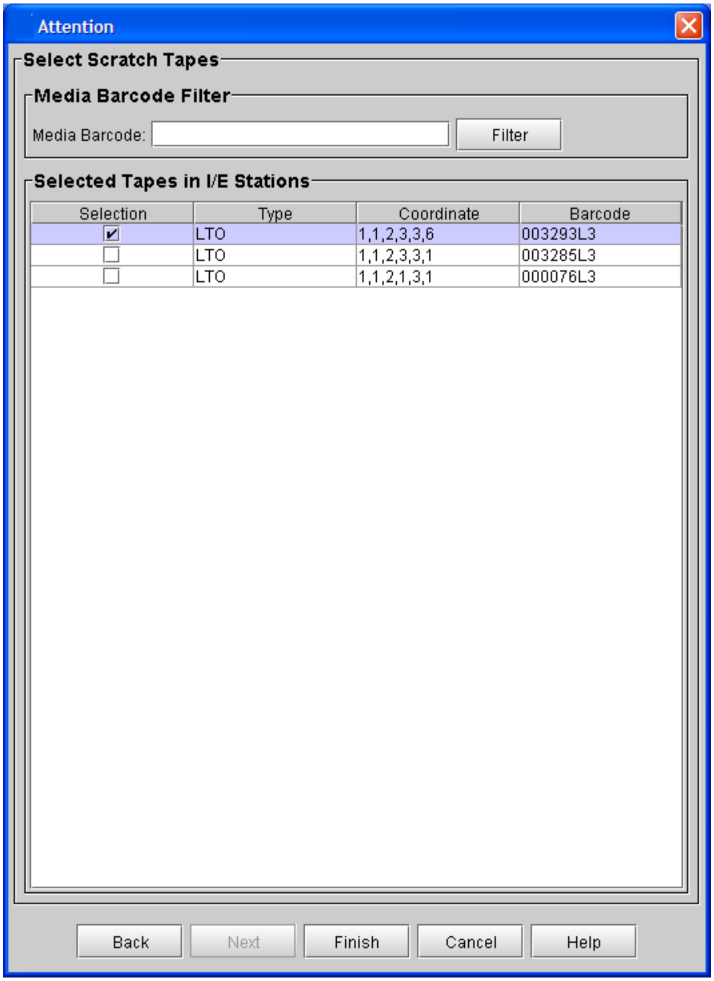
Note

- 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. You can load both LTO and DLT scratch cartridges if your library has mixed media.
- 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.

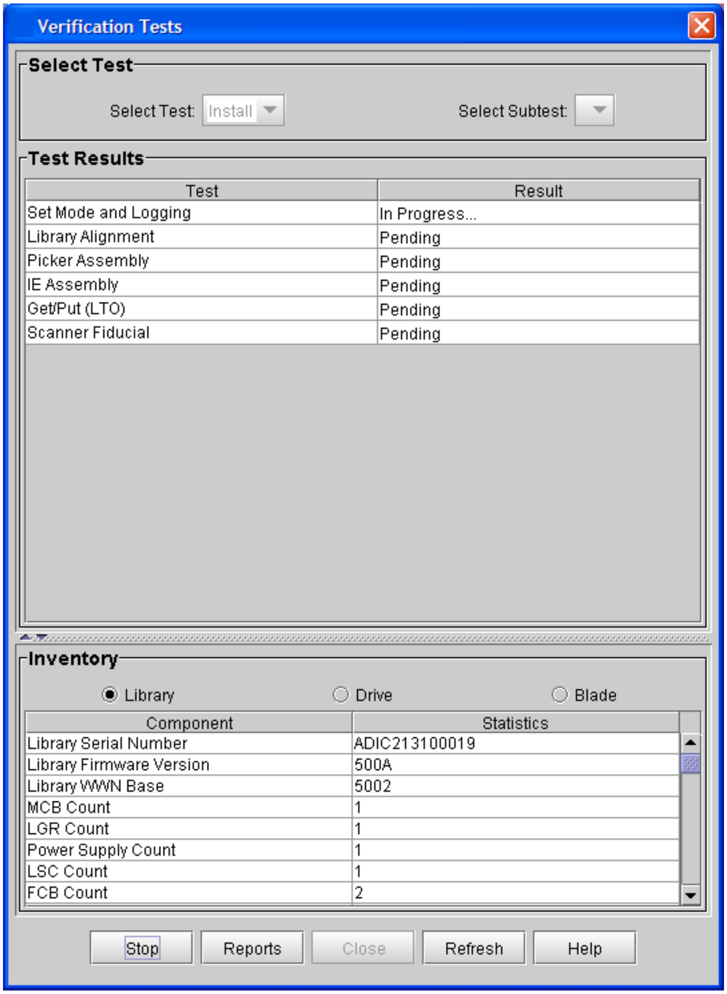
Note You can select one “scratch” cartridge per media type. Each test that requires a scratch cartridge will call the media types as needed.



Selection	Type	Coordinate	Barcode
☑	LTO	1,1,2,3,3,6	003293L3
□	LTO	1,1,2,3,3,1	003285L3
□	LTO	1,1,2,1,3,1	000076L3

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.



Verification Tests

Select Test

Select Test: Install

Select Subtest:

Test Results

Test	Result
Set Mode and Logging	In Progress...
Library Alignment	Pending
Picker Assembly	Pending
IE Assembly	Pending
Get/Put (LTO)	Pending
Scanner Fiducial	Pending

Inventory

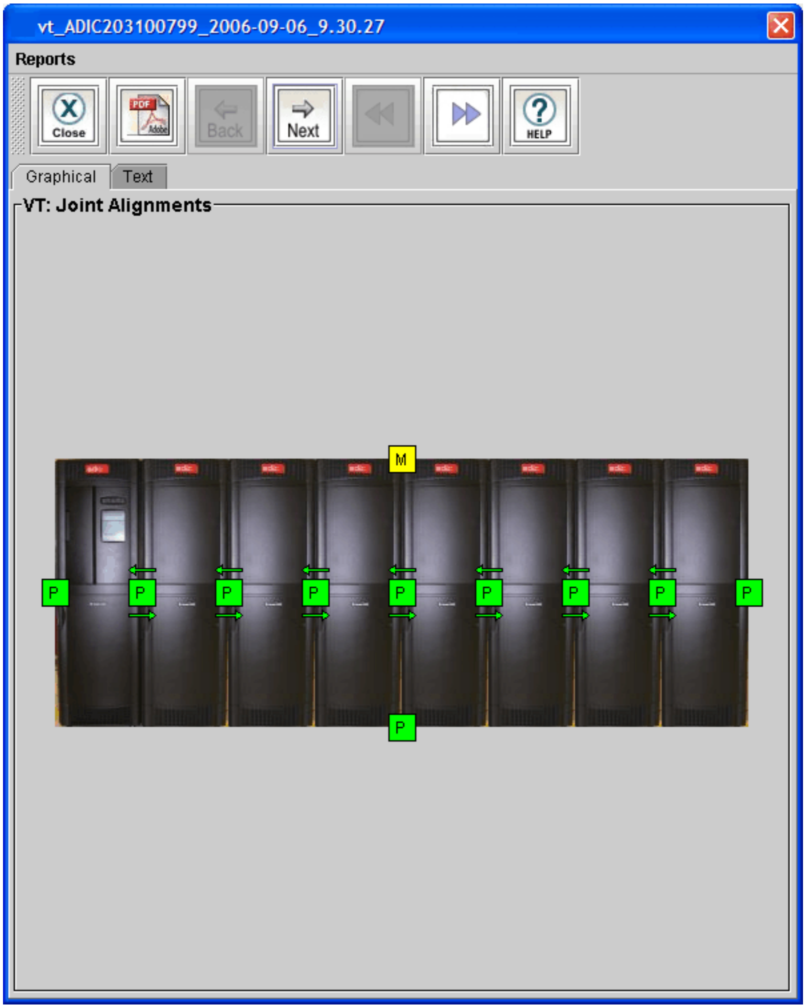
● Library ○ Drive ○ Blade

Component	Statistics
Library Serial Number	ADIC213100019
Library Firmware Version	500A
Library WWN Base	5002
MCB Count	1
LGR Count	1
Power Supply Count	1
LSC Count	1
FCB Count	2

12 After the test is complete, click **Reports** to view the test results.

The report window appears with the **Graphical** tab displayed.

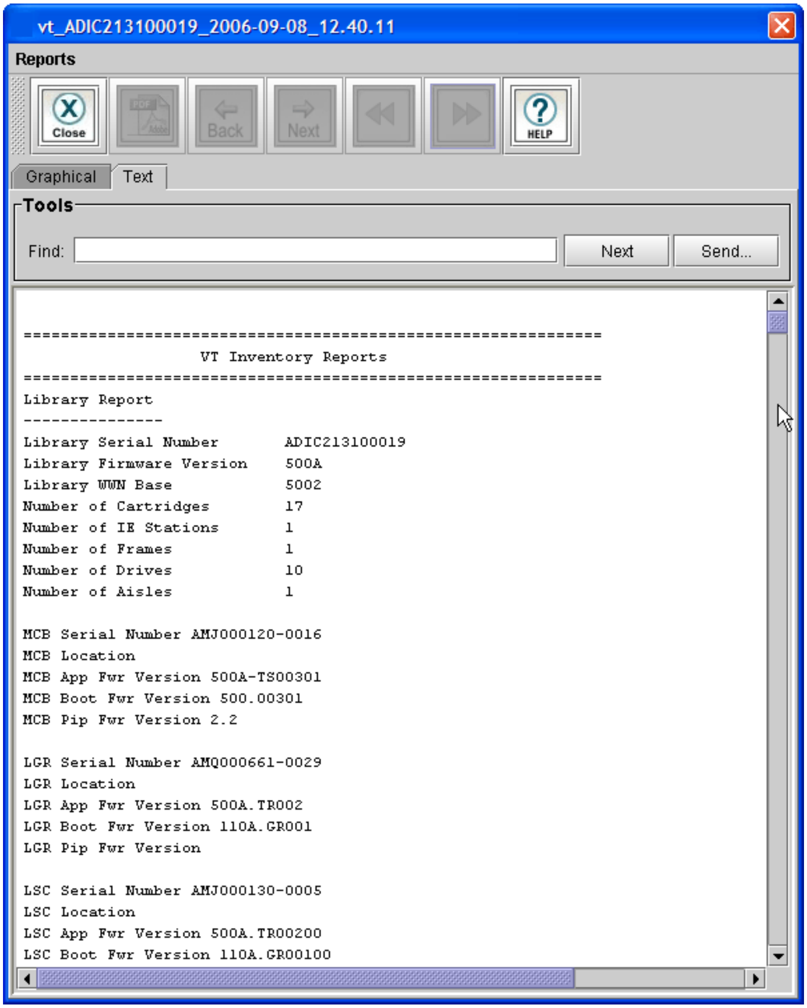
- Use the **Graphical** tab to view graphical reports and to quickly identify areas where marginal or failed results occurred.
- Use the toolbar to navigate between graphical reports or to save the results in PDF format. For more information about how to work with graphical reports, see Verification Test Graphical Reports on page 438.



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 marginal or failed test results, and to see troubleshooting information. For information about how to interpret test logs, see Verification Test Logs on page 456.

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, seeMailing, Saving, and Printing Status Information on page 354.



```
===============================================================
                   VT Inventory Reports
===============================================================
Library Report
---------------
Library Serial Number       ADIC213100019
Library Firmware Version    500A
Library WWN Base            5002
Number of Cartridges        17
Number of IE Stations       1
Number of Frames            1
Number of Drives            10
Number of Aisles            1

MCB Serial Number AMJ000120-0016
MCB Location
MCB App Fwr Version 500A-TS00301
MCB Boot Fwr Version 500.00301
MCB Pip Fwr Version 2.2

LGR Serial Number AMQ000661-0029
LGR Location
LGR App Fwr Version 500A.TR002
LGR Boot Fwr Version 110A.GR001
LGR Pip Fwr Version

LSC Serial Number AMJ000130-0005
LSC Location
LSC App Fwr Version 500A.TR00200
LSC Boot Fwr Version 110A.GR00100
```

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.

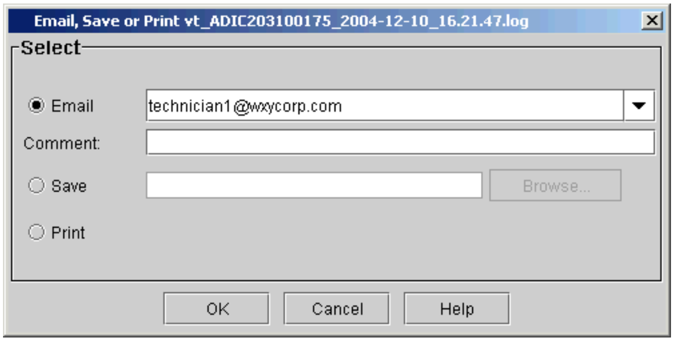
The information that is sent will be the same as what the **Text** tab appears at the time that you click **Send**.

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 164.

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.



Email, Save or Print vt_ADIC203100175_2004-12-10_16.21.47.log

Select

● Email technician1@wxycorp.com

Comment:

○ Save

○ Print

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**.

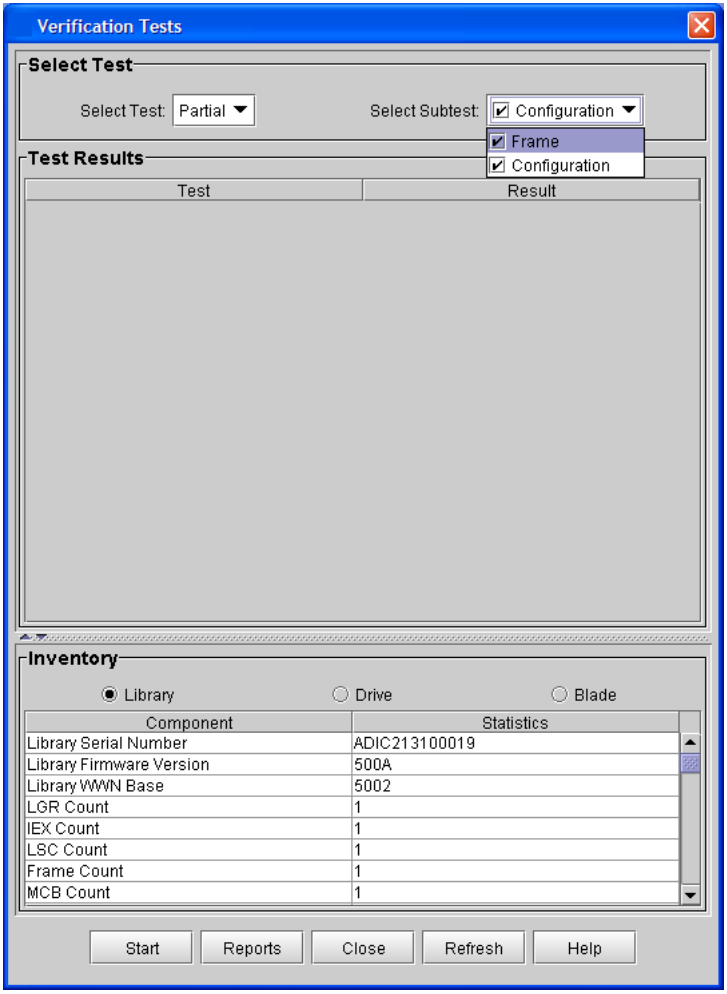
Note The **Print** option is available to remote client users only. It appears grayed out on the touch screen.

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.



Select Test: Partial

Select Subtest: ☑ Configuration

● Library ○ Drive ○ Blade

Component	Statistics
Library Serial Number	ADIC213100019
Library Firmware Version	500A
Library WWN Base	5002
LGR Count	1
IEX Count	1
LSC Count	1
Frame Count	1
MCB Count	1

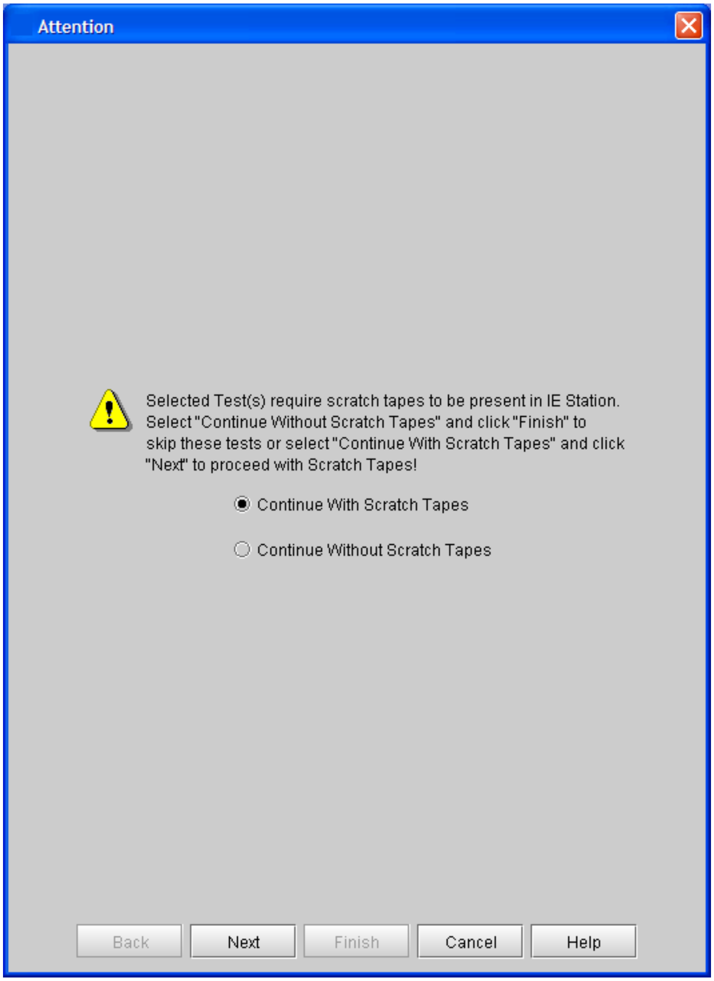
4. From the **Select Test** drop-down list, click **Partial**.

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.



Selected Test(s) require scratch tapes to be present in IE Station. Select "Continue Without Scratch Tapes" and click "Finish" to skip these tests or select "Continue With Scratch Tapes" and click "Next" to proceed with Scratch Tapes!

● Continue With Scratch Tapes

○ Continue Without Scratch Tapes

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**.

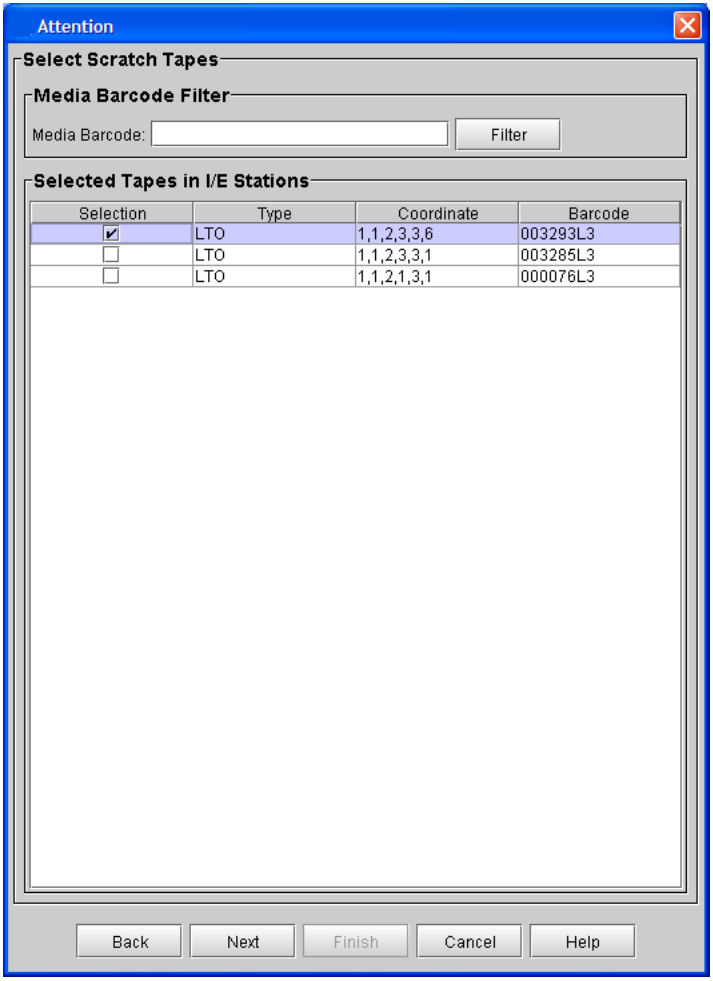
Note

- 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. You can load both LTO and DLT scratch cartridges if your library has mixed media.
- 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.

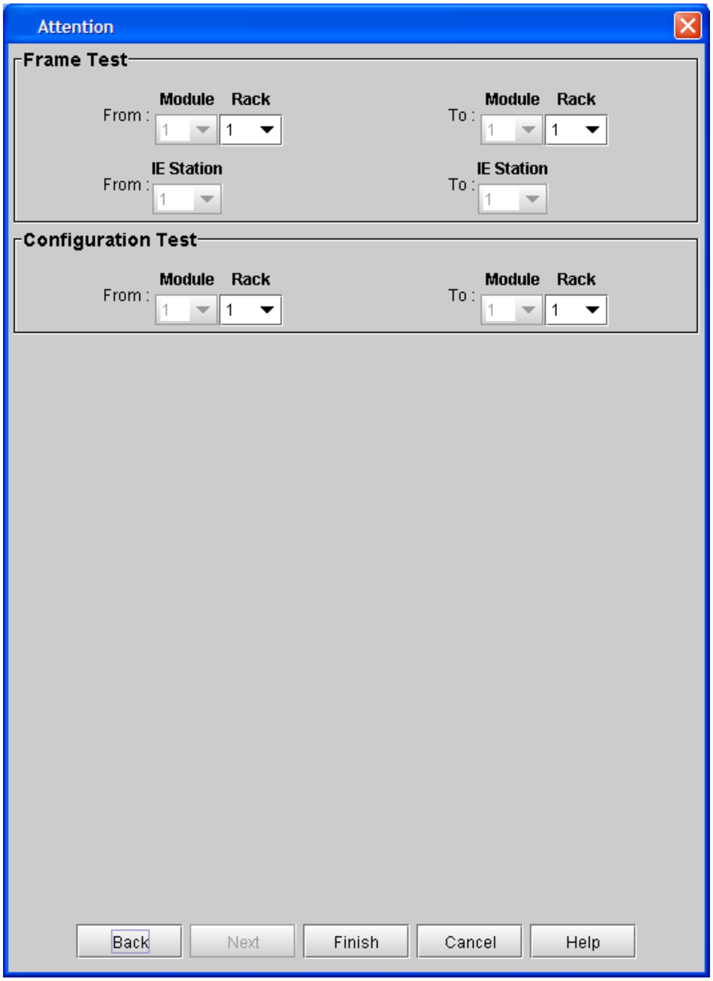
10 Select a “scratch” cartridge of each media type listed on the following dialog box, and then click **Next**.

Note You can select one “scratch” cartridge per media type. Each test that requires a scratch cartridge will call the media types as needed.



Selection	Type	Coordinate	Barcode
☑	LTO	1,1,2,3,3,6	003293L3
□	LTO	1,1,2,3,3,1	003285L3
□	LTO	1,1,2,1,3,1	000076L3

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.



Attention

Frame Test

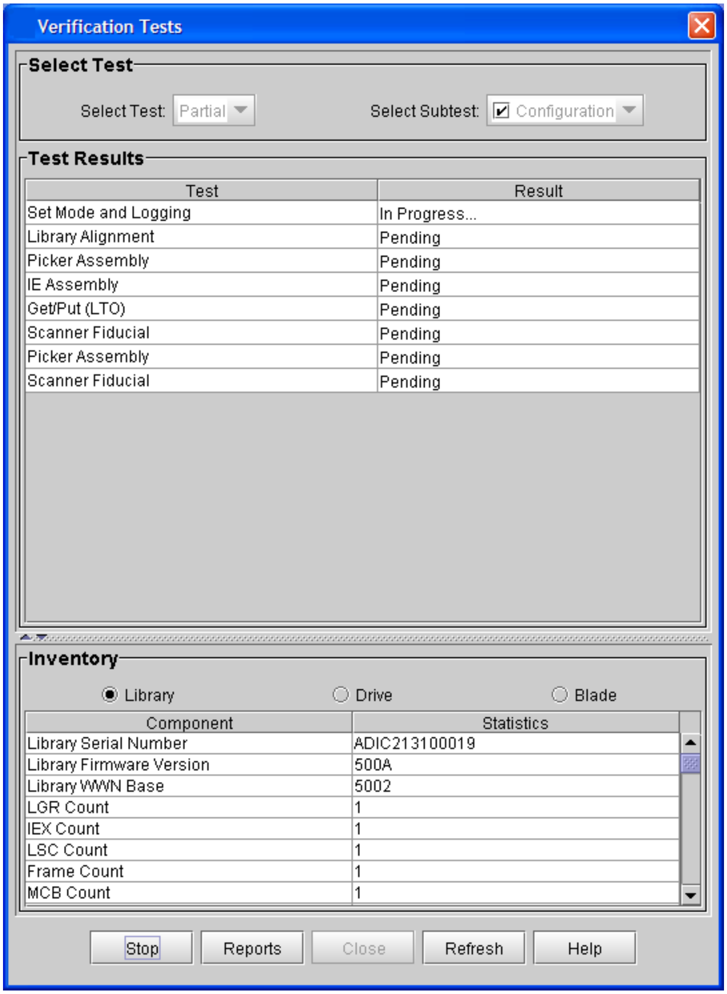
	Module	Rack		Module	Rack
From :	1	1	To :	1	1

	IE Station		IE Station
From :	1	To :	1

Configuration Test

	Module	Rack		Module	Rack
From :	1	1	To :	1	1

Test progress is shown in the **Verification Tests** dialog box.



Verification Tests

Select Test

Select Test: Partial

Select Subtest: ☑ Configuration

Test Results

Test	Result
Set Mode and Logging	In Progress...
Library Alignment	Pending
Picker Assembly	Pending
IE Assembly	Pending
Get/Put (LTO)	Pending
Scanner Fiducial	Pending
Picker Assembly	Pending
Scanner Fiducial	Pending

Inventory

● Library ○ Drive ○ Blade

Component	Statistics
Library Serial Number	ADIC213100019
Library Firmware Version	500A
Library WWN Base	5002
LGR Count	1
IEX Count	1
LSC Count	1
Frame Count	1
MCB Count	1

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 438.

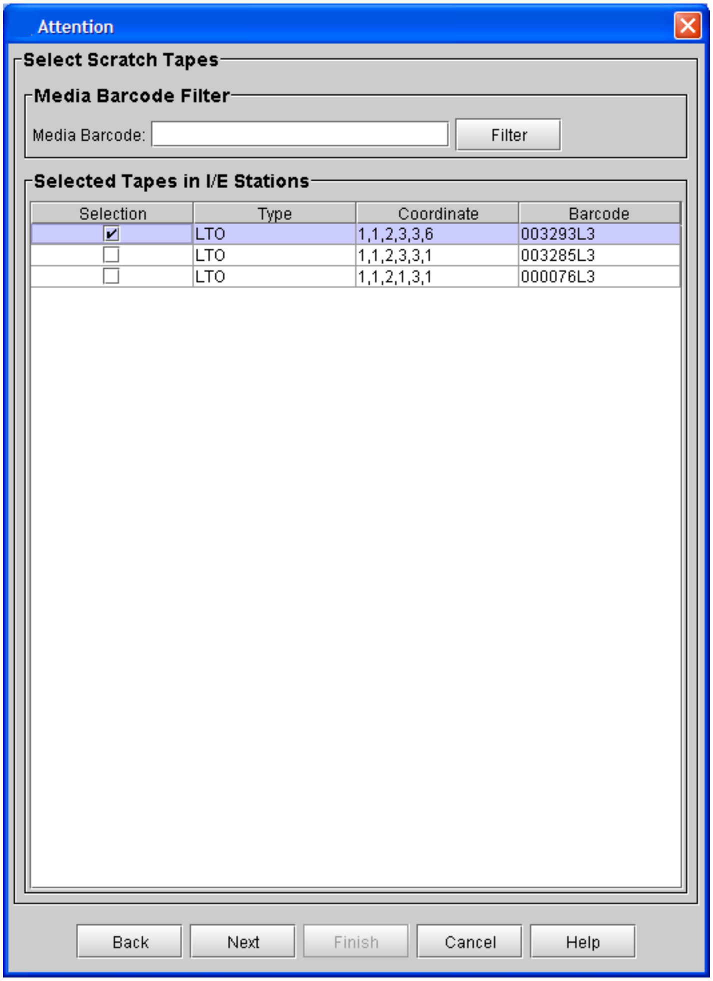
For information about how to interpret test logs, see Verification Test Logs on page 456.

For information how to e-mail, print, or save text logs, see Mailing, Saving, and Printing Test Logs on page 467.

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.



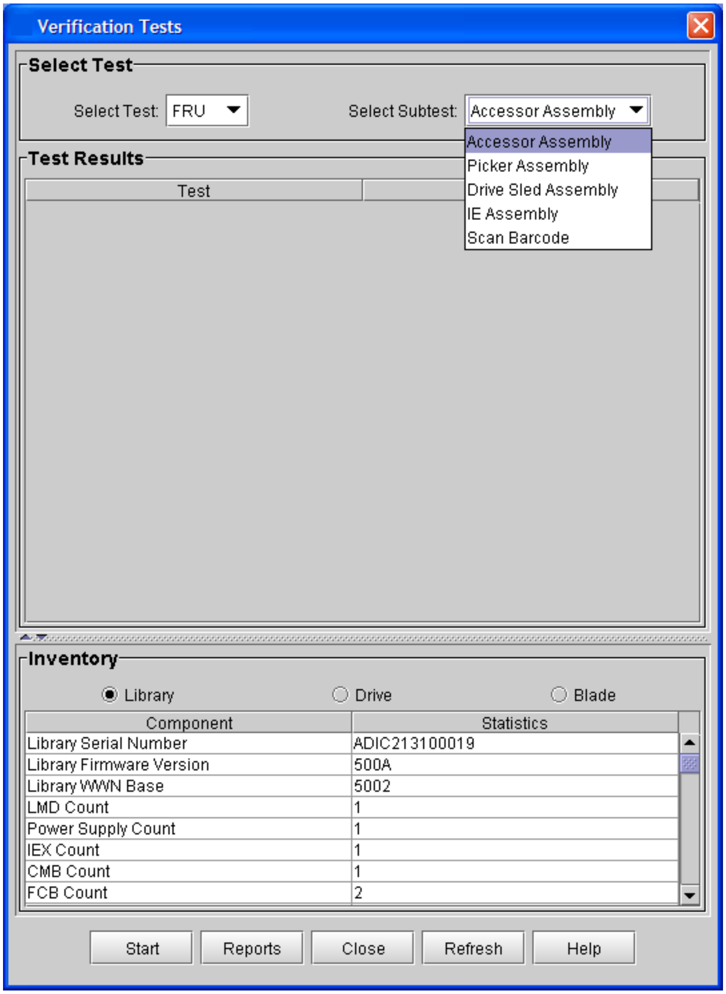
Selection	Type	Coordinate	Barcode
☑	LTO	1,1,2,3,3,6	003293L3
□	LTO	1,1,2,3,3,1	003285L3
□	LTO	1,1,2,1,3,1	000076L3

To run FRU operational tests from the **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.



Verification Tests

Select Test

Select Test: FRU

Select Subtest: Accessor Assembly

Inventory

● Library ○ Drive ○ Blade

Component	Statistics
Library Serial Number	ADIC213100019
Library Firmware Version	500A
Library WWN Base	5002
LMD Count	1
Power Supply Count	1
IEX Count	1
CMB Count	1
FCB Count	2

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.

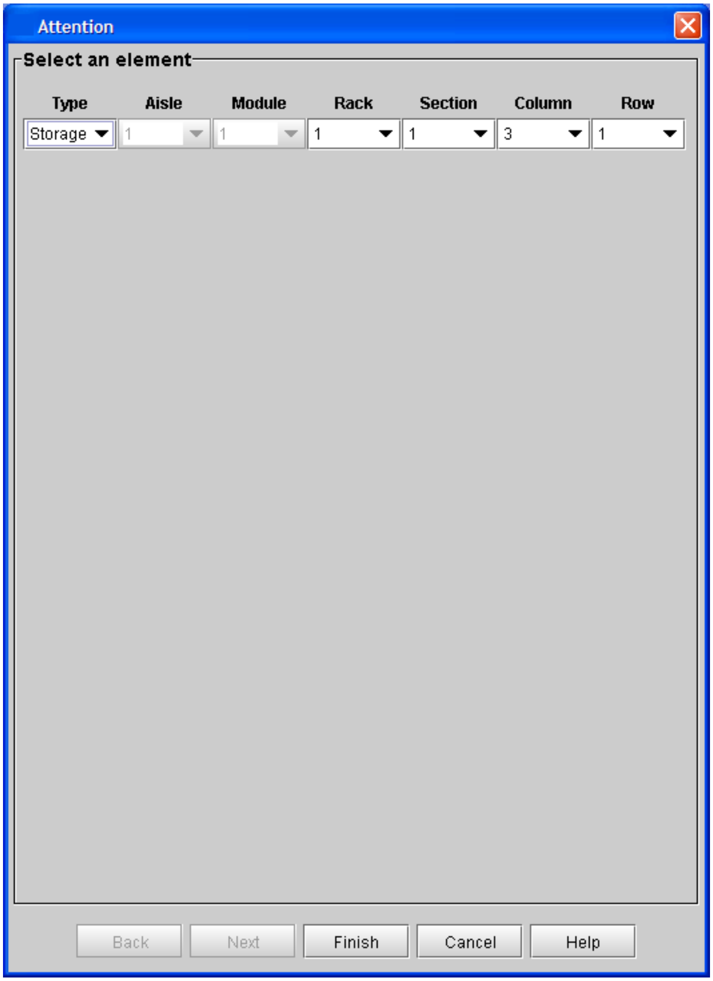
4 From the **Select Test** drop-down list, click **FRU**.

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.



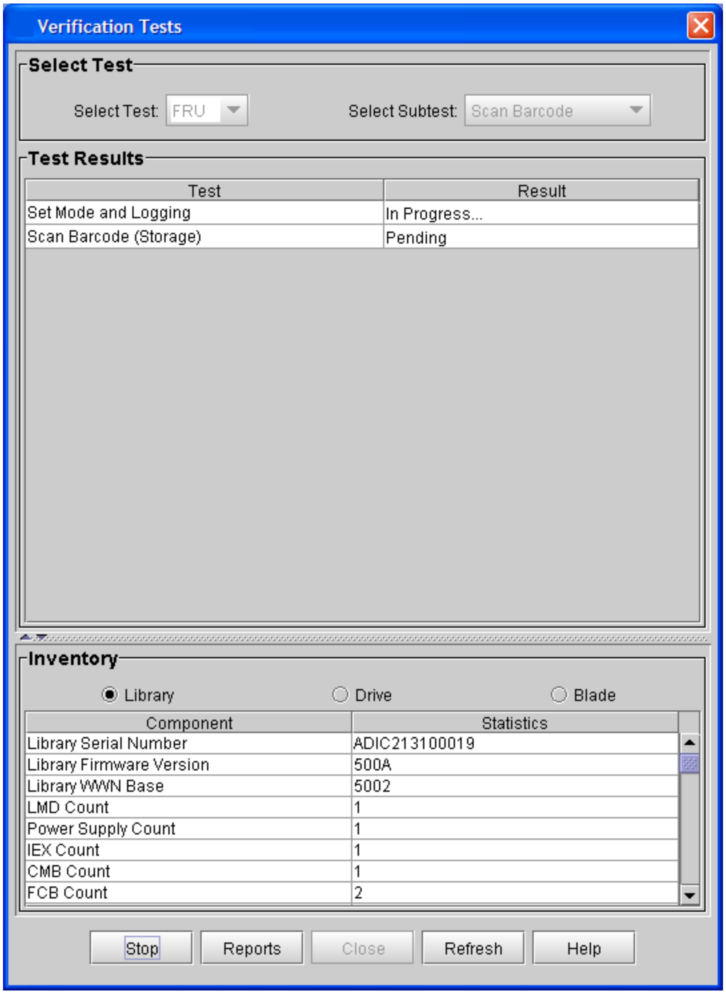
Select an element

Type	Aisle	Module	Rack	Section	Column	Row
Storage	1	1	1	1	3	1

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.



Test	Result
Set Mode and Logging	In Progress...
Scan Barcode (Storage)	Pending

Component	Statistics
Library Serial Number	ADIC213100019
Library Firmware Version	500A
Library WWN Base	5002
LMD Count	1
Power Supply Count	1
IEX Count	1
CMB Count	1
FCB Count	2

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 438.

For information about how to interpret test logs, see Verification Test Logs on page 456.

For information how to e-mail, print, or save text logs, see Mailing, Saving, and Printing Test Logs on page 467.

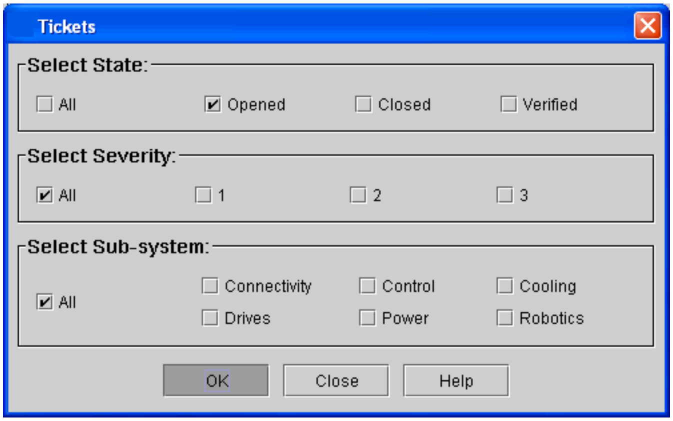
To run FRU operational tests from the **Ticket Details** dialog box:

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**.

4 From the **Tickets** dialog box, click the categories of the tickets you want to view.



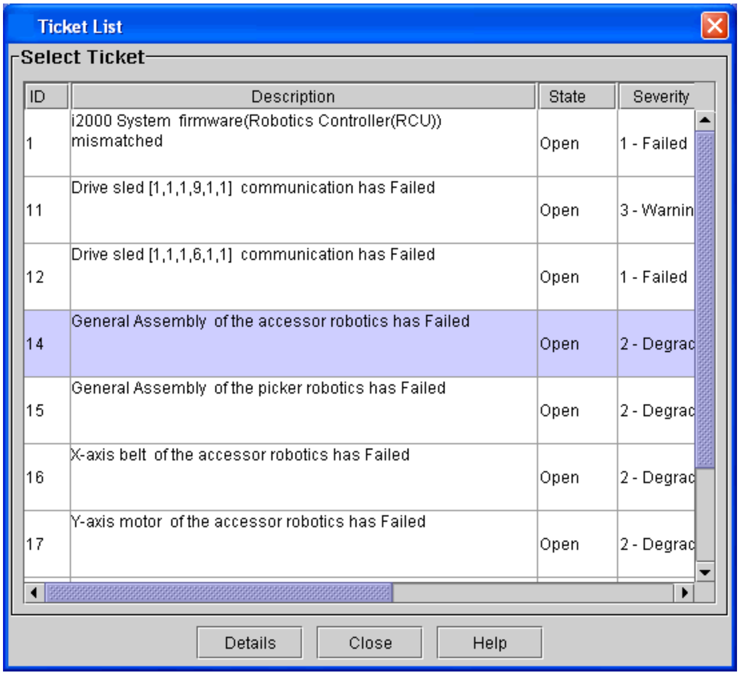
Tickets

Select State:
☐ All ☑ Opened ☐ Closed ☐ Verified

Select Severity:
☑ All ☐ 1 ☐ 2 ☐ 3

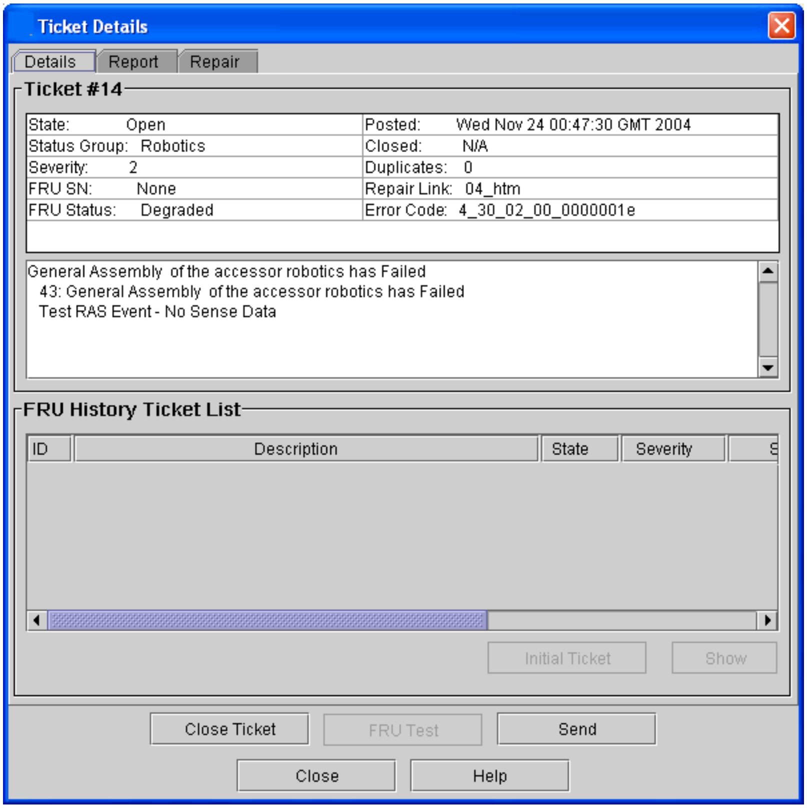
Select Sub-system:
☑ All ☐ Connectivity ☐ Control ☐ Cooling ☐ Drives ☐ Power ☐ Robotics

5 Click a ticket to highlight it, and then click **Details**.



ID	Description	State	Severity
1	i2000 System firmware(Robotics Controller(RCU)) mismatched	Open	1 - Failed
11	Drive sled [1,1,1,9,1,1] communication has Failed	Open	3 - Warnin
12	Drive sled [1,1,1,6,1,1] communication has Failed	Open	1 - Failed
14	General Assembly of the accessor robotics has Failed	Open	2 - Degrac
15	General Assembly of the picker robotics has Failed	Open	2 - Degrac
16	X-axis belt of the accessor robotics has Failed	Open	2 - Degrac
17	Y-axis motor of the accessor robotics has Failed	Open	2 - Degrac

6 From the **Ticket Details** dialog box, click **FRU Test**.



State: Open	Posted: Wed Nov 24 00:47:30 GMT 2004
Status Group: Robotics	Closed: N/A
Severity: 2	Duplicates: 0
FRU SN: None	Repair Link: 04_htm
FRU Status: Degraded	Error Code: 4_30_02_00_0000001e

General Assembly of the accessor robotics has Failed
43: General Assembly of the accessor robotics has Failed
Test RAS Event - No Sense Data

7 After the FRU test successfully verifies that the FRU has PASSED or is MARGINAL, all tickets associated with the failure are transitioned to the Verify state.

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.**

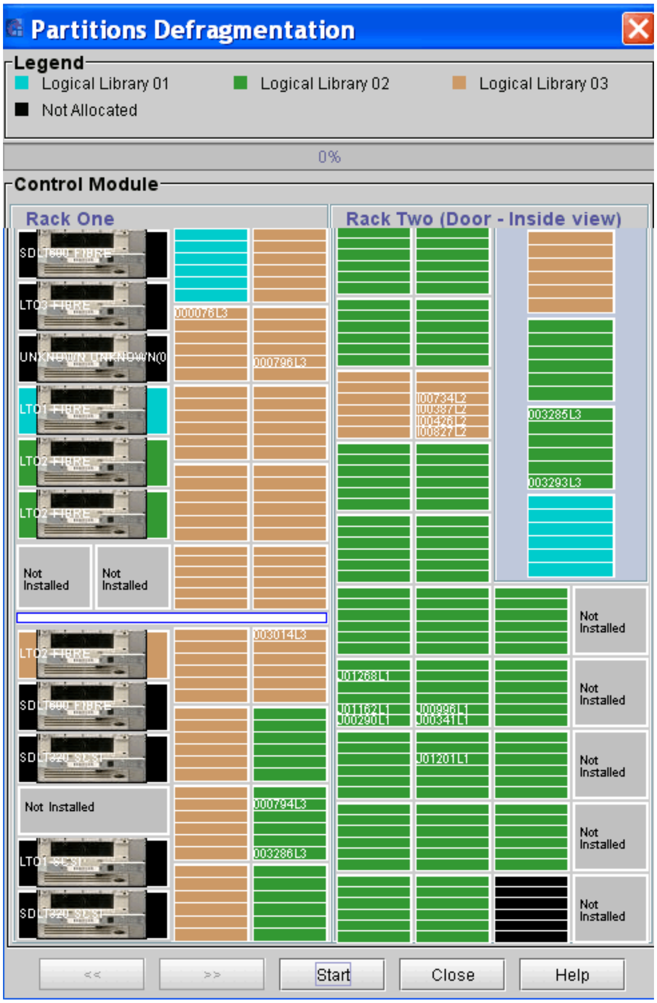
Defragmenting Partitions

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 to indicate which partition they belong to.

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, seeImporting Cartridges Into Partitions on page 511.

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 316, Powering On the Library on page 318, and Powering On the Library on page 318.

⚠ 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.

Running MeDIA Test Reports

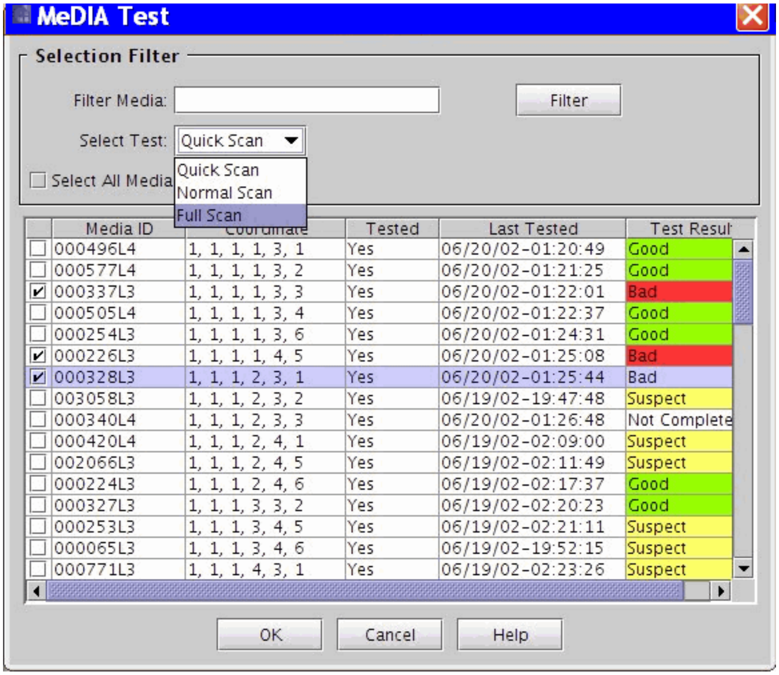
You may need evaluate your media as part of long term data retention, or you may want to evaluate media prior to rotating it back into usage. To perform this task, you can run a MeDIA test to assess tape media and the usability of data stored on it.

MeDIA Tests can be run only on a library managed partition. Use the Media Test dialog box to scan media on the library managed partition of your library.

1 Log on as an administrator.

2 From the main menu, select **Tools > MeDIA > Test Selection**.

The **Media Test** dialog box appears.



MeDIA Test

Selection Filter

Filter Media:

Select Test: Quick Scan

☐ Select All Media

☐	Media ID	Coordinate	Tested	Last Tested	Test Resul
☐	000496L4	1, 1, 1, 1, 3, 1	Yes	06/20/02-01:20:49	Good
☐	000577L4	1, 1, 1, 1, 3, 2	Yes	06/20/02-01:21:25	Good
☑	000337L3	1, 1, 1, 1, 3, 3	Yes	06/20/02-01:22:01	Bad
☐	000505L4	1, 1, 1, 1, 3, 4	Yes	06/20/02-01:22:37	Good
☐	000254L3	1, 1, 1, 1, 3, 6	Yes	06/20/02-01:24:31	Good
☑	000226L3	1, 1, 1, 1, 4, 5	Yes	06/20/02-01:25:08	Bad
☑	000328L3	1, 1, 1, 2, 3, 1	Yes	06/20/02-01:25:44	Bad
☐	003058L3	1, 1, 1, 2, 3, 2	Yes	06/19/02-19:47:48	Suspect
☐	000340L4	1, 1, 1, 2, 3, 3	Yes	06/20/02-01:26:48	Not Complete
☐	000420L4	1, 1, 1, 2, 4, 1	Yes	06/19/02-02:09:00	Suspect
☐	002066L3	1, 1, 1, 2, 4, 5	Yes	06/19/02-02:11:49	Suspect
☐	000224L3	1, 1, 1, 2, 4, 6	Yes	06/19/02-02:17:37	Good
☐	000327L3	1, 1, 1, 3, 3, 2	Yes	06/19/02-02:20:23	Good
☐	000253L3	1, 1, 1, 3, 4, 5	Yes	06/19/02-02:21:11	Suspect
☐	000065L3	1, 1, 1, 3, 4, 6	Yes	06/19/02-19:52:15	Suspect
☐	000771L3	1, 1, 1, 4, 3, 1	Yes	06/19/02-02:23:26	Suspect

3 To filter media to be displayed, in the **Filter Media** field, type the desired Media ID and click **Filter**. If you choose not to filter media, skip this step.

4 From the **Select Test** drop down menu, select the test you want to run.

- **Quick Scan** - does not require reading a tape, retrieves data from the cartridge memory (CM)
- **Normal Scan** - assesses a nominal portion of data written to tape
- **Full Scan** - assesses all data written to tape

5 If a **Normal Scan** or **Full Scan** is selected the Continue On Error can be selected. This option will continue to do a read scan of the tape if the cartridge memory (CM) test fails.

6 To select all media listed click the **Select All Media** check box, or click the box to the left of each individual Media ID.

The media selection table contains the following fields:

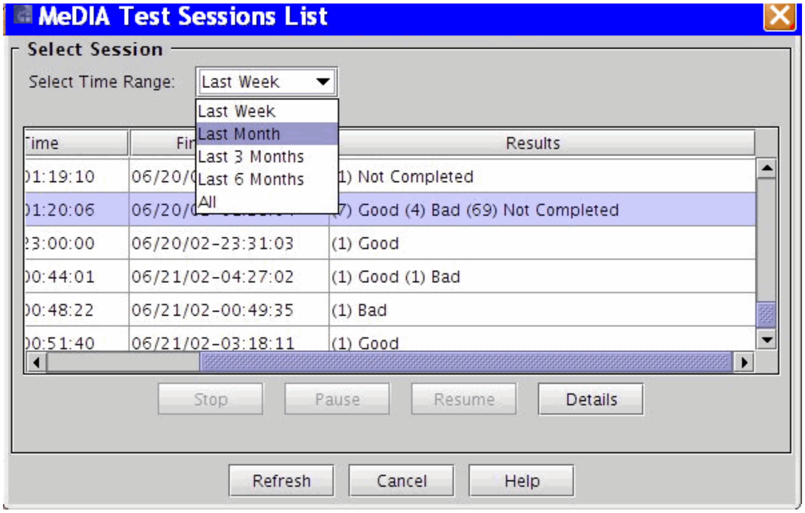
- **Media ID** – the media barcode.
- **Coordinate** – where the media is located within the library.
- **Tested** – indicates whether the media has already been tested (Yes/No). It will also indicate if the media is currently part of a test session that has not yet completed (Pending) and the cell will be highlighted in yellow.
- **Last Tested** – the date the media was last tested.
- **Test Result** – the last test result for the media, values are “Good”, “Bad”, “Suspect” or “N/A”.
- **Supported** – indicates whether the media can be tested by the drives currently configured in the LMP. For example, an LTO1 tape cannot be read by an LTO4 drive.

7 Click **OK**.

The message **MeDIA tests have started successfully...** is displayed.

8 To retrieve results, go to **Tools > MeDIA > Test Reports**.

The **MeDIA Test Sessions List** dialog box appears.



MeDIA Test Sessions List

Select Session

Select Time Range: Last Week

ime	Fir	Results
)1:19:10	06/20/(	1) Not Completed
)1:20:06	06/20/(	7) Good (4) Bad (69) Not Completed
:3:00:00	06/20/02-23:31:03	(1) Good
)0:44:01	06/21/02-04:27:02	(1) Good (1) Bad
)0:48:22	06/21/02-00:49:35	(1) Bad
)0:51:40	06/21/02-03:18:11	(1) Good

The MeDIA Test Session List displays the set of media tests that have run based on the time range selected. Each entry in the table presents an overview of a single MeDIA Test session that was requested from the MeDIA Test dialog (**Tools > MeDIA > Test Selection**).

The **Select Session** section displays.

1. A filter, **Select Time Range**, that displays the Test Sessions that were run during a certain time period. The following options are supported:
   - **Last Week** – the test sessions that were run in the last week.
   - **Last Month** – sessions run in the last month.
   - **Last 3 Months** – sessions run in the last 3 months.
   - **Last 6 Months** – sessions run in the last 6 months.
   - **All** – report all test sessions that were run on the library.
2. A table listing the test sessions that were run based on the **Select Time Range** selected. The table reports the following information:
   - **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", will be reported.
- **Results** - reports a summary of results for the media that were in the test session, you can select one of the test sessions listed and then click the Details button to view the details for each media tested. The reported values include the status and the number of media associated with that status.

  Good - success

  Bad - failure

  Suspect - failed to read data – media error or non-fatal drive error

  Incompleted - test did not complete.

9 In the **Select Time Range** field, select the range of time for test session runs that you want displayed.

10 To work with a session, highlight the appropriate row.

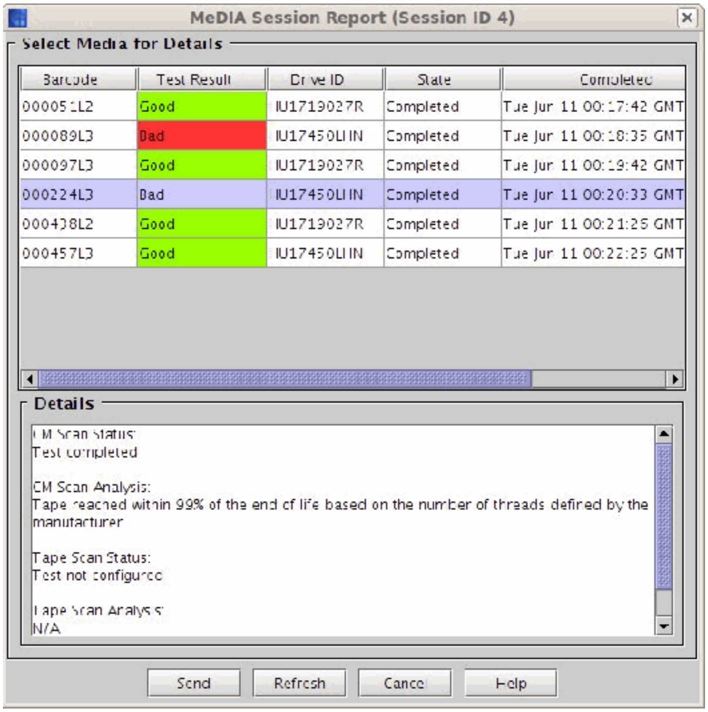
11 Click your desired option:

- If a session is in the **Pause** mode, click **Resume** to continue testing sessions on the list.

Note Pending media will be placed into a Pause state.

- To stop a test, click **Stop**.
- To view the latest Test Session List, click **Refresh**.
- To view details of a test, click **Details**.

The **Session Report** dialog box appears.



Barcode	Test Result	Drive ID	State	Completed
000051L2	Good	IU1719027R	Completed	Tue Jun 11 00:17:42 GMT
000089L3	Bad	IU17450LIIN	Completed	Tue Jun 11 00:18:35 GMT
000097L3	Good	IU1719027R	Completed	Tue Jun 11 00:19:42 GMT
000224L3	Bad	IU17450LIIN	Completed	Tue Jun 11 00:20:33 GMT
000438L2	Good	IU1719027R	Completed	Tue Jun 11 00:21:25 GMT
000457L3	Good	IU17450LIIN	Completed	Tue Jun 11 00:22:25 GMT

CM Scan Status:
Test completed

CM Scan Analysis:
Tape reached within 99% of the end of life based on the number of threads defined by the manufacturer

Tape Scan Status:
Test not configured

Tape Scan Analysis:
N/A

The MeDIA Session Report is divided into two sections:

- The top section displays a table containing the media information that were tested for the MeDIA Test Session that was selected from the **MeDIA Test Sessions List** dialog. The following information is reported:
  - **Barcode** – the media barcode identifier
  - **Test Result** – the outcome of the test, Good, Bad or Suspect
  - **Drive ID** – the serial number of the drive for which the media was tested
  - **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

- The lower section contains the test details for the media selected in the table. The details section contains the following information:
    - **CM Scan Status** – the cartridge memory status: Test completed, Test paused, Test pending, Test not run, or Test in progress.
    - **CM Scan Analysis** – a summary of the cartridge memory scan analysis
    - **Tape Scan Status** – the scan status: Test completed, Test paused, Test pending, Test not run, Test in progress, or Test not configured
    - **Tape Scan Analysis** – a summary of the tape scan test

12 To send a copy of the report via email, click **Send**. To update the dialog with the Sessions current status, click **Refresh**.

Using Sift Sort

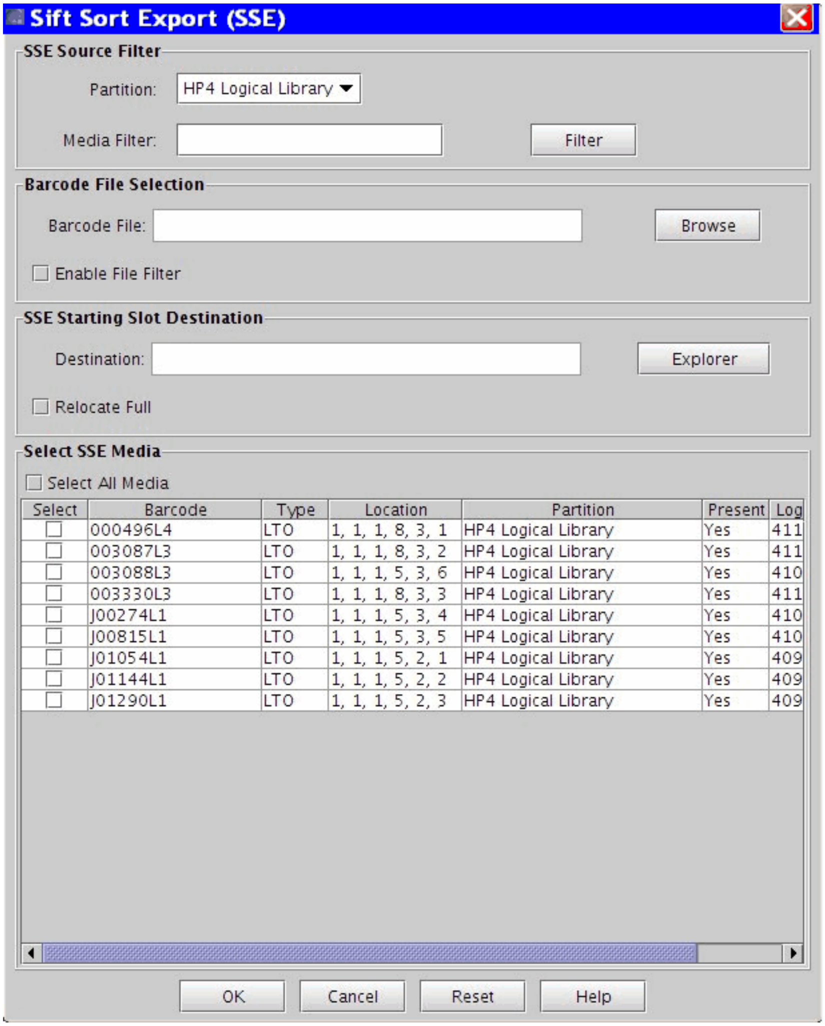
The Sift/Sort/Export functionality is to facilitate bulk movement of cartridges from their standard slot locations to either specific storage area within the library or the load port elements (the default setting will be the left upper storage area within the library). The default mode of operation of the SSE will be to put or relocate cartridges in sort order within the library, based on slot # or other logical grouping (this facilitates quickly locating like cartridge ID's, easier visualization of daily/weekly/monthly tapes (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.



Sift Sort Export (SSE)

SSE Source Filter

Partition: HP4 Logical Library

Media Filter:

Barcode File Selection

Barcode File:

☐ Enable File Filter

SSE Starting Slot Destination

Destination:

☐ Relocate Full

Select SSE Media

☐ Select All Media

Select	Barcode	Type	Location	Partition	Present	Log
☐	000496L4	LTO	1, 1, 1, 8, 3, 1	HP4 Logical Library	Yes	411
☐	003087L3	LTO	1, 1, 1, 8, 3, 2	HP4 Logical Library	Yes	411
☐	003088L3	LTO	1, 1, 1, 5, 3, 6	HP4 Logical Library	Yes	410
☐	003330L3	LTO	1, 1, 1, 8, 3, 3	HP4 Logical Library	Yes	411
☐	J00274L1	LTO	1, 1, 1, 5, 3, 4	HP4 Logical Library	Yes	410
☐	J00815L1	LTO	1, 1, 1, 5, 3, 5	HP4 Logical Library	Yes	410
☐	J01054L1	LTO	1, 1, 1, 5, 2, 1	HP4 Logical Library	Yes	409
☐	J01144L1	LTO	1, 1, 1, 5, 2, 2	HP4 Logical Library	Yes	409
☐	J01290L1	LTO	1, 1, 1, 5, 2, 3	HP4 Logical Library	Yes	409

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 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.

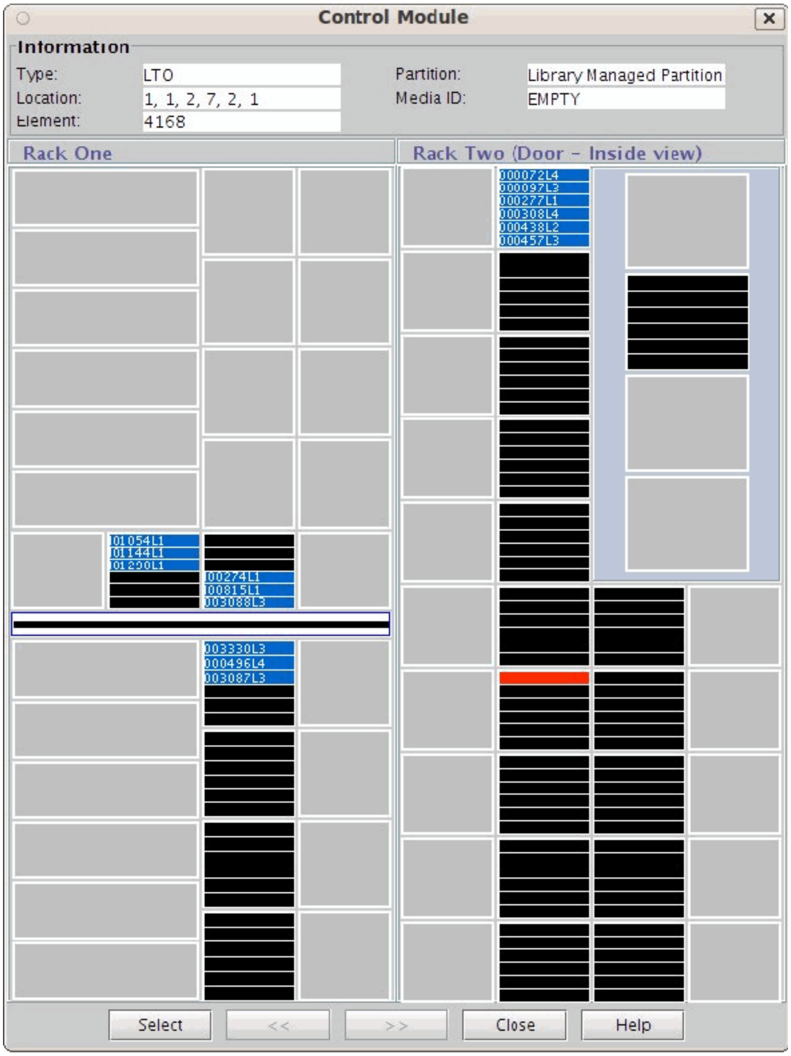
Note The **Relocate Full** box is checked as the default condition.

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.



Control Module

Information

Type: LTO

Location: 1, 1, 2, 7, 2, 1

Element: 4168

Partition: Library Managed Partition

Media ID: EMPTY

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 emailed to a recipient.

1 Log on as an administrator.

2 From the **Tools** menu, select **Sift Sort > Capture Report**.

The **Capture Sift Sort** Screen Shot 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.

Email 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

Click **Save**, and then click **Browse** to locate the location where you want to save the capture on your computer.

Retrieving MIBs

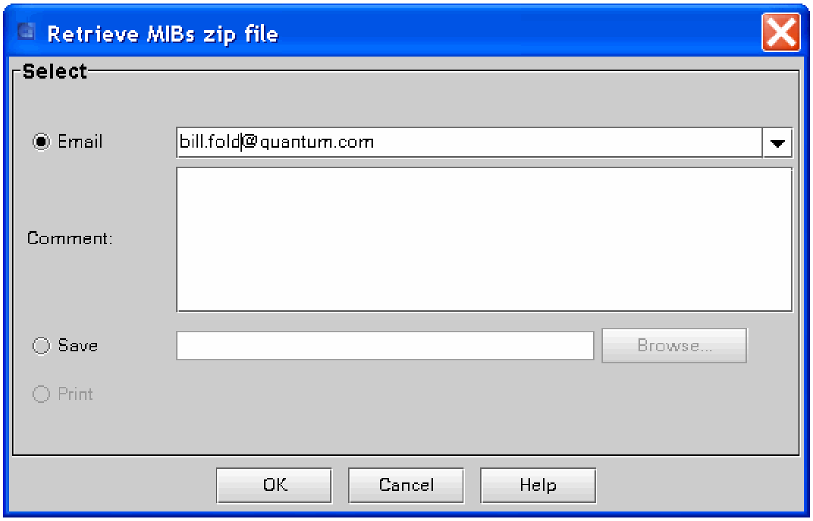
The Tools menu's Retrieve MIBs option allows you to retrieve the Scalar i6000 MIB files, which can be compiled into your SNMP Management tools. After retrieving the MIB files, you can extract the contents and then use a third-party SNMP tool such as Landesk or HP Operations Manager.

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.



Retrieve MIBs zip file

Select

● Email bill.fold@quantum.com

Comment:

○ Save

○ Print

3 Send the MIB file via email, or save it on your computer.

Email 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.

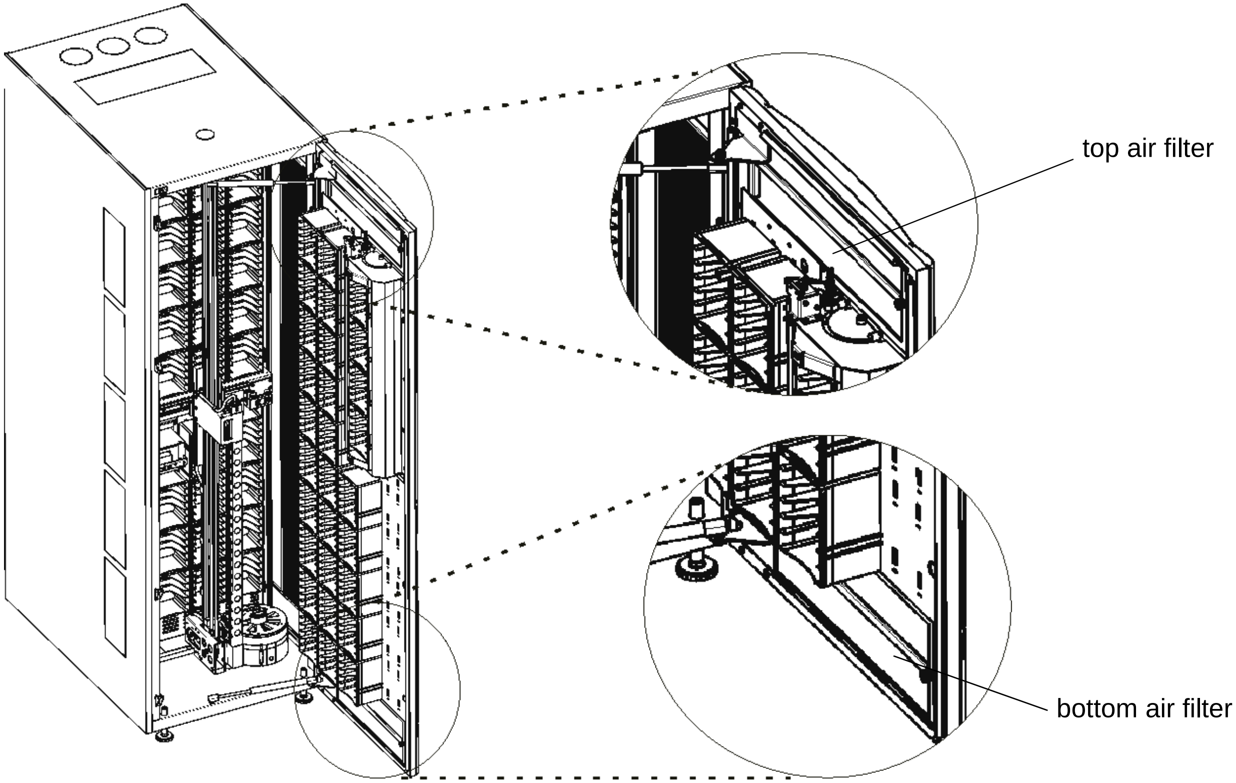
Save the MIB File

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 49.

Figure 49 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 303.

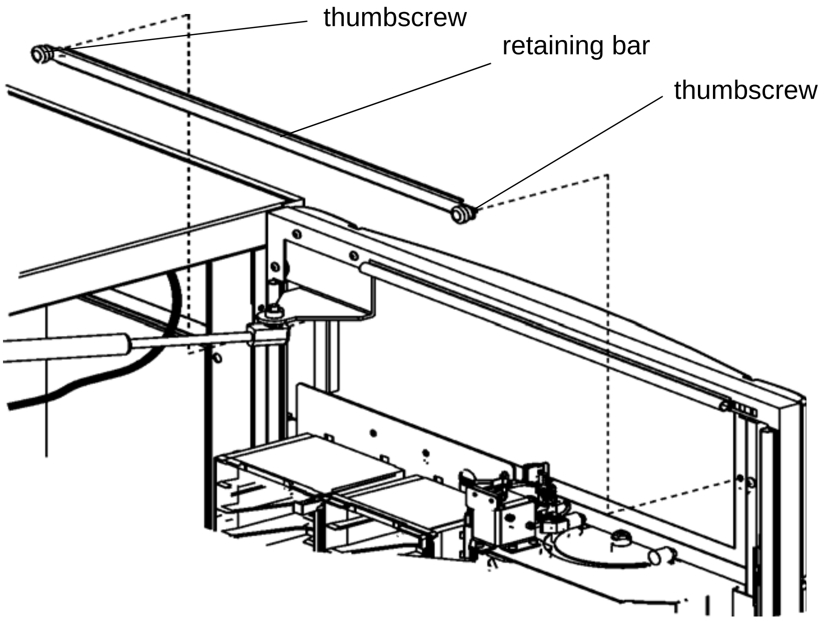
2 On the operator panel, press **Robotics Enabled** to turn off power to the picker and return it to the home position.

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 303.

2 On the operator panel, press **Robotics Enabled** to turn off power to the picker and return it to the home position.

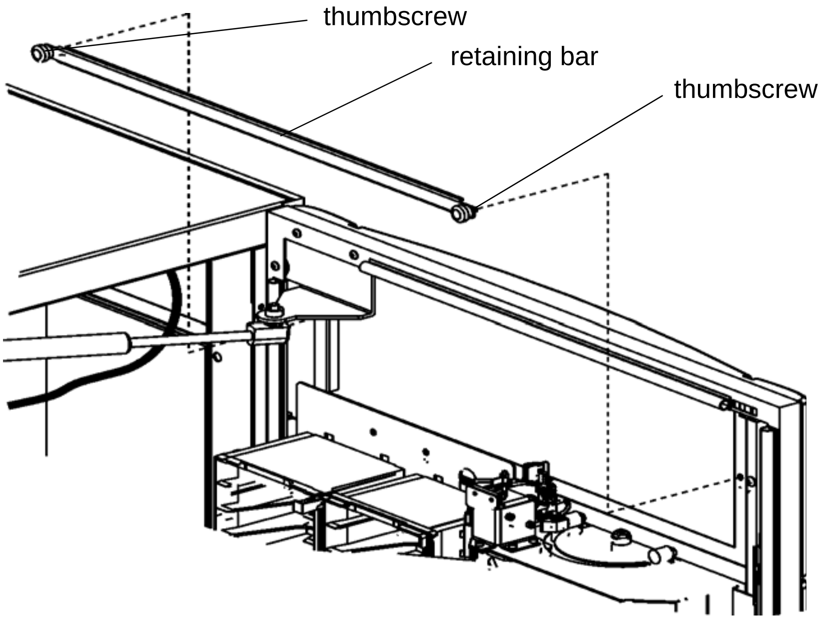
The power is on to all other components.

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 303.

Chapter 7

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 configuration can accommodate from 102 to 5316 LTO cartridges or from 100 to 2,910 DLT cartridges for the following drive types:

- SCSI or Fibre LTO-1
- SCSI or Fibre LTO-2
- Fibre LTO-3
- Fibre LTO-4
- Fibre LTO-5
- SCSI SDLT-320
- Fibre SDLT-600
- Fibre DLT-S4

⚠ CAUTION **Although the physical library can contain more than one media domain or drive domain, you cannot have a mix of domain types within a partition (for example, LTO and DLT). 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).**

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 10° to 35°C. The storage temperature range is 16° to 32°C 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.

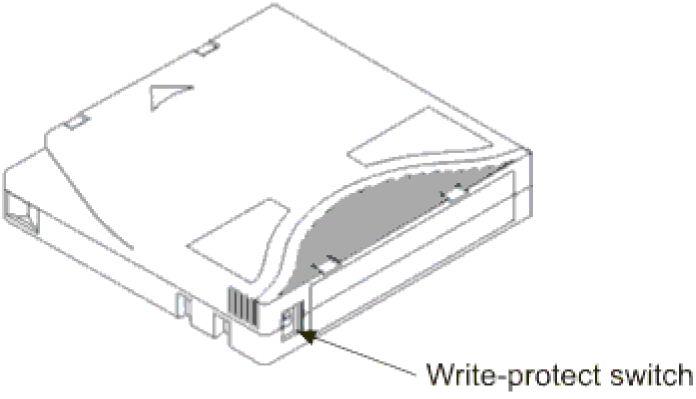
- Do not place cartridges near sources of electromagnetic energy or strong magnetic fields, such as computer monitors, electric motors, speakers, or x-ray equipment. Exposure to electromagnetic energy or magnetic fields can destroy data and the embedded servo code written on the media by the cartridge 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, whether LTO or DLT, 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 50 on page 506 for the location of the switch on an LTO cartridge.
- For DLT cartridges, slide the write-protect switch to the left so that the switch window shows orange. The switch is located on the left side of the cartridge front.

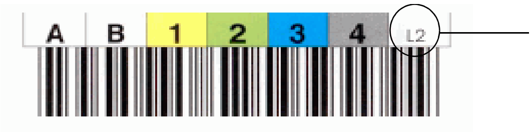
Figure 50 Write-protect Switch on an LTO-1 Cartridge



Barcode Requirements

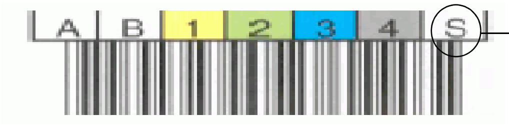
Cartridges must have an external barcode label that is machine-readable to identify the volume serial number. A barcode must use only uppercase letters A to Z and/or numeric values 0 to 9. The library supports Code 39 (3 of 9) type barcode labels.

For LTO media barcodes, the library dynamically supports 1 to 14 characters for volume serial number plus a two-character media type identifier. See the image below for an example of a supported LTO barcode label.



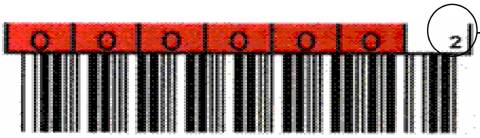
two-character media identifier (L1, L2, L3, LT, L4, LU, L5, LV)

For SDLT I media barcodes, the library dynamically supports 1 to 6 characters for volume serial number plus a one-character media type identifier. The image below is an example of a supported SDLT I barcode label.



character media identifier must be an “S”

For SDLT II media barcodes, the library dynamically supports 1 to 6 characters for volume serial number plus a one- character media type identifier. The image below is an example of a supported SDLT II barcode label.



character media identifier must be a “2”

For DLT-S4 media barcodes, the library dynamically supports 1 to 6 characters for volume serial number plus a one-character media type identifier. The media identifier should be “4”.

Quantum-supplied barcode labels will provide the best results. Barcode labels from other sources can be used, but they must meet the following requirements:

- ANSI MH10.8M-1983 Standard
- Number of digits: 6+1 (DLT) or 6+2 (LTO)
- Background reflection: greater than 25 percent
- Print contrast: greater than 75 percent
- Ratio: greater than 2.2
- Module: >= .254 mm
- Print tolerance: ± 57 mm

Additional Requirements:

- Height of the visible portion of the barcode: 10 mm ±2 mm

- Length of the rest zones: 5.25 mm ± 0.25 mm
- No black marks should be present in the intermediate spaces or rest zones
- No white areas should be present on the bars

Installing Barcode Labels

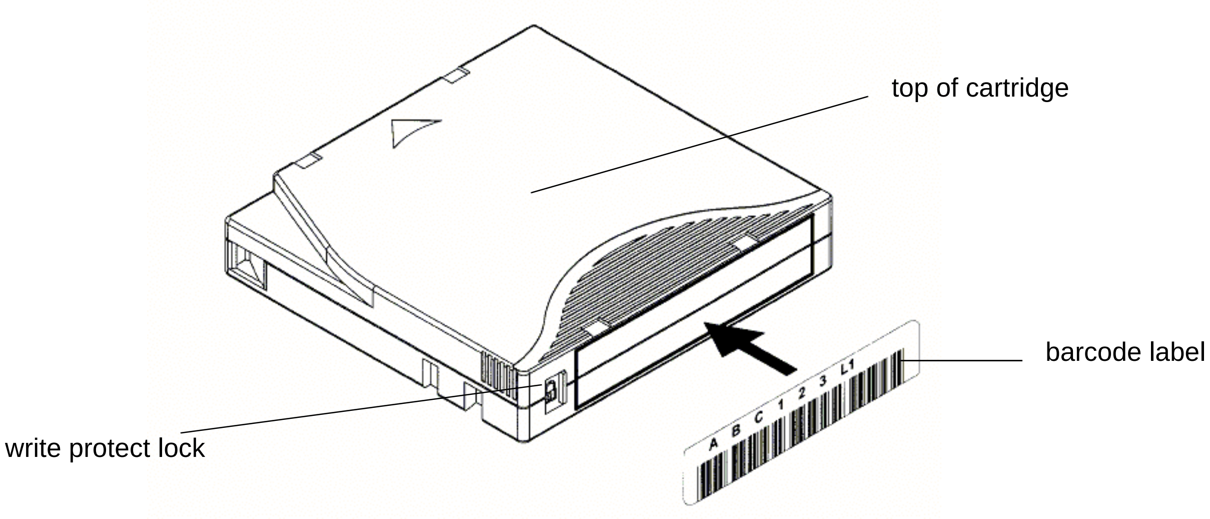
Each cartridge in the library must have an external label that is operator and machine readable to identify the barcode number. Most manufacturers offer cartridges with the labels already applied or with the labels included that you can attach.

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 51 on page 509 shows an example of a barcode label being applied to an LTO cartridge.

CAUTION **Do not place a barcode label on top of a cartridge. Doing so can cause inventory operations to fail.**

Figure 51 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. In some cases, specific labels have been established as industry standard. For instance, the prefix “CLN” might be used to identify a cleaning tape. The library does not require a specific content to the label and accepts conventional tape labels.
- 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 Media

The LMC provides you with commands for:

- Importing and exporting cartridges
- Moving media from one storage location to another
- Loading and unloading drives
- Taking inventory

The following sections provide step-by-step instructions for performing these tasks.

Note Unless the situation requires it, uses 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.

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.

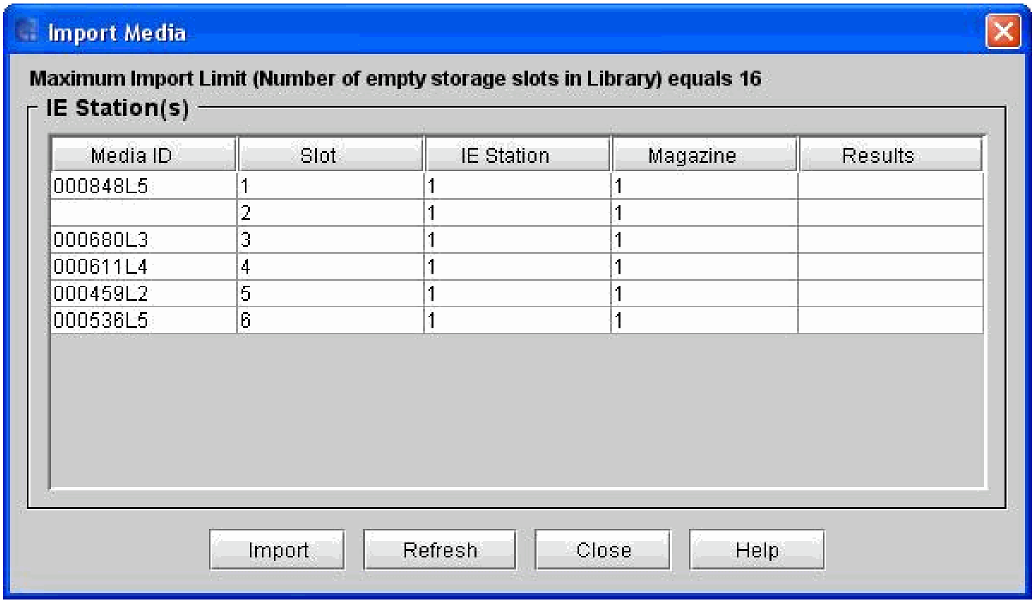
3 To see which I/E stations are associated with a particular partition, click **Monitor** > **IE Station**.

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.



Maximum Import Limit (Number of empty storage slots in Library) equals 16

IE Station(s)

Media ID	Slot	IE Station	Magazine	Results
000848L5	1	1	1	
	2	1	1	
000680L3	3	1	1	
000611L4	4	1	1	
000459L2	5	1	1	
000536L5	6	1	1	

The following table describes the elements on the **Import Media** dialog box.

Element	Description
Media ID	The volume serial number of the cartridge.
Slot	The number of the slot in the I/E station magazine. To understand the location designation, see Understanding Location Coordinates on page 288.
IE Station	The number of the module. To understand the location designation, see Understanding Location Coordinates on page 288.
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 288.
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.

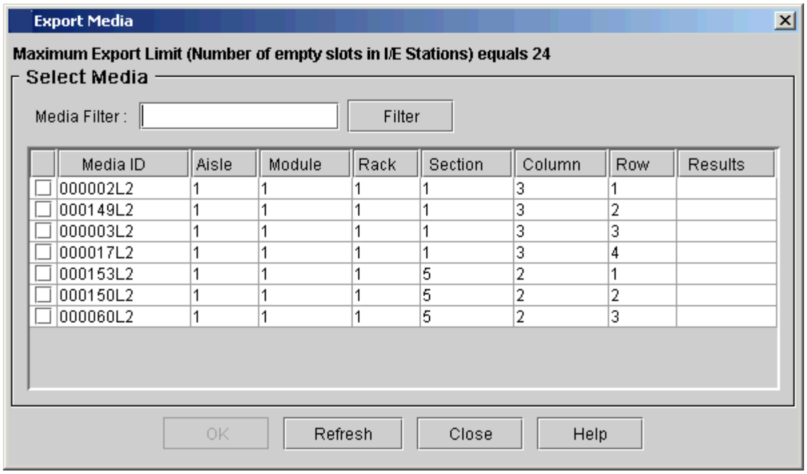
1 Make sure that you are viewing the partition from which you want to export a data cartridge. From the **View** menu, click the name of the appropriate partition.

2 Click **Operations** > **Export** or click the **Export** toolbar button.

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**.

The **Export Media** dialog box appears with a list of cartridges in the partition displayed.



Export Media

Maximum Export Limit (Number of empty slots in I/E Stations) equals 24

Select Media

Media Filter :

	Media ID	Aisle	Module	Rack	Section	Column	Row	Results
□	000002L2	1	1	1	1	3	1	
□	000149L2	1	1	1	1	3	2	
□	000003L2	1	1	1	1	3	3	
□	000017L2	1	1	1	1	3	4	
□	000153L2	1	1	1	5	2	1	
□	000150L2	1	1	1	5	2	2	
□	000060L2	1	1	1	5	2	3	

3 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”.

4 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.

5 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.

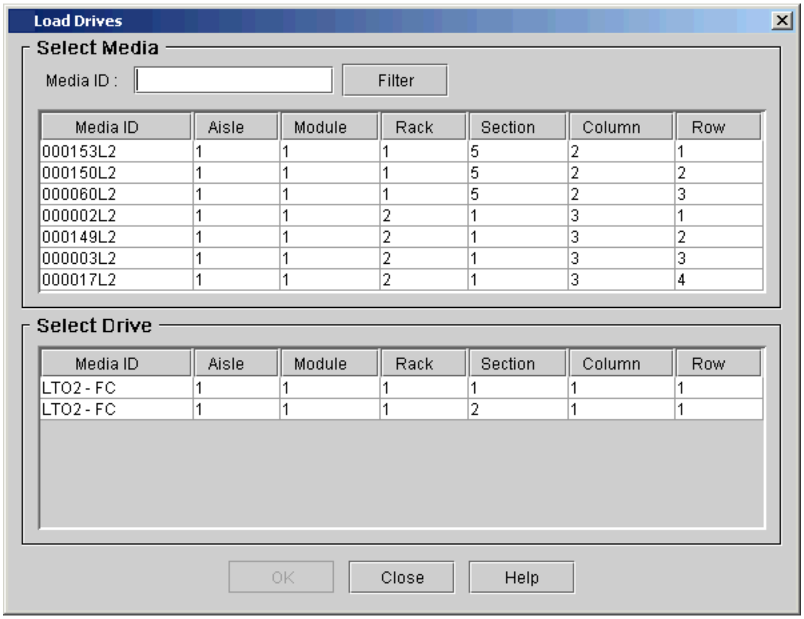
Loading Drives

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.



Media ID	Aisle	Module	Rack	Section	Column	Row
000153L2	1	1	1	5	2	1
000150L2	1	1	1	5	2	2
000060L2	1	1	1	5	2	3
000002L2	1	1	2	1	3	1
000149L2	1	1	2	1	3	2
000003L2	1	1	2	1	3	3
000017L2	1	1	2	1	3	4

Media ID	Aisle	Module	Rack	Section	Column	Row
LTO2 - FC	1	1	1	1	1	1
LTO2 - FC	1	1	1	2	1	1

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 288.

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**.

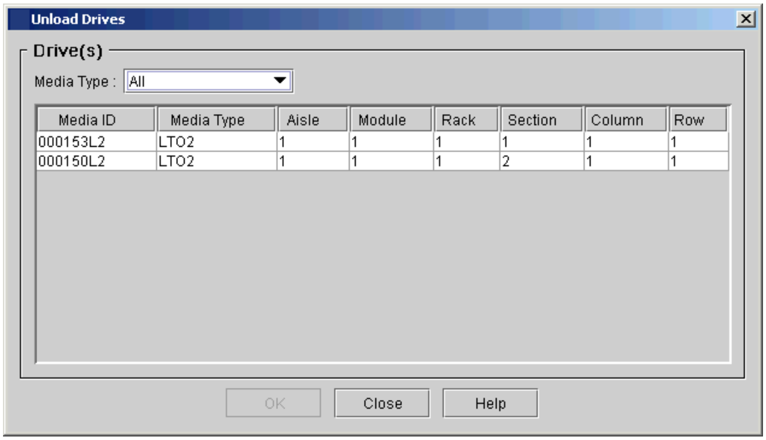
Unloading Drives

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.



Media Type : All

Media ID	Media Type	Aisle	Module	Rack	Section	Column	Row
000153L2	LTO2	1	1	1	1	1	1
000150L2	LTO2	1	1	1	2	1	1

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 288.

5 Click **OK**.

The library rewinds the data cartridge, unloads it from the drive, and returns it to storage.

Moving Media

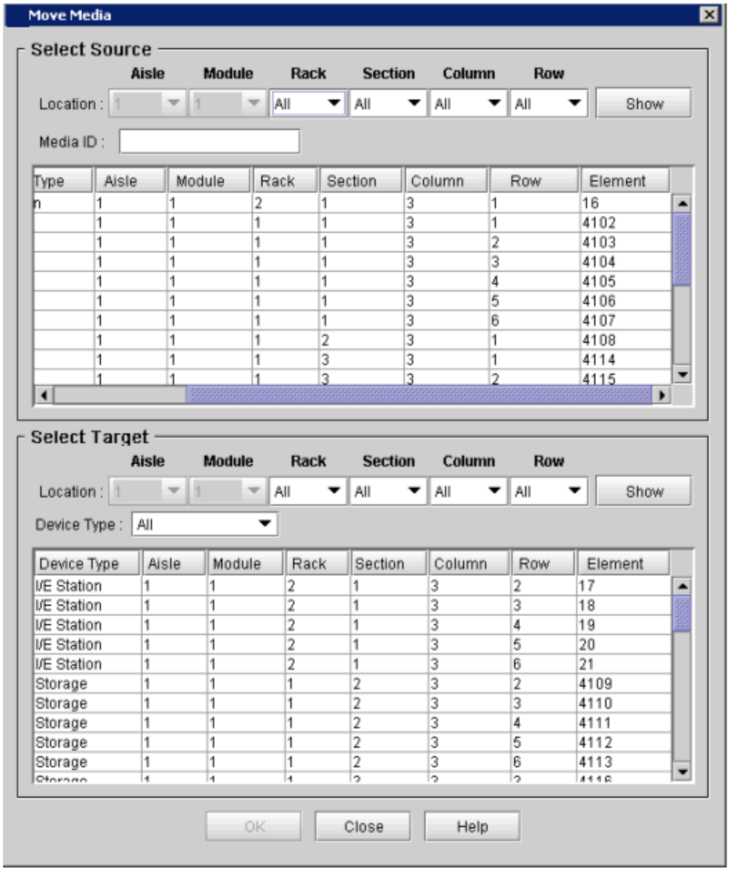
The **Move Media** dialog box enables you to move media from one location to another within a partition.

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.



Move Media

Select Source

	Aisle	Module	Rack	Section	Column	Row	
Location :	1	1	All	All	All	All	Show

Media ID :

Type	Aisle	Module	Rack	Section	Column	Row	Element
n	1	1	2	1	3	1	16
	1	1	1	1	3	1	4102
	1	1	1	1	3	2	4103
	1	1	1	1	3	3	4104
	1	1	1	1	3	4	4105
	1	1	1	1	3	5	4106
	1	1	1	1	3	6	4107
	1	1	1	2	3	1	4108
	1	1	1	3	3	1	4114
	1	1	1	3	3	2	4115

Select Target

	Aisle	Module	Rack	Section	Column	Row	
Location :	1	1	All	All	All	All	Show

Device Type : All

Device Type	Aisle	Module	Rack	Section	Column	Row	Element
I/E Station	1	1	2	1	3	2	17
I/E Station	1	1	2	1	3	3	18
I/E Station	1	1	2	1	3	4	19
I/E Station	1	1	2	1	3	5	20
I/E Station	1	1	2	1	3	6	21
Storage	1	1	1	2	3	2	4109
Storage	1	1	1	2	3	3	4110
Storage	1	1	1	2	3	4	4111
Storage	1	1	1	2	3	5	4112
Storage	1	1	1	2	3	6	4113
Storage	1	1	1	2	3	2	4116

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 288.

- 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.

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 159.

1 Log on as an administrator.

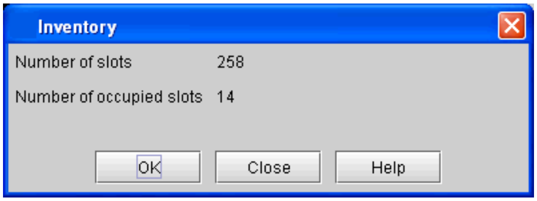
2 You can perform this procedure while either viewing the physical library or a partition. From the **View** menu, click the name of the physical library or the appropriate partition.

3 Click **Operations** > **Inventory**.

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**.

The **Inventory** dialog box appears.



Inventory

Number of slots 258

Number of occupied slots 14

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.

4 To perform an inventory, click **OK**.

The inventory process take a few minutes to complete.

5 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 37.

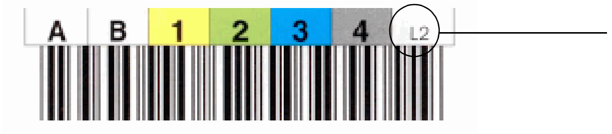
How do I clean a drive? Use your backup software to clean the drives. For detailed instructions, see Using Cleaning Cartridges on page 509.

How do I know when the drives need cleaning? The host application informs you when drives need to be cleaned. See Using Cleaning Cartridges on page 509.

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 112. To learn how to create a partition, see Creating Partitions on page 118.

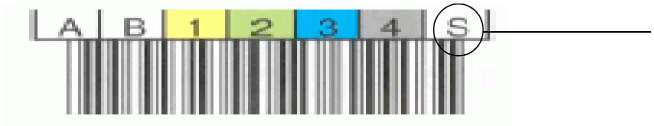
Where can I find the library's serial number? The serial number appears in the **ID** column for the first line of output on the **System Status** dialog box (**Monitor**→ **System**). Use the serial number when contacting technical support for assistance.

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.



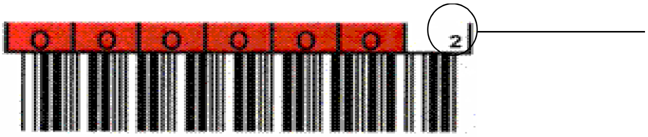
two-character media identifier (L1, L2, L3, LT L4, LU, L5 or LV)

For SDLT I media barcodes, the library dynamically supports 1 to 6 characters for volume serial number plus a one-character media type identifier. The image below is an example of a supported SDLT I barcode label.



character media identifier must be an "S"

For SDLT II media barcodes, the library dynamically supports 1 to 6 characters for volume serial number plus a one- character media type identifier. The image below is an example of a supported SDLT II barcode label.



character media identifier
must be a “2”

For DLT-S4 media barcodes, the library dynamically supports 1 to 6 characters for volume serial number plus a one-character media type identifier. The media identifier should be “4”.

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 Updated Contact Info on page 6.

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 316, Powering Off the Library on page 317, and Powering On the Library on page 318. The blue LED on the power supply will be on and not blinking.

Appendix C

Glossary

This glossary consists of terms unique to the library along with some storage industry terminology.

Access door
Refers to the doors on either the control module or expansion module from which you can access the magazines and accessor assembly.

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.

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.

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.

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.

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.

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 management 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 MeDIA (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.

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.

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.

Quantum Encryption Key Manager (Q-EKM)
Quantum's encryption key management solution that supports IBM LTO-4 and LTO-5 FC and SAS tape drives.

Scalar Key Manager (SKM)
Quantum's encryption key management solutions that supports HP LTO-4 and LTO-5 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 host access configuration features of 8 GB/ HP LTO-5 tape drives, without those drives being connected to a 4 GB/Fibre Channel I/O blade.

Universal drive sled (UDS)
A sheet metal case that houses LTO or SCSI drives in the drive clusters.

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-axis
The horizontal position of the accessor assembly.

Y-axis
The vertical position of the accessor assembly.

Index