Quantum

Quantum Scalar i500 Tape Library

Scalar i500

6-01210-06 B

Scalar i500 User's Guide, 6-01210-06, Rev. B, February 2014, 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.

Contents

Chapter 2   **Understanding the User Interface**   **39**

Chapter 3   **Configuring Your Library**   **52**

Chapter 8   **Extended Data Lifecycle Management**   **203**

Chapter 9   **Running Your Library**   **237**

Appendix B   **TapeAlert Flag Descriptions**   **531**

Glossary   **541**

Tables

Figures

Preface

Audience

This guide is intended for anyone interested in learning about or anyone who needs to know how to install, configure, and operate the Scalar® i500 library. Be aware that administrator level privileges are required to configure many of the features described in this guide.

Purpose

This guide contains information and instructions necessary for the normal operation and management of the Scalar i500 library, including:

- Installing the library
- Basic library operations
- Operator commands
- Troubleshooting

Product Safety Statements

This product is designed for data storage and retrieval using magnetic tapes. 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.

> **Warning:** Before operating this product, read all instructions and warnings in this document and in the *System, Safety, and Regulatory Information Guide*. The *System, Safety, and Regulatory Information Guide* is located on the *Scalar i500 Documentation, Training, and Resource CD*.

⚠️ 警告　操作本產品前，請先閱讀本文件及系統、安全與法規資訊指南中的指示與警告說明。

⚠️ 警告　在使用本产品之前，请先阅读本文档及系统、安全和法规信息指南中所有的说明和警告信息。

⚠️ ADVERSAL　Læs alle instruktioner og advarsler i dette dokument og i *Vejledning om system-sikkerheds- og lovgivningsoplysninger*, før produktet betjenes.

⚠️ AVERTISSEMENT　Avant d'utiliser ce produit, lisez la totalité des instructions et avertissements de ce document et du *Guide d'informations sur le système, la sécurité et la réglementation*.

⚠️ HINWIES　Lesen Sie vor der Verwendung dieses Produkts alle Anweisungen und Warnhinweise in diesem Dokument und im System, Safety, and Regulatory Information Guide (Info-Handbuch: System, Sicherheit und Richtlinien).

לפני ההפעלה של מוצר זה, קרא את כל ההוראות והאזהרות הכלולות במסמך זה וכן במדריך *מידע בנושאי מערכת, בטיחות ותקינה* אזהרה ⚠️

⚠ 警告　この製品を使用する前に、本文書、および『システム、安全、規制に関する情報ガイド』に記載しているすべての警告と指示をお読みください。

⚠ 경고　이 제품을 작동하기 전에 이 문서 및 시스템, 안전, 및 규제 정보 안내서에 수록된 모든 지침과 경고 표지를 숙지하십시오.

⚠ ПРЕДУПРЕЖДЕНИЕ　Перед началом эксплуатации данного устройства ознакомьтесь во всеми инструкциями и предупреждениями, приведенными в данном документе и в *Справочном руководстве по устройству, технике безопасности и действующим нормативам*.

⚠ ADVERTENCIA　Antes de utilizar este producto, lea todas las instrucciones y advertencias en este documento y en la Guia informativa sobre sistema, seguridad y normas.

⚠ VARNING　Läs alla anvisningar och varningar i detta dokument och i *System, säkerhet och krav från myndigheter - Informationshandbok* innan denna produkt tas i bruk.

Mercury Statement

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://www.quantum.com/AboutUs/weee/Index.aspx or contact your local government authority, your household waste disposal service or the business from which you purchased the product.

Document Organization

This document is organized as follows:

- Chapter 1, Description, describes basic library configurations and features.

- Chapter 2, Understanding the User Interface, discusses the operator panel and the Web client, and the features available on each.

- Chapter 3, Configuring Your Library, explains how to configure your library for use.

- Chapter 4, Advanced Reporting, describes the features available with the Advanced Reporting license.

- Chapter 5, Capacity on Demand, describes how to purchase additional slot capacity for the library.

- Chapter 6, Storage Networking, describes the features available with the Storage Networking license.

- Chapter 7, Encryption Key Management, describes the features available with the Encryption Key Management license.

- Chapter 9, Running Your Library, explains how to perform library, tape drive, and media operations.

- Chapter 10, Getting Information – Logs and Reports, explains how to use the library's built-in reports to get information you need.

- Chapter 11, Updating Library and Tape Drive Firmware, explains how to update library and tape drive firmware.

- Chapter 12, Installing, Removing, and Replacing, provides instructions on how to install, remove, and replace hardware components in the library, including modules, tape drives, power supplies, and cables.

- Chapter 13, Troubleshooting, describes the library's diagnostic reporting system (RAS tickets) and how to use it. It also describes a number of diagnostic tests you can run to troubleshoot problems.

- Chapter 14, Working With Cartridges and Barcodes, provides cartridge handling guidelines.

- Appendix A, Library Specifications, lists the library's specifications.

- Appendix B, TapeAlert Flag Descriptions, describes of all the TapeAlerts you may see listed in RAS tickets and reports on your library.

This document concludes with a glossary.

Notational Conventions

This manual uses the following conventions:

> **Note:** Note emphasizes important information related to the main topic.

> **Caution:** Caution indicates potential hazards to equipment or data.

> **Warning:** Warning indicates potential hazards to personal safety.

This manual uses the following:

- Right side — Refers to the right side as you face the component being described.

- Left side — Refers to the left side as you face the component being described.

Related Documents

Documents related to the Scalar i500 are shown below. For the most up to date product information and documentation, see:

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

Document No.	Document Title	Document Description
6-01741-xx	*Scalar i500 Getting Started Guide*	Provides basic cabling and setup instructions.
6-01317-xx	*Quantum Scalar Intelligent Libraries SMI-S Reference Guide*	Provides an interface standard that can be used in a SAN environment.
6-01370-xx	*Scalar i500 Tape Library Basic SNMP Reference Guide*	Describes information you can obtain from the Scalar i500 library SNMP.
6-00676-xx	*Quantum SNC Firmware 4 and 5 Reference Guide*	Provides information about the Storage Network Controller, an optional component that provides Fibre-Channel to Fibre-Channel connectivity.
6-01385-xx	*Scalar i500 Unpacking Instructions (5U)*	Unpacking instructions.
6-01524-xx	*Scalar i500 Unpacking Instructions (9U)*	Unpacking instructions.
6-01525-xx	*Scalar i500 Unpacking Instructions (14U)*	Unpacking instructions.
6-01378-xx	*Scalar i500 Release Notes*	Describes changes to your system or firmware since the last release, provides compatibility information, and discusses any known issues and workarounds.

Refer to the appropriate product manuals for information about your tape drive and cartridges.

SCSI-2 Specification

The SCSI-2 communications specification is the proposed American National Standard for information systems, dated March 9, 1990. Copies may be obtained from:

Global Engineering Documents
15 Inverness Way, East
Englewood, CO 80112
(800) 854-7179 or (303) 397-2740

Contacts

Quantum company contacts are listed below.

Quantum Corporate Headquarters

For information about contacting Quantum, including Quantum office locations, go to:

http://www.quantum.com/aboutus/contactus/index.aspx

Quantum Home Page

Visit the Quantum home page at:

http://www.quantum.com

Getting More Information or Help

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

Accelerate service issue resolution with these exclusive Quantum StorageCare services:

- **Service and Support Web site** — Register products, license software, browse Quantum Learning courses, check backup software and operating system support, and locate manuals, FAQs, firmware downloads, product updates and more in one convenient location. Benefit today at: http://www.quantum.com/ServiceandSupport/Index.aspx.

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

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

- **Quantum Vision™** — Quantum Vision management software provides industry-leading administration and helps users make informed decisions about their growing backup needs. Vision™ software saves users time and increases data security by giving users centralized, global monitoring and reporting for their for all their Quantum DXi Series disk systems and Quantum tape libraries. More StorageCare Vision information can be found at: http://www.quantum.com/products/Software/quantumvision/Index.aspx

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

United States	800-284-5101 (toll free)
	949-725-2100
EMEA	00800-4-782-6886 (toll free)
	+49 6131 3241 1164
APAC	+800 7826 8887 (toll free)
	+603 7953 3010

For worldwide support:

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

Description

The Scalar i500 tape library automates the retrieval, storage, and management of tape cartridges. Tape cartridges are stored in the library and mounted and dismounted from tape drives using firmware running on the library or software running on the host systems.

The Scalar i500 tape library offers advanced management features and reliability as well as scalable performance and storage capacity. As your storage capacity and tape drive requirements change, expansion modules can be added to the library, allowing a configuration of up to a full 41 rack units (41U, where 1U = 1.75").

This chapter covers:

- [Intelligent Storage](#)
- [Library Configuration](#)
- [Modules](#)
- [Front Panel Components](#)
- [Back Panel Components](#)
- [Robotic System and Barcode Scanner](#)
- [Tape Drive Support](#)
- [Library Features](#)
- [Understanding the Location Coordinates](#)
- [Understanding Logical Element Addressing](#)

Intelligent Storage

The Scalar i500 is the intelligent library platform that gives growing midrange storage environments faster, easier, and more reliable data protection. The Scalar i500 combines modular design with continuous robotics to provide industry-leading scalability, performance, and reliability. Designed with Quantum's iPlatform architecture and iLayer management approach, the Scalar i500 makes backup easier to manage. Its proactive monitoring and remote diagnostics can reduce service calls by 50% and shorten issue resolution times by 30%. Its Capacity on Demand (COD) scalability lets it grow non-disruptively with users' data. And the Scalar i500 is designed to integrate easily with disk backup, making it the perfect library for next-generation backup architectures. With the Scalar i500, Information Technology managers can be assured they will have reliable, high-performance backup, certain restores, and effective long-term protection for years into the future, no matter how their storage needs evolve.

Library Configuration

The Scalar i500 library is designed for ease of installation, configuration, and field upgrades. The Scalar i500 library is built upon two basic building blocks: the 5U control module and 9U expansion module.

These building blocks form the basis of the following library configurations:

- A 5U library, consisting of a 5U stand-alone control module. shows the front view of a 5U library.

- A 14U library, consisting of one 5U control module and one 9U expansion module. shows the front view of a 14U library.

- A 23U library, consisting of one 5U control module and two 9U expansion modules. shows the front view of a 23U library.

The 5U, 14U, and 23U libraries are the base Scalar i500 systems. By adding 9U expansion modules, you can upgrade a base system to:

- A 32U library, consisting of one 5U control module and three 9U expansion modules

- A 41U library, consisting of one 5U control module and four 9U expansion modules

Figure 1 5U Library Configuration (Standalone Control Module)
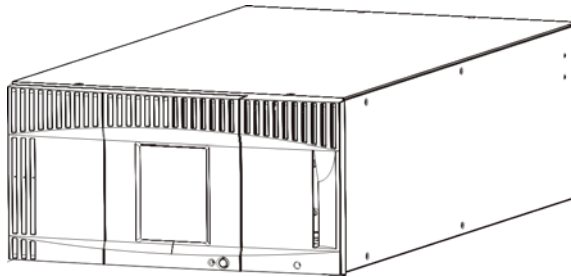
Figure 2 14U Library
Configuration (5U Control
Module Plus One 9U
Expansion Module)
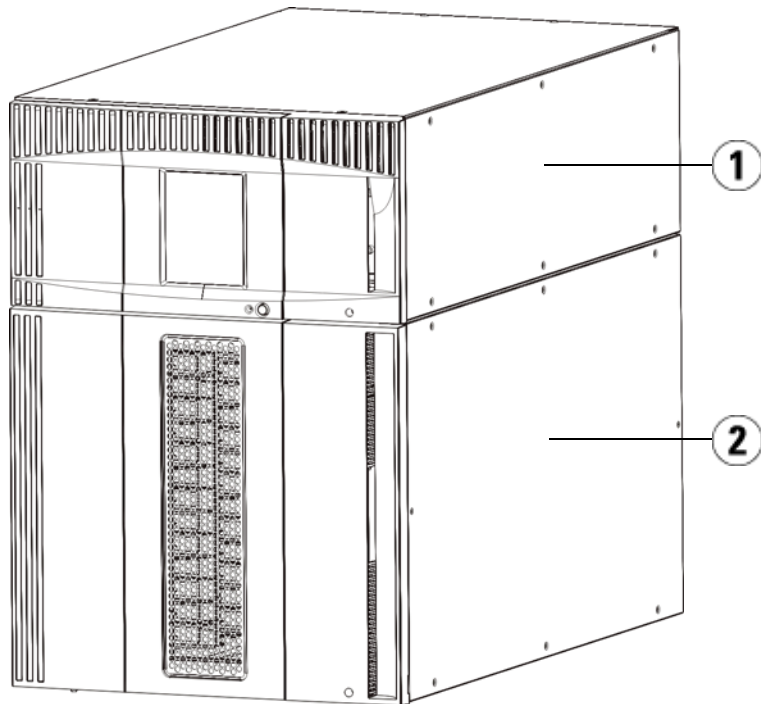
1	Control module
2	Expansion module

Figure 3 23U Library
Configuration (5U Control
Module Plus Two 9U
Expansion Modules)
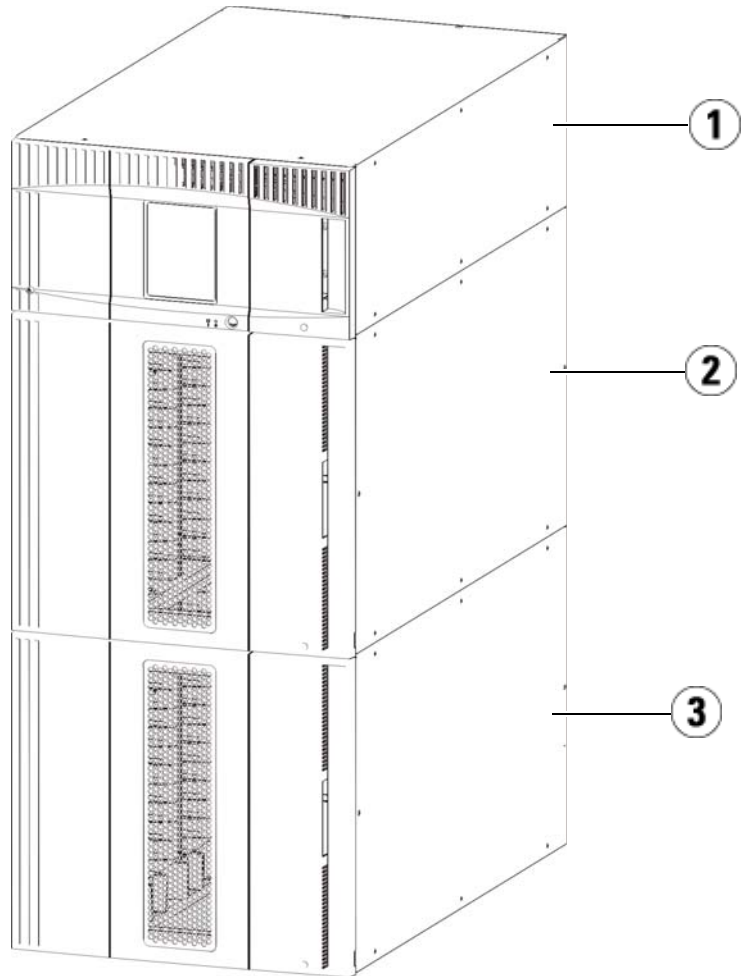
1	5U control module
2	9U expansion module
3	9U expansion module

Warning:	All libraries taller than 14U must be installed in a rack having a main protective earthing (grounding) terminal, and power must be supplied via an industrial plug and socket-outlet and/or an appliance coupler complying with IEC 60309 (or an equivalent national standard) and having a protective earth (ground) conductor with a cross-sectional area of at least 1.5 mm2 (14 AWG).
	To ensure proper airflow and access space, allow 60 cm (24 inches) in the front and back of the library.

Modules

Scalar i500 libraries are modular, and you can increase the size at any time. The three base systems for the Scalar i500 library are as follows:

- The 5U library, consisting of a control module

- The 14U library, consisting of a 5U control module and a 9U expansion module

- The 23U library, consisting of a 5U control module and two 9U expansion modules

These configurations can be scaled up by adding 9U expansion modules to a maximum rack height of 41U. Expansion modules provide additional capacity as your storage and tape drive requirements change. See Figure 4 on page 17 for an illustration of library scalability. For information on installing, removing, and replacing modules, see Installing, Removing, and Replacing on page 286.

Each module has a specific number of fixed storage slots, I/E station slots, and tape drive slots available. See Library capacity is as follows. on page 526 for the number of slots available for each library configurations.

Note:	Slot counts in this document do not include five inaccessible slots in the bottom row of any library configuration. For more information about these slots, see Unused Slots on page 247.

Control Module

The control module is required in any Scalar i500 library configuration. The control module contains the robotic controls, library control blade (LCB), and touch screen display. The control module also contains an import/export (I/E) station, fixed storage slots, tape drives, and at least one power supply.

Expansion Modules

Expansion modules are supplementary modules that can be stacked above or below the control module. Each expansion module contains fixed storage slots, tape drive slots, and power supply slots.The I/E stations on expansion modules are included and may be configured as storage. Expansion modules also contain bays for optional Fibre Channel (FC) Input/Output (I/O) blades, which provide FC connections for FC drives in the library.

If an expansion module is used only for storage and does not contain tape drives or FC I/O blades, it does not need a separate power supply. All power is derived from the control module.

Stackability

The maximum rack height of the library is 41U, which consists of a 5U control module and four 9U expansion modules. Figure 4 illustrates the stackability of the library and the recommended library configurations.

Figure 4 Base Systems Plus
Expansion Modules

5U (41 slots)	14U (133 slots)	23U (225 slots)	32U (317 slots)	41U (409 slots)
				9U Expansion Module
			5U Control Module	5U Control Module
		5U Control Module	9U Expansion Module	9U Expansion Module
	5U Control Module	9U Expansion Module	9U Expansion Module	9U Expansion Module
5U Control Module	9U Expansion Module	9U Expansion Module	9U Expansion Module	9U Expansion Module
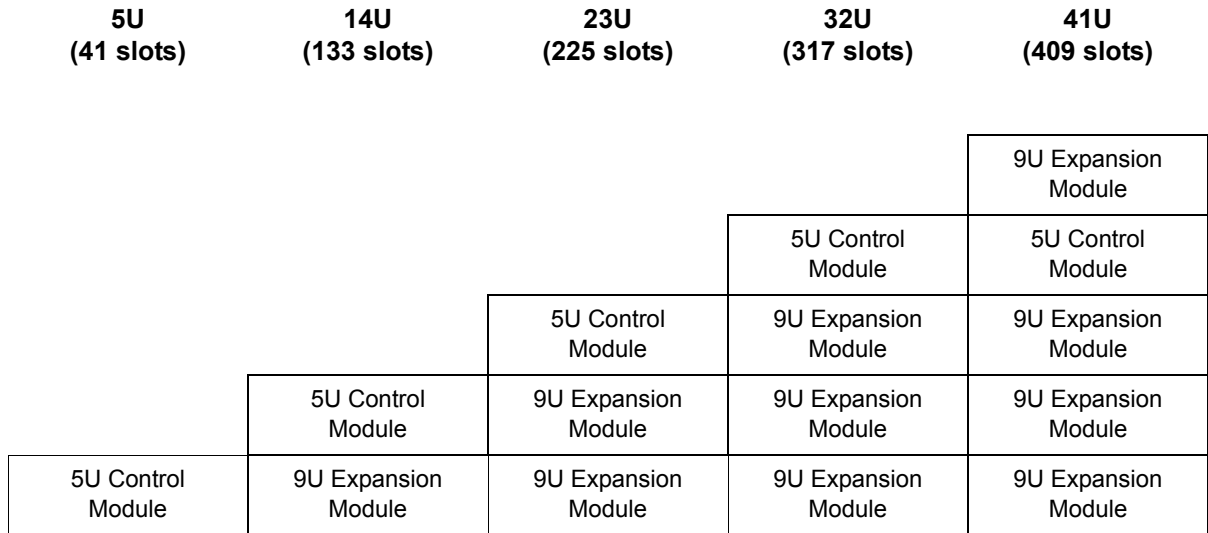
Front Panel Components

Figure 5 shows the front panel components of the library. The paragraphs following Figure 5 describe the components in detail.

Figure 5 Front Panel
Components
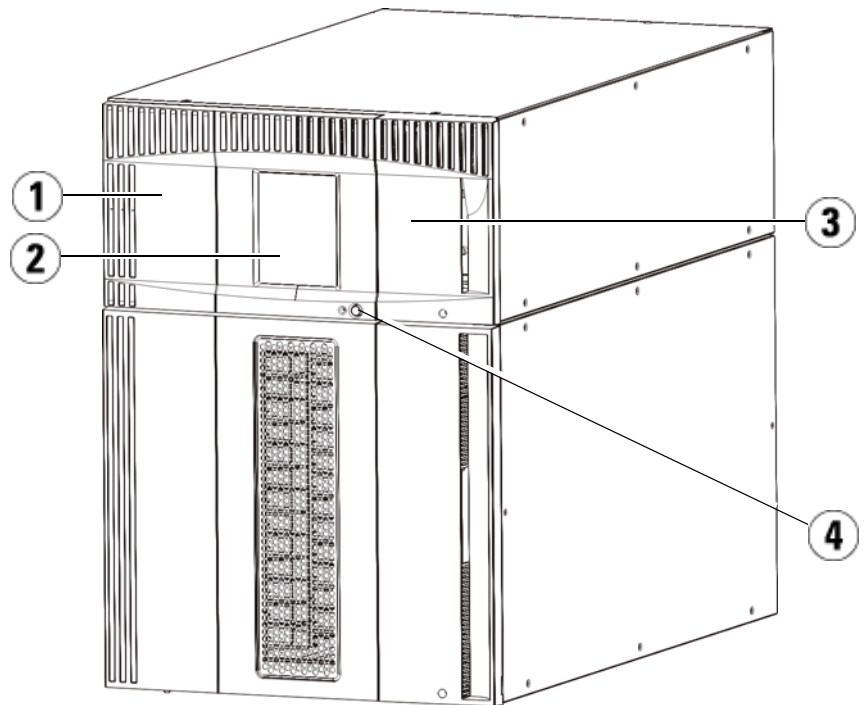
1   Access door

2   Operator panel

3   I/E station

4   Front power button

Access Door

The access door allows access to the internal components of the library. Each control module and expansion module has an access door. In most

cases, you will not need to access the library through this door except when you want to bulk load or unload cartridges from the library.

The access door is locked by the I/E station door. To open the access door, you must first open the I/E station door. If you want to prohibit access to the library, which is recommended for security reasons, lock the I/E station door. This keeps unauthorized users from accessing tape cartridges.

You can lock and unlock the I/E station door using commands on the **Operations** menu. For more information, see <u>Locking and Unlocking the I/E Stations</u> on page 262.

If the access door is opened, the library is not available for use. When an access door (on any module) is opened, all in-progress motion commands are stopped, and the picker slowly lowers to the bottom of the library. When the access door is closed, the library returns any media in the picker to its original slot and also performs a library inventory.

Caution:	Care should be taken to avoid opening the access door during robotic operations since the robot will stop immediately and will fail to complete the current operation.

I/E Station

I/E stations enable importing and exporting cartridges with minimal interruption of normal library operations. I/E stations are located on the front of the control module and on the front of expansion modules. A 5U I/E station has a capacity of six cartridges within a removable magazine. A 9U I/E station has a capacity of 12 cartridges within two removable magazines.

The I/E stations can also be configured as storage as well as become part of a logical division of library resources known as a partition. The I/E station is shared among all partitions, but the I/E station slots are owned by one partition at a time. When an I/E station slot is assigned to a partition, only the assigned partition can access that slot.

Operator Panel

The operator panel is the touch screen display device upon which the graphical user interface (GUI) appears. The operator panel is located on the access door of the control module. The library operations and service functions are performed from this screen. The GUI is also accessible

through a remote Web client. For more information on the library user interfaces, see <u>Chapter 2, Understanding the User Interface</u>.

Front Power Button

Turning off the front power button turns off the robot and operator panel, but power still runs to the power supplies. Use the front power button to manually shut down the library. See <u>Shutting Down, Powering Off, and Completely Removing Power</u> on page 238 for instructions on how to shut down or restart the library safely.

Back Panel Components

<u>Figure 6</u> shows the back panel components of the library. The paragraphs following <u>Figure 6</u> describe the components in detail.

Figure 6 Back Panel
Components
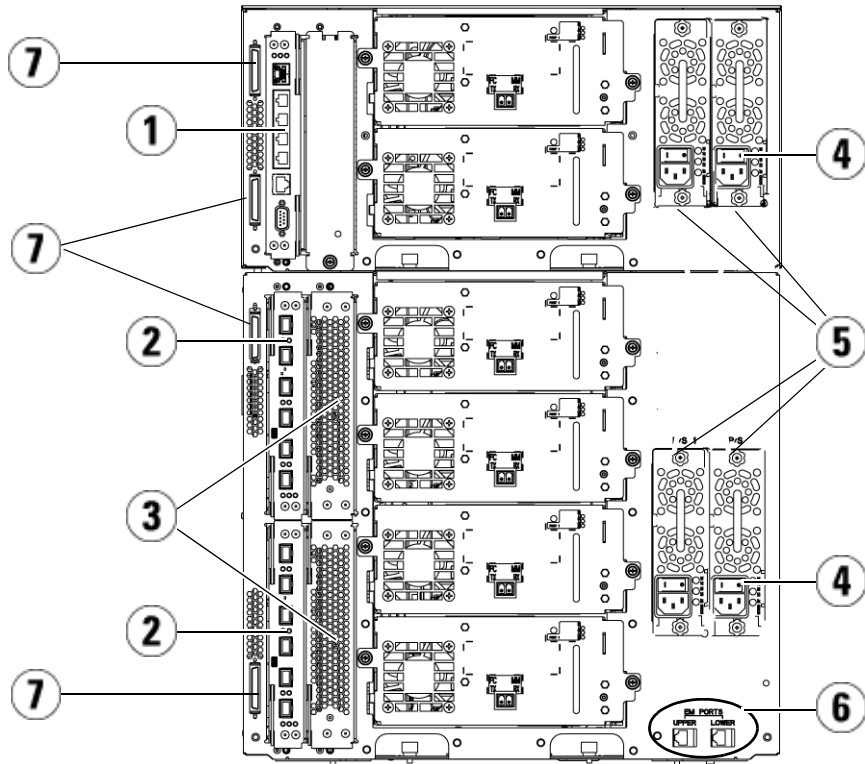
1   Library control blade (LCB)

2   FC I/O blade (optional)

3   FC I/O fan blades (required with FC I/O blades)

4   Rear power switch

5   Power supplies

6   Upper and lower Ethernet ports on expansion
    module

7   Module terminator connectors

Rear Power Switches   Rear power switches are located on each power supply. Turning off the
rear power switch on a power supply removes all power from the library.

The rear power switches should be used in all emergency and service situations.

> **Warning:** Turn off the rear power switch whenever you are servicing the library. In the event of danger to personnel or property, immediately turn off the rear power switch and remove all power cords.

> **Caution:** Except in emergencies, use the shutdown procedure before switching off the rear power switch. See [Shutting Down, Powering Off, and Completely Removing Power](#) on page 238 for instructions on how to shut down the library.

Power System

The library supports single and redundant power configurations. The single power 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.

If you have redundant power supplies, you can "hot swap" a power supply (power to the library remains on while you exchange the hardware), and you can "hot add" power supplies to other modules (power to the library remains on while you are adding the hardware).

> **Caution:** At least one power supply must be plugged in at all times.

> **Warning:** The power outlet must be available near the library and must be easily accessible.

> **Caution:** The control module and each expansion module that contains drives must have at least one power supply for every four drives. You can add a redundant power supply to each module. Installing one power supply in one module and another power supply in another module does not provide redundant power; the two power supplies must reside in the same module.

The power system consists of the following components:

- Power supply
- AC power cord

The power supply has three light-emitting diodes (LEDs) that provide status information. These LED status indicators are green and blue in color.

- **Green** represents AC OK or DC OK.
- **Blue** represents swap-mode power status.

Figure 7 shows the power supply LEDs. For more information on the behavior of the LEDs, see Power Supply LEDs on page 508.

Figure 7 Power Supply LEDs
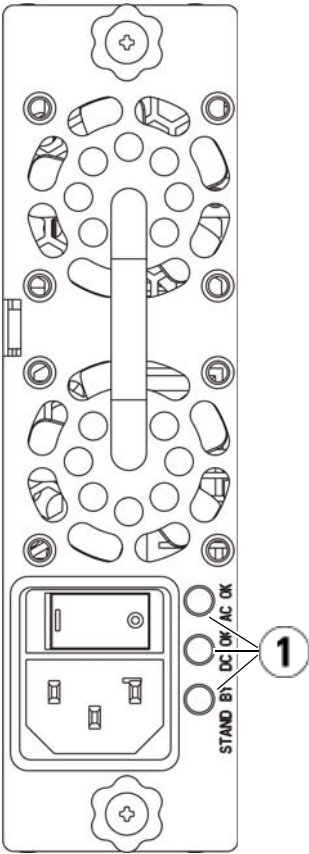
| 1 | LEDs |

Library Control Blade

The library control blade (LCB) manages the entire library, including the operator panel and picker assembly, and is responsible for running system tests to ensure that the library is functioning properly. The LCB also provides internal communication to Fibre Channel (FC) I/O blade slots. The LCB has four Ethernet ports, supporting a total of four FC I/O blades in the library.

The LCB indicates its status with three LED Reliability, Availability, and Serviceability (RAS) status indicators. These indicators are green, amber, and blue in color.

- **Green** represents processor status.

- **Amber** represents health status.

- **Blue** represents power-control status.

Figure 8 shows the location of the LCB components, including LEDs. For more information on the behavior of the LCB LEDs, see Blade Port LEDs on page 503.

Figure 8 Library Control Blade
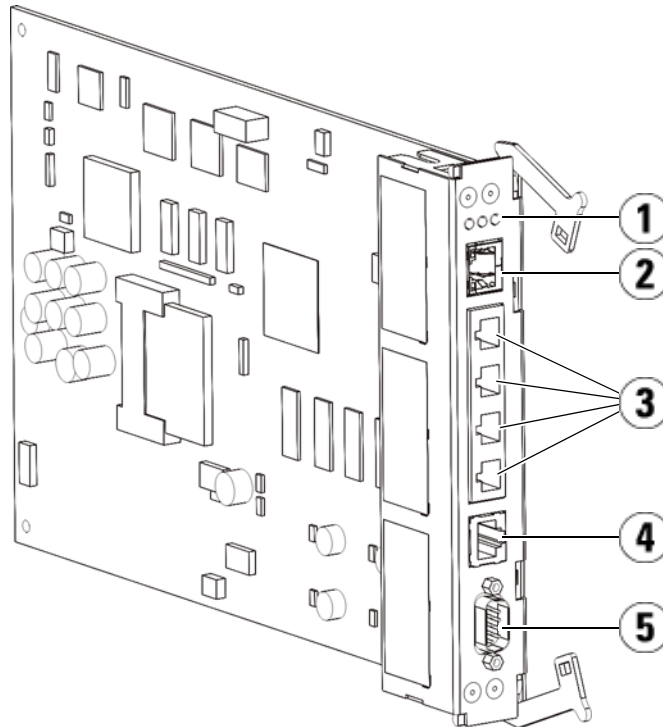
1   LEDs (blue, amber, green)

2   Gigabit Ethernet (external network) port

3   Ethernet I/O blade control ports (inactive if FC I/O
     blades are not installed)

4   Service Ethernet port

5   Service serial port

**Fibre-Channel
Input/Output Blades**

Expansion modules support optional Fibre Channel (FC) Input/Output
(I/O) blades that provide connections for FC tape drives in the library.
Each FC I/O blade has an embedded controller that provides
connectivity and features that enhance the performance and reliability of
tape drive operations. I/O blades also aggregate FC tape drive
connections, reducing switch port and cabling requirements.

Each FC I/O blade has six auto-negotiating, 4 Gb/s FC ports and backplane connections. The FC I/O blade provides two host communication ports and four connection ports to FC drives. Each FC I/O blade is cooled by a fan blade that is installed next to the FC I/O blade in the expansion module. FC I/O blades and fan blades are hot-swappable.

FC I/O blades cannot be installed in the control module, so your library configuration must include at least one expansion module to include FC I/O blades. Each expansion module can house up to two FC I/O blades. Depending on the number of installed expansion modules, the library can support from one to four FC I/O blades. No library configuration can contain more than four FC I/O blades. Any FC drive in the library, including drives in the control module, can be connected to an FC I/O blade in an expansion module.

> **Note:** FC I/O menu commands are available for use only when FC I/O blades are installed in the library.

The FC I/O blade indicates its status with three LED status indicators. These indicators are green, amber, and blue in color.

- **Green** represents processor status.

- **Amber** represents health status.

- **Blue** represents power-control status.

Figure 9 shows the FC I/O Blade, including LEDs. For more information on the behavior of the FC I/O Blade LEDs, see Blade Status LEDs on page 500.

For information on configuring I/O blades, see Working With FC I/O Blades on page 109.

For information on installing and cabling FC I/O blades and FC tape drives, see Chapter 12, Installing, Removing, and Replacing.

Figure 9 FC I/O Blade
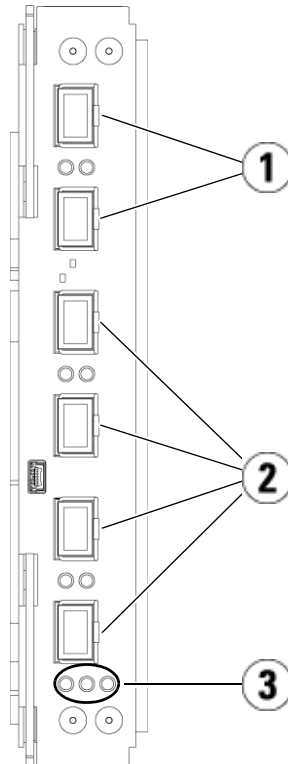
1	FC ports to host(s)
2	FC ports to drive(s)
3	LEDs (blue, amber, green)

Each FC I/O blade is cooled by a fan blade that is installed next to the FC I/O blade in the expansion module. For information on installing the fan blade, see Adding, Removing, and Replacing the FC I/O Fan Blade on page 454.

Figure 10 shows the FC I/O fan blade, including the LED. The single amber LED represents health status. For more information on the behavior of the FC I/O fan blade LED, see Tape Drive LEDs on page 505.

Figure 10 FC I/O Fan Blade
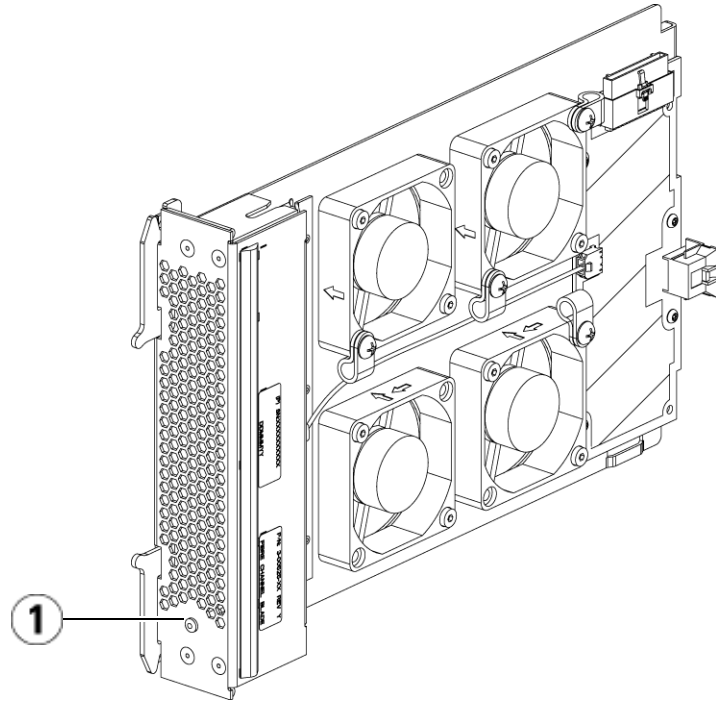
1	LED (amber)

Robotic System and Barcode Scanner

The robotic system identifies and moves the cartridges between the storage slots, tape drives, and the I/E station. The robotic arm (picker) has picker fingers that enable it to grab tape cartridges and move them into positions along X, Y, and Z motion coordinates. The robotic system and the barcode scanner work together to identify the locations of resources within the library.

Each tape cartridge must contain a barcode that the barcode scanner reads during the inventory process. During the inventory process, the

barcode scanner reads the fiducial labels to identify the types of magazines and tape drives that are installed in the library.

Every tape cartridge must have a unique machine-readable barcode attached to it. Tape cartridges cannot have duplicate barcode labels. This barcode identifies the cartridge. The library stores the physical location of the tape cartridge in an inventory database. All library or host requests typically reference the location of the tape cartridges based on this barcode number. Barcode labels are mandatory and must adhere to specific standards. For more information on barcodes, see Chapter 14, Working With Cartridges and Barcodes.

Tape Drive Support

Details about tape drive support include:

- Every library configuration must contain at least one tape drive.
- Control modules can hold a maximum of two tape drives.
- Expansion modules can hold a maximum of four tape drives.

Please see Supported Components on page 524 for a list of tape drives and media supported by the Scalar i500 library.

The library supports mixing different tape drive types within the library and within partitions. For information on how to do this, see Working With Partitions on page 68.

SCSI and SAS tape drives are attached directly to the host. FC tape drives can be directly attached to hosts or to the Storage Area Network (SAN). FC tape drives can also be attached to FC I/O blades, which manage communication between the hosts and the drives. For more information on FC I/O blades, see Working With FC I/O Blades on page 109. HP LTO-5 Fibre Channel tape drives can use the library's Storage Networking features (see Chapter 6, Storage Networking).

Tape drives are installed into tape drive slots in the rear of the library. If a tape drive slot is empty, a filler plate covers the empty tape drive slots to prevent debris from entering the library. Tape drives are shipped filling

the tape drive slots from the bottom to the top of the library, but the tape drives can be reinstalled in any available tape drive slot.

> **Note:**   Tape drive filler plates must be in place for the library to operate at normal speed.

For information on adding tape drives, see <u>Adding a Tape Drive</u> on page 438.

Library Features

This section describes several features of Scalar i500 libraries.

User Interface

The operator panel is located on the front door of the control module and allows you to work locally on the library via the user interface. The Web client allows you to view and perform library functions from remote sites and is accessible through a browser. The operator panel and Web client contain a similar user interface and functionality.

See <u>Chapter 2, Understanding the User Interface</u> for more information about the operator panel and the Web client.

Partitions

Partitions are virtual sections within a library that present the appearance of multiple, separate libraries for purposes of file management, access by multiple users, or dedication to one or more host applications.

Organizing the library into partitions divides the resources into virtual sections. Partitions can be used to control access to portions of the library by granting permissions to user accounts to access certain partitions.

For more information on partitions, see <u>Working With Partitions</u> on page 68.

Control Path Modification

The control path tape drive is used to connect a partition to a host application. Only one tape drive can be selected as the control path at one time. For more information, see <u>Working With Control Paths</u> on page 86.

Support for WORM

Scalar i500 tape libraries support WORM (write once, read many) technology in LTO-3, LTO-4, LTO-5 and LTO-6 tape drives. WORM allows non-rewriteable and non-erasable data to be written and provides extra data security by prohibiting accidental data erasure. The WORM feature is supported whenever you use WORM cartridges.

Licensable Features

In addition to the standard features, the following additional, licensable features are available for the Scalar i500:

- Advanced Reporting, described in <u>Chapter 4, Advanced Reporting</u>
- Capacity on Demand, described in <u>Chapter 5, Capacity on Demand</u>
- Storage Networking, described in <u>Chapter 6, Storage Networking</u>
- Encryption Key Management, described in <u>Chapter 7, Encryption Key Management</u>

If you purchase these features with your library, the license will be installed when you receive the library. If you upgrade or add new features after the initial purchase, you will need to obtain and install a license key. For information on how to obtain and install a license key, see <u>Obtaining and Installing a License Key</u> on page 88.

Understanding the Location Coordinates

This section describes the numbering system the library uses to identify components of the library. The library location coordinates contain the following digits: [Module],[Column],[Slot]. <u>Figure 11</u> shows how a

library with a control module and an expansion is numbered.

> **Note:** The library location coordinates are different from the logical element addressing; see <u>Understanding Logical Element Addressing</u> on page 35 for more information.)

Figure 11 Library Location
Coordinates
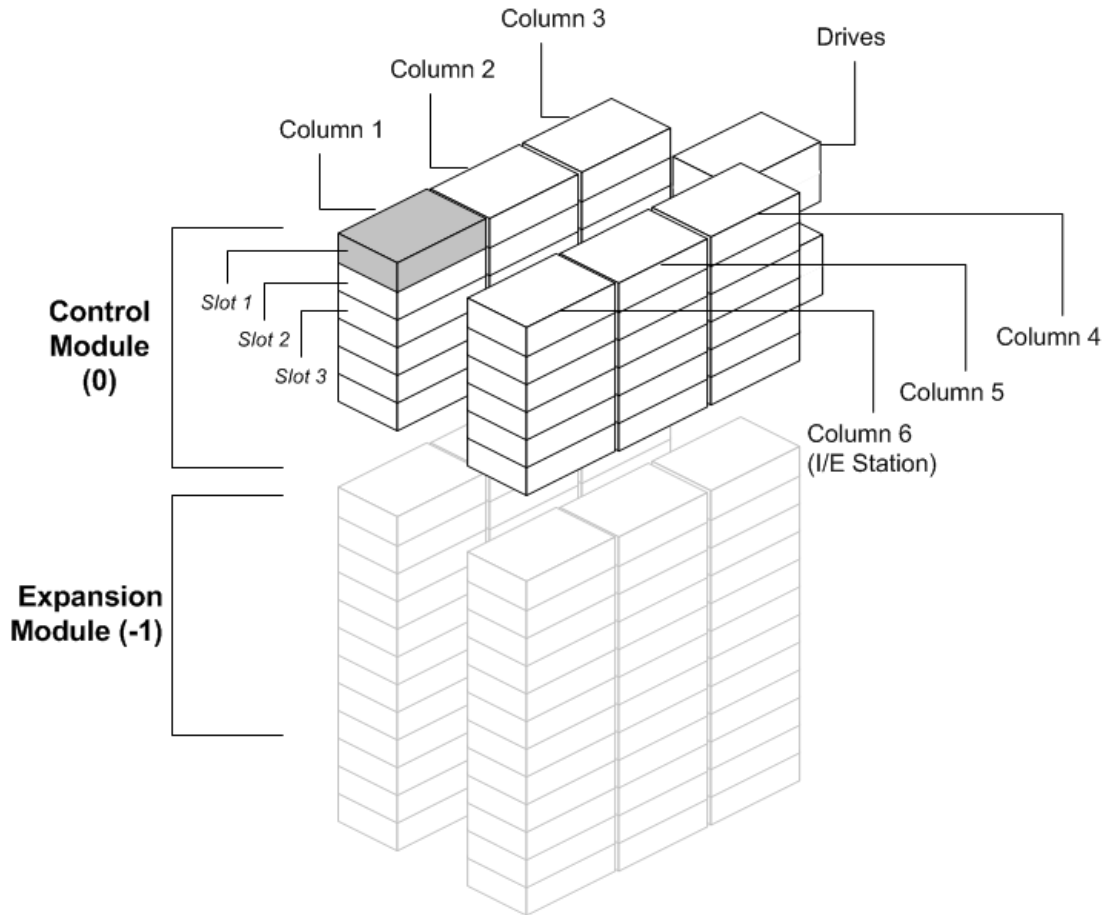
Modules

Library modules are represented by the first digit of a library coordinate. Modules are identified relative to the control module.

The control module is numbered 0 (zero). Expansion modules stacked above the control module are addressed with positive integer digits depending on their position above the control module. For example, the expansion module stacked directly above the control module is number 1. The expansion module stacked directly above module 1 is number 2, and so on.

Modules stacked below the control module are numbered with negative integer digits, also depending on their relative position to the control module. For example, the expansion module stacked directly below the control module is number –1. The expansion module stacked directly below module –1 is number –2, and so on.

Columns

A storage column is a group of slots arranged vertically in the library. Columns are represented by the second digit of a library coordinate. Columns are identified relative to the front left of the library. The column in the front left of the library is number 1. The column numbering continues around the library in a clockwise direction. The I/E station column is always number 6.

Slots

Fixed storage slots are represented by the third digit of the library location coordinate. Within each column, slots are numbered from top to bottom, starting at 1. For example, in Figure 11 on page 33, the full location coordinate of Slot 1 is 0, 1, 1.

Tape Drives

Tape drives are addressed first by module and then by tape drive bay within the module. The drive bays within a module are numbered from top to bottom. A one-based numbering system is used. The full address of a tape drive is in the form of [module,drive bay]; for example: [0,1], [1,3], [-1,2].

Fibre Channel I/O Blades

Fibre Channel (FC) I/O blades are addressed first by module and then by FC I/O blade bay within the expansion module. The blade bays within a module are numbered from top to bottom. A one-based numbering system is used. The full address of a an FC I/O blade bay is in the form of [module,FC I/O blade bay]; for example: [1,1], [-1,2].

Ethernet Expansion Blades

Ethernet Expansion Blades (EEBs) are addressed first by module and then by EEB bay within the expansion module9U Library Expansion Module. The blade bays within a module are numbered from top to bottom. The blade bay is always on the bottom of the unit. A one-based numbering system is used. The full address of a an EEB blade bay is in the form of [module,EEB]; for example: [1,2], [-1,2].

Power Supplies

Power supplies are addressed as [module,PS#], where *PS#* is 1 for the left power supply and 2 for the right power supply. The PS# is also etched on the module chassis, above each power supply.

Understanding Logical Element Addressing

The library uses standard industry conventions to logically number every storage slot, I/E station slot, and tape drive in the library. Host software is designed to understand this addressing system, and generally there are no problems relating to tape cartridge slots. However, hosts sometimes have problems relating to tape drives, particularly when tape drives, library control modules, or library expansion modules are added or removed, or empty tape drive slots exist. This section explains how the library logically addresses tape drives and slots, so that you can avoid common problems with host software.

> **Note:**   The logical element addressing described in this section is different from the library-specific location coordinates described in <u>Understanding the Location Coordinates</u> on page 32.)

Tape Drive Logical Element Addressing

Tape drive logical element addresses are assigned by partition. The numbering is sequential within a partition and starts over with each partition. The addresses start with the lowest library module in a partition. The top tape drive in the module and partition is always number 256. The tape drive beneath that is 257, and so on until all tape drives in that module/partition have been accounted for. Numbering

continues with the top tape drive in the next module up. Empty tape drive slots are skipped (they are not given an element address).

Host software may have problems recognizing tape drives when tape drives, control modules, or expansion modules are added, removed, or replaced; or when partitions are added, deleted, or modified, because existing logical element addresses can change. Therefore, after making any of these types of modifications, you must refresh the configuration of any backup application that manages the library to reflect new tape drive positions. In addition, you may need to reboot the host server(s) or rescan the bus to detect the changes.

See for a simple example of element addressing in a 14U library with a single partition, six tape drives installed and no empty tape drive slots. Note that multiple partition can create complexity. If you need help with the element addressing in your library, contact Quantum Support.

Cartridge Slot Logical Element Addressing

Tape cartridge slots are assigned logical element addresses by partition. The numbering is sequential within a partition and starts over with each partition. Numbering begins at the top left slot (as you look at the library from the front) in the lowest module in the library and moves sequentially down the left-most column. The top left slot of every partition is always number 4096, the slot beneath that is 4097, and so on. When the numbering reaches the bottom of the column, it continues to the top slot in the next column to the right (as long as it is in the same module and partition) and moves down that column. When all of the slots in the lowest module belonging to a partition have been accounted for, numbering continues to the top left slot in the next module above (as long as it is in the same partition). The numbering can get tricky when partitions span modules and do not use all of the slots in a module.

Tape cartridge slots are assigned a logical element address whether they contain a cartridge or not. Cartridges themselves are not given a logical element address; only the slot is. Slot element addresses change when slots are added or removed; partitions are added, removed, or modified; or cleaning slots are added or removed.

I/E station slots are numbered differently from partitions. Numbering begins at the top I/E station slot in the uppermost module that contains I/E station slots, and continues sequentially downward. This top slot has element address 16. The slot beneath that is 17, and so on.

Cleaning slots belong to the System partition and are not reported to the host. Cleaning slots are skipped (they are not given a logical element address), so adding or removing a cleaning slot will renumber all of the slots in a partition.

Generally, host software easily recognizes logical slot element addresses, even when they change. The next time the host issues a READ ELEMENT STATUS command, it will process the new number and recalculate all of the slot addresses.

See <u>Figure 12</u> on page 38 for a simple example of element addressing in a 14U library with a single partition.

Figure 12 Logical Element
Addressing, 14U, One Partition,
Six Tape Drives Installed

4183	4191	4199		260	Drv Bay 5	4207	4215	
4184	4192	4200		261	Drv Bay 6	4208	4216	16
4185	4193	4201		**CM 0**		4209	4217	17
4186	4194	4202				4210	4218	18
4187	4195	4203				4211	4219	19
4188	4196	4204				4212	4220	20
4189	4197	4205				4213	4221	21
4190	4198	4206				4214	4222	
4096	4111	4126		256	Drv Bay 1	4141	4156	
4097	4112	4127		257	Drv Bay 2	4142	4157	4171
4098	4113	4128		258	Drv Bay 3	4143	4158	4172
4099	4114	4129		259	Drv Bay 4	4144	4159	4173
4100	4115	4130		**EM -1**		4145	4160	4174
4101	4116	4131		**Note: Empty drive bay		4146	4161	4175
4102	4117	4132		element addresses are		4147	4162	4176
4103	4118	4133		skipped. This picture		4148	4163	4177
4104	4119	4134		assumes six tape drives are		4149	4164	4178
4105	4120	4135		installed.**		4150	4165	4179
4106	4121	4136				4151	4166	4180
4107	4122	4137				4152	4167	4181
4108	4123	4138				4153	4168	4182
4109	4124	4139				4154	4169	
4110	4125	4140				4155	4170	

Tape cartridge slots in partition

I/E station slots

Tape drives

Unused slots

Understanding the User Interface

The user interface of Scalar i500 libraries is available in two formats: the operator panel and the Web client. Operations on the library can be performed locally on the control module using the operator panel or remotely on your computer using the Web client. Similar functionality with common elements is used for both formats.

Both the Web client and operator panel user interfaces are required to operate the library. Some functionality is only available through the Web client, and some functionality is only available through the operator panel. However, using the Web client rather than the operator panel to perform library operations (when possible) is recommended.

Caution:	Do not perform inventory operations (for example, working with RAS tickets, creating/modifying/deleting partitions) while the library is performing an inventory. Doing so may result in inventory discrepancies, such as missing tape cartridges.

This chapter covers:

- Common User Interface Elements
- Operator Panel
- Web Client
- Menu Trees

- User Privileges

- User Access

Common User Interface Elements

The user interface consists of the following areas:

- **Header** — appears on every screen and contains the company logo, product name, and the three main navigation buttons. The main navigation buttons are:

  - **Home** — Home page.

  - **Help** — Context-sensitive Help for the active screen.

  - **Logout** — Ability to log out.

- **Title Bar/Menu Tabs (operator panel)** — This area appears below the header. On the home page, it provides the library/partition name and access to the menu tabs on the main screen. On all other screens, this area is a single bar and provides the screen name.

- **Menu Bar (Web client)** — Lists the menu choices.

- **Main** — Main content area of the screen.

- **Health/Navigation** — provides information about the "health" of the library by means of three subsystem status buttons: **Library**, **Drives**, and **Media**. See System Summary and Subsystem Status on page 42 for more information on the subsystem buttons.

> **Note:** A message in the header alerts you when the robot is not ready to perform library functions. See Troubleshooting "Library Not Ready" Messages on page 490 for more information on "Library Not Ready" messages displayed in the header.

Figure 13 and Figure 14 show the operator panel and the Web client interfaces.

Figure 13 Operator Panel User Interface
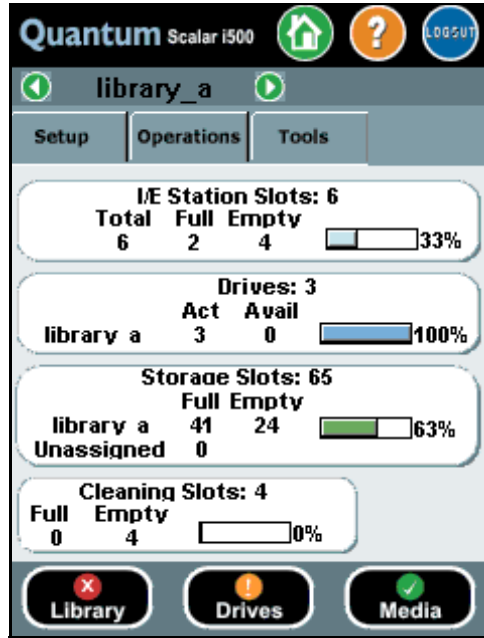
Figure 14 Web Client User Interface
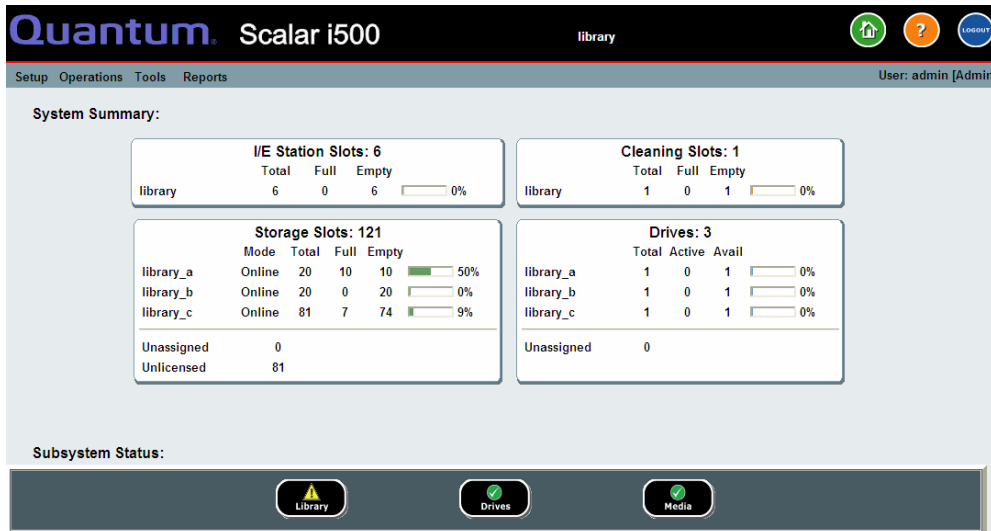
System Summary and Subsystem Status

You can quickly gauge the health of the library by observing the color of the three subsystem status buttons located at the bottom of the home page. These buttons provide quick access to information about the "health" of the library for faster recovery if problems occur. You can select the buttons to view Reliability, Availability, and Serviceability (RAS) tickets that report problems in the subsystems.

The three subsystems are:

- **Library** — This subsystem represents connectivity, control, cooling, power, and robotics.
- **Drives** — This subsystem represents tape drive components, such as tape drives, tape drive firmware, and tape drive sleds.
- **Media** — This subsystem represents media components, such as cartridges and barcode labels.

Each subsystem button will be in one of three states indicated by color. The three states are:

- **Green** — No RAS tickets exist for this subsystem, or, if any tickets do exist, they have all been closed.
- **Yellow** — The library contains open or unopened, low- or high-priority RAS tickets for this subsystem.
- **Red** — The library contains open or unopened urgent RAS tickets for this subsystem.

If the color of a subsystem button is red or yellow, you can click the button to display the corresponding **RAS Tickets** screen. This screen lists library, drives, or media RAS tickets, depending on which button was selected. RAS tickets display in order of last occurrence of each event, starting with the most recent.

Note:	**Last Occurrence** indicates the last time a ticket event occurred. This information updates any time the event recurs. **Last Occurrence** does NOT update if you open, close, or resolve the RAS Ticket.

You can change the order in which the RAS tickets are displayed by clicking any header item (for example, Priority, Last Occurrence, or Name).

On the Web client, you can view closed tickets by selecting the **Include Closed Tickets** check box.

You can also open the **All RAS Tickets** screen by selecting **Tools > All RAS Tickets**. See About RAS Tickets on page 481 for more information about RAS tickets.

Home Page

The home page is common to both the operator panel and the Web client. The home page provides tabular data on the capacity of the library's partitions, slots, and drives. You can use the home page to see a quick summary of the capacity of the library. You can also see which partitions are online (in the Storage Slots section). The current user's login privileges determine the information that is displayed on the home page.

Details about the home page include:

• On the Web client, users see the partitions (in alphabetical order) to which they have access.

• On the operator panel, if users have access to more than one partition, they can navigate to other partitions using the arrows next to the partition name in the title bar at the top of the screen.

For more information about user privileges, see User Privileges on page 50 and Working With User Accounts on page 97.

Operator Panel

The operator panel is physically attached to the front door of the control module. The user interface appears on the touch-screen LCD display of the operator panel for executing basic library management functions. Audible feedback, or "key click" sounds, are generated when a user presses a button on the operator panel. Users can choose to disable the audible feedback. See Configuring System Settings on page 126.

Operator Panel Keypads

When a user touches a text box requiring data entry, a keypad screen appears. The alpha, numeric, or month keypad appears, depending on the type of input field touched. All alphabetic character entries are lower case. The text box appears at the top of screen, and the numbers/characters appear as they are entered. Pressing **123** opens the numeric keypad.

Operator Panel Indicates Intervention Required

The operator panel lights up (screen saver turns off) if intervention is required. For example, when manual cartridge assignment is enabled, the operator panel lights up following an import of tapes into the I/E station so that the operator sees the prompt to assign tapes to a partition.

Web Client

The Web client user interface is similar to the operator panel user interface. The Web client interface is accessible from supported Web browsers. See <u>Library Capacity</u> on page 526 for information about supported browsers.

To manage the library from a remote location, you must set up the library's initial network configuration from the operator panel touch screen. See <u>Configuring Library Security Settings</u> on page 124 for information on setting the network configuration settings for remote use.

You must disable Web browser popup blockers to use the Web client interface and the library's online Help. Add the Scalar i500's Internet Protocol (IP) address to the list of trusted/allowed sites on your Scalar i500-supported browser, so the Web client pages will automatically refresh.

Note:	Do not use your Internet browser **Back** button to navigate the Web client pages. Instead, use the buttons provided within the Web client.

Note:	Log out of the library before closing the Internet browser window when you are using the Web client. If you do not log out, the session will remain open.

Menu Trees

The following menus organize operations and commands into logical groupings:

- The **Setup** menu consists of commands that administrators can use to set up and configure various aspects of the library, including partitions, I/E station slots, cleaning slots, control paths, network settings, drive settings, users, notifications, date and time, licenses, FC I/O blades, library registration, and e-mail.

- The **Operations** menu consists of commands that enable users to change the library's mode of operations, import and export cartridges, load and unload tape drives, move media, perform diagnostics, and log off. Administrators can also access commands to lock or unlock the I/E station and to shut the library down.

- The **Tools** menu consists of commands that you can use to maintain your library, such as viewing RAS Tickets, generating diagnostic logs, identifying drives, configuring the internal network, saving and restoring the library configuration, setting system and security settings, and updating firmware.

- The **Reports** menu (Web client only) consists of summaries of library information.

A hidden **Service** menu is available to service users with the appropriate login information.

The menus vary somewhat between the Web client and operator panel user interfaces. Administrators have access to all menu commands; users with user privileges have more limited access.

Table 1 lists the Web client menus. Some menu commands are available only to administrators.

I/O blade menu items are available for libraries that contain I/O blades.

Table 1   Web Client Menus

Setup Menu[*]	Operations Menu	Tools Menu[*]	Reports Menu
• **Setup Wizard**	• **Media**	• **All RAS Tickets**	• **System Information**
• **Partitions**	• Move	• **Capture Snapshot**	• **Library Configuration**
• **Host Access**	• Import	• **Save/Restore Configuration**	• **Network Settings**
• Host Registration	• Export	• **E-mail Configuration Record**	• **Logged In Users***
• Host Connections	• **Cleaning Media**	• **Save Configuration Record**	• **All Slots**
• **Cleaning Slots**	• Import	• **Identify Drives**	• **Log Viewer***
• **I/E Station Slots**	• Export	• **Drive Operations**	• **Advanced Reporting***
• **Drive Settings**	• **Partitions**	• **Download SNMP MIB**	• Drive Resource Utilization
• **Control Path**	• Change Mode	• **FC I/O Blade Info****	• Media Integrity Analysis
• **License**	• **Drive**	• **FC I/O Blade Port Info****	• **About**
• **Notifications**	• Load	• **EKM Management**	
• E-mail Configuration	• Unload	• Import Communication Certificates	
• Advanced Reporting (if licensed)	• Change Mode	• Encryption Certificate	
• Receiver Addresses	• **I/E Station Lock/Unlock***	• Import	
• Media Security	• **System Shutdown***	• Export	
• RAS	• **Logout**	• Encryption Key	
• Receiver Addresses		• Import	
• Contact Information		• Export	
• **Network Management**		• Retrieve SKM Logs (if SKM enabled)	
• Network			
• SNMP			
• SNMP Trap Registrations			

Setup Menu[*]	Operations Menu	Tools Menu[*]	Reports Menu

• **User Management**
  • User Accounts
  • Remote Authentication
• **FC I/O Blades****
  • Port Configuration
  • Channel Zoning
  • Host Mapping
  • Host Management
  • Host Port Failover
  • Data Path Conditioning
  • FC I/O Blade Control
• **Encryption** (if licensed)
  • System Configuration
  • Partition Configuration
• **System Settings**
• **Date & Time**
• **Register Library**
		• **Update Library Firmware**
		• **Diagnostics**	

[*]Administrators only. [**]Available only when the library contains I/O blades.

Table 2 lists the operator panel menus. Some menu commands are available only to administrators. I/O blade menu items are available for libraries that contain I/O blades.

Table 2   Operator Panel
Menus

Setup Menu[a]	Operations Menu	Tools Menu
• **Partition Mgmt**	• **Move Media**	• **All RAS Tickets[a]**
• Create Partition	• **Import Media**	• **Capture Snapshot[a]**
• Delete Partition	• **Export Media**	• **Drive Mgmt[a]**
• Configure I/E Station Slots	• **Import Cleaning Media**	• Clean drive
• Configure Cleaning Slots	• **Export Cleaning Media**	• Reset drives
• **User Mgmt**	• **Change Partition Mode**	• **Drive Info**
• Create User	• **Load Drive**	• **About Library**
• Modify User	• **Unload Drive**	• Network Info
• **Drive Settings**	• **Change Drive Mode**	• View Drive Info
• Fibre	• **Lock/Unlock I/E Station[a]**	• Partition Info
• SCSI	• **Shutdown[a]**	• **Internal Network[a]**
• SAS		• **System Settings**
• **Notification**		• User Session Timeout (minutes)[a]
• E-mail Alerts		• Touch Screen Audio
• E-mail Account		• Unload Assist[a]
• Customer Contact		• Logical SN Addressing[a]
• **Licenses**		• Manual Cartridge Assignment[a]
• **Date & Time**		• Disable Remote Service User[a]
• **Network Mgmt**		• Enable SSL
• IP version 4		• Enable SNMP V1/V2
• IP version 6 (if enabled)		• Enable IPv6
• Port Settings		• Enable SMI-S
• **Control Path**		• Unlabeled Media Detection

Setup Menu[a]	Operations Menu	Tools Menu
• **FC I/O Blades[b]**		**Security[a]**
• Port Configuration		• Network Interface
• Channel Zoning		• SSH Services
• Host Mapping[c]		• ICMP
• Host Management[c]		• Remote UI
• Host Port Failover		• SNMP
• Data Path Conditioning		• SMI-S
• FC I/O Blade Control		**Display Settings**
		• Brightness
		• Contrast
		• Defaults
		• **Library Tests[a]**
		• Installation & Verification Tests
		• Library Demo
		• View Last Summary Log
		• View Last Detailed Log
		• E-mail Last Detailed Log
		• **Blade Info[b]**
		• Port Info
		• **Command History Log[ab]**

[a]Administrators only. [b]Available only when the library contains I/O blades. [c]Visible only when host mapping has been enabled.

User Privileges

User privilege levels are manually assigned to user accounts created within the library. Controlling access to screens and operations within the library preserves the integrity of the library and the data that is stored in it. See Working With User Accounts on page 97 for more information on setting user privilege levels.

Three types of users are defined in Scalar i500 libraries:

- **Administrators** have access to the entire physical library and all of its partitions, and can configure the library and set up user and administrator accounts. The library ships with a default administrator account. The user name for the default administrator account is **admin** and the password is **password**. You cannot modify or delete the user name for the default administrator account, but you can modify the password. If you misplace the password for the default administrator account, contact Quantum Technical Support (see Getting More Information or Help on page 8).

- **Users** have access to one or more assigned partitions, as well as portions of the **Operations** and **Reports** menus. Users cannot access the **Setup** and **Tools** menus. Users can perform functions within a partition (such as performing cartridge and tape drive operations), but cannot set up or configure the library (for example, creating or deleting partitions).

- **Service** has access to the entire physical library and all of its partitions as well as to a hidden **Service** menu that includes service and diagnostic tools. Each library has only one service account.

Details on user privileges include:

- The library can contain eighteen user accounts (user or administrator or both), including the default administrator account.

- Eighteen user (user or administrator or both) sessions can be active at one time.

- The same user can be logged in to a library from multiple remote locations.

- Clicking the close button (**X**) in the upper-right corner of the Web client closes the browser window but does not log the user or administrator out.

- All users are logged out automatically after a configurable period of inactivity. The default user session timeout period is 30 minutes, but administrators can change the user session timeout to a value from 15 minutes to 480 minutes (eight hours). See Configuring System Settings on page 126.

- A screen saver is invoked after 10 minutes of inactivity on the operator panel. After an hour of inactivity, the screen will appear black. If the user has not been logged out for inactivity, touching the operator panel will reactivate it, returning the user to the screen last in use. (The Web client does not use a screen saver.)

- An administrator can disable any access to the library from the Web client. For more information, see Configuring System Settings on page 126.

- When a service user logs in, all other active users are automatically logged out.

- For security purposes, an administrator can prevent a service user from logging on to the library remotely, from either the Web client or over the Ethernet service port. The service user will still be able to log on to the library from the operator panel interface. For more information, see Configuring System Settings on page 126.

User Access

Administrators have access to the entire library. Users with user privileges can only access some of the menus. See Table 1 on page 46 for the Web client menu tree and privilege level information. See Table 2 on page 48 for the operator panel menu tree and privilege level information.
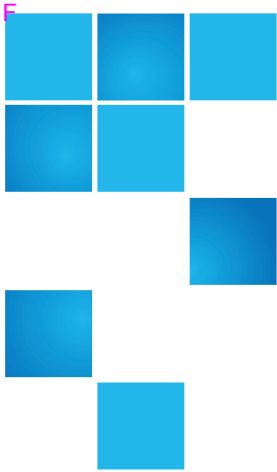
Configuring Your Library

Once you have installed the hardware as described in the *Scalar i500 Getting Started Guide*, you are ready to configure your library's settings. A Setup Wizard helps you get started configuring your library, and menu commands on both the operator panel and the Web client allow you to reconfigure your library at any time.

Caution:	Always save the library configuration after modifying configurable items. This will allow you to restore the most current settings if necessary. See <u>Saving and Restoring the Library Configuration</u> on page 488.

This chapter covers:

- <u>About the Setup Wizard</u>
- <u>Using the Setup Wizard</u>
- <u>Accessing the Web Client</u>
- <u>Managing the Network</u>
- <u>Working With Partitions</u>
- <u>Configuring Cleaning Slots</u>
- <u>Configuring I/E Station Slots</u>
- <u>Setting Tape Drive Parameters</u>
- <u>Working With Control Paths</u>

About the Setup Wizard

When you first power on the library, the operator panel displays the Setup Wizard, which walks you through the initial configuration of the library's basic operational settings.

The Setup Wizard on the operator panel only runs once, at initial startup. After that, administrators access the Setup Wizard any time via the Web client or use commands on the **Setup** and **Operations** menus to modify all library settings, including network settings. See Completing the Library Configuration With Menu Commands on page 54.

While completing the Setup Wizard at initial startup is recommended, you may need to begin using the library locally immediately. In this case, you can cancel out of the Setup Wizard and allow the library to run on the default configuration settings. See <u>Default Configuration Settings</u> on page 57.

For additional information, see <u>Using the Setup Wizard</u> on page 55.

Using the Default Administrator Account

When you power on the library for the first time, you do not need to log in to use the operator panel. You can start using the **Setup Wizard** immediately. After the initial setup session on the operator panel, however, you will need to log in to the operator panel as well as the Web client.

The library ships with a default administrator account. The user name on the account is **admin** and the password is **password**. When you see the **Login** screen on the operator panel or Web client, type **admin** in the **User Name** text box and **password** in the **Password** text box. As soon as the initial setup is complete, you should change the password on the default administrator account. For information on changing passwords, see <u>Modifying Local User Accounts</u> on page 98.

Note:	You cannot delete the default administrator account or modify the user name. You can, however, change the password.

Note:	If you misplace the password for the default administrator account, contact Quantum Technical Support (see <u>Getting More Information or Help</u> on page 8).

Completing the Library Configuration With Menu Commands

The Setup Wizard is an aid to assist you with the initial configuration of the library. The Setup Wizard, however, contains only a subset of configuration tasks. The operator panel tabs and Web client menus provide access to all configuration options that are included in the Setup Wizard and many that are not. Once the initial Setup Wizard session is complete, administrators can choose whichever method is most convenient or necessary for modifying library settings.

The following topics cover using the Setup Wizard as well as Setup and Operations commands to configure the library. Paths to open the appropriate screens on both the operator panel and the Web client are

given for each task. For the operator panel, the paths refer to the navigation tabs at the top of the home page. For the Web client, the paths refer to the menus.

For the menu trees on both the operator panel and Web client, see <u>Menu Trees</u> on page 45.

> **Note:** Power cycling (powering the library on and off) is not necessary to configure the library.

Using the Setup Wizard

The Setup Wizard simplifies the process of configuring the library. When you first power on the library, the operator panel displays the Setup Wizard. After that, you can no longer access the Setup Wizard from the operator panel. You can always access the Setup Wizard from the **Setup** menu on the Web client.

The recommended procedure for using the Setup Wizard for the initial configuration is as follows:

1 Turn on the library and begin using the Setup Wizard on the operator panel.

2 Work through all of the screens as prompted (see <u>Setup Wizard Tasks</u> on page 57).

3 When you get to the network configuration screens, configure the network settings as follows:

> **Note:** You cannot log into the Web client until you have configured the network settings.

- **If you are using IPv4:** On the **Setup Wizard: Enable IPv6** screen, do NOT select the **Enable IPv6** check box. Click **Next**. Configure the network settings.

- **If you are using IPv6:** On the **Setup Wizard: Enable IPv6** screen, select the **Enable IPv6** check box and click **Next**. You have enabled IPv6 but you will not be prompted to configure IPv6 settings here. Continue with the Setup Wizard screens. Then, when you are finished using the Setup Wizard, configure the IPv6 network settings by going to **Setup > Network Mgmt** on the operator panel.

4 Log out of the operator panel.

5 Using the default administrator account, log in to the Web client. Type **admin** in the **User Name** text box and **password** in the **Password** text box.

6 Complete the **Setup Wizard** screens on the Web client interface. The final **Setup Wizard** screen will prompt you to apply your settings.

When you have completed the **Setup Wizard**, the Library Configuration report appears on the Web client. The Library Configuration report provides information on the library's tape drives, partitions, I/E stations, storage slots, cleaning slots, and loaded media. See <u>Viewing the Library Configuration Report</u> on page 268 for more information on the Library Configuration report.

> **Note:** Depending on the size of the library, there may be a slight delay after you apply the settings in the Setup Wizard while the Library Configuration report page loads.

Details on using the **Setup Wizard** include:

- The only time that you do not need to log in to the library is when the Setup Wizard appears on the operator panel the first time the library is powered on.

- After a timeout period of one hour, the Setup Wizard will close, and you will be logged out of the library. Use the default administrator account to log in to the operator panel.

- If you time out of the Setup Wizard or do not complete all the Setup Wizard screens, the library will apply the default configuration settings plus whatever modifications you made (see <u>Default Configuration Settings</u> on page 57).

- You cannot log in to the library from the Web client until you have configured network settings on the operator panel. To change IPv4 settings and configure IPv6 settings, go to **Setup > Network Mgmt**.

- You can return to the **Setup Wizard** from the Web client.

- Any administrators you create will also be able to use the Setup Wizard from the Web client as well as **Setup** and **Operations** menu commands to reconfigure the library.

- If necessary, you can cancel out of the **Setup Wizard** on the operator panel and begin using the library locally with the default settings in place. If you accept the default network configuration settings, you will not be able to access the library remotely from the Web client. You can, however, use **Setup > Network Mgmt** on the operator panel at any time to modify network settings. See Default Configuration Settings on page 57 for more information.

Default Configuration Settings

The default configuration settings are as follows:

- **License keys:** COD, 41 slots minimum. The total number depends on number of pre-activated slots purchased.

- **Network settings:** DHCP enabled, IPv6 disabled

- **Import/export (I/E) station slots:** 6

- **Cleaning cartridge slots:** 0

- **Partitions:** By default, the library creates partitions and assigns available library resources proportionately among the partitions, grouping tape drives according to distinct combinations of tape drive interface type (SCSI, FC, or SAS) and tape drive vendor. To mix tape drive types/vendors within a partition, create partitions manually. See Manually Creating Partitions on page 71.

See also About the Setup Wizard on page 53.

Setup Wizard Tasks

As you work through the **Setup Wizard** screens, follow the on-screen instructions.

The **Setup Wizard** screens contains only a subset of all configuration options. The **Setup** and **Operations** menus contain most configuration options, including those in the **Setup Wizard**. This section includes detailed descriptions of the configuration tasks, including how and when to access them through the **Setup** and **Operations** menus.

- Welcome (operator panel) — Welcomes you to the **Setup Wizard**.

- Hardware Installation (operator panel) — Reminds you to install tape drives and the Ethernet cable.

- <u>Setting the Date, Time, and Time Zone</u> (operator panel and Web client) — Allows you to set the date and time on your library.

- <u>Managing the Network</u> (operator panel) — Allows you to configure your IPv4 network settings for remote access using the Web client. Allows you to enable IPv6 so that you can configure IPv6 network settings later using **Setup > Network Mgmt**.

- <u>Applying a License Key</u> (operator panel and Web client) — Allows you to enter license keys for licensable features. For more information, see <u>Obtaining and Installing a License Key</u> on page 88.

- <u>Configuring Cleaning Slots</u> (operator panel and Web client) — Allows you to configure dedicated cleaning slots. Configuring at least one cleaning slot enables the AutoClean feature.

- <u>Configuring I/E Station Slots</u> (operator panel and Web client) — Allows you to configure import/export (I/E) station slots.

- <u>Working With Partitions</u> (operator panel and Web client) — Allows you to set the number of library partitions.

- **Confirm Settings** (operator panel and Web client) — Allows you to confirm your library settings.

> **Caution:** Always take a library snapshot and save the library configuration after modifying configurable items. If modifying items results in problems, the library snapshot will help technical support personnel to troubleshoot the problem. Saving the library configuration will allow you to restore the most current settings if necessary. For more information on taking a library snapshot and saving and restoring the library configuration, see <u>Saving and Restoring the Library Configuration</u> on page 488.

> **Note:** Setup Wizard operations cannot be performed concurrently by multiple administrators logged in from different locations. You can access the screens, but you cannot apply changes while another administrator is performing the same operation.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Setup > Setup Wizard**.

- From the operator panel, the **Setup Wizard** is available only upon first power-on of library.

Accessing the Web Client

Once you have configured network settings on the operator panel, you can log on to the library's Web client.

The operator panel network configuration screen lists the IP address of the library. Use this IP address to access the Web client using a Web browser. When typing the IP address into the Web browser, make sure to precede it with **http://**; for example, **http://123.123.123.123**.

Managing the Network

Administrators can configure the following:

- Network settings that allow remote access to the library. For more information, see <u>Modifying Network Settings</u> on page 60.

- Secure Socket Layer (SSL) settings that increase data protection so that data from the library can be sent over the internet securely. For more information, see <u>Enabling SSL</u> on page 62.

- Simple Network Management Protocol (SNMP) settings that allow you to use an external management application to monitor the status of the library. For more information, see <u>Configuring SNMP Settings on the Library</u> on page 63.

> **Caution:** Security settings must be enabled to allow SNMP, SMI-S, and IP address access to the library network. These security settings are enabled by default. For more information, see Configuring Library Security Settings on page 124.

Modifying Network Settings

The operator panel Setup Wizard allows administrators to configure network settings that allow remote access to the library from the Web client. You must initially configure network settings from the operator panel. After the initial configuration, you can modify the network settings from either the operator panel or the Web client.

From the operator panel, you can modify the following network settings: library name, stateless configuration enable/disable (IPv6 only), static IP configuration enable/disable (IPv6 only), DHCP enable/disable, IP address, subnet mask, network prefix, and default gateway.

From the Web client, you can use the **Setup - Network** screen to modify the following network settings: library name; Dynamic Host Configuration Protocol (DHCP) enable/disable; stateless autoconfiguration enable/disable (IPv6 only); static IP enable/disable (IPv6 only), IP address; subnet mask (IPv4 only); net prefix (IPv6 only); and default gateway address.

In addition, from the Web client, when DHCP is disabled, can configure the primary and secondary Domain Name System (DNS) server addresses. DNS servers provide IP address resolution of fully qualified domain names. DNS settings are optional.

If you modify the IP address, you will need to type the new IP address in the **Address** field of your Web browser to access the Web client.

> **Note:** Make sure that the library is connected to the network before modifying network settings. If the Ethernet cable is not installed properly, you cannot configure the network settings. Install one end of the Ethernet cable in the top Ethernet port of the library control blade (LCB) just below the three LEDs. The LCB is located at the back of the control module. Make sure the other end of the Ethernet cable is installed in the appropriate LAN port on your LAN.

Details on network settings include:

- **Library Name** is the network name you want to assign to the library. The library name is limited to 12 lowercase alphanumeric characters and dashes (-).

- **DHCP** defaults to enabled. When DHCP is enabled, the library obtains an IP address automatically. If DHCP is not enabled, you must manually enter an IP address, default gateway, and subnet mask/net prefix.

- **IPv4 addresses** must be entered in dot notation (for example, 192.168.0.1). They are limited to numeric characters and do not allow values exceeding 255 for dot-separated values.

- **IPv6 addresses** must be entered in the proper notation. IPv6 address can be entered in the most common notation, as eight groups of four hexadecimal digits. 2001:0ff8:55cc:033b:1319:8a2e:01de:1374 is an example of a valid IPv6 address. Also, if one or more of the four-digit groups contains 0000, you can omit the zeros and replace them with two colons (::), as long as there is only one double colon used in an address. Using this notation, 2001:0ff8:0000:0000:0000:0000:01de:1374 is the same as 2001:0ff8::01de:1374.

- **IP Address** is the IP address of the library. For IPv4, this text box is available only if DHCP is disabled.

- **Default Gateway Address** is the IP address of the default gateway for your portion of the Ethernet network. For IPv4, this text box is available only if DHCP is disabled.

- **Subnet Mask** (IPv4 only). Text box is available only if DHCP is disabled.

- **Network Prefix** (IPv6 only).

- **Primary DNS Address** (optional, Web client only) must be entered as an IP address. This text box is available only if DHCP is disabled.

- **Secondary DNS Address** (optional, Web client only) must be entered as an IP address. This text box is available only if DHCP is disabled.

- **Port Settings** (operator panel only) allows you to change the autonegotiate mode, speed, and duplex settings on the Ethernet port.

> **Caution:** Modifying network settings will modify network connectivity parameters, requiring remote communication configuration changes. Your current Web client browser session might become invalid, requiring you to close your current browser session. Access the Web client using the new network configuration settings and log in again.

> **Note:** Be sure to add your library's IP address to the list of trusted/allowed sites on your library-supported browser, so the Web client pages automatically refresh.

> **Note:** For step-by-step network configuration instructions, see your library's online Help. To access the online Help system, click the **Help** icon at the top right of the Web client or operator panel user interface.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Setup > Network Management > Network**.

- From the operator panel, select **Setup > Network Mgmt**.

Enabling SSL

Administrators can enable or disable SSL settings on the library. Enabling SSL settings encrypts all Web browser connections to the Web client, and it enables SSL-based authentication for SMI-S. SMI-S is the newest standard of SNMP, which makes sets of data continuously available. SMI-S is disabled by default. You can enable SMI-S on the **Tools > System Settings** screen on the operator panel.

The default SSL setting is **Disabled**. Disabling SSL settings creates an unencrypted connection from a Web browser to the Web client.

See the *Scalar Intelligent Libraries SMI-S Reference Guide (6-01317-xx)* for further configuration and access details.

> **Note:** Before enabling SSL settings, make sure you enter a name for
> the library in the **Library Name** text box when configuring
> network settings (**Setup > Network Mgmt** on the operator
> panel). After enabling SSL settings, use that library name to
> access the library. If you do not use that name, you will receive
> a security alert. In addition, make sure to complete all the text
> boxes listed on the Web client **Contact Information** screen
> (**Setup > Notification > Contact Information**) before enabling SSL
> settings. This information is used to identify company
> information in the SSL certificate.

You cannot enable the SSL settings from the Web client. The path to open
the appropriate screen is as follows:

- From the operator panel, select **Tools > System Settings > Enable SSL**.

**Configuring SNMP
Settings on the Library**

SNMP is a light-weight protocol designed for remote management and
monitoring of infrastructure devices. The library provides SNMP
support, so an external management application can be configured to
receive library SNMP information. The library supports SNMP by
publishing a Management Information Base (MIB) that can be queried to
obtain the status of the library and many of its individual components.
SNMP information can be obtained from the library using SNMP Traps
and GET queries.

For more information about SNMP, see the *Scalar i500 Basic SNMP
Reference Guide (6-01370-xx)*. For information on integrating MIBs with an
SNMP management application, contact your network management
application vendor.

Administrators can perform the following SNMP procedures:

- Register the IP addresses and port numbers of external management
  applications, enabling them to receive SNMP traps from the library.
  For more information, see <u>Registering External Management
  Applications</u> on page 64.

- Enable or disable support for SNMP v1 and v2c. SNMP v3 is enabled
  by default and cannot be disabled. For more information, see
  <u>Enabling SNMP Versions</u> on page 65.

- Choose which version of SNMP the library uses to report traps. You
  can choose SNMPv1 or SNMPv2. The default is SNMPv1.

- Modify the default SNMP community string, which is used as a password to authenticate GET and GET-NEXT SNMP v1 and SNMP v2c messages exchanged between the library and a remote management application. For more information, see Modifying the SNMP Community String on page 66.

- Enable or disable SNMP authentication traps, which are messages indicating an authentication failure. For more information, see Enabling and Disabling SNMP Authentication Traps on page 67.

- Download the library MIB, which can be used to integrate the library with an SNMP management application. For more information, see Downloading the SNMP MIB on page 67.

Registering External Management Applications

Administrators can register transport protocols, IP addresses, and port numbers of external management applications to enable them to receive SNMP traps from the library. (By default, the library ignores all SNMP SET operations, so external management applications cannot register themselves to receive SNMP traps from the library.)

After registering the transport protocols, IP addresses, and corresponding port numbers, you can perform a test to verify that the library can send the SNMP traps to the addresses.

When registering external management applications to receive SNMP traps, you can set the following parameters:

- **Transport** — The transport protocol. This should be the same as the transport protocol configured on the SNMP trap receiver. Select one of the following:

  - UDP/UDP6 — User Datagram Protocol. For IPv4, select UDP; for IPv6, select UDP6.

  - TCP/TCP6 — Transmission Control Protocol. For IPv4, select TCP; for IPv6, select TCP6.

- **Host Name/IP Address** — The host name or the IP address of the external management application you want to register. A host name may be entered only if DNS is enabled. Otherwise, IP addresses must entered. For information on DNS, see Modifying Network Settings on page 60.

- **Port** — the port number of the external application you want to register. The default port number for an external application is 162.

- **Create** — Adds the IP address and port number of the external application to the list of registered addresses that will be sent SNMP traps.

- **Delete** — Allows you to delete a selected IP address and port number.

- **Test** — Verifies only that the library has sent SNMP traps to all registered IP addresses. Check the external applications to verify that the traps were received.

  While the test is in progress, the **Progress Window** appears. If the test is successful, **Success** appears in the **Progress Window** and the traps were successfully sent. If the test is unsuccessful, **Failure** appears in the **Progress Window**. Follow the instructions listed in the **Progress Window** to resolve any issues that occur during the operation.

See the *Scalar i500 Basic SNMP Reference Guide (6-01370-xx)* for further configuration and access details.

Note:	This operation should not be performed concurrently by multiple administrators logged in from different locations. You can access the appropriate screens, but you cannot apply changes while another administrator is performing the same operation.

The path to open the appropriate screen is as follows:

- From the Web client select **Setup > Network Management > SNMP Trap Registrations**.

Enabling SNMP Versions

The library supports SNMP v1, v2c, and v3.

Administrators can enable or disable support for SNMP v1 and v2c. The recommended practice is to disable SNMP v1 and SNMP v2c in highly secure environments.

SNMP v3 is always enabled and cannot be disabled. The authentication algorithm is set to MD5, and the encryption is disabled system-wide.

See the *Scalar i500 Basic SNMP Reference Guide (6-01370-xx)* for further configuration and access details.

The paths to open the appropriate screens are as follows:

- From the Web client select **Setup > Network Management > SNMP**.

- From the operator panel select **Tools > System Settings > Enable SNMP V1/V2**.

Choosing SNMP Trap Versions

The library supports SNMP v1 and v2 traps as defined by RFC 1157 (v1 is the default). Administrators can choose which version the library uses to report traps (v1 is the default)

The timeout for all SNMP requests to the library must be at 10 seconds or greater (command line parameter-t).

The path to open the appropriate screen is as follows:

- From the Web client select **Setup > Network Management > SNMP**.

Modifying the SNMP Community String

Administrators can modify the SNMP community string. The SNMP community string is a text string that acts as a password to authenticate GET and GET-NEXT SNMP v1 and SNMP v2c messages exchanged between the library and an external management application. The SNMP community string used by the library must match the string used by the external management application.

The default SNMP community string on the library is: **publicCmtyStr**. For security purposes, this string should be modified. When modifying the community string, adhere to the following guidelines: the community string is case-sensitive, cannot be empty, and cannot exceed 32 characters.

See the *Scalar i500 Basic SNMP Reference Guide (6-01370-xx)* for further configuration and access details.

You cannot modify the SNMP community string from the operator panel.

The path to open the appropriate screen is as follows:

- From the Web client select **Setup > Network Management > SNMP**.

Enabling and Disabling SNMP Authentication Traps

Administrators can enable or disable SNMP authentication traps. When the library receives an SNMP message that does not contain the correct community string or other authentication information, the library sends an SNMP authentication trap message to registered remote management systems, indicating the authentication failure. SNMP authentication traps are disabled by default.

See the *Scalar i500 Basic SNMP Reference Guide (6-01370-xx)* for further configuration and access details.

You cannot enable or disable SNMP authentication traps from the operator panel. The path to open the appropriate screen is as follows:

- From the Web client select **Setup > Network Management > SNMP**.

Downloading the SNMP MIB

The library supports an SNMP MIB that can be used to integrate the library with commercial SNMP management applications. The MIB can be queried to obtain the status of the library and many of its individual components. Administrators can download the SNMP MIB from the library. The MIB can then be installed on an SNMP external management application.

For more information about the library MIB, see the *Scalar i500 Basic SNMP Reference Guide(6-01370-xx)* or contact Quantum Technical Support (see Getting More Information or Help on page 8). For information on integrating MIBs with an SNMP management application, contact your network management application vendor.

> **Note:** The SNMP MIB is also available on the *Scalar i500 Documentation and Training* CD.

You cannot download the SNMP MIB from the operator panel. The path to open the appropriate screen is as follows:

- From the Web client select **Tools > Download SNMP MIB**.

Working With Partitions

Partitions are virtual sections within a library that present the appearance of multiple, separate libraries for purposes of file management, access by multiple users, or dedication to one or more host applications. The library must contain at least one unassigned tape drive and slot to create a partition.

The **Setup Wizard: Partitioning** screens allow administrators to select the number of new library partitions to create.

At any time after the initial configuration of the library, administrators can create, modify, and delete partitions by selecting **Setup > Partitions** on the Web client, or create and delete partitions by selecting **Setup > Partition Mgmt** on the operator panel.

There are two ways to create partitions:

- **Automatically —** Library resources are assigned proportionately among the partitions. Tape drives are grouped according to their interface type (SCSI, FC, or SAS), tape drive vendor, and media generation (LTO-3, LTO-4, LTO-5, LTO-6). You cannot mix interface type, tape drive vendor, and media generation in partitions that you create automatically. To create a partition with mixed interface types, tape drive vendors, and media generations, you must create the partition manually. You can create partitions automatically on either the operator panel or the Web client. When you automatically create partitions, you add to the number of existing partitions.

- **Manually —** An administrator creates one partitions at a time and allocates resources as desired. You can mix tape drive interface types, tape drive vendor, and media generations in partitions that you create manually. You can create partitions manually only on the Web client. When you manually create partitions, you add to the number of existing partitions.

> **Note:** You may not mix drive vendor types (for example, HP and IBM) in partitions that are configured for library managed encryption (see <ins>Step 6: Configuring Partitions for Library Managed Encryption</ins> on page 180).

The maximum number of partitions that can be created is equal to the number of drives in the library. Table 3 shows the possible number of partitions that can be created for each of the available library configurations.

Table 3   Number of Partitions Supported

Available Configurations	Tape Drives Minimum, Maximum	Partitions Minimum, Maximum
5U	1, 2	1, 2
14U	1, 6	1, 6
23U	1, 10	1, 10
32U	1, 14	1, 14
41U	1, 18	1, 18

Details on partitions include:

• Administrators can create, modify, delete, and control access to all partitions. Users can be given access to only certain partitions and denied access to others.

Partition names are limited to 12 lower-case alphanumeric characters and underscores (_).

• The maximum number of partitions that can be created is equal to the number of tape drives in the library.

• At minimum, a partition consists of one tape drive and one slot. The tape drive or slot cannot be shared with another partition.

• I/E station slots are shared between all partitions. Partitions take temporary ownership of I/E station slots when importing or exporting tape cartridges.

> **Caution:** Before permanently removing an expansion module from your library, you need to perform a set of configuration operations that includes deleting all partitions. See Deleting Partitions on page 74 and Removing the Expansion Module on page 365.

Automatically Creating Partitions

At any time after the initial configuration of the library, administrators can add to the number of existing partitions by using the automatic partitioning process. Automatic partitioning assigns available library resources proportionately among the partitions, grouping tape drives according to their interface type (SCSI, FC, or SAS), tape drive vendor, and media generation. The default number of partitions created is the number of distinct tape drive interface/vendor/media type combinations of the tape drives that are not currently assigned to a partition. You cannot mix tape drive interface types, vendors, or media generations in partitions that you create automatically. To create a partition with mixed interface types, vendors, and media generations you must create the partition manually (see Manually Creating Partitions on page 71).

 For example:

- If your library contains two tape drives, an FC IBM LTO-4 and an FC IBM LTO-5, two partitions would be created because although they have the same interface type, they have different media generations (LTO-4 and LTO-5).

- If your library contains two tape drives, a Fibre Channel IBM LTO-4 and a Fibre Channel HP LTO-4, two partitions would be created because the tape drive vendors are different.

On the **Automatically Create Partitions** screen, you can select the number of partitions to create, from a minimum of the default specified by the library to a maximum that equals the number of unassigned tape drives in your library.

The library must contain at least one unassigned tape drive and one unassigned slot to automatically create a partition. If no unassigned tape drives or slots exist, you must modify or delete one or more partitions to free up resources. For more information, see Modifying Partitions on page 73 and Deleting Partitions on page 74.

When the library automatically creates partitions, it creates control paths. See Working With Control Paths on page 86 for a description of the default control paths and how to change them.

By default, the library applies the Standard barcode format to each partition. You can change this setting by modifying the partitions after it has been created. For information on modifying partitions, see Modifying Partitions on page 73.

> **Note:** This operation cannot be performed concurrently by multiple administrators logged in from different locations. You can access the screen, but you cannot apply changes while another administrator is performing the same operation.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Setup > Partitions**.

- From the operator panel, select **Setup > Partition Mgmt > Create Partition**.

Manually Creating Partitions

Using the Web client, administrators can manually create additional partitions any time after the initial configuration of the library. The maximum number of partitions that can be created is equal to the number of drives in the library.

You can mix tape drive interface type, vendor, and media generation in partitions that you create manually. **Exception:** You may not mix tape drive vendor types (for example, HP and IBM) in partitions that are configured for library managed encryption (see Step 6: Configuring Partitions for Library Managed Encryption on page 180).

The library must contain at least one unassigned tape drive and slot to create a partition. If no tape drives or slots are available, you must modify or delete an existing partition to free up resources. For more information, see Modifying Partitions on page 73 and Deleting Partitions on page 74. When you manually create partitions, the library creates control paths. See Working With Control Paths on page 86 for a description of the default control paths and how to change them.

When creating partitions manually, you need to provide the following information:

- **Partition Name** — Limited to a maximum of 12 lower-case alphanumeric characters and underscores (_)

- **Emulation Type** — This setting allows the partition to appear as a different library type to the host. In most cases, you can ignore this setting and just use the default. However, if your host application does not support the default and cannot recognize the partition using

the default setting, you can choose a library type that your host has previously qualified. This makes the partition appear to the host as the selected library type and should allow the host to communicate.

- ADIC Scalar i500 (default)

- Quantum Scalar i500

- Quantum Scalar i2000

- ADIC Scalar i2000

- ADIC Scalar 100

- ADIC Scalar 24

- **Media Barcode Format** — This setting tells the library how to read and report barcodes of the tape cartridges in the partition. The library supports the following options (for definitions of each of the options, see <u>Supported Barcode Formats</u> on page 521).

  - **Standard** (default)

  - **Standard Six**

  - **Plus Six**

  - **Extended**

  - **Media ID Last**

  - **Media ID First**

- **Number of Slots** — The number of storage slots allocated to the new partition.

- **Drives** — The tape drive or drives assigned to the partition.

Note: Before creating partitions, verify that all tape drives are unloaded. For information on unloading tape drives, see <u>Unloading Tape Drives</u> on page 252.

Note: Creating Partitions operations cannot be performed concurrently by multiple administrators logged in from different locations. You can access the screen, but you cannot apply changes while another administrator is performing the same operation.

You cannot create partitions manually from the operator panel. The path to open the appropriate screen is:

• From the Web client, select **Setup > Partitions**.

Mixing Tape Drive Types Within Partitions

When you automatically create partitions, tape drives with different interface types, vendor types, and media generation are placed in different partitions. If you manually create partitions, you can mix tape drive types as follows.

• For non-encrypted partitions and for partitions that use Application Managed Encryption:

  • SCSI, FC, and SAS tape drives can be mixed.

  • HP and IBM tape drives can be mixed.

  • Different media generations (for example, LTO-3, LTO-4, LTO-5) can be mixed.

• For partitions that use Library Managed Encryption:

  • Tape drives must be FC or SAS. FC and SAS tape drives can be in the same partition.

  • **Q-EKM partitions** can only contain IBM LTO-4 and IBM LTO-5 tape drives.

  • **SKM partitions** can only contain HP LTO-4 and HP LTO-5 tape drives.

For more information on partitions with Library Managed Encryption, see Step 6: Configuring Partitions for Library Managed Encryption on page 180.

Modifying Partitions

Using the Web client, administrators can modify partition settings any time after the partition is created.

The tape drive set as the control path for a particular partition cannot be deleted from that partition. The check box associated with the control path is grayed out. For more information on setting the control path, see Working With Control Paths on page 86.

The library automatically takes the partition offline before modifying it and places the partition back online after it is modified.

> **Note:** If the operation does not complete successfully, the partition remains offline until you turn it back online manually or restart the library (see <u>Taking a Partition Online or Offline</u> on page 76).

When modifying a partition, you may need to provide the following information:

- **Emulation Type** — This setting allows the partition to appear as a different library type to the host. See <u>Manually Creating Partitions</u> on page 71 for a description and available options.

- **Partition Name** — limited to a maximum of 12 lower-case alphanumeric characters and underscores (_).

- **Media Barcode Format** — This setting tells the library how to read and report barcodes of the tape cartridges in the partition. The default selection is **Standard** (for definitions of each of the options, see <u>Supported Barcode Formats</u> on page 521).

- Number of Slots — the number of tape cartridge slots allocated to the partition.

- Drives — the tape drive or drives assigned to the partition.

> **Note:** Before deleting a tape drive from a partition, verify that it is unloaded. For information on unloading tape drives, see <u>Unloading Tape Drives</u> on page 252.

You cannot modify partitions manually from the operator panel. The path to open the appropriate screen is:

- From the Web client, select **Setup > Partitions**.

Deleting Partitions

A partition can be deleted when it is no longer needed or in preparation for removing a module from the library. Administrators can delete one partition at a time.

Unload all tape drives and export all cartridges assigned to the partition that is to be deleted. After exporting the cartridges, remove them from the I/E station. For more information, see <u>Unloading Tape Drives</u> on page 252 and <u>Exporting Media</u> on page 249.

Details about deleting partitions include the following:

- After a partition is deleted, its resources (for example, tape drives and slots) become available and can be reassigned to new or existing partitions.

- Deleting a partition does not delete users assigned to that partition. However, if these users are not assigned to other partitions, they will not be able to perform library operations. See Changing Partition Access on page 75.

- Because partitions may extend across the library's physical modules and share resources, the library will report errors if you permanently remove or replace a module in your library without first deleting or modifying partitions and modifying shared resources such as cleaning slots and I/E slots. See Preparing to Remove or Replace a Module on page 356 for detailed instructions on preparing your library for the permanent removal or replacement of a module.

> **Note:** You may need to modify settings in your host application as a result of deleting a partition. See your host application documentation.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Setup > Partitions**.
- From the operator panel, select **Setup > Partition Mgmt**.

Changing Partition Access

An administrator can control which partitions a specified user can access by modifying the user's account. Also, any user assigned to a partition that has been deleted can be reassigned to other partitions.

To change partition access, you must provide the following information:

- **Password** — A unique password that can be viewed and modified by the administrator.

- **Privilege Level** — Determines the user's access privileges. See User Privileges on page 50 for more information on user privilege levels.

- **Partition Access** — the partitions to which the user has access.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Setup > User Management > User Accounts**.

- From the operator panel, select **Setup > User Mgmt > Modify User**.

Taking a Partition Online or Offline

There are two partition modes: online and offline.

- **Online** — SCSI hosts control the partition. In this mode, all host application SCSI commands are processed.

- **Offline** — SCSI hosts cannot control the partition. In this mode, library operations can be performed via the operator panel or Web client.

This topic focuses on using the library user interface to manually change a partition mode to online or offline. Changing a partition mode using the library user interface may affect your host application. See your host application documentation for more information.

Details about changing the partition mode include:

- When you access the **Change Partition Mode** screens, you will see only partitions to which you have been given access.

- The **Online/Offline** buttons toggle between modes.

- If a partition is in use, the **Online/Offline** button is grayed out.

- Restarting the library will bring all offline partitions back online (see).

Note: Some maintenance activities require that the entire library be taken offline. To take the library offline, change the mode of all partitions from online to offline.

Note: When changing the partition mode from online to offline, all host application commands in progress at the start of the mode change are completed.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Operations > Partitions > Change Mode**.

- From the operator panel, select **Operations > Change Partition Mode**.

**Disabling/Enabling
Manual Cartridge
Assignment**

Administrators can disable or enable manual cartridge assignment. When manual cartridge assignment is enabled (the default setting), the **Assign I/E** screen automatically appears on the operator panel once cartridges are placed into the I/E station. The **Assign I/E** screen prompts you to use the operator panel to assign the cartridges to a specific partition or to the system partition.

When manual cartridge assignment is disabled, the **Assign I/E** screen does not appear on the operator panel, and the cartridges in the I/E station remain unassigned until they are moved or imported into the library.

For more information on how manual cartridge assignment affects importing of media, see .

You can disable manual cartridge assignment by clearing the **Manual Cartridge Assignment** check box on the operator panel **System Settings** screen. For more information on system settings, .

Manual cartridge assignment cannot be configured from the Web client. The path to open the appropriate screen is as follows:

- From the operator panel, select **Tools > System Settings**.

Understanding Host Application Notification

When manual cartridge assignment is enabled, SCSI Unit Attention 6/2801 notifies the host application when the I/E station has been accessed, allowing the host to automatically detect the presence of media in the I/E station and update its I/E station status information.

When manual cartridge assignment is disabled, host notification via SCSI Unit Attention 6/2801 depends on the number of configured partitions:

- If multiple partitions are defined, the host application is not notified when the I/E station has been accessed. Media presence in the I/E station is reported to any partition requesting it.

- If a single partition is defined, the host application is notified when the I/E station has been accessed. Media presence is reported to the sole defined partition, as well as to the system partition, when either of these partitions checks for changes in the status of the I/E station.

For information about using the host to perform tape operations, see your host application documentation.

Configuring Cleaning Slots

Cleaning slots are used to store cleaning cartridges that are used to clean tape drives. The **Setup Wizard: Cleaning Slot Configuration** screens prompt you to enter the number of cleaning slots (if any) you want to designate for your library. You can also access the **Cleaning Slot Configuration** screens directly on the operator panel and Web client.

> **Note:** Only slots that are licensed, unassigned, and empty can be used for cleaning. If there are unassigned slots, but no cleaning slots available, make sure there are no RAS tickets for unassigned media.

The **Setup Wizard** default configuration settings include zero dedicated cleaning slots. Configuring at least one cleaning slot enables the library's AutoClean feature. When AutoClean is enabled, the library allows you to import and export cleaning cartridges. When a tape drive needs cleaning, it notifies the library. If AutoClean is enabled, the library automatically cleans the tape drive using a cleaning cartridge loaded in a cleaning slot.

> **Note:** If you configure zero I/E station slots, you will not be able to import or export cleaning cartridges using I/E stations. See Configuring I/E Station Slots on page 79.

Cleaning slots are not assigned to specific partitions. Each partition can access cleaning cartridges located in the dedicated cleaning slots.

The maximum number of cleaning slots that can be configured is four. To disable AutoClean, configure zero cleaning slots.

Administrators can configure cleaning slots during the initial library configuration and at any time after that, as long as unassigned slots are

available. If no slots are available in the library, you must modify or delete a partition to free up slots. For more information see <u>Modifying Partitions</u> on page 73 and <u>Deleting Partitions</u> on page 74.

Administrators can also clean tape drives manually. For information, see <u>Manually Cleaning Tape Drives</u> on page 260.

Note: Cleaning slots are not visible to the host application. To choose host-based cleaning, do not configure any cleaning slots, and configure your host application to manage cleaning tape drives. Configuring cleaning slots on the library may affect the host application. See your host application documentation for information.

Note: This operation should not be performed concurrently by multiple administrators logged in from different locations. You can access the screen, but you cannot apply changes while another administrator is performing the same operation.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Setup > Cleaning Slots**.

- From the operator panel, select **Setup > Partition Mgmt > Configure Cleaning Slots**.

Configuring I/E Station Slots

I/E station slots are used to import and export tape cartridges into and out of the library without disrupting normal library operations. The **Setup Wizard: I/E Station** screens allow you to configure I/E station slots. Administrators can also configure these slots on either the operator panel or the Web client.

Each control module contains six I/E station slots, and each expansion module contains 12 I/E station slots. The available library configurations support a minimum of six I/E slots in the 5U library to a maximum of 54 I/E slots in the 41U library configuration. You can also choose to

configure zero I/E station slots and use all slots in all I/E stations for tape cartridge storage. For more information on configuring zero I/E slots, see Configuring Zero I/E Station Slots on page 82.

Each I/E station (6-slot or 12-slot) is configured as a complete unit. When configuring an I/E station, configure all the slots in the I/E station the same way: all storage or all I/E slots.

If the library consists of a control module, all six I/E station slots must be configured either as storage or as I/E station slots. A 14U library consists of a control module (with six I/E station slots) and an expansion module (with 12 I/E station slots). All 12 of the slots in the expansion module must be configured the same way, as either I/E station slots or storage slots. Therefore, a 14U library can contain a minimum of six and a maximum of 18 dedicated I/E station slots. Table 4 lists the number of I/E station slots available per library for all base library configurations.

Table 4   Number of I/E Station
Slots Available

Library Configuration	5U Control Module		9U Expansion Module		Library Total	
	I/E Stations	I/E Slots	I/E Stations	I/E Slots	I/E Stations	I/E Slots
5U	1	6	–	–	1	6
14U	1	6	1	12	2	18
23U	1	6	2	24	3	30
32U	1	6	3	36	4	42
41U	1	6	4	48	5	54

Details on configuring I/E station slots include:

- Before changing the number of I/E station slots, remove all tape cartridges from any slots currently configured as I/E station slots.

- An I/E station that has been configured for storage may contain cleaning slots. These cleaning slots must be deleted before you can reconfigure the storage slots as I/E station slots.

- The default number of dedicated I/E slots is six. If you accept the **Setup Wizard** default configuration settings, six I/E slots will be created in the control module.

- If you increase the size of your library by adding expansion modules, the I/E stations in the new modules will be storage slots by default. You can select to reconfigure these slots as I/E slots.

- Based on the number of I/E slots you configure, the library automatically determines which I/E stations to configure as I/E slots and which to configure as storage.

- The library configures I/E slots in the control module I/E station first and then works outward to the I/E stations in the expansion modules. I/E stations in expansion modules below the control module have precedence over I/E stations in expansion modules above the control module.

- All slots in an I/E station must be configured the same way: as either storage or I/E slots. For this reason, if your library includes one or more expansion modules and you configure an even number of I/E slots greater than six, the control module I/E station may be configured automatically as storage.

- If the I/E station is configured as data storage slots, its door is always locked. For information on unlocking I/E stations, see Locking and Unlocking the I/E Stations on page 262.

- I/E station slots are shared by all partitions within a library.

- To identify how a specific I/E station magazine is configured, view the **Library Configuration** report available from the **Reports** menu on the Web client. See Viewing the Library Configuration Report on page 268.

Configuring Zero I/E Station Slots

Configuring zero I/E slots increases the number of storage slots in your library but has the following consequences:

- You will not be able to use the I/E station to import and export tape cartridges, including cleaning media.

- You will be required to open the library access door to bulk load and unload tape cartridges, disrupting library operations. See Bulk Loading on page 246.

- You will not be able to manually clean tape drives with a cleaning cartridge.

For more information on using the I/E station to import and export media, see Running Your Library on page 237.

Caution:	Configuring I/E station slots with cartridges already loaded compromises data security. First, remove cartridges from the I/E station and then configure the I/E station slots.

Note:	This operation cannot be performed concurrently by multiple administrators logged in from different locations. You can access the screen, but you cannot apply changes while another administrator is performing the same operation.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Setup > I/E Station Slots**.

- From the operator panel, select **Setup > Partition Mgmt > Configure I/E Station Slots**.

Setting Tape Drive Parameters

Administrators can view and modify certain tape drive parameters. You can set the SCSI ID for a SCSI-attached tape drive. You can set the loop IDs, topology connection mode, and interface speed for a Fibre-attached tape drive. You can view but not set parameters for SAS tape drives. A SAS tape drive's SAS address is automatically and uniquely generated based on a unique World Wide Node Name (WWNN) that the drive receives when it is configured.

If the affected partition is online, it will be taken offline before the parameters are set, and brought back online after they are set.

> **Note:** If the operation does not complete successfully, the partition remains offline until you turn it back online manually or restart the library (see <u>Taking a Partition Online or Offline</u> on page 76).

Each device on a SCSI bus, including the host bus adapter (HBA) needs to have a unique SCSI ID. Changing the SCSI ID is necessary when there is a duplicate ID on a single bus. Typically, the HBA SCSI ID is set to 7. For example, if two tape drives are connected together on the same bus, each tape drive must have different SCSI IDs and they must be different from the HBA SCSI ID.

For SCSI tape drives, you can set the SCSI ID to a value from 0 to 15. The library assigns the following default SCSI IDs to SCSI tape drives:

- Control module: 1 and 2

- Each expansion module: 3, 4, 5, and 6

For FC tape drives:

- **DPF** (Data Path Failover) — You can enable data path failover on HP LTO-5 Fibre Channel tape drives with a Storage Networking license by selecting the DPF check box (see).

- The loop ID can be set to a value from 0 to 125. A unique loop ID is selected by default for all FC tape drives installed in the library. For example, the tape drive installed in the top drive bay of a control module is assigned a default loop ID of 61. The tape drive installed in the control module's bottom drive bay is assigned a default loop ID of 63.

  If you change the default loop IDs, make sure each FC tape drive with a topology setting of Auto (LN), Loop (L), or Auto (NL) has a unique loop ID.

  You cannot change the Loop ID if the Topology is set to Point to Point.

- The requested topology connection mode can be set to one of the following:

  - **Auto (LN)** — Auto-configure trying L-Port first

  - **Loop (L)** — Force L-Port

  - **Point to Point** — Force N-Port

- **Auto (NL)** — Auto-configure trying N-Port first (default)

Notes About Point to Point:

- You can use Point to Point if the tape drive is connected via a switch.
- You can use Point to Point with HP drives if the tape drive is connected to a host.
- You cannot use Point to Point if the tape drive is connected directly to a host.
- You cannot use Point to Point if the tape drive is connected to an FC I/O blade.
- You must use Point to Point if the tape drive is being used for control path failover (see Configuring Control Path Failover on page 150) or data path failover (see Configuring Data Path Failover on page 154). If a tape drive is being used for control path failover or data path failover, you cannot change its topology from Point to Point to anything else.

- The requested interface speed can be set to Auto (default), 1 Gb/s, 2 Gb/s, 4 Gb/s, or 8 Gb/s (depending on drive type).

Caution: LTO-5 Fibre Channel tape drives can be configured for speeds of up to 8 Gb/s. If they are configured for 8 Gb/s, you should connect them directly to a host and not to an FC I/O blade, because the FC I/O blade only allows speeds up to 4 Gb/s. If you connect an LTO-5 Fibre Channel tape drive to an FC I/O blade, you must configure the tape drive speed to 4 Gb/s or less.

- If the requested FC topology and speed settings are not supported, the next appropriate settings are negotiated. On the Web client, the **Drive Settings** screen displays both the requested and the actual FC topology connection mode and interface speed. If FC drives are not connected to the host, the negotiated actual settings appear on the screen as "unknown."

Note: On the Web client, the **Drive Settings** screen displays tape drive information in tables. Bold column headings in the tables can be sorted. For example, selecting the **Location** column heading will sort by location coordinates.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Setup > Drive Settings**.
- From the operator panel, select **Setup > Drive Settings**.

Working With Control Paths

The control path tape drive is used to connect a partition to a host application.

The library automatically assigns control paths when you set up partitions. You can modify the control path at any time. Table 5 describes how these control paths are assigned and how to change them.

Table 5   Control Path
Assignment During Partition
Creation

If the library contains:	And the partition contains:	Then the default control path for the partition is:	If you want to change the control path, note the following:
No FC I/O blades	Any combination of tape drive interface types (SCSI, FC, or SAS)	The first tape drive assigned to the partition	You must select a tape drive as the control path.

If the library contains:	And the partition contains:	Then the default control path for the partition is:	If you want to change the control path, note the following:
One or more FC I/O blades	At least one FC tape drive	The FC I/O blade	Using the FC I/O blade as the control path allows you to utilize the LUN mapping and host port failover features. You can select a tape drive as control path if the tape drive is not connected to an FC I/O blade. However, it is recommended that you allow the FC I/O blade to be the control path for the partition. You cannot select a tape drive as control path if the tape drive is connected to an FC I/O blade.
One or more FC I/O blades	No FC tape drives	The first tape drive assigned to the partition	You must select a tape drive as the control path.

Only one tape drive in a partition can be selected as the control path per partition. In the event that the control path connection to the host application fails, you can select a new control path for the partition. Additionally, if the control path for the partition is an HP LTO-5 Fibre Channel tape drive and you have Storage Networking licensed on the library, you can select another HP LTO-5 Fibre Channel tape drive for control path failover (see Configuring Control Path Failover on page 150 for details).

The **Setup > Control Path** screens list a selected partition's tape drives, including the tape drive that is currently designated as the control path. You can designate a new control path for the partition by selecting a different tape drive. You can also disable a partition's control path by clearing the current control path selection.

Caution:	Do not select an FC tape drive as control path if it is connected to an FC I/O blade. The control path will be filtered out by the I/O blade and will not be visible to the host.

> **Note:** You may need to modify settings in your host application as a
> result of modifying the control path. See your host application
> documentation.

> **Note:** Bold column headings in the table can be sorted. For example,
> selecting the **Location** column heading will sort by location
> coordinates.

> **Note:** If you have more than one FC I/O blade in the library, each FC
> I/O blade will present each partition — that does not have a
> tape drive as the control path — as a target device to the host.
> Thus the host may see the same partition multiple times. To
> minimize confusion, you should configure host mapping so
> that each host sees each device only once. See Configuring
> Host Mapping on page 118.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Setup > Control Path**.

- From the operator panel, select **Setup > Control Path**.

Obtaining and Installing a License Key

Several features can be added to the standard library configuration either
with your initial purchase or afterward (see Licensable Features on
page 32).

This section describes how to license these features on your library, in the
following sections:

- About License Keys

- Viewing Licenses and License Keys

- Obtaining a License Key

- Applying a License Key

About License Keys

If you purchase a licensable feature with your library, the license will be installed when you receive the library. If you upgrade or add new features after the initial purchase, Quantum issues you a license key certificate. The license key certificate contains an authorization code that enables you to retrieve your license key from the Quantum Web site. Once you install the license key on the library, the feature becomes available.

Details about license keys include:

- An authorization code to obtain a license key can be used one time only.

- The license key may contain up to 12 alphanumeric characters. The license key can also contain the "at" (@), hyphen (-), or underscore (_) symbols. Alpha characters must be lowercase. The user interface automatically converts entries to lowercase.

- A given license key can only be used on the library to which it is assigned and cannot be transferred to another library. The key is verified when it is applied to the library to make sure it is the proper key associated with the library serial number.

- License keys do not expire.

- Once installed on the library, license keys cannot be removed (unless you replace the control module or the library control blade (LCB) compact flash card).

    - **If you replace the control module:** The license key is associated with the serial number of the control module. If you replace your control module, you must replace all your installed license keys. Request replacement license keys from Quantum.

    - **If you replace the LCB compact flash:** The LCB compact flash card contains information about your library configuration. If you replace your LCB compact flash card, you must reinstall your license key(s) onto the library. You may be able to reinstall them yourself if you have saved the license keys or can retrieve them from the Web sites listed above. In some cases, factory installed license keys will not be listed on the Web site and you will need to contact Quantum for a replacement. If you cannot retrieve your license keys or need assistance, contact Quantum.

Viewing Licenses and License Keys

To see the licenses you have purchased and obtained, go to: http://www.quantum.com/licensekeys.The license history for each feature is listed (feature licensed, amount licensed, authorization code, and date license key was obtained). The most recent license contains the full amount of the license for that feature (for example, the most recent COD license contains the total number of COD slots licensed) and replaces previous license keys.

To see which licensable features are enabled on your library, go to the **Licenses** screen:

• From the Web client, select **Setup > License**.

• From the operator panel, select **Setup > Licenses**.

Obtaining a License Key

To obtain your license key for a new feature or upgrade:

1 Contact your Quantum technical sales representative to submit your order for the feature or upgrade. See Getting More Information or Help on page 8.

2 Upon receipt of your order, Quantum will ship you a license key certificate containing your authorization code.

Note: **If you order more than 46 COD slots:**
COD licenses come in 46-slot increments. If you order more than 46 slots, you will receive more than one license key certificate. For example, if you want to activate 92 slots, you will receive two license key certificates. You need to follow the procedure outlined here twice, once for each certificate. However, because each additional license key replaces the previous ones, you only need to apply one license key (the final one) to the library.

---

3 On your library, locate the serial number. You will need the Serial Number to retrieve your license key from the Web site. To view the serial number:

• On the operator panel, select **Tools > About Library**, or

• On the Web client, select **Reports > About > Scalar i500**.

4 Access the Quantum License Key Management Web site at http://www.quantum.com/licensekeys.

5 In the **Serial Number** box, enter your serial number.

6 Click **Submit**.

If you have entered a valid serial number, the Web site displays existing license keys for this feature. Exception: If the license was applied at the factory, the word "**Factory**" may appear instead of the actual license key. If you need to retrieve the license key in this case, contact Quantum Technical Support (see <u>Contacts</u> on page 7).

7 Type the authorization code from your License Key Certificate in the **Authorization Code** text box.

8 Click the **Get License Key** button.

If you have entered a valid authorization code, the Web site allows you to retrieve the license key for your new feature or upgrade.

You are now ready to apply the license key to the library. See <u>Applying a License Key</u>.

Applying a License Key

A license key may be applied to the library during the initial configuration or whenever licensed features are purchased. If increased capacity is purchased, the new license key will replace the current license key.

> **Note:** This operation should not be performed concurrently by multiple administrators logged in from different locations. You can access the screen, but you cannot apply changes while another administrator is performing the same operation.

> **Caution:** While you are installing a license key, backup operations may be interrupted.

> **Note:** If you have more than one license key to apply, you may enter them all at the same time, separated by a space or a hyphen.

You can enter the license key on the **Setup Wizard: Licensing** screen, and you can also use commands on the operator panel or Web client to directly enter a license key at any time after exiting the Setup Wizard.

You may need to refresh your Internet browser after installing a license key to see the new menus and functionality.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Setup > License**.

- From the operator panel, select **Setup > Licenses**.

Setting Customer Contact Information

Administrators can use the Web client to enter contact information into the library for the person who is the primary customer contact for the library. Keep this information current to expedite the Service process.

When a problem occurs with the library, the contact information is mailed to techsup@quantum.com along with Reliability, Availability, and Serviceability (RAS) ticket information, assuming that the default e-mail notification has been configured. For information on configuring the default e-mail notification see Creating RAS E-mail Notifications on page 95.

You can set customer contact information from the Web client only, but you can view it from the operator panel.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Setup > Notifications > RAS > Contact Information**.

- From the operator panel, select **Setup > Notification**.

Configuring the Library E-mail Account

The library uses the library e-mail account whenever library e-mail services are used, such as when the library automatically sends e-mail notifications about library issues.

Before configuring the e-mail account, ask your network administrator for an IP address, valid login account (optional), and valid password

(optional) for your SMTP server. The login account name and password can contain the following special characters: @ and #. E-mail account settings are not case-sensitive.

After configuring the e-mail account, you can send a test message to an e-mail address to verify that the account is configured properly.

The **Setup > Notifications > E-mail Configuration** screen contains the following options:

- **SMTP Server** includes the IP address or host name of the SMTP server. IP addresses must be entered in dot notation (for example, 192.168.0.1) and cannot exceed 255.

- **Sender E-mail Address** includes an e-mail address for the library (for example, "libraryname@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.

Send snapshot with e-mail notifications instructs the library to automatically attach a library snapshot file (ASCII format) to certain RAS ticket e-mail notifications (see Working With RAS E-mail Notifications on page 94). (Snapshots are only auto-generated for this purpose if they help to clarify or diagnose the problem.) This feature is turned off by default. Library snapshot files can also be sent to specified e-mail addresses using the **Capture Snapshot** operation (see Capturing Snapshots of Library Information on page 485). If the library is in the process of capturing an automatic snapshot, you will not be able to manually capture a snapshot via the Web client until the automatic snapshot is complete. If this happens, an error message will display. Wait about 10 minutes and try again.

- **Authentication** includes a means to enter the login account name and password for the library. Selecting the box enables use authentication. Clearing the box disables use authentication. The following fields are only available if use authentication is enabled:

    - **Login Account** includes the name of a valid account on the SMTP server (for example, "John.User"). The login account name can contain the following special characters: @ and #.

    - **Password** is the password for the account that you specified in the **Login Account** text box. The password can contain the following special characters: @ and #.

- **Send a test e-mail to** allows you to enter an e-mail address you want to test. Enter the address and click **Send e-mail**. Then check the e-mail account to verify that an e-mail message was sent from the library.

After configuring the e-mail account, save the library configuration. For information, see <u>Saving and Restoring the Library Configuration</u> on page 488.

You can configure the library e-mail account from the Web client only, but you can view e-mail account information from the operator panel.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Setup > Notifications > E-mail Configuration**.

- From the operator panel, select **Setup > Notification > E-Mail Account**.

Working With RAS E-mail Notifications

The library can be configured to automatically send e-mail notifications to specified e-mail addresses whenever an issue of a particular severity level occurs with one of its components. The information in the e-mail notification provides details about the issue and the library conditions at the time of the error.

Before you can configure e-mail notifications, you must configure the library's e-mail account so that the library can send notifications to the designated recipients. See <u>Configuring the Library E-mail Account</u> on page 92 for information on how to configure the e-mail account.

See <u>Creating RAS E-mail Notifications</u> on page 95 for information on setting up additional e-mail notifications. The library supports a maximum of 20 e-mail notification recipients, including the default support e-mail notification.

Note:	RAS e-mail notifications are closed when the library reboots. From the operator panel, select **Tools > System Settings** to configure this setting.

> **Note:** The default techsup@quantum.com e-mail notification settings can be modified, but not deleted. The e-mail address, techsup@quantum.com, cannot be modified.

There are three e-mail notification filter levels:

- All tickets
- High and urgent tickets only
- Urgent tickets only

) Administrators can configure the library e-mail account and e-mail notifications. Users can receive e-mail notifications, but they cannot configure the library e-mail account and/or notifications.

You can configure e-mail notifications from the Web client only, but you can view them from the operator panel.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Setup > Notifications > RAS > Receiver Addresses**.
- From the operator panel, select **Setup > Notification > E-mail Alerts**.

Creating RAS E-mail Notifications

Administrators can create e-mail notifications. The library supports a maximum of 20 e-mail notification recipients, including the default support e-mail notification. Each e-mail notification recipient must have a unique e-mail address.

To set e-mail notifications, you need to provide the e-mail address and filter level setting for the recipient. For more information on filter levels, see Working With RAS E-mail Notifications.

Each e-mail notification includes an optional **Comments** text box you can use to enter important system configuration details, such as the network environment or third-party software applications that interface with the library. Such information will appear in the body of the e-mail and can help technical support personnel to troubleshoot the library.

> **Note:** Do not enter more than one address in the **Enter E-mail Address** text box. If you need to send e-mail notifications to multiple addresses, create an e-mail notification for each e-mail address.

The path to open the appropriate screen is as follows:

• From the Web client, select **Setup > Notifications > RAS > Receiver Addresses > Create**.

Modifying RAS E-mail Notifications

Administrators can modify existing e-mail notification settings at any time after the e-mail notification is created. For example, you can modify the e-mail address; add, delete, or modify a comment; change the filter level; and enable or disable the notification. For more information on filter levels, see <u>Working With RAS E-mail Notifications</u> on page 94.

> **Note:** The default <u>techsup@quantum.com</u> e-mail notification settings can be modified, but not deleted. The e-mail address, <u>techsup@quantum.com</u>, cannot be modified.

The path to open the appropriate screen is as follows:

• From the Web client, select **Setup > Notifications > RAS > Receiver Addresses > Modify**.

Deleting RAS E-mail Notifications

Administrators can delete an e-mail notification when it is no longer needed.

> **Note:** The default <u>techsup@quantum.com</u> e-mail notification settings can be modified, but not deleted. The e-mail address, <u>techsup@quantum.com</u>, cannot be modified.

The path to open the appropriate screen is as follows:

• From the Web client, select **Setup > Notifications > RAS > Receiver Addresses > Delete**.

Working With User Accounts

Administrators can create local user accounts on the library for local authentication, or enable and configure the Lightweight Directory Access Protocol (LDAP) for remote authentication. You may use either or both methods, according to your needs. This section covers how to set up user accounts and authentication for both local and remote authentication.

Local Authentication vs. Remote Authentication

Local authentication control is managed on the library. An administrator sets up accounts and privileges on the library. To use local authentication, a user must enter a local user name and password.

Remote authentication is managed by an LDAP server. Enabling LDAP allows existing user accounts residing on an LDAP server to be integrated into the library's current user account management subsystem. User account information is centralized and shared by different applications, simplifying user account management tasks.

To use remote authentication, you must enable LDAP on the library. Once LDAP is enabled, users can log into the library using either LDAP or local authentication. See for more information.

About Local User Accounts

Administrators can create and modify two types of local user accounts: user and administrator. These users have different library privilege levels.

- **User** — has access to one or more assigned partitions and can perform functions within a partition, such as performing media and tape drive functions. A user cannot perform actions that affect the physical library, such as creating, modifying, or deleting a partition.

- **Administrator** — has access to the entire physical library and all of its partitions.

The library ships with a default administrator account. The user name for this account is **admin** and the password is **password**. You cannot delete this user account or change the user name, but you can change the password. The default administrator account is used to perform the initial configuration of the library. If you misplace the password for the

default administrator account, contact Quantum Technical Support. See Getting More Information or Help on page 8.

See User Privileges on page 50 for more information on library permission levels. For information on changing passwords, see Modifying Local User Accounts on page 98.

Creating Local User Accounts

During or after the initial configuration, you can use the default administrator account to create up to eighteen additional local user accounts, including other administrator accounts. These administrators can themselves create other local administrator and user accounts. Users without administrator privileges cannot create accounts. The library can contain eighteen user accounts, including the default administrator account.

To create local user accounts, you need to provide information for the following fields:

- **User Name** — the login name of the user account you are creating. User names are limited to 1–12 lower-case letters, numbers, and underscores (_). For example: **john_usa**.

- **Password** — the unique password for the user account you are creating. Passwords are limited to 6–16 lower-case alphanumeric characters and can include also include underscores (_), periods (.), hyphens (-), asterisks (*), and the "at" symbol (**@**). For example: **pass_19**.

- **Privilege** — is set to either **User** or **Admin**. See User Privileges on page 50 for more information on user privilege levels.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Setup > User Management > User Accounts**.

- From the operator panel, select **Setup > User Mgmt> Create User**.

Modifying Local User Accounts

After a local user account has been created, administrators can modify the account settings, such as the password, privilege level, and partition access. You cannot modify the user name. Instead, you will need to delete the user account and create a new one.

To modify local user accounts, you need to provide information for the following fields:

- **Password** — the unique password for the user account you are creating. Passwords are limited to 6–16 lower-case alphanumeric characters and can include also include underscores (_), periods (.), hyphens (-), asterisks (*), and and the "at" symbo (**@**). For example: **pass_19**.

- **Privilege** — set to either **User** or **Admin**. See <u>User Privileges</u> on page 50 for more information on user privilege levels.

- **Partition Access** — the partitions to which this user has access. Any user assigned to a partition that has been deleted can be reassigned to other partitions.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Setup > User Management > User Accounts**.

- From the operator panel, select **Setup > User Mgmt > Modify User**.

Deleting Local User Accounts

Administrators can delete other local administrator and user accounts when they are no longer needed.

Note: The default administrator account cannot be deleted.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Setup > User Management > User Accounts**.

- From the operator panel, select **Setup > User Mgmt > Modify User**.

Configuring LDAP

Administrators can enable and configure Lightweight Directory Access Protocol (LDAP). LDAP is the industry standard Internet protocol that provides centralized user account management.

Administrators can add, delete, and modify only local user account information. The library Web client does not allow you to create, modify, or delete user account information on an LDAP server. This must be done by the directory service provider. For more information on working with local user accounts, see <u>About Local User Accounts</u> on page 97.

The library supports all LDAP servers. You can also use Kerberos for added security. For specific instructions on configuring Kerberos, see Configuring Kerberos on page 104.

The **Login** screen displays remote authentication login options only when LDAP is enabled.

LDAP Server Guidelines

The following groups must be created on the LDAP server to enable remote login on the library:

- Library user group — Assign users to this group who need user-privilege access to the library. Enter the name of this group in the **Library User Group** field on the **Setup - Remote Authentication** screen on the library Web client (see Configuring LDAP on the Library on page 101).

- Partition groups — For LDAP users 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 match the library partition names (names must match but are not case sensitive). Users with user privileges must be assigned to these groups on the LDAP server to have access to the corresponding partitions on the library.

- Library admin group — Assign users to this group who need administrator-privilege access to the library. LDAP users with administrator privileges have access to all partitions and administrator functions and do not need to be assigned to partition-related groups on the LDAP server. Enter the name of this group in the **Library Admin Group** field on the **Setup - Remote Authentication** screen on the library Web client (see Configuring LDAP on the Library on page 101).

You will need to have at least one user assigned to both the Library User Group and the Library Admin Group on the LDAP server in order to test the LDAP settings on the library (see Testing LDAP Settings on page 103). Since most normal users will not be members of both these groups, you may need to create a special or temporary user specifically for this purpose.

Configuring Secure LDAP on the Library

Configuring Secure LDAP is optional. You can configure Secure LDAP using one of the following methods (do not use both).

- **LDAPS —** Uses Secure Sockets Layer (SSL) over a specific port for LDAP (636). You may enable LDAP over SSL (LDAPS) by entering a URI in the form of "ldaps://hostname" in the Server URI field. This will use SSL to send secure communication via port 636. If the LDAP server does not support LDAPS or does not have LDAPS enabled, then login operations will fail. LDAPS has been deprecated in favor of using StartTLS (see option below). Do not use LDAPS if you are using StartTLS. Once you apply LDAPS, StartTLS will not be available.

- **StartTLS —** Uses Transport Layer Security (TLS) over the same port as regular LDAP (389). Select the **StartTLS** check box to configure secure LDAP communication using TLS. If TLS mode is not supported on your LDAP server, then login operations will fail. Do not use StartTLS if you are using LDAPS. See <u>Figure 15</u> on page 103.

Installing an LDAP TLS CA Certificate

If you are using LDAPS or StartTLS, you can also install a TLS CA certificate for additional verification that the LDAP server has not been compromised. The certificate must be the same certificate that is installed on your LDAP server and must be in .pem format. The library will only perform the verification if you have configured Secure LDAP (using either LDAPS or StartTLS). Place a copy of the certificate file in an accessible location on your computer and use the **Browse** button to locate and install it. Once a certificate is installed, you can remove it by selecting the **Remove TLS CA Certificate** check box. See <u>Figure 15</u> on page 103.

Configuring LDAP on the Library

Before configuring LDAP, obtain the following LDAP parameters from your network administrator. You need to enter these parameters in the **Setup - Remote Authentication** screen on the Web client.

- **Server URI —** The Uniform Resource Identifier (URI) of the LDAP server where user account information is stored. The URI includes the LDAP server host name or IP address and can include the LDAP server network port. Port 389 is the default.

Examples:

ldap://hostname:389

ldap://10.50.91.103

ldap://mycompany.com

- **LDAPS** — Optional. See <u>Configuring Secure LDAP on the Library</u> on page 101.

- **StartTLS —** Optional. See <u>Configuring Secure LDAP on the Library</u> on page 101.

- **Install TLS CA Certificate** — Optional. See <u>Installing an LDAP TLS CA Certificate</u> on page 101.

- **Remove TLS CA Certificate** — This check box is available if a TLS CA certificate is installed. You can remove the certificate by selecting this check box. The certificate will be removed after you click **Apply**.

- **Principal** — An LDAP user login ID with permissions to search the LDAP directory. The library logs on to LDAP using this ID. For an example, see <u>Figure 15</u> on page 103.

- **Password** — The password for the principal authorization login ID.

- **User DN** — The Fully Qualified Distinguished Name that contains the users. For an example, see <u>Figure 15</u> on page 103.

- **Group DN —** The Fully Qualified Distinguished Name that contains the groups. For an example, see <u>Figure 15</u> on page 103.

- **Library User Group** — The value of the Common Name attribute for the group entry on the LDAP server associated with library users who have user-level privileges (see <u>User Privileges</u> on page 50 for information on privilege levels). This group must exist on your LDAP server (see <u>LDAP Server Guidelines</u> on page 100). For an example, see <u>Figure 15</u> on page 103.

- **Library Admin Group** — The value of the Common Name attribute for the group entry on the LDAP server associated with library users who have administrator-level privileges (see <u>User Privileges</u> on page 50 for information on privilege levels). This group must exist on your LDAP server (see <u>LDAP Server Guidelines</u> on page 100). For an example, see <u>Figure 15</u>.

Figure 15 LDAP Setup
Example

**The simple LDAP server
configuration shown below would
give the library settings shown at
right.**

Simple LDAP Server Configuration:

Testing LDAP Settings

The **Test Settings** button tests communication between the library and the
LDAP server, and tests the currently applied LDAP settings. If there are
any problems, an error message identifies the problem area.

If you change the LDAP settings, click **Apply** to save your changes before
testing them. Otherwise, any changes you made will be lost and will not
be tested.

To test the settings, you must type a user name and password, then click
the **Test Settings** button. **The user you use for the test must be a member of
both the Library User Group and the Library Admin Group on the LDAP
server.** Since most normal users will not be members of both these
groups, you may need to create a special or temporary user specifically
for this purpose.

After configuring LDAP settings, save the library configuration.

> **Note:** For step-by-step instructions on configuring LDAP on the library, see your library's online Help. To access the online Help system, click the **Help** icon at the top right of the Web client.

You can view, enable, and configure LDAP settings from the library Web client. You cannot use the operator panel to configure LDAP settings.

The path to open the appropriate screen is as follows:

• From the Web client, select **Setup > User Management > Remote Authentication**.

Configuring Kerberos

Use Kerberos if you want extra security with remote authentication.

Make sure that both the library and the Kerberos/Active Directory® server are set to the same time (within 5 minutes). Otherwise, the authentication will fail. It is recommended that you use Network Time Protocol (NTP) to synchronize the time between the library and the Kerberos server. See Setting the Date and Time Using the Network Time Protocol on page 107.

Fill in the following Kerberos fields in addition to all the LDAP fields:

• **Realm** — The Kerberos realm name, typed in all uppercase letters. Usually the realm name is the DNS domain name.

   Example: MYCOMPANY.COM

• **KDC (AD Server)** — The key distribution center (in other words, the server on which Kerberos/Active Directory is installed).

   Example: mycompany.com:88

• **Domain Mapping** — The domain portion of the library's fully qualified domain name.

   Example: mycompany.com

• **Service Keytab** — Click the **Browse** button to select the service keytab file. The service keytab file is a file you generate on your Kerberos/Active Directory server. See Generating the Service Keytab file on page 105.

You can view, enable, and configure Kerberos settings from the Web client. You cannot use the operator panel to configure Kerberos settings.

The path to open the appropriate screen is as follows:

- From the Web client, select **Setup > User Management > Remote Authentication**.

Generating the Service Keytab file

These instructions are for generating the service keytab file for use with Microsoft® Active Directory®. If you not using Active Directory, refer to your Kerberos vendor for instructions on generating this file.

1 Set up an Active Directory domain on the Windows server.

2 If Active Directory is not already configured, run **dcpromo**.

3 **Windows 2003 servers only:** Install Windows Support Tools on the Windows 2003 server as follows:

   a Go to www.microsoft.com and search for "windows server 2003 support tools sp2" or click on the following link:

   http://www.microsoft.com/downloads/details.aspx?FamilyID =96a35011-fd83-419d-939b-9a772ea2df90&DisplayLang=en

   b Download both **support.cab** and **suptools.msi**.

   c Run **suptools.msi** to begin installation.

4 Create a computer account in Active Directory.

   - Do not select any of the check boxes during creation.

   - The account name will be used for <computer account> fields shown in the following steps.

5 At the command prompt, map SPN to the computer account. Use the following format:

   setspn -A library/<fqdn of library> <computer account>

   For example:

   setspn -A library/delos.dvt.mycompany.com kerbtest

6 At the command prompt, create the keytab file for the SPN. Use one of the following formats:

- **For Windows 2003:**

```
ktpass -out library.keytab -princ
library/<fqdn of library>@<realm>
+rndPass -ptype KRB5_NT_SRV_HST -crypto RC4-HMAC-NT -
mapUser <realm>/computers/<computer account>
```

For example:

```
ktpass -out library.keytab -princ
library/delos.dvt.mycompany.com@OURREALM.LOCAL
+rndPass -ptype KRB5_NT_SRV_HST -crypto RC4-HMAC-NT -
mapUser ourrealm.local/computers/kerbtest
```

- **For Windows 2008:**

```
ktpass -out library.keytab -princ library/
<fqdn of library>@<realm>
+rndPass -ptype KRB5_NT_SRV_HST -crypto AES256-SHA1
-mapUser <realm>/computers/<computer account>
```

For example:

```
ktpass -out library.keytab -princ
library/delos.dvt.mycompany.com@OURREALM.LOCAL
+rndPass -ptype KRB5_NT_SRV_HST -crypto AES256-SHA1
-mapUser ourrealm.local/computers/kerbtest
```

Setting the Date, Time, and Time Zone

Administrators can either set the library date, time, and time zone settings manually or configure the Network Time Protocol (NTP).

> **Note:** The following operations should not be performed concurrently by multiple administrators logged in from different locations. You can access the appropriate screens, but you cannot apply changes while another administrator is performing the same operation.

> **Note:** For step-by-step date and time configuration instructions, see your library's online Help. To access the online Help system, click the **Help** icon at the top right of the Web client or operator panel user interface.

> **Note:** The library may log you off after you change the time or time zone. If this happens, simply log back on.

Setting the Date and Time Manually

The **Setup Wizard - Date & Time** screen allows you to set the date and time for the library. You can also access the date and time setup screen by selecting **Date & Time** from the **Setup** menu on either the operator panel or the Web client.

Date and time settings are used to log the date and time events take place and to set the time for automatic backup and restore functions. At a minimum, you should set the library's date and time as part of the initial library configuration.

The time is set to a 24 hour clock. For example, four o'clock in the afternoon is entered as 16:00.

Setting the Date and Time Using the Network Time Protocol

The library supports the Network Time Protocol (NTP). NTP allows you to synchronize the library date and time with other components in your IT infrastructure. Administrators can either modify the date and time zone settings manually or configure NTP.

If NTP is enabled, the time zone and IP addresses of at least one NTP server must be configured on the library. Contact your network administrator for NTP server IP address information.

You can use the Web client **Setup Wizard - Date & Time** screen to enable and configure NTP. You can also access the date and time setup screen by selecting **Date & Time** from the **Setup** menu on the Web client.

Details on NTP settings include:

• NTP servers must be configured in available in groups of 3 or more, with one exception: a single NTP server configuration is also allowed.

- NTP is enabled on the **Date & Time** screen. When NTP is enabled, you cannot manually configure date and time. For more information on setting date and time manually, see Setting the Date and Time Manually on page 107.

- You can enter an IP address for a primary and an alternate (optional) NTP server.

- NTP server IP addresses must be entered in the proper format. See Modifying Network Settings on page 60 for the proper format of IPv4 and IPv6 addresses.

- After you apply NTP settings, system clock synchronization may take several minutes.

You can only enable and configure NTP on the Web client. The path to open the appropriate screen is as follows:

- From the Web client, select **Setup > Date & Time**.

Setting the Time Zone

To select your time zone from a list, disable **Use Custom Time Zone** setting and select your time zone.

If your time zone does not appear on the list, or you want more control over your time settings, enable **Use Custom Time Zone** and set a Universal Coordinated Time (UTC) offset.

You can only set the time zone on the Web client. The path to open the appropriate screen is as follows:

- From the Web client, select **Setup > Date & Time**.

Setting Daylight Saving Time

If you selected your time zone from the drop-down list (see Setting the Time Zone), the library automatically adjusts for daylight saving time. There is no need to manually reset the clock for time changes.

However, if you set a custom time zone, the library will not automatically adjust for daylight saving time. You must enable the **Use Custom Daylight Saving Time** setting. Once enabled, you can set start and stop times to an accuracy of one minute.

You can only set daylight saving time on the Web client. The path to open the appropriate screen is as follows:

- From the Web client, select **Setup > Date & Time**.

Working With FC I/O Blades

The library supports optional FC I/O blades, which provide host connections to LTO-2, LTO-3, LTO-4, LTO-5 and LTO-6 FC drives. The number of FC I/O blades in any library configuration cannot exceed four, and each FC I/O blade in the library supports up to four FC tape drives.

FC I/O blades reduce switch port and cabling requirements and increase backup reliability. When tape drives are connected to FC I/O blades, the library proactively checks the status and readiness of the data paths from the hosts through the FC I/O blade to the FC tape drives.

In addition, two powerful features provide ways to manage the interaction between hosts and target devices:

- **Channel zoning** allows you to control access between FC I/O blade ports configured for host servers and ports configured for target devices. For more information, see Configuring FC I/O Blade Channel Zoning on page 111.

- **Host Mapping** allows you to control visibility to target devices and access from individual host servers to target devices. For more information, see Managing FC Hosts and Host Mapping on page 113.

The topics in this section cover configuring FC I/O blades. For additional information on FC I/O blades, see:

- Fibre-Channel Input/Output Blades on page 26
- Controlling FC I/O Blade Power on page 263
- Viewing FC I/O Blade Information on page 275
- Viewing FC I/O Blade Port Information on page 276
- Cabling Libraries With Fibre Channel Tape Drives Connected to Fibre Channel I/O Blades on page 308
- Recommended Library Cabling for FC I/O Blades on page 313
- Identifying FC I/O Blades on page 496
- Resetting FC I/O Blade Ports on page 498

> **Note:** FC I/O blade menu commands are available for use only when FC I/O blades are installed in the library.

Configuring FC I/O Blade Ports

When FC I/O blades are installed, administrators can configure FC I/O blade port parameters.

Each FC I/O blade has six ports. Ports 1 and 2 are always target ports and are configurable. Ports 3 through 6 are always initiator ports and are not configurable. For information on viewing the current configured settings for all I/O blade ports, see <u>Viewing FC I/O Blade Port Information</u> on page 276.

Details on configuring FC I/O blade ports include:

- The **Setup - I/O Blade Port Configuration** screen lists all I/O blades found in the library. The screen lists the following information for each I/O blade: location in the library, World Wide Node Name (WWNN), status, and ports. You can select the I/O blade target port (1 or 2) you want to configure and proceed to the next screen. For the target port you selected, the screen displays the World Wide Port Number (WWPN).

- For the selected target port (ports 1 and 2), you can configure the following parameters:

  - **Loop ID** — Loop IDs can be set to **Auto** or a hard value from 0 through 125. Selecting **Auto** automatically selects a unique loop ID. Some FC host operating systems require hard loop ID settings. The default setting is **Auto**.

  - **Speed** — The interface speed can be set to **Auto**, **1 Gb/s**, **2 Gb/s**, or **4 Gb/s**. Selecting **Auto** automatically sets the interface speed. The default setting is **Auto**.

  - **Frame Size** — Frame size can be set to **512**, **1024**, or **2048**. The default setting for ports 1 and 2 is **2048**. Your FC host might require a different setting.

  - **Connection** — The connection mode for the ports can be set to **Loop**, **Loop Preferred,** or **Point to Point**. The default setting is **Loop Preferred**.

- After modifying these parameters, save the library configuration. For instructions on how to save the library configuration, see <u>Saving and Restoring the Library Configuration</u> on page 488.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Setup > FC I/O Blades > Port Configuration**.

- From the operator panel, select **Setup > I/O Blades > Port Configuration**.

**FC I/O Blade Internal
Virtual Port for Media
Changers**

FC I/O blades use an internal virtual port to access the media changer devices (partitions). Each FC I/O blade can access all media changer devices, except those that are defined in association with drive-based access (also known as "LUN-1"). The Scalar i500 library can have up to 18 partitions. These internal virtual ports are not configurable via channel zoning; thus, all media changer devices are accessible via ports 1 and 2 of each FC I/O blade present within the library. This may lead to one or more media changer devices being discovered multiple times, depending on how the system is connected to host servers (for example, if four partitions are defined in a system that has two FC I/O blades, there would be four media changer devices visible on ports 1 and 2 of both FC I/O blades, for a total of 16). To minimize unnecessary discovery of media changer devices, you need to configure host mapping. See Managing FC Hosts and Host Mapping on page 113.

**Configuring FC I/O Blade
Channel Zoning**

When FC I/O blades are installed in the library, administrators can configure channel zoning for selected FC I/O blades. Channel zoning, also called port zoning, configures access to an entire FC 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 ports 1 and 2 and initiator ports 3–6 on an FC I/O blade.

> **Note:** Channel zoning acts upon the FC tape drive LUNs seen through the initiator ports on the FC I/O blade. Channel zoning does not affect media changer (partition) LUNs. If you want to map hosts to media changer LUNs though an FC I/O blade, you must use the FC I/O blade's FC host mapping feature. For information on FC host mapping, see Managing FC Hosts and Host Mapping on page 113.

> **Note:** If both channel zoning and host mapping are enabled, the channel zoning settings supersede any host LUN mapping on the FC I/O blade.

Details on configuring channel zoning include:

- By default, all target FC ports (ports 1 and 2) on an FC I/O blade have access to all initiator ports (ports 3–6).

- Changing channel zoning setting will cause the affected FC I/O blade to reboot.

- If host port failover is enabled on the FC I/O blade, channel zoning must be configured so that all target FC ports have access to all initiator ports. For information on host port failover, see Configuring FC Host Port Failover on page 119.

- The **Setup - FC I/O Blade Channel Zoning** screen on the Web client lists all FC I/O blades found in the library. FC I/O blades are listed by the following: location in the library, WWNN, and status. The corresponding **Channel Zoning Select Blade** screen on the operator panel lists the location in the library and state. You can select the FC I/O blade you want to configure for channel zoning and proceed to the next screen.

- The two FC target ports (ports 1 and 2) and the four FC initiator ports (ports 3–6) are displayed in a grid, with the target ports listed in columns and the initiator ports listed in rows. Check boxes allow you to associate a target port with an initiator port.

  - To permit access, select the check box at the intersection of the target port and the initiator port. You can associate each initiator port with more than one target port.

  - To restrict access, clear the check box at the intersection of the target port and the initiator port.

  - When you select a check box, the entire FC channel is zoned. This zoning affects any host application that might be accessing the FC I/O blade. If both channel zoning and host mapping are enabled, the channel zoning settings supersede any host LUN mapping on the FC I/O blade.

  - After configuring channel zoning, save the library configuration. For instructions on how to save the library configuration, see Saving and Restoring the Library Configuration on page 488.

> **Note:** This operation should not be performed concurrently by multiple administrators logged in from different locations. You can access the appropriate screens, but you cannot apply changes while another administrator is performing the same operation.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Setup > FC I/O Blades > Channel Zoning**.

- From the operator panel, select **Setup > FC I/O Blades > Channel Zoning**.

Managing FC Hosts and Host Mapping

An FC host is the main processing server on a storage area network (SAN) that receives data and initiates communication with other devices. When FC I/O blades are installed in the library, administrators can access, add, modify, and delete FC hosts and also configure FC host mapping. Before you can perform any of these FC host management operations, you need to enable host mapping, which is disabled by default. See <u>Enabling/Disabling FC Host Mapping</u> on page 113.

> **Note:** On the operator panel, the host management screens (**Setup > I/O Blades > Host Management**) are not available unless FC host mapping is enabled.

> **Note:** If both channel zoning and host mapping are enabled, the channel zoning settings supersede any host LUN mapping on the I/O blade.

Enabling/Disabling FC Host Mapping

Administrators can enable or disable the optional FC host mapping feature. This feature is disabled by default. When host mapping is enabled, you can add, modify, and delete hosts as well as configure FC host mapping.

Note: This operation should not be performed concurrently by multiple administrators logged in from different locations. You can access the appropriate screens, but you cannot apply changes while another administrator is performing the same operation.

The paths to open the appropriate screens are as follows:

- From the Web client select **Setup > FC I/O Blades > FC I/O Blade Control**.

- From the operator panel, select **Setup > I/O Blades > Blade Control**.

Viewing FC Host Information

The following information is provided for FC hosts:

- **Host Name** — The host device name

- **I/O Blade** — The location of the FC I/O blade in the library

- **Status** — The online/offine (connectivity) status of the host (Web client only)

- **Host Port** — The host port number

- **WWPN** — The World Wide Port Name of the host device

- **Type** — The operating system of the host device

The paths to open the appropriate screens are as follows:

- From the operator panel, select **Setup > FC I/O Blades > Host Management**.

- From the Web client, select **Setup >FC I/O Blades > Host Management**.

Creating, Modifying, and Deleting an FC Host Connection

Administrators can manually create a connection to an FC host if the host was not already connected to the library when it was turned on. You can also modify and delete an existing FC host connection. You can perform these operations without down the library. You can add up to 32 FC host connections per FC I/O blade.

After creating, modifying, or deleting an FC host connection, save the library configuration. For instructions on how to save the library configuration, see <u>Saving and Restoring the Library Configuration</u> on page 488.

> **Note:** These operations should not be performed concurrently by multiple administrators logged in from different locations. You can access the appropriate screens, but you cannot apply changes while another administrator is performing the same operation.

Creating an FC Host Connection

For each FC host connection you want to create, you can set the following parameters:

- **Host Name** — The host device name.
- **Host Port** — The host port number.
- **WWPN** — The World Wide Port Name of the host device. The **WWPN** text box is limited to 17 lowercase alphanumeric characters and colons (:). The WWPN must be typed in the following format: 12345678:0b33ef12.
- **Type** — The appropriate host operating system.
- **I/O blades** — Lists the I/O blades you can select for the host.

Modifying an FC Host Connection

For each FC host connection you want to modify, you can set the following parameters:

- **Host Name** — The host device name.
- **Host Port** — The host port number.
- **Type** — The appropriate host operating system.

You cannot modify the WWPN. If you want to change the WWPN, you must delete and re-create the FC host connection.

Deleting an FC Host Connection

Administrators can delete connections to FC hosts without powering down the system. Before deleting an FC host connection, make sure the FC host is disconnected (offline) from the I/O blade.

A message will appear if the FC host is online when you attempt to delete it. To continue, take the FC host offline or disconnect the FC host from the I/O blade, wait for the FC host to go offline, and then continue to delete the FC host connection.

> **Note:** If the host application is connected through an FC switch, a power cycle of the I/O blade might be required to make the host go offline. For instructions on how to power cycle an I/O blade, see Controlling FC I/O Blade Power on page 263.

The paths to open the appropriate screens are as follows:

- From the operator panel, select **Setup > I/O Blades > Host Management**.

- From the Web client, select **Setup > I/O Blades > Host Management**.

Host Mapping - Overview

Host mapping enables you to manually modify host information and set logical unit number (LUN) mappings, and to map specific hosts to library LUN devices.

I/O blades discover target devices that are attached to ports 3–6, as well as their internal virtual port (see FC I/O Blade Internal Virtual Port for Media Changers on page 111). Each of these devices has its own native logical unit number (LUN) that is used to address the device via the port to which it is attached. These LUNs can be re-mapped to new LUNs for presentation via ports 1 and 2. Further, custom LUN maps can be simultaneously defined for individual hosts.

For example, the FC I/O blade may discover tape drives attached to ports 3–6, each of which report themselves at LUN 0. The FC I/O blade could be configured to re-map these to LUNs 1, 2, 3, and 4 for discovery on ports 1 and 2. If desired, they could also be simultaneously mapped to LUNs 3, 5, 7 and 9 for a specific host server.

There is also an internal (i.e., not attached to a port) controller device presented at LUN 0 by default. The controller device facilitates initialization and device discovery. In some instances it may be useful to

map the controller device to a different LUN if an application typically expects to see a media changer device (partition) or tape drive at LUN 0.

LUNs can also be mapped to be accessible by specific host server World Wide Port Name (WWPN). Mapping a LUN to a specific WWPN can be used instead of channel zoning to control device visibility. Mapping a LUN to more than one WWPN may be useful for creating redundant paths to a media changer device (partition), tape drive, or controller device. LUNs will need to be mapped to each WWPN for host servers that use multiple ports (e.g., multi-ported HBAs or multiple HBAs) if access is desired via all the host server ports (e.g., a LUN would need to be mapped to both WWPNs of a server that uses a dual-port HBA).

LUN masking is a complementary concept to host mapping in that LUNs that are mapped to specific host server WWPNs are hidden (i.e., masked) from other host servers. This is useful when more than one host server is attached to the FC I/O blade (e.g., in a SAN). One or more of the LUNs can be masked from discovery by specific host servers while maintaining their mapping and accessibility to other host servers via the same port(s).

Host Mapping Vs. Channel Zoning

Channel zoning places an operational restriction on mapped LUNs (for example, if port 1 is zoned to ports 3 and 4, but LUNs from ports 3 through 6 have been mapped to a specific host server WWPN, the devices on ports 5 and 6 cannot be accessed from that host via port 1, even though they are mapped to it; only the devices on ports 3 and 4 would be accessible from the host via port 1).

Host mapping can be used to control visibility of the media changer devices (partitions) found on the FC I/O blade internal virtual port, while channel zoning can be used to create simple access control to the other target devices. If the host mapping capabilities are used to control visibility and access for all the LUNs, channel zoning might not be necessary or desired.

> **Note:** On the operator panel, the host mapping screens (**Setup > FC I/O Blades > Host Mapping**) are not available unless FC host mapping is enabled. See <u>Enabling/Disabling FC Host Mapping</u> on page 113.

Configuring Host Mapping

To configure host mapping, you need to select the media changer device (partition) or tape drive you want to map and assign a new LUN number for the device.

> **Note:** Depending on host operating system constraints, it might be necessary to reboot or reconfigure the host due to device mapping changes that result from configuring host mapping.

Details on configuring host mapping include:

- Host mapping is an optional feature and is disabled by default. For instructions on how to enable or disable host mapping, see <u>Enabling/Disabling FC Host Mapping</u> on page 113.

- The **Setup - I/O Blade Host Mapping** screen on the Web client lists the host name, I/O blade location, World Wide Port Name (WWPN), and operating system type of each available FC host. You can select the FC host to configure and proceed to the next screen.

  The screen lists the available partitions and tape drives connected to the FC I/O blade to which the FC host is attached. For each available partition and tape drive, the screen lists the following:

  - **Description** — For tape drives: Drive [location coordinates][(associated partition)]. For partitions: the name assigned to the partition during the partition creation process.

  - **Type** — Device type, for example, processor, media changer (partition), tape drive.

  - **Serial Number** — Serial number of the partition or tape drive.

  - **Vendor** — Device manufacturer.

  - **Product** — Name of the device.

  - **LUN** — Current logical unit number (LUN) assignment. Assign a new LUN number for the device.

  > **Note:** The operator panel host mapping configuration screens show less information about each device; however, you still select the host and device(s) and configure the LUN number(s(.)

• After configuring FC host mapping, save the library configuration. For instructions on how to save the library configuration, see Saving and Restoring the Library Configuration on page 488.

Note: A warning message will display if the command and control LUN (CCL) or another device is not mapped to LUN 0 (zero). LUN 0 is typically occupied by the command and control LUN (CCL), unless it has been manually mapped to another LUN. Make sure at least one device is mapped to LUN 0.

Note: If an FC switch is attached to an FC I/O blade target port, the FC switch will appear in the Blade Host Management list as if it were an FC host. Do not map library devices to an FC switch. To avoid confusion, it is recommended that you modify the FC switch host name and type using Blade Host Management. See Modifying an FC Host Connection on page 115.

Note: If both channel zoning and host mapping are enabled, the channel zoning settings supersede any host LUN mapping on the FC I/O blade. For information on channel zoning, see Configuring FC I/O Blade Channel Zoning on page 111.

The paths to open the appropriate screens are as follows:

• From the operator panel, select **Setup > FC I/O Blades > Host Mapping**.

• From the Web client, select **Setup > FC I/O Blades > Host Mapping**.

Configuring FC Host Port Failover

When FC I/O blades are installed in the library, administrators can enable and configure the optional FC host port failover feature. This feature is disabled by default.

You can configure the FC host port failover feature so that a "standby" target port (1 or 2) on an I/O blade can assume the identity and LUN mapping configuration of the designated "active" target port if the active port fails. Host port failover enables the library to continue operations without requiring you to reconfigure the host or the SAN.

To enable host port failover, you must configure target ports 1 and 2 on the FC I/O blade as point-to-point connections (**Setup > FC I/O Blades > Port Configuration**). FC I/O blade target ports 1 and 2 must be attached to the same SAN fabric to provide host access. The primary active port is used for host communications, while the passive standby port is kept idle. In addition, channel zoning must be configured so that target ports 1 and 2 have access to all initiator ports (ports 3–6) (**Setup > FC I/O Blades > Channel Zoning**). If these conditions are not met, an error message will display when you attempt to enable host port failover.

Note:	The current feature implementation does not support arbitrated loop or target/initiator mode.

Note:	Ports on the 4 Gb FC I/O blade used for failover must connect to the same SAN fabric.

Note:	When both target ports on the FC I/O blade are attached to the same SAN fabric, you may see duplicate media changer devices (partitions) being reported. To stop this from happening, you need to enable host port mapping and configure host mapping. For more information, see Configuring Host Mapping on page 118.

Note:	When Fibre Channel port 2 is selected to be the active port in a host port failover configuration, the active port can switch to the default setting, port 1, following a reboot. Reconfigure the host port failover settings so that the intended port is the active port.

For information on configuring FC I/O blade ports and channel zoning, see Configuring FC I/O Blade Ports on page 110 and Configuring FC I/O Blade Channel Zoning on page 111.

The library generates a Reliability, Availability, and Serviceability (RAS) ticket when port failover occurs. Examine the ticket to determine the reason for the failover. When the failed port is repaired, the port must be re-enabled to make it available for host port failover as the standby or active port. For more information, see Repairing and Enabling a Failed Target Port on page 121.

Details on configuring host port failover include:

- The **Setup - Host Port Failover** screen displays all the FC I/O blades found in the library. FC I/O blades are listed by the following: location in the library, WWNN (Web client only), and status/state. You can select the FC I/O blade you want to configure for host port failover and proceed to the next screen.

- To enable FC host port failover for the selected FC I/O blade, you can select a check box to enable FC Host Port Failover. Clearing the check box disables FC host port failover for the selected FC I/O blade.

- If you are enabling FC host port failover, select one target port on the FC I/O blade as the **Active Port**. The selected target port becomes active by default. The other target port will go on passive standby until failover occurs.

- After enabling or disabling FC host port failover, save the library configuration. For instructions on how to save the library configuration, see Saving and Restoring the Library Configuration on page 488.

Note:	This operation should not be performed concurrently by multiple administrators logged in from different locations. You can access the appropriate screens, but you cannot apply changes while another administrator is performing the same operation.

- The paths to open the appropriate screens are as follows:

- From the Web client, select **Setup > I/O Blades > Host Port Failover**.

- From the operator panel, **Setup > I/O Blades > Host Port Failover**.

Repairing and Enabling a Failed Target Port

After host port failover occurs, the failed target port must be repaired and enabled before it can be configured as an active or standby port for the host port failover feature. To repair the failed port, use the information in the RAS ticket that was generated when the host port failover occurred. For information on viewing and resolving RAS tickets, see About RAS Tickets on page 481.

Once the port has been repaired, you can enable it. Details on enabling a repaired target port include:

- The **Setup - Host Port Failover** screen displays all the I/O blades found in the library. I/O blades are listed by the following: location in the library, WWNN (Web client only), and status/state. You can select the I/O blade that had a failed target port and proceed to the next screen.

- In the **Physical Ports** section of the Web client screen, check the **State**, **Failure Type**, and **Intervention** columns for the port that failed.

> **Note:** If you are using the operator panel user interface, select the Port Info button to view the physical ports information.

- If the link is down or has an error, the port's state is offline, a failure type is indicated, and the Intervention is "Fix Link." You must repair the failed port using information in the RAS ticket that was generated for the host port failover. You can then return to this screen and enable the repaired port.

- After you fix the problem, the Intervention is "Enable Failover" and the **Enable** button becomes available. Click **Enable** to make the port available for another failover or for reconfiguration as the active port.

- Once the error is corrected and the link is enabled, the port's state is online and the Intervention is "Not Required."

- After enabling the repaired target port, save the library configuration. For instructions on how to save the library configuration, see <u>Saving and Restoring the Library Configuration</u> on page 488.

> **Note:** This operation should not be performed concurrently by multiple administrators logged in from different locations. You can access the appropriate screens, but you cannot apply changes while another administrator is performing the same operation.

For information on how to configure the repaired port as the standby or active target port, see <u>Configuring FC Host Port Failover</u> on page 119.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Setup > I/O Blades > Host Port Failover**.

- From the operator panel, **Setup > I/O Blades > Host Port Failover**.

Working With Data Path Conditioning

When I/O blades are installed, administrators can configure data path conditioning, an automatic means of verifying, monitoring, and protecting data path integrity between FC I/O blades and FC tape drives. Data path conditioning allows you to proactively detect and resolve data path problems before they affect backup, restore, and other data transfer operations.

The I/O blade does not manage data path conditioning along the path between the host and the I/O blade. It does manage data path conditioning along the path between itself and the FC tape drives. Data path monitoring automatically occurs at regular, configurable intervals. The I/O blade generates a RAS ticket if the monitoring tests fail for two intervals.

To configure data path conditioning, set the following parameters for the selected I/O blade:

- The level at which the data path is monitored between an I/O blade and the FC tape drives connected to it. The two levels are as follows:

    - **Interface Test** — performs tests to verify that FC controllers on I/O blades are responsive to commands. This is the default level.

    - **Device Datapath Test** — performs tests at the Interface Test level and also performs a device inquiry on each target device.

- **Test Interval** — the time interval between monitoring checks. You can configure the test interval. It can range from 5 to 2,880 minutes (48 hours). If you do not configure the test interval, the default test interval is 60 minutes. If you disable data path conditioning and then re-enable it in the future, the interval reverts to the default of 60 minutes regardless of whether you changed the interval previously.

Note: This operation should not be performed concurrently by multiple administrators logged in from different locations. You can access the appropriate screens, but you cannot apply changes while another administrator is performing the same operation.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Setup > I/O Blades > Data Path Conditioning**.

- From the operator panel, select **Setup > I/O Blades > Data Path Conditioning**.

Configuring Library Security Settings

Administrators can use the operator panel **Security Settings** screen to change the following security features:

- **Network Interface** — Enables external access to the library over Ethernet. This setting is enabled by default to allow external access.

- **SSH Services** — Opens port 22 to allow Secure Shell (SSH) services, to access the library. This setting is enabled by default.

- **ICMP** — Enables external attempts to discover the library by pinging it (by means of the Internet Control Message Protocol [ICMP] Echo packets). This setting is enabled by default.

- **Remote UI** —Opens port 80 to allow remote access to the library via the Web client. This setting is enabled by default.

- **SNMP** — Opens port 161 to allow SNMP communication to the library. This setting is enabled by default.

Note:	This setting differs from enabling SNMP services in the **Tools > System Settings** menu (see <u>Enable SNMP V1/V2</u> on page 129). In order to run SNMP, the port must be open and the SNMP services must be enabled.

- **SMI-S** — Opens port 5988 to allow SMI-S communication to the library. This setting is enabled by default.

> **Note:** This setting differs from enabling the SMI-S service in the
> **Tools > System Settings** menu (see <u>Enable SMI-S</u> on
> page 129). In order to run SMI-S, the port must be open
> and the SMI-S service must be enabled.

You cannot configure the security settings from the Web client. The path
to open the appropriate screen is as follows:

• From the operator panel, select **Tools > Security**.

Configuring the Internal Network

Use the **Internal Network Configuration** screen to configure your library's
internal network setting. The default internal network address is
10.10.10.X.

The library's internal network enables communication among library
components. While rare, it is possible that the default addressing of the
internal network could conflict with your network, potentially causing
the library to become confused. When installing the library, make sure
that the external network setting is different from the internal network
setting on the library. If DHCP is enabled or you do not know what your
external network setting is, check with your network administrator.

> **Caution:** Do not change the library's internal IP address during
> backup/restore operations.

From the operator panel, administrators can change the setting of the
internal network using the **Internal Network Configuration** screen. Select
the new internal IP address from the list on the screen. You can select
from nine IP addresses.

The **Internal Network Configuration** screen is only accessible from the
operator panel. The path to open the appropriate screen is as follows:

• From the operator panel, select **Tools > Internal Network**.

Configuring System Settings

This section describes the system-wide settings you can configure on the library. Each setting is described in detail below.

Details on the system settings include:

- The only setting users with User privileges can configure is the **Touch screen audio** setting.

- Administrators can configure all the system settings.

- All of the system settings are available on the operator panel. The only settings available on the Web client are user session timeout and unlabeled media detection.

The paths to open the appropriate screens are as follows:

- From the operator panel, select **Tools > System Settings**.

- From the Web client, select **Setup > System Settings**.

User Session Timeout (minutes)

The library automatically logs out a user or administrator when the library has detected no activity for a specified length of time. You can adjust the user session timeout by entering a numeric value in the **User session timeout (minutes)** text box. Valid user session timeout values are 15 minutes to 480 minutes. You can change this setting from either the operator panel or the Web client. When you change the setting on the operator panel, the Web client is updated at the same time, and vice versa.

- **Touch Screen Audio** — Allows you to enable or disable the beep sound that occurs each time you press a button on the operator panel. The **Touch screen audio** setting is enabled by default.

- **Unload Assist** — Allows you to specify whether the library should automatically eject cartridges from tape drives. When the setting is enabled, the library will assist with tape drive unload operations in the event that a tape drive is not unloaded by a host command. When the setting is disabled, the library will not assist with tape drive unload operations and reject a move request from a tape drive, if the cartridge is not already unloaded. The **Unload Assist** setting is enabled by default.

The paths to open the appropriate screens are as follows:

- From the operator panel, select **Tools > System Settings**.From the Web client, select **Setup > System Settings**.

Tape Drive Logical SN Addressing

The library assigns a fixed logical serial number to each tape drive slot in the library (whether it is occupied or not). When the **Logical SN Addressing** setting is enabled, the library reports only the logical serial number to the host instead of the tape drive's physical serial number. If the tape drive is later replaced by another tape drive in the same slot, the logical serial number remains the same. From the host application's perspective, the replacement tape drive is the same as the original. Logical SN Addressing is enabled by default.

When the Logical SN Addressing setting is disabled, the library reports only the tape drive physical serial number to the host.

The library System Information Report shows both the logical and physical serial numbers on installed tape drives for your convenience (**Reports > System Information**).

Caution:	If you change the logical serial number addressing setting, you must power cycle the library in order for the change to take effect.

Caution:	Use caution with this feature, as it can be accessed by both Admin and Service login users. Enabling this feature in an existing installation will change the presentation of the tape drive serial numbers to the host computer and host applications. Some host operating systems, and some application software, will no longer see a tape drive if the serial number changes (by use of this feature) from a previously set host configuration. If this happens, you will need to reconfigure the tape drives in your backup application.

The path to open the appropriate screen is as follows:

- From the operator panel, select **Setup > System Settings**.

Manual Cartridge Assignment

Administrators can disable or enable manual cartridge assignment. When manual cartridge assignment is enabled (the default setting), the **Assign I/E** screen automatically appears on the operator panel once cartridges are placed into the I/E station. The **Assign I/E** screen prompts the user to use the operator panel to assign the cartridges to a specific partition or to the System partition. The cartridges can then be used only by the assigned partition.

For more information on manual cartridge assignment, see Disabling/Enabling Manual Cartridge Assignment on page 77.

The path to open the appropriate screen is as follows:

• From the operator panel, select **Setup > System Settings**.

Disable Remote Service User

For security purposes, prevents a service user from logging in to the library remotely, from either the Web client or over the Ethernet service port. The service user will still be able to log in to the library from the operator panel interface. This option is disabled by default.

The path to open the appropriate screen is as follows:

• From the operator panel, select **Setup > System Settings**.

Enable SSL

Enables Secure Socket Layer (SSL) for secure data transmission between the library and remote clients. This option is disabled by default.

The path to open the appropriate screen is as follows:

• From the operator panel, select **Setup > System Settings**.

Enable SNMP V1/V2

Enables Simple Network Management Protocol (SNMP) V1 and V2c services to run on the library. This option is disabled by default.

> **Note:** SNMP v3 is always enabled. For more information on SNMP, see <u>Configuring SNMP Settings on the Library</u> on page 63.

> **Note:** This setting differs from opening the SNMP port in the **Tools > Security** menu (see <u>Configuring Library Security Settings</u> on page 124). In order to run SNMP, the port must be open and the SNMP service must be enabled.

Enable IPv6

Enables support for IPv6. This option is disabled by default.

The path to open the appropriate screen is as follows:

• From the operator panel, select **Setup > System Settings**.

Enable SMI-S

Enables the SMI-S service to run on the library. This setting is disabled by default.

> **Note:** This setting differs from opening the SMI-S port in the **Tools > Security** menu (see <u>Configuring Library Security Settings</u> on page 124). In order to run SMI-S, the port must be open and the SMI-S service must be enabled.

The path to open the appropriate screen is as follows:

• From the operator panel, select **Setup > System Settings**.

Unlabeled Media Detection

At bootup and other times the library performs an inventory of all slots and media. If a slot contains media with an unreadable barcode label (for example, the label is missing, torn, or marked up), the scanner cannot identify it, so the library normally reports the slot as empty.

With the Unlabeled Media Detection feature, you can configure the library to detect and report which slots contain media with unreadable barcodes. Since cartridges with unreadable barcodes will not work for

some library functions, knowing which labels are bad enables you to replace them with good ones as soon as possible.

When you enable Unlabeled Media Detection, the calibration sensor re-scans slots identified as empty in the inventory to see if a cartridge is physically in the slot. If so, the library reports the cartridge as having an unreadable barcode.

> **Note:** The library always re-scans "empty" slots in the top and bottom rows of the library, even if you don't enable the Unlabeled Media Detection feature. This is because occasionally a small or poorly placed label cannot be read by the barcode scanner in those two rows. The calibration sensor re-scans the bottom row, and the picker physically checks the top row because the calibration sensor cannot reach it.
>
> "Bottom row" here means the bottommost available row as indicated in the library configuration report.

This feature is disabled by default. When enabled, the following occurs:

- The re-scan may take up to several minutes to complete.

- You can configure the library to re-scan only the I/E station slots that were identified as empty, or all the slots in the library that were identified as empty.

- The library configuration report indicates media with unreadable barcodes by displaying a red triangle in the corner of the slot.

- The library user interface lists **No_Label** as the barcode for all cartridges with unreadable labels.

- The library posts a RAS ticket (T143) when an unreadable barcode label is detected. As long as that ticket remains open, no more T143 tickets will be issued, even if more unreadable barcode labels are found.

- An unreadable barcode label is re-scanned every time the cartridge moves to a new location to check if it is readable in the new location.

The paths to open the appropriate screens are as follows:

- From the operator panel, select **Tools > System Settings**.

- From the Web client, select **Setup > System Settings**.

Auto-Ticket Closure

For information about this feature, see <u>Closing RAS Tickets Automatically</u> on page 485.

Configuring the Library for FIPS

To configure your library for FIPS, perform the following steps:

1 Upgrade library firmware to version 600G or later.

2 For all HP LTO-5 FC tape drives that you plan to enable for FIPS, upgrade firmware to the latest version qualified with the Scalar i500 library (see the *Scalar i500 Release Notes* for qualified firmware levels).

3 Shut down the library.

4 Do one of the following:

If your library is...	Do this...
5U	Perform <u>Cabling a 5U Library for Ethernet Connectivity</u> on page 460.
14U or larger	Perform <u>Installing the Ethernet Expansion Blade</u> on page 461.

5 Power on the library.

6 Install Storage Networking and Encryption Key Management licenses on the library, if they are not already installed.

7 Enable FIPS mode (see <u>Enabling and Disabling FIPS Mode on HP LTO-5 Tape Drives</u> on page 131).

Enabling and Disabling FIPS Mode on HP LTO-5 Tape Drives

To operate your HP LTO-5 Fibre Channel tape drives to be compliant with FIPS, you must enable "FIPS mode." FIPS mode is configured by partition. You enable FIPS mode on a partition, which enables FIPS mode on all of the tape drives in the partition.

To change FIPS mode for a partition:

1 On the library web client, select **Setup > Encryption > Partition Configuration**.

The **Setup - Encryption Partition Configuration** page displays (see <u>Figure 16</u> on page 132).

Change the Encryption Method of a partition to **Enable Library Managed**.

2 Select the **FIPS** check box to enable FIPS mode for the partition. Clear the **FIPS** check box to disable FIPS mode for the partition.

3 Click **Apply**.

Figure 16 Enabling FIPS Mode

Viewing FIPS Status on the Library

There are three ways to view FIPS status on the library:

• The Partition Configuration screen **(Setup > Encryption > Partition Configuration)** shows which partitions are enabled for FIPS. All tape drives in FIPS partitions are enabled.

• The System Information Report (**Reports > System Information)** contains a **FIPS** column in the **Library Partitions** section. The column displays "Yes" if FIPS is enabled on the partition and "No" FIPS is disabled.

• The tape drive information pop-up screen on the Library Configuration Report (**Reports > Library Configuration**) contains a **FIPS Enabled** item. This item only displays when the tape drive is an HP LTO-5 Fibre Channel tape drive. The item displays "Yes" when FIPS is enabled on the drive and "No" when FIPS is disabled.

Configuring Operator Panel Display Settings

You can use the operator panel **Display Settings** screen to adjust the operator panel's brightness and contrast settings. The current applied settings appear on the screen. Adjust the brightness and contrast settings by tapping the up and down arrows. The **Defaults** button sets the brightness and contrast to the default settings.

You cannot configure the display settings from the Web client. The path to open the appropriate screen is as follows:

• From the operator panel, select **Tools > Display Settings**.

Registering the Library

Registering the library activates the warranty. After completing the initial setup of the library, choose **Setup > Register Library** on the Web client to automatically register the library. The library uploads the information you entered in the **Setup - Contact Information** screen (**Setup > Notifications > RAS > Contact**). If you have not filled out the contact information yet, you will receive a message with a link. Complete the **Setup - Contact Information** screen, and then return to the **Setup > Register Library** screen to complete registration.

You cannot register the library from the operator panel. The path to open the appropriate screen is as follows:

• From the Web client, select Setup > Register Library.

Advanced Reporting

Advanced Reporting is a licensable feature. You must have an Advanced Reporting license installed on your library in order to use the features described in this chapter. For more information on licensing, see <u>Obtaining and Installing a License Key</u> on page 88.

Advanced Reporting provides the following reports that you can configure, view, save, and e-mail:

- **Drive Resource Utilization Report**—Provides tape drive usage information, showing you which tape drives are working at optimum capacity and which are under-utilized. This can help you allocate your tape drive resources properly.

- **Media Integrity Analysis Report**—Provides TapeAlert count for various combinations of tape drives, tape cartridges, and TapeAlert flags. This can help you determine if a problem is due to a specific tape drive or tape cartridge.

Advanced Reporting provides the following logs that you can view, save, and e-mail:

- **Media Security Log** — Lists media that has been removed from the library.

- **Media Usage Log** — Lists information on all media that have ever been in the library.

In addition, you can automatically e-mail any of the reports and logs to designated recipients at specified, scheduled times.

> **Note:** To use all the features of Advanced Reporting, your library firmware must be at version 580G or higher.

This chapter covers:

- [About the Advanced Reporting License](#)
- [Working With Advanced Reporting Reports](#)
    - [Configuring the Drive Resource Utilization Report](#)
    - [Configuring the Media Integrity Analysis Report](#)
    - [Using Advanced Reporting Templates](#)
    - [Loading and Reloading Advanced Reporting Data](#)
    - [Deleting Advanced Reporting Data](#)
    - [Saving and E-mailing Report Data Files](#)
- [Configuring and Viewing the Media Security Log](#)
- [Viewing the Media Usage Log](#)
- [Automatically E-mailing Advanced Reporting Reports and Logs](#)

About the Advanced Reporting License

The Advanced Reporting license applies to your entire library, regardless of library size. This means you only need to purchase the license once. If you increase the size of your library, your existing license applies to your new library configuration.

Working With Advanced Reporting Reports

Details about Advanced Reporting reports include:

- The data for the reports is collected in log files. When the log files reach their maximum size, the oldest information is deleted as new information is added. This may affect how much historical data you can access.

- The on-screen reports contain a chart and a data table. When the log files are large, it would take an excessively long time to load all the historical data into the data table. For this reason, the table displays a maximum of 1000 rows of data, beginning with the most recent, even if more data is available. (The graph displays information for the entire range.) To view all of the data, you need to save or e-mail the data file. See Saving and E-mailing Report Data Files on page 142.

- The reports are built according to data in the log files, not your current library configuration. For this reason, your library may contain tape drives or cartridges that do not show up in the report. Similarly, the report may contain tape drives and cartridges that no longer reside in the library.

- Information about a tape drive, cartridge, or operation is not recorded in the Drive Resource Utilization log file until after a tape cartridge has been mounted (loaded) *and* unmounted (unloaded) from the tape drive.

Configuring the Drive Resource Utilization Report

This report identifies how tape drive resources are utilized in your library. You can use this report to help you determine the proper work load distribution between the tape drives in your library.

The following information is collected for each tape drive installed in the library:

- Drive location (module, row)

- Drive serial number

- Partition

- Megabytes read

- Megabytes written

- Time and date of mount (UTC)
- Time and date of dismount (UTC)
- Media motion time (in seconds)
- Tape cartridge barcode

To configure the report, specify the following:

- **Date Range** — Specifies the range of time covered in the report. Choose one of the following:
    - Last 7 days
    - Last 4 weeks (default)
    - Last 3 months
    - All History (as far back as there is data in the log file)
- **Attribute** — Specifies which values are included in the report. Select one of the following:
    - Data Written/Read (default) — The amount of data written to and read from each tape drive, shown separately in the chart.
    - Total Read and Write — The combined total amount of data written to and read from each tape drive.
    - Media Mount Count — The number of tape cartridge mounts.
    - Media Mount Time — The total amount of time media spent in the selected drive(s).
    - Media Motion Time — The total amount of time media spent in motion while in the tape drive (writing, reading, rewinding, etc.).
- **Chart** — How the data is displayed in the chart. Select Area, Bar (default), Line, or Pie.
- **Type** — The chart type. Select one of the following:
    - Rollup (default) — Displays the Grouping on the x-axis and the Attribute amount on the y-axis.
    - Trend — Shows how the Attribute amount changes over time for the selected Grouping.

- **Grouping** — Specifies which tape drive(s) or partition(s) to include in the report. Select one of the following:

  - All Drives by Coordinate (default) — Presents the sum total of the selected Attribute for all tape drives according to their location in the library. If more than one tape drive resided in that location during the selected Date Range, then the Attribute values for all the tape drives that resided in that location are combined in the chart.

  - All Drives by Physical SN — Presents the sum total of the selected attribute for all drives according to the physical tape drive serial number.

  - All Partitions — Presents a comparison of all drives grouped by partition in the physical library.

  - Selected Drive by Coordinate — The report chart is based on an individual tape drive location in the library. If more than one tape drive resided in that location during the selected Date Range, then the attribute values for all the tape drives that resided in that location are combined in the chart.

  - Selected Drive by Physical SN — The report chart is based on an individual tape drive identified by its physical drive serial number.

  - Selected Partition — The report chart is based on an individual partition in the physical library.

You can only access this report from the Web client. The path to open the report is **Reports > Advanced Reporting > Drive Resource Utilization**.

Configuring the Media Integrity Analysis Report

This report provides TapeAlert counts for various combinations of tape drives, tape cartridges, and TapeAlert flags. You can use this report to help determine if a problem is due to a specific tape drive or tape cartridge.

The report displays the number of TapeAlerts for the selected Grouping and combination of Attributes. Additionally, the downloaded report includes the last 10 tape drive error codes for each TapeAlert, displayed in columns with the headings **Error #1**, **Error #2**, and so on. (The onscreen report does not contain the tape drive error codes.)

The Media Integrity Analysis report collects the following information for each TapeAlert:

- Date and time (UTC) of TapeAlert occurrences

- Tape drive physical serial number

- Cartridge barcode

- TapeAlert value

- Occurrence count of each TapeAlert

- Tape drive error codes for each TapeAlert

To configure the report, specify the following:

- **Date Range** — Specifies the range of time covered in the report. Choose one of the following:

    - Last 7 days

    - Last 4 weeks (default)

    - Last 3 months

    - All History (as far back as there is data in the log file)

- **Attribute**—Specifies which values are included in the report, and how they are combined. Select in any combination, including all (default). If you select no attributes, the report uses Cartridge Barcode.

    - Cartridge Barcode — All relevant tape cartridges.

    - Drive Physical SN — All relevant tape drives.

    - TapeAlert — All TapeAlert flags that were issued. For a description of all TapeAlert flags, see <u>Appendix B, TapeAlert Flag Descriptions</u>.

- **Chart** — Specifies how the data is displayed in the chart. Choose Area, Bar (default), Line, or Pie.

- **Type** — Specifies the chart type. Select one of the following:

    - Rollup (default) — Displays the number of TapeAlerts for the combination of Grouping and Attributes you selected (default).

    - Trend — Shows the occurrence of TapeAlerts over time.

- **Grouping**—Specifies which drive(s) or tape cartridge(s) on which to base the report. Choose one of the following:

  - All (default) — All tape drives and tape cartridges for which a TapeAlert was issued during the specified Date Range.

  - Selected Drive by Physical SN — An individual tape drive. Only tape drives which issued a TapeAlert during the specified Date Range appear in the report.

  - Selected Cartridge by Barcode — An individual tape cartridge. Only tape cartridges that were associated with a TapeAlert during the specified Date Range appear in the report.

- **Sorting**— Specifies how the data will be sorted. Choose from the following:

  - Alphabetical

  - Count (ascending)

  - Last Occurrence (default)

You can only access this report from the Web client. The path to open the report is **Reports > Advanced Reporting > Media Integrity Analysis**.

Using Advanced Reporting Templates

If you want to use the same configuration repeatedly, you can save it as a template. You can save up to 20 templates for each type of advanced report.

Creating a Template

1 From the report configuration page, make the selections you want.

2 In the **Report Templates** box at the bottom of the screen, type a name for the template in the empty field next to the **Save** button. The name can have a maximum of 15 characters. You can use only lowercase letters, numbers, and the underscore character (_) in template names.

3 Click **Save**.

The report appears in the drop-down list next to the **Load** button.

Using a Template

To use a saved template, select the template from the drop-down list and click **Load**.

Deleting a Template

To delete a template, select the template from the drop-down list and click **Delete**.

Loading and Reloading Advanced Reporting Data

When you first open an Advanced Report configuration page, the system loads all the data from the library log file for that report to the Internet browser in preparation for creating your reports. If there is a lot of information in the log files, this may take several minutes.

The data that is loaded in the Internet browser remains unchanged until you log out of your library session or reload the data. If new data is added to the library log file during your session (for instance, a TapeAlert occurs), it will not appear in the onscreen report until you either log out of the library and log on again, or reload the data. To reload the data without logging out, click the **Reload** button. This reloads the entire data set, which may again take several minutes.

You can see how many records were loaded from the log files for this report by looking at the Report Data section of the report configuration page. A note says "XX records read," where XX is the number of records (see Figure 17).

Deleting Advanced Reporting Data

In some circumstances, you may wish to delete the information contained in the log files used to build the advanced reports. To do this, click the **Delete** button in the Report Data section of either report configuration page. This deletes the data for **both** the Drive Resource Utilization report and the Media Integrity Analysis report.

> **Caution:** Once you delete the data in the log files, you cannot get it back. The **Reload** button does NOT retrieve deleted data! It is recommended that you save all the data for both the Drive Resource Utilization report and the Media Integrity Analysis report before deleting the data (see <u>Saving and E-mailing Report Data Files</u>).

Figure 17 Report Data Buttons

Saving and E-mailing Report Data Files

You cannot save the report as it appears on the screen, but you can save or e-mail the report data as a comma-separated values (.csv) file. You can then import the .csv data into a spreadsheet program and manipulate it to create your own reports for analysis. The .csv file contains all of the data in the log file that falls within the date range you specify.

1 Generate a report.

2 Scroll down to the bottom of the report viewing screen to a box titled **Retrieve the Report Data File**.

3 To save the report data as a .csv file, click **Save**.

Note: To e-mail a saved report from the Web client, you must save the report, and then go to another page in the web client. Return to the report viewer page, scroll down to the bottom of the report viewing screen to a box titled **Retrieve the Report Data File**, and click **E-mail**.

4 To e-mail the report data as a .csv file, type the name of a recipient in the empty field next to the **E-mail** button, then click **E-mail**.

Figure 18 Saving and
E-mailing the Report Data

Retrieve the report data file:

| Save | E-mail | : recipient@company.com |

Configuring and Viewing the Media Security Log

Media removal is detected by the library when it performs an inventory (at boot up; after an open door is closed, etc.). The media security log lists media that have been removed from the library. You can enable the library to collect information about media removal, and then view, save, and/or e-mail the log.

You can configure the library to collect any or all of the following information. By default, the library collects nothing and the log is empty. You must select each item you want the library to collect:

• **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**

Note: **Unexpected removal** refers to tape cartridges that were removed from the library without being properly exported via the I/E station.
Expected removal refers to tape cartridges that were exported properly via the I/E station.

The log file contains the following information:

• Date and time of media removal

• Tape cartridge barcode

• Type of removal (expected or unexpected)

• Slot location coordinates (of the slot the cartridge is missing from)

• Slot type (I/E, storage, or cleaning)

When the log file reaches its maximum size, the oldest information is replaced as new information is added.

To configure what information gets tracked in the log, select **Setup > Notifications > Advanced Reporting > Media Security** from the Web client.

To view, save, or e-mail the report, select **Reports > Log Viewer** from the Web client. Select **Media Security Log** from the list of logs and click **Next**.

Viewing the Media Usage Log

The Media usage report lists information regarding data written and read on the media and lists statistics pertaining to soft and hard read and write errors.The media usage log collects information on all media that have ever been in the library, including media that are no longer in the library. Lifetime media usage metrics are associated with the cartridge and are kept on the embedded cartridge memory. The log reflects what the drive reports from the embedded cartridge memory whenever the media is unloaded. If the tape cartridge was never mounted and unloaded, it will not appear in the log. When the log file reaches its maximum size, old information is deleted as new information is added. This may affect the amount of available historical data.

The log provides the following information:

*   **Volser** — Media cartridge barcode label
*   **SN** — Media cartridge serial number
*   **Mfr** — Media cartridge manufacturer
*   **Date** — Media cartridge manufacturing date (format: YYYYMMDD)
*   **Type** — Media type
*   **Mounts** — Cartridge mount count
*   **RRE** — Recovered read errors
*   **URE** — Unrecovered read errors
*   **RWE** — Recovered write errors
*   **UWE** — Unrecovered write errors

- **LW** — Cartridge lifetime MB written

- **LR** — Cartridge lifetime MB read

- **Enc** — Cartridge encryption status (U=Unknown, E=Encrypted, N=Not Encrypted)

To view, save, or e-mail the report, select **Reports > Log Viewer** from the Web client. Select **Media Usage Log** from the list of logs and click **Next**.

Automatically E-mailing Advanced Reporting Reports and Logs

You can configure the library to automatically e-mail Advanced Reporting logs and reports to specified recipients on a daily or weekly basis.

You can create up to 20 e-mail recipients. If you want to send the same recipient a different set of reports, you can enter the same e-mail address more than once, with different reports selected for each. Each entry counts as a unique recipient toward the 20 total.

> **Note:** Duplicate entries are not allowed. A duplicate entry means the same recipient is set to receive the exact same reports in two different entries, regardless of the day or time. If you have duplicate recipients, make sure that the reports selected in each entry are not an exact match.
>
> For example, if you have one entry in which Recipient A receives the Drive Utilization and Media Integrity reports on Monday, you cannot create another entry to send Recipient A the Drive Utilization and Media Integrity reports on Thursday. Instead, you can create one entry for Recipient A and send the reports every day (select **Daily** as the day to send the report), or you can change the reports you are sending so that they are not the same as the first entry. You could create three entries for Recipient A as follows: 1) send both reports out on Monday; 2) send Drive Utilization out on Thursday; and 3) send Media Integrity out on Thursday (in a different entry). The recipient is the same, but the reports sent in each entry are different.

Each e-mail notification includes an optional comment text box you can use to enter information about the library or the reports and logs that you want the recipient to know. This information appears in the body of the e-mail.

You can modify the settings of an existing e-mail notification at any time after it is created. If an e-mail notification is no longer needed, you can delete it.

Before the library can send e-mail notifications, you must configure the library e-mail account. For information on how to configure the e-mail account, see <u>Configuring the Library E-mail Account</u> on page 92.

Administrators can configure the library e-mail account and e-mail notifications. Users with user privileges can receive e-mail notifications, but they cannot configure the library e-mail account or e-mail notifications.

The path to open the appropriate screen is as follows:

- From the Web client, select **Setup > Notifications > Advanced Reporting > Receiver Addresses**.

Capacity on Demand

All Scalar i500 library configurations ship with the purchased number of slots pre-activated. The number of available pre-activated slots begins at 41 for all library configurations and increases in 46-slot increments to a maximum of 409 slots in the 41U library configuration.

After the initial purchase of your library, you can activate any remaining inactive slots in your library by purchasing a COD license upgrade. Upgrades are sold in 46-slot increments. For example, a 14U library could have 87 slots licensed at the time of the initial purchase (41 default + 46 purchased = 87). The remaining 46 slots of the 14U library can be activated at a later time by purchasing an upgrade. The full 133 slots would then be available for use.

If you upgrade to more slots, your new license key contains the entire license corresponding to your expanded slot count. The new license key replaces your current license key. For more information on licensing, see Obtaining and Installing a License Key on page 88.

It is possible to license more slots than are physically available in the library. In that case, when expansion modules are added, the extra licensed slots then become available for use.

To see your library's current configuration and slot availability, open the Library Configuration Report (choose **Reports > Library Configuration** from the Web client).

Table 6 shows the number of default and available pre-activated slots available for purchase and the number of slots you can activate with a COD license key for each library configuration.

Table 6   Available Slots and
COD Upgrades Per
Configuration

	5U	14U	23U	32U	41U
Minimum, Maximum Available Slots (including I/E station slots)	41, 41	41, 133	41, 225	41, 317	41, 409
Default Pre-Activated Slots	41	41	41	41	41
Available Pre-Activated Slots	41	41, 87, 133	41, 87, 133, 179, 225	41, 87, 133, 179, 225, 271, 317	41, 87, 133, 179, 225, 271, 317, 363, 409
Available COD Slot Upgrades	NA	87, 133	87, 133, 179, 225	87, 133, 179, 225, 271, 317	87, 133, 179, 225, 271, 317, 363, 409

Storage Networking

Storage Networking (SNW) is a licensable feature that allows you to take advantage of the control path failover, data path failover, and host access configuration features of 8 Gb/s HP LTO-5 FC tape drives, without those drives being connected to a 4 Gb/s FC I/O blade. (Since the FC I/O blade has a maximum speed of 4 Gb/s, you can only get the full speed by NOT being connected to the FC I/O blade.)

The SNW license is also required for FIPS compliance. For more information on FIPS, see FIPS-Certified Encryption Solution on page 199.

This chapter covers:

- About the Storage Networking License
- Configuring Control Path Failover
    - Forcing Control Path Failover
- Configuring Data Path Failover
    - Enabling Data Path Failover
    - Forcing Data Path Failover
- Configuring Host Access
    - Registering a Host for Host Access
    - Enabling Tape Drives for Host Access
    - Mapping a Host to Tape Drives and Partitions
    - Modifying a Host
    - Deleting a Host

About the Storage Networking License

If you purchase a Storage Networking (SNW) license after you purchase your library, you must install the license key on your library to enable the SNW functionality.

The SNW license is sold on a per-drive basis. The license installed on the library indicates the number of tape drives that are licensed.

If you purchase an SNW license for a particular number of tape drives and later want to license more drives, you must purchase additional SNW licenses.

The licenses are not tied to specific tape drives, but to how many tape drives are currently using SNW features. If you remove all SNW features from a tape drive, then the license becomes available to use on another tape drive.

For more information on licensing, see

Configuring Control Path Failover

If an HP LTO-5 FC tape drive is the control path for a partition, you can select another HP LTO-5 FC tape drive in that partition for control path failover. This means that if the control path tape drive fails, the failover tape drive becomes the control path for the partition. The failed-over tape drive remains the control path for the partition unless it fails or the library is restarted. When either of these events occurs, the library starts over and attempts to use the original control path tape drive as the control path, and the original failover tape drive for failover.

Details about control path failover include:

- The SNW license must be sufficient to cover both the control path and failover tape drives in order to enable a tape drive for failover.

- The control path and failover tape drives must both be HP LTO-5 Fibre Channel tape drives.

- Both the control path and failover tape drives must have their topology configured as **Point to Point** (see Setting Tape Drive Parameters on page 83). Previously, the library allowed you to change the topology once control path failover was configured, even though this prevented the feature from working. Now, the library will not enable control path failover unless both the control path and failover tape drives are configured as Point to Point, and will not allow you to change the topology from Point to Point on any tape drives configured for control path failover.

- The control path and failover tape drives must be connected to an NPIV-enabled switch on the same fabric. They must not be connected to an FC I/O blade.

- The control path and failover tape drives are assigned by location in the library, so even if you replace a tape drive, the library will still fail over or revert to the specified location.

- When control path failover is configured for a partition, the partition uses a virtual port as the control path communication port. The World Wide Port Name (WWPN) for this virtual port is listed in the library's System Information Report in the Library Partitions section under Control Path (see Viewing the System Information Report on page 267).

- A tape drive can be configured for both control path failover and data path failover (see Configuring Data Path Failover on page 154).

- You can manually force a failover (see Forcing Control Path Failover on page 151).

You can only configure control path failover from the Web client. The path to open the appropriate screen is:

- From the Web client, select **Setup > Control Path**.

Forcing Control Path Failover

You can manually force a control path failover. You might want to force a failover to check that the non-active tape drive still works, or to switch back to the original control path tape drive once the issue that originally caused the failover has been fixed.

To force a control path failover:

1 From the Web client, click **Tools > Drive Operations**.

The **Tools - Drive Operations** screen displays (see Figure 19).

Figure 19 Forcing Control Path
Failover
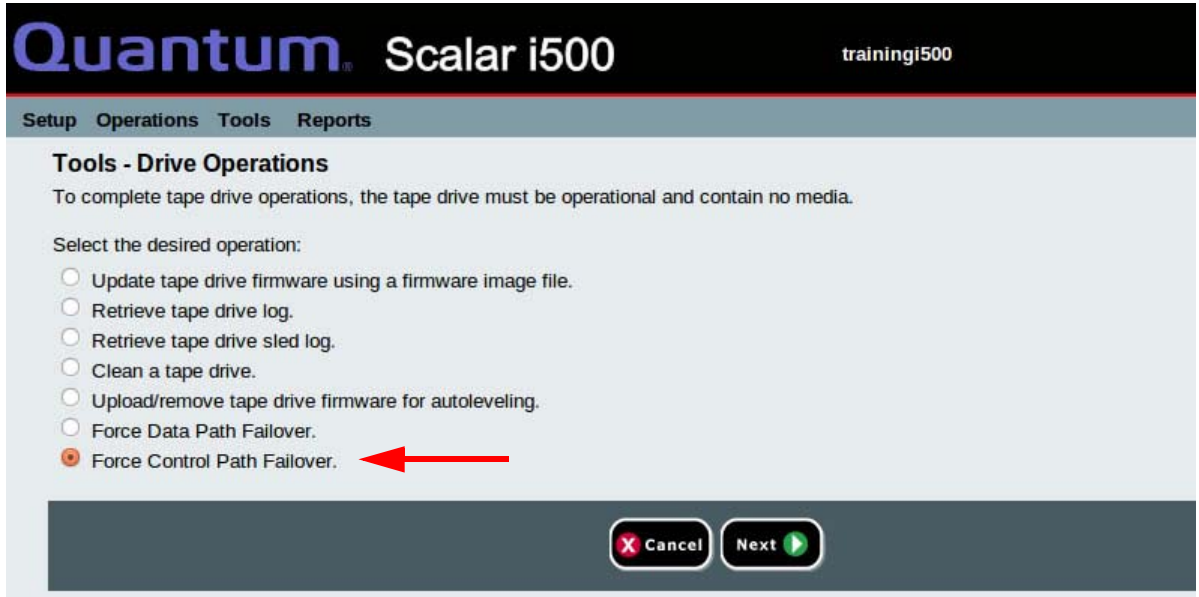
2 Select **Force Control Path Failover** and click **Next**.

The **Force Control Path Failover** screenu displays (see Figure 20). All of the partitions that have control path failover enabled are listed. The location and status of the tape drive that is currently serving as the control path are listed in the **Active** columns. The location and status of the tape drive that is currently serving as the standby control path are listed in the **Standby** columns. For each partition, the following information is listed:

Column	Indicates
Active Drive	Location of the current control path tape drive.
Active Status	Ready status of the current control path tape drive.
Active Connected	Whether the current control path tape drive is connected and has a working link.

Column	Indicates
Standby Drive	Location of the standby tape drive.
Standby Status	Ready status of the standby tape drive.
Standby Connected	Whether the standby tape drive is connected and has a working link.

Figure 20 Forcing Control Path Failover
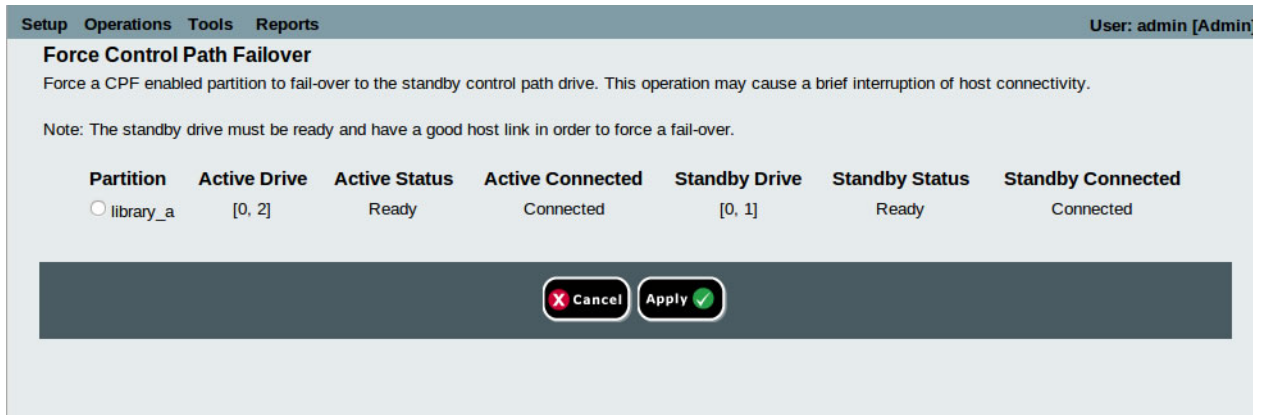
3 Select the partition on which you want to force the failover.

> **Note:** The standby tape drive must be "ready" and "connected" in order to force a failover.

4 Click **Apply**.

The new active tape drive location displays in the **Active Drive** column. The new standby tape drive location displays in the **Standby Drive** column.

> **Note:** If the new tape drive locations do not display, refresh the browser.

Configuring Data Path Failover

Data Path Failover provides an alternate data path when a preferred data path fails. The Data Path Failover functionality is provided as part of the Storage Networking license and applies to HP LTO-5 Fibre Channel tape drives only.

HP LTO-5 Fibre Channel tape drives have two Fibre Channel ports. If you enable data path failover on the tape drive, one port will be used as the "active port" for data transmission, and the other port will stand by to be used if the active port fails. If the tape drive loses its Fibre Channel link with the active port, it will automatically "fail over" and use the standby port to continue drive operations. The library issues a RAS ticket when automatic failover occurs. In addition, the library monitors the standby port and issues a RAS ticket if the standby port does not report a good Fibre Channel link status.

The library uses Port 1 for data path transmission unless a failover occurs. Once failover occurs, the library uses Port 2 until failover occurs again or the library is rebooted. Similarly, if a tape drive configured for data path failover is the control path for a partition, the host uses Port 1 for media changer commands unless a failover occurs. Once failover occurs, the host uses Port 2 until failover occurs again or the library is rebooted.

Note:	Performing a drive reset operation is another way to make Port 1 the active port again, unless the reason Port 2 is active is due to a forced failover (see Forcing Data Path Failover on page 157). If you forced a failover to Port 2 and then reset the tape drive, the library and host will continue to use Port 2 until failover occurs again or the library is rebooted.

A tape drive can be configured for both data path failover and control path failover. If both are configured, the control path will not fail over to another tape drive unless both ports on the control path tape drive fail.

If desired, you can manually switch the active port (see Forcing Data Path Failover on page 157).

> **Note:** If you are NOT using data path failover on a tape drive, then only Port 1 is used for data path or control path transmission. The library and host will not recognize Port 2 unless data path failover is enabled on the tape drive.

Details about data path failover include:

• The tape drives must be HP LTO-5 Fibre Channel tape drives.

• HP LTO-5 FC tape drive firmware must be at the version qualified with the Scalar i500 library (see the *Scalar i500 Release Notes* for qualified firmware levels).

• The library must have a Storage Networking license sufficient to cover the tape drive(s) on which you want to configure data path failover.

• Both FC ports on the tape drive must be connected to a host or switch. Neither tape drive port may be connected to a Fibre Channel I/O blade.

• Data path failover must be enabled on the tape drives (data path failover is disabled by default).

• Tape drive topology settings must be set to Point to Point.

Enabling Data Path Failover

To enable data path failover:

1 Connect both tape drive Fibre Channel ports (Port 1 and Port 2) to a host or switch (see Figure 21).

Figure 21 HP LTO-5 Fibre
Channel Tape Drive Ports
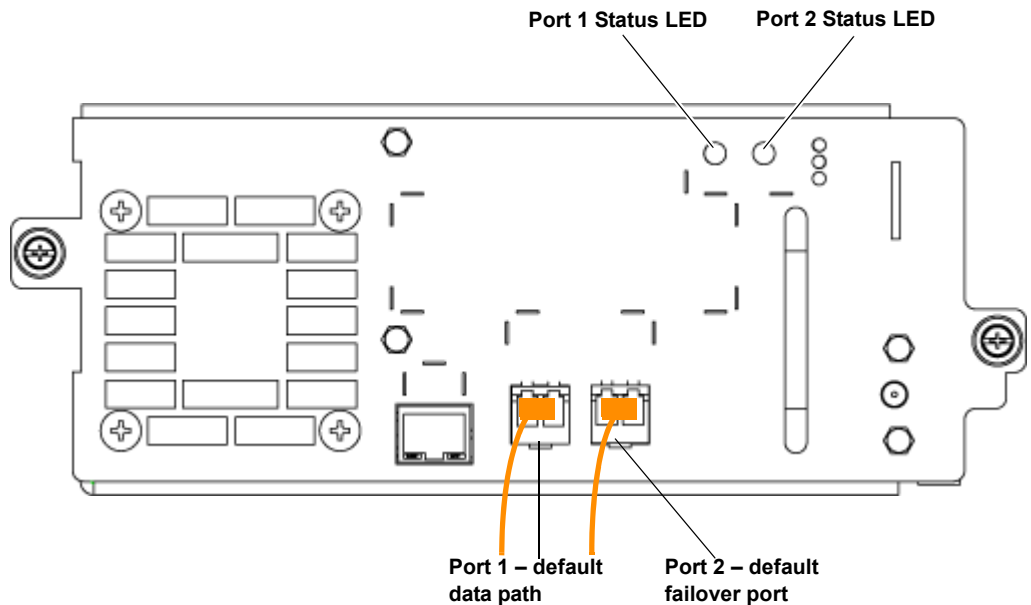
2 From the library **Setup** menu, click **Drive Settings**.

The **Setup - Drive Settings** page displays (see Figure 22).

3 For each tape drive on which you want to enable data path failover, do the following:

    a First, change the **Requested Topology** setting to **Point to Point**.

    b Then select the **DPF** check box.

4 Click **Apply**.

> **Note:** The illustration shows Port 1 as the default data port and Port 2 as the default failover port, but these defaults apply **only** if the data path failover feature is not enabled when you insert cables.
>
> If data path failover is enabled, the first port into which you insert a cable becomes the active data port and the second port becomes the failover port. For example, if data path failover is enabled and you insert a cable into Port 2, that port becomes the active data port. Inserting a cable into Port 1 makes that the port used for data path failover.

Figure 22 Enabling Data Path Failover

Setup - Drive Settings

Modify the settings on Fibre Channel drives.

Fibre Channel Drives

Total Number of Drives: 17

Type	Location	DPF	Loop ID	Requested Topology	Speed	Actual Topology	Speed	WWNN	FC I/O Blade Connected	▲ Partition
LTO-5	1,4	☑	59 ˅	Point to Point ˅	Auto ˅	Loop (L)	8 Gb/s	500308C0:9894F01C	No	library_5
LTO-5	0,2	☐	63 ˅	Auto (NL) ˅	Auto ˅	Loop (L)	8 Gb/s	500308C0:9894F004	No	library_5
LTO-5	-1,2	☐	71 ˅	Auto (NL) ˅	Auto ˅	Loop (L)	8 Gb/s	500308C0:9894F094	No	library_5
LTO-5	3,1	☐	37 ˅	Auto (NL) ˅	Auto ˅	Loop (L)	8 Gb/s	500308C0:9894F030	No	library_5
LTO-5	-1,1	☐	69 ˅	Auto (NL) ˅	Auto ˅	Loop (L)	8 Gb/s	500308C0:9894F090	No	library_5
LTO-5	1,2	☐	55 ˅	Auto (NL) ˅	Auto ˅	Loop (L)	8 Gb/s	500308C0:9894F014	No	library_b5

◀ Page 1 of 3 ▶   Drives: 1 through 6

❌ Cancel   Apply ✔

Forcing Data Path Failover

You can manually swich the active Fibre Channel port on a DPF-enabled tape drive by forcing a failover. You might want to force a failover to check that the non-enabled port still works, or to switch back to using Port 1 once the issue that originally caused it to fail over is fixed.

You can only force a failover on one tape drive at a time. Both Fibre Channel ports must be connected to a host or switch.

You can only force a failover from the Web client.

To force a data path failover:

1 From the **Tools** menu, click **Drive Operations**.

The **Tools - Drive Operations** screen displays (see Figure 23).

Figure 23 Forcing Data Path
Failover

2 Select **Force Data Path Failover** and click **Next**.

The **Force Data Path Failover** page displays (see Figure 24). All of the tape drives that have data path failover enabled are listed. The port currently being used as the data path is listed in the **Active Port** column. The **Active Port** column will state "No Link" if neither port is connected.

Figure 24 Forcing Data Path
Failover

3 Select the tape drive on which you want to force the failover.

Note:	The tape drive must be in the "ready" state in order to be selected.

4 Click **Apply**.

The new active port displays in the **Active Port** column.

Note:	If the new active port does not display, refresh the page in the browser.

Note:	The library will issue a RAS ticket if the forced failover fails. The library will not issue a RAS ticket if the forced failover succeeds.

Configuring Host Access

Host Access provides a way to limit host access to specific tape drives and partitions via the library interface.

To use host access, you must have a Storage Networking license on the library. The Storage Networking license must be sufficient to cover the tape drive(s) you want to configure for host access.

To configure host access, you must first register the host(s) for host access, and enable host access on the desired tape drive(s). Then you will map the host to the tape drives or partitions you want the host to access.

Details about host access include:

- A registered host has full access to all tape drives in the library that have not been enabled for host access, and full access to all tape drives that are enabled for host access and have been mapped to that host. A registered host has no access to drives that have been enabled for host access but are not mapped to that host.

- An unregistered host has full access to all tape drives in the library that have not been enabled for host access, but no access to tape drives that have been enabled for host access.

- Tape drives that are enabled for host access can only be accessed by registered hosts that are mapped to them.

- Tape drives that are not enabled for host access can be accessed by all hosts.

- If the control path and any failover tape drives for a partition are enabled for host access, then only the hosts mapped to that partition will be able to send media changer commands to that partition. Unregistered hosts and registered hosts not mapped to that partition will not be able to send media changer commands to that partition. However, unregistered hosts and registered hosts that are not mapped to that partition do still have access and can send commands to any non-host-access-enabled tape drives in the partition, as well as any host-access-enabled tape drives in the partition to which they are mapped.

• A maximum of 64 host entries can be mapped for access control to each tape drive, regardless of whether the hosts are mapped to the tape drive, to the partition for which the drive provides the library control path, or both. If the same host is mapped to both the tape drive and the partition, the same host consumes two host entries.

You can only configure host access control from the Web client. The menu paths are:

• **Setup > Host Access > Host Registration** and

• **Setup > Host Access > Host Connections**

Registering a Host for Host Access

There are two ways to register a host: using the **Create** and **Add** buttons.

Create

Create allows you to manually create and register a host by entering the host information.

1 From the Web client, select **Setup > Host Access > Host Registration**.

2 Click **Create**.

3 Enter a user-defined host name.

4 Enter the host WWPN.

5 Select the host type from the pull-down list.

6 Click **Apply**.

The host appears in the list of registered hosts on the **Setup - Host Registration** screen.

Add

Add allows you to choose a host for registration from a list of unregistered hosts.

1 From the Web client, select **Setup > Host Access > Host Registration**.

2 Click **Add**.

The library displays a list of all currently unregistered hosts that are connected to tape drives or FC I/O blades in the library.

3 Select a host and click **Add** (you can only add one host at a time).

4 Under **Add a Host**, enter or modify the host name in the **Name** field and select the host type from the **Select Type** drop-down list.

5 Click **Apply**.

This registers the host. The page reloads so you are now viewing the Registered Hosts list on the **Setup - Host Registration** screen. The host you just added appears on the Registered Hosts list (and no longer appears on the Unregistered Hosts list).

6 If you need to register more hosts from the Unregistered Hosts list, click **Add** again to see the list of unregistered hosts, and proceed from Step 4.

Enabling Tape Drives for Host Access

Tape drives must be enabled for host access before you can map hosts to them.

1 Navigate to **Setup > Host Access > Host Connections**, or click the **Access** button from the **Setup - Host Registration** screen.

The **Setup - Host Connections** screen appears, displaying a list of all tape drives that can be enabled for host access.

2 Select the **Access Control** check box of all tape drives you want to enable for host access.

3 Clear the **Access Control** check box of any tape drives you do not want to enable for host access.

> **Note:** If you disable a tape drive that was previously enabled and mapped to hosts, the tape drive can be accessed by all hosts. However, the library keeps track of the mapped connections, so that if you re-enable the tape drive later, the connections you had before are reinstated.

4 Click **Apply**.

5 Click **Next** to go to the next screen to map hosts to tape drives and partitions. (If the **Next** button does not appear on the screen, it means no tape drives are enabled for host access.)

Mapping a Host to Tape Drives and Partitions

You must map one host at a time, and click **Apply** after configuring each host.

1 Navigate to **Setup > Host Access > Host Connections**, or click the **Access** button from the **Setup - Host Registration** screen.

2 Select drives to enable for host access (described in <u>Enabling Tape Drives for Host Access</u> on page 162) and click **Next**.

The **Setup - Connection Configuration** screen appears, displaying two or three sections of items to map, as follows:

- **Hosts** — Displays all registered hosts.

- **Partitions** — Partitions will only display if the control path tape drive for the partition is enabled for host access. If the control path tape drive has a failover tape drive associated with it, then the failover tape drive must also be enabled for host access. Mapping a partition to a host allows the host send media changer commands to the partition through the control path tape drive.

- **Devices** — Displays all tape drives that are enabled for host access. Mapping a host to a tape drive gives the host access to the tape drive.

3 Select a host.

The **Partitions** and **Devices** lists refresh showing the currently selected partitions and drives mapped to that host.

4 Select the check boxes corresponding to partitions/drives to give the host access; clear the check boxes to make the partitions/drives inaccessible to the host.

5 Click **Apply**.

6 Repeat the above steps on another host if desired.

Modifying a Host

You can modify the host name and host type of a registered host. Changing these settings will not affect your host access connections.You cannot modify the WWPN of a registered host. If you need to change the WWPN, you must delete the host and create a new one.

To modify a host:

1 Click **Setup > Host Access > Host Registration**.

2 Select a host and click **Modify**.

3 Modify the host name or type and click **Apply**.

Deleting a Host

Deleting a host un-registers it with the library. The host is deleted from the Registered Host list.

If the host is mapped to drives or partitions on the **Setup - Connection Configuration** screen, you will need to disable all the mapped connections before you can delete the host.

To delete a host:

1 Click **Setup > Host Access > Host Registration**.

2 Select a host and click **Delete**.

A dialog box opens asking you to confirm you want to delete the host.

3 Click **OK**.

Chapter 7

Encryption Key Management

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.

The Scalar i500 supports three encryption key management systems, which are described in Table 1. These systems work in conjunction with the library to generate, protect, store, and manage encryption keys. The keys are used by tape drives to encrypt information being written to, and decrypt information being read from, tape media. The library communicates with the encryption key management server(s). The encryption keys pass through the library, so that encryption is "transparent" to the applications. Using the library in this way is known as "library managed encryption."

Note:	These three solutions are not interoperable. The Scalar i500 library does not support more than one encryption key management system on a single library.

Note:	Library firmware version 607G.GS003 (release i7.2) only supports KMIP Key Managers. Other encryption systems are not supported.

Table 1 Encryption Systems

Encryption System	Supported Tape Drives	Supported Media
Quantum Encryption Key Manager (Q-EKM)	IBM LTO-4 Fibre Channel and SAS IBM LTO-5 Fibre Channel IBM LTO-6 Fibre Channel You must be running Q-EKM version 2.0 (or higher) to support IBM LTO-5 tape drives.	LTO-4, LTO-5, and LTO-6 tape cartridges
Scalar Key Manager (SKM)	HP LTO-4 Fibre Channel and SAS HP LTO-5 Fibre Channel and SAS HP LTO-6 Fibre Channel and SAS	LTO-4, LTO-5, and LTO-6 tape cartridges
KMIP-compliant key managers*	HP LTO-4 Fibre Channel and SAS HP LTO-5 Fibre Channel and SAS HP LTO-6 Fibre Channel and SAS	LTO-4, LTO-5, and LTO-6 tape cartridges

*   The Key Management Interoperability Protocol (KMIP®) is a specification developed by OASIS®. Its function is to standardize communication between enterprise key management systems and encryption systems. The Scalar i500 library provides a KMIP version 1.0 compliant encryption solution.

KMIP is only supported in certain environments. See the release notes for details.

If you purchase Q-EKM, Quantum Support will schedule an appointment to install the application onto your key server(s). If you purchase SKM, you will receive the software application, two key servers (optional), and installation and configuration instructions. Installation for KMIP-compliant systems differ according to the manufacturer, and may include up to 10 key servers.

This chapter describes how to configure your encryption key management (EKM) solution on the library. This chapter also describes all of the EKM functions available on the library.

Refer to the *Quantum Encryption Key Manager User's Guide*, the *Scalar Key Manager User's Guide,* or your KMIP key manager user's guide for information on how to manage your encryption system outside of the library.

This chapter covers:

KMIP-compliant Encryption Key Management

The Key Management Interoperability Protocol (KMIP®) is a specification developed by OASIS®. Its function is to standardize communication between enterprise key management systems and encryption systems. With version i7.2, the Scalar i500 provides a KMIP version 1.0 compliant encryption solution.

KMIP is currently only supported with SafeNet® KeySecure servers. Contact your Quantum representative for details.

Details about the Scalar i500 KMIP-compliant implementation include:

- As with other encryption systems supported by the library, in order to use KMIP-compliant encryption systems with the Scalar i500, you must have an Encryption Key Management license installed on the library.

- A minimum of two KMIP-compliant encryption servers are required for failover purposes. A total of 10 KMIP-compliant encryption servers are allowed, for increased failover capability.

See Configuring Encryption Key Management on the Library on page 169 for more information and instructions on how to configure KMIP-compliant encryption systems on the library.

General Notes About Encryption on the Library

Keep the following points in mind when using encryption on the library:

- Data written to encryption-supported and encryption-capable media in EKM-supported tape drives will be encrypted *unless* data was previously written to the media in a non-encrypted format. In order for data to be encrypted, 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).

- You cannot append encrypted data to a non-encrypted tape.

- You cannot append non-encrypted data to an encrypted tape.

- Only one data encryption key can be used per tape cartridge.

- Encryption is configured by partition. Partitions must be configured for "Library Managed Encryption." EKM partitions must contain only the tape drives supported by the encryption system you are using. (For more information, see Step 6: Configuring Partitions for Library Managed Encryption on page 180.

About the EKM License

If you purchase an EKM license after you purchased your library, you must install the license key on your library to enable the EKM functionality. The EKM license is sold on a per-drive basis. The license corresponds to the number of tape drives that you can enable for library managed encryption. If your library contains more encryption-enabled tape drives than are covered by the license, you will need to purchase an additional license to cover them. Your new license key replaces your current license key and contains the entire license for the total number of tape drives.

Configuring Encryption Key Management on the Library

Make sure your Q-EKM, SKM, or KMIP-compliant key servers are installed and running before configuring the library (see the *Quantum Encryption Key Manager User's Guide*, the *Scalar Key Manager User's Guide,* or your KMIP key manager user's guide for instructions).

Then follow these steps, in order, to configure the library:

> **Note:** Scalar Key Manager is very sensitive to network instability due to the large amount of operations occurring in rapid succession. If you get an error stating that an SKM operation failed, check network functionality and try the operation again.
>
> Make sure ports 80, 6000, and 6001 on the SKM servers are opened up in a bi-directional mode on all firewalls in your network. If they are not, the library will not be able to communicate with the SKM servers.

Step 1: Installing the EKM License Key on the Library

If your EKM license key is not already installed on the library, install it now.

Step 2: Preparing Partitions for Library Managed Encryption

For each partition on which you want to enable library managed encryption, do the following:

1 Make sure the partition contains encryption-supported and encryption-capable tape drives and media. Note the following:

- **Q-EKM partitions** must contain only IBM LTO-4, IBM LTO-5, and/or IBM LTO-6 tape drives.

  > **Note:** You must be running Q-EKM version 2.0 (or higher) to support IBM LTO-5 or LTO-6 tape drives.

- **SKM partitions** must contain only HP LTO-4, HP LTO-5, and/or HP LTO-6 tape drives. **SKM media** must have valid barcode labels affixed. SKM does not support the use of unlabeled media.

- **KMIP partitions** must contain only HP LTO-4 and/or HP LTO-5 tape drives.

1 On the tape drives, install the latest version of firmware that is qualified for the library firmware installed on your library. Refer to the library release notes for the correct version of tape drive firmware. (It is recommended that you upgrade library firmware to the latest release.)

2 Unload tape cartridges from all tape drives in the partitions on which you are configuring EKM.

Step 3: Configuring Encryption Settings and Key Server Addresses

Configure encryption settings and key server information as follows:

1 From the Web client, select **Setup > Encryption > System Configuration.**

The **Setup - Encryption System Configuration** screen displays (see Figure 25).

Figure 25 Setup - Encryption
System Configuration (KMIP
Key Manager)

2 **Key Server Type —** This field only appears if you have HP tape
   drives installed in the library. If this field is visible, select which
   encryption solution you plan to use (**Q-EKM**, **SKM**, or **KMIP Key
   Manager**).

3 **Automatic EKM Path Diagnostics —** Enable or disable as desired;
   however, it is recommended you leave the default. For more
   information, see Using Automatic EKM Path Diagnostics on
   page 186). When enabled, this feature performs a check, at specified
   intervals, to make sure both key servers are connected to the library
   and functioning properly. The library generates a RAS ticket if there
   are problems.

4 Interval — If Automatic EKM Path Diagnostics is enabled, select the interval at which the library performs the diagnostics.

5 Test Warning Threshold — For Q-EKM only. If Automatic EKM Path Diagnostics is enabled, specify the number of consecutive missed test intervals required to generate a RAS ticket.

6 SSL Connection — Enable or disable as follows, depending on which key server you are using:

- **Q-EKM** — To enable SSL for communication between the library and the EKM servers, select the **SSL Connection** check box. The feature is disabled by default. If you enable SSL, you must make sure that the port numbers listed in the **Port** text boxes (below) match the SSL port numbers set on the Q-EKM servers. The default SSL port number is 443.

> **Note:** Keys are always encrypted before being sent from the Q-EKM key server to a tape drive, whether SSL is enabled or not. Enabling SSL provides additional security.

- **SKM** — SSL is always enabled. The SSL port number is always 6000.

- **KMIP Key Manager** — SSL is always enabled.

> **Note:** For SKM and KMIP Key Manager, the library actually uses Transport Layer Security (TLS), a more secure successor to SSL, to communicate with the encryption servers.

7 Key Server IP Address or Host Name — In the text boxes, assign your key servers in the order in which you want failover to occur. The **"#"** column denotes the server failover order. Once you add the servers, you can change the failover order by clicking the up/down arrow buttons in the **Order** column.

> **Note:** **Q-EKM** requires one or two servers. If you do not plan to use a secondary key server, you may type a zero IP address, 0.0.0.0, in the #2 text box, or you may leave the text box blank.
>
> **SKM** requires two servers.
>
> **KMIP Key Manager** requires at least two servers and can have up to 10 servers for increased failover capacity.

For an initial key request, the library tries server #1 (the primary server) first. If server #1 is not available to perform a key request, the library tries server #2. For KMIP key managers, if server #2 is not available, the library will try server #3, and so on, in order.

Once the library identifies a server that can perform the request, this server remains the active server until it fails a key request or the library is rebooted. At that point, the library starts over and uses server #1 for key requests.

In the text boxes, type either:

- The IPv4 or IPv6 address of the key server (if DNS is not enabled), or

- The host name of the key server (if DNS is enabled).

8 **Port —** In the **Port** text boxes, type the port numbers corresponding to the listed servers. The port number listed in the text box must match the port number on the server. Note the following:

- **Q-EKM —** The default port number is 3801 unless SSL is enabled. If SSL is enabled, the default port number is 443.

> **Note:** If you change the Q-EKM port number listed in the Port text box from the default setting on the library, you must also change the port number on the actual key server to match, or library managed encryption will not work properly. See the *Quantum Encryption Key Manager User's Guide* for information on setting the port number on the Q-EKM key server.

> **Note:** If you are using a secondary Q-EKM key server, then the port numbers for both the primary and secondary key servers must be set to the same value. If they are not, synchronization and failover will not occur.

- **SKM** — The port number is always 6000. You cannot change SKM port numbers.

- **KMIP Key Manager** — The port number must match the configured port number on the KMIP key manager server. A typical port number used for communication between the KMIP key manager server and the library is port 9003.

9 Click **Apply**.

> **Note:** You cannot edit the encryption system configuration settings when any partition is enabled for library managed encryption. If this happens, go to **Setup > Encryption > Partition Configuration**, change all EKM partition settings from **Enable Library Managed** to **Allow Application Managed**. Then make your changes to the system configuration settings. Finally, go back and change all the EKM partition settings to **Enable Library Managed**.

10 Ensure all ports corresponding to the EKM servers are open on your firewall to allow the library to connect to the servers. For SKM, ports 80, 6000, and 6001 must be open.

Step 4: Installing TLS Certificates on the Library (SKM Only)

If you are running SKM or a KMIP key manager, Transport Layer Security (TLS) communication certificates with valid dates must be installed on the library in order for the library to communicate securely with attached EKM servers.

> **Note:** If you are using Q-EKM, skip this step. No TLS certificates are required.

At any time, you may install a new set of TLS certificates to overwrite the existing set. The new TLS certificates must all be valid or the overwrite will not occur and the existing certificates will remain in place.

Take one the following actions, according to which encryption system you are using.

Encryption System	Action
Scalar Key Manager (SKM)	If you purchased your library with firmware version 570G or higher, the library came with TLS certificates pre-installed. You can check the Web client to see whether TLS certificates are installed (see Checking for Current Certificates on page 175).
	If valid TLS certificates are currently installed, you do not need to do anything. However, if you wish, you may install your own certificates to replace the existing certificates (see Installing Your Own TLS Certificates on the Library on page 177).
	If valid TLS certificates are not installed, you must install them. You can install either of the following:
	Quantum-provided TLS certificates (see Installing Quantum-Supplied TLS Certificates on the Library on page 176).
	Your own TLS certificates (see Installing Your Own TLS Certificates on the Library on page 177).
KMIP-compliant key management	TLS certificates will be provided by your KMIP server administrator. Install certificates as described in Installing Your Own TLS Certificates on the Library on page 177.

Checking for Current Certificates   From the **Tools** menu, select **EKM Management > Import Communication Certificates**.

The **Tools - TLS Communication Certificate Import** screen appears (see Figure 26).

If TLS certificates are currently installed, they will be listed in a table at the bottom of the screen. If they are not installed, a message appears at the bottom of the screen stating that certificates are not installed.

Figure 26 TLS Communication Certificate Import Screen

Tools - SKM Communication Certificate Import

Import TLS communication certificate(s).

Note: Transport layer security (TLS) certificates may be uploaded by browsing to the files and selecting Apply.
Either individual certificates or a Quantum certificate bundle may be uploaded if applicable.
Quantum bundles are only applicable for SKM certificates.

Select the Certificate Type to install: | KMIP Key Manager ⊕

Root Certificate File: [   ] Browse...

Admin Certificate File: [   ] Browse...

Admin Certificate Password: [   ]

Client Certificate File: [   ] Browse...

Client Certificate Password: [   ] ☐ Use Admin Password

Use the Quantum Certificate Bundle: ☐

Quantum Communication Certificate Bundle File: [   ] Browse...

Type	Location	Serial Number	Valid Between Dates	Status	Issuer and Subject
Root	Library	0	Mar 29 13:20:05 2011 GMT Mar 27 13:20:05 2021 GMT	Valid	**Issuer:** C:US S:Colorado L:Englewood O:Quantum OU:Tape Automation CN:Quantum **Subject:** C:US S:Colorado L:Englewood O:Quantum OU:Tape Automation CN:Quantum
Client	Library	47C4	Mar 29 13:26:05 2011 GMT Mar 26 13:26:05 2021 GMT	Valid	**Issuer:** C:US S:Colorado L:Englewood O:Quantum OU:Tape Automation CN:Quantum **Subject:** C:US S:Colorado L:Englewood O:Quantum OU:Tape Automation CN:bwentz

Installing Quantum-Supplied TLS Certificates on the Library
Quantum-supplied TLS certificates are only available for use with SKM. The Quantum-supplied certificates come on a CD which you received. The TLS certificates are bundled in a single file.

1 Ensure that the date on both SKM servers and the library are set to the current date. Incorrect date settings may interfere with the TLS certificates and cause the library to stop communicating with the SKM servers.

2 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.

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

The `Tools - TLS Communication Certificate Import` screen opens (see <u>Figure 26</u>). If TLS certificates are currently installed, they will be listed in a table at the bottom of the screen. If they are not installed, a message appears at the bottom of the screen stating that certificates are not installed.

4 From the **Select the Certificate Type to install** drop-down list, select **SKM**.

5 Select the **Use the Quantum Certificate Bundle** check box.

6 Click the **Browse** button next to the Quantum Communication Certificate Bundle File field to locate the TLS certificate file.

7 Click **Open**.

8 Click **Apply**.

9 Verify that the table at the bottom of the screen is present and contains the required certificates.

Installing Your Own TLS Certificates on the Library   Follow these instructions to install your own TLS certificates (for SKM), or when installing TLS certificates for KMIP key managers. When providing your own certificates, it is assumed you understand the concepts of PKI and can access the tools or third-party resources needed to generate or obtain certificates.

Note: **If you are using SKM:** You must be running SKM 1.1 or higher on your SKM servers in order to install your own TLS certificates. If you install your own TLS certificates on the library, you must also install your own certificates on the SKM servers. Similarly, if you use the Quantum-provided TLS certificates on the SKM servers, you must also use the Quantum-provided TLS certificates on the library. See the *Scalar Key Manager User's Guide* for information about installing TLS certificates on the SKM servers.

Note: **If you are using KMIP key managers:** Your KMIP server provider will provide TLS communication certificates.

You need to provide the following certificates:

Encryption System	Certificates Required
SKM	• Root Certificate (also called the CA certificate, or Certificate Authority Certificate) • Client Certificate • Admin Certificate
KMIP key managers	• Root Certificate (also called the CA certificate, or Certificate Authority Certificate) • Client Certificate

These files must be in the proper format, as follows. If any of the following requirements is not met, none of the certificates will be imported.

- The Root Certificate must be 2048 bits and be in PEM format.

- The Admin and Client certificates must be 1024 bits and be in pkcs#12 (.p12) format, with a separate certificate and private key contained in each.

- The Admin and Client certificates must be signed by the Root Certificate.

- Certificates must have the Organization name (O) set in their Issuer and Subject info.

- The Admin certificate must have its Organizational Unit name (OU) set as "akm_admin" in its Subject Info.

- The same Root Certificate must be installed on the encryption key servers and the library.

- All the certificates must have a valid validity period according to the date and time settings on the encryption key server.

To install your own certificates:

1 Ensure that the date on all encryption key servers and the library are set to the current date. Incorrect date settings may interfere with the TLS certificates and cause the library to stop communicating with the key servers.

2 Place the TLS certificate files in a known location on your computer.

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

The **Tools - TLS Communication Certificate Import** screen opens (see Figure 26 on page 176). If TLS certificates are currently installed, they will be listed in a table at the bottom of the screen. If they are not installed, a message appears at the bottom of the screen stating that certificates are not installed.

4 From the **Select the Certificate Type to install** drop-down list, select your encryption key management system (**SKM** or **KMIP Key Manager**).

5 Retrieve the certificate files as follows:

For SKM

  a Make sure the **Use the Quantum Certificate Bundle** check box is deselected.

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

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

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

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

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

  g If you used the same password for the client and admin certificates, you can select the **Use Admin's Password** check box.

For KMIP Key Manager

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

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

  c In the **Client Certificate Password** field, type the password used when generating the certificate files.

6 Click **Apply** to import the files onto the library.

7 Verify that the table at the bottom of the screen is present and contains the required TLS certificates.

Step 5: Running EKM Path Diagnostics

Perform EKM Path Diagnostics as described in <u>Using EKM Path Diagnostics</u> on page 183.

Step 6: Configuring Partitions for Library Managed Encryption

Encryption on the Scalar i500 tape library is enabled by partition only. You cannot select individual tape drives for encryption; you must select an entire partition to be encrypted.

Configure the partitions as follows:

1 From the Web client, select **Setup > Encryption > Partition Configuration**.

The **Setup - Encryption Partition Configuration** screen appears (see <u>Figure 27</u>).

Note:	Your screen might look slightly different depending on which encryption system you are using.

Figure 27 Setup - Encryption
Partition Configuration Screen

Setup - Encryption Partition Configuration

Set up EKM encryption for library partitions.

Note: Encryption is supported on LTO-4 and LTO-5 media and IBM and HP LTO-4 and LTO-5 Fibre Channel and SAS tape drives. Encryption is n
supported on SCSI tape drives. For more information refer to the online help or user's guide.
Select "Allow Application Managed" as the encryption method to disable library managed encryption. The "Allow Application Managed"
encryption selection allows your backup application to control when encryption is used. If your backup application is not configured to contr
encryption, data will not be encrypted.

Partition	FIPS	Encryption Method
library_a	☐	Allow Application Managed ⌄
library_b	☐	Allow Application Managed ⌄

− Click here to run EKM Path Diagnostics −

X Cancel   Apply ✓

A list of all your partitions displays, along with a drop-down list
displaying the encryption method for each partition. The Encryption
Method applies to all encryption-capable tape drives and media in that
partition. Table 7 on page 181 describes the partition encryption methods.

Table 7 Partition Encryption
Methods

Encryption Method	Description
Enable Library Managed	**For use with EKM.** Enables encryption support via a connected EKM key server for all tape drives and encryption-capable media assigned to the partition.

Allow Application Managed	**Not for use with EKM.** 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 EKM key server on this partition. This is the default setting if you have encryption-capable tape drives in the partition. This option should remain selected *unless* you are connecting the library to an external EKM server. **Note:** If you want an external application to manage encryption, you must specifically configure the application to do so. The library will not participate in performing this type of encryption.
Unsupported	Means that no tape drives in the partition support encryption. If **Unsupported** is shown, it will be greyed out and you will not be able to change the setting.

2 For each partition on which you are configuring EKM, change the Encryption Method to **Enable Library Managed**. (To disable EKM, select **Allow Application Managed**).

> **Note:** When you change the encryption method on a partition, the partition is taken offline. When the change completes successfully, the partition comes back online automatically. If the operation does not complete successfully, the partition remains offline until you turn it back online manually or restart the library.

> **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**.

3 **SKM Only —** FIPS (Federal Information Processing Standard) is a U.S. government standard relating to computer security and encryption. To enable FIPS mode on an SKM partition, select the **FIPS** check box. To disable FIPS, clear the **FIPS** check box.

See for more information. FIPS mode is only available with SKM.

4 Click **Apply**.

5 Save the library configuration.

Using EKM Path Diagnostics

The EKM Path Diagnostics consists of a series of short tests to validate whether the key servers are running, connected, and able to serve keys as required.

Run the Manual EKM Path Diagnostics any time you change the key server settings or library encryption settings. **If you are running Q-EKM**, you should also run the Manual EKM Path Diagnostics whenever you replace a tape drive. It is recommended that you test each tape drive that communicates with Q-EKM key servers.

The diagnostics consists of the following tests:

Note: **For Q-EKM only:** The tape drive used for the test must be unloaded, ready, and online in order to run any of the tests.

- **Ping —** Verifies the Ethernet communication link between the library and the key servers.

- **Drive (Q-EKM only) —** Verifies the tape drive's path in the library (communication from library to tape drive sled and from tape drive sled to tape drive). The tape drive must be unloaded, ready, and online in order to run this test. If this test fails, the Path and Config tests are not performed.

- **Path —** Verifies that EKM services are running on the key servers.

  Note: **For Q-EKM only:** This test cannot run if the Drive test fails.

- **Config —** Verifies that the key servers are capable of serving encryption keys.

> **Note:**   **For Q-EKM only:** This test cannot run if the Drive test fails.

If any of the tests fail, try the following resolutions and run the test again to make sure it passes:

- **Ping Test Failure** — Verify that the key server host is running and accessible from the network to which the library is connected.

- **Drive Test Failure** — Look for any tape drive RAS tickets and follow the resolution instructions in the ticket.

- **Path Test Failure** — Verify that the key server is actually running and that the IP address, port, and SSL settings configured on the library are correct. Check to see if there is a network configuration issue, such as a firewall, preventing communication with the server.

- **Config Test Failure** —

  - **Q-EKM:** Verify that the key server is set up to accept the tape drive you are testing.

  - **SKM:** A database inconsistency has been detected. Contact Quantum Support.

  - **KMIP Key Manager:** Indicates a KMIP key server configuration problem. The server does not support all features necessary for the library to use it as a key server. Contact your KMIP server administrator for assistance.

Differences Between Manual and Automatic EKM Path Diagnostics

There are two ways to perform EKM Path Diagnostics:

-

-

For SKM and **KMIP key management**, the manual and automatic diagnostics run in the same way. Partitions remain online for either the Manual or Automatic diagnostics.

For Q-EKM, the Manual diagnostics differs from the Automatic diagnostics in the following ways:

- The Manual diagnostics takes affected partitions offline during the tests. When the tests complete, the partitions are returned to the online/offline state they were in before the tests began.

- The Automatic diagnostics does not take partitions offline, but it may delay moves to tape drives while they are being tested.

- The Manual diagnostics requires that you select one tape drive to use for the test. Since the test only validates the selected drive, if you want to test the path for each tape drive, you must run the test multiple times (once for each drive). In addition, if the tape drive is not available (it must be unloaded, ready, and online), the Drive, Path, and Config tests are not performed.

- The Automatic diagnostics tests every connected EKM server in turn, and the library selects the tape drive to use for each test. If the selected tape drive is not available (it must be unloaded, ready, and online), then the library tries another tape drive that is connected to the key server until it finds one that is available. If no tape drives connected to a particular key server are available, then that server is skipped and the tests are not performed. If a server is skipped for "X" number of consecutive test intervals (where "X" is configurable on the Web client), the library generates a RAS ticket. If a tape drive remains loaded for a long time, it is possible that it will never be tested. If you want to test a specific tape drive, then you should use the Manual EKM Path Diagnostics. In particular, if you replace a tape drive, run the Manual EKM Path Diagnostics.

Using Manual EKM Path Diagnostics

1 Access the EKM Path Diagnostics screen in one of two ways:

- Enter library Diagnostics. From the Web client select **Tools > Diagnostics**, and click **OK** to the message that appears. From the Diagnostics menu, select **EKM > EKM Path Diagnostics**.

Note:	Performing Diagnostics will log off all other users of the same or lower privileges and take your partitions offline. When you exit Diagnostics, the partitions automatically come back online.

- Select **Setup > Encryption > System Configuration** or **Setup > Encryption > Partition Configuration** and click the link that says "Click here to run EKM Path Diagnostics."

2 **Q-EKM Only:** A list of all the tape drives enabled for library-managed encryption is displayed, along with the tape drive status and the partition in which each tape drive resides.

3 **Q-EKM Only:** Select the tape drive on which you want to perform diagnostics and click **Apply**. Tape drives must be unloaded, ready, and online in order for the test to run.

A dialog box appears telling you that the selected partition will be taken offline. When the test completes, the partition automatically comes back online.

4 Click **OK** to start the Q-EKM diagnostics, or click **Apply** to start the SKM or KMIP diagnostics.

5 The library performs the diagnostics and displays pass/fail results on each of the tests in the Progress Window.

> **Note:** The diagnostics tests may take several minutes to complete.

6 Do one of the following:

- If **Completed** appears in the Progress Window, the diagnostics were performed (this does not mean that the diagnostics passed, just that the diagnostics were performed). Click **Close** to close the Progress Window.

- If **Failure** appears in the Progress Window, the diagnostics were not performed. Follow the instructions listed in the Progress Window to resolve any issues that occurred during the operation.

7 If you are entered the Diagnostics menu, select **Exit** from the menu bar and then click **OK** in the dialog box that appears.

Using Automatic EKM Path Diagnostics

You can enable the library to automatically perform EKM Path Diagnostics at selected intervals. During each interval, the library tests every configured key server. The default test interval is 10 minutes. The library generates a RAS ticket if there are problems.

- **For Q-EKM:** Automatic EKM Path Diagnostics is disabled by default. It is recommended that you leave Automatic EKM Path Diagnostics disabled, unless network interruptions are a common cause of encryption failures at your site.

> **Caution:** **Q-EKM Only:** Running Automatic EKM Path
> Diagnostics may cause an increase in RAS tickets
> if tests are skipped due to tape drives being
> unavailable for a configurable number of
> consecutive test intervals. To reduce the
> occurrences of RAS tickets, you can specify the
> number of consecutive test intervals required to
> generate a RAS ticket to a higher number, or you
> can set the library to never generate a RAS ticket
> for missed test intervals.

- **For SKM and KMIP Key Manager:** Automatic EKM Path Diagnostics is
  enabled by default and should always be left enabled. You should not
  need to disable it unless Quantum Support directs you to do so.

For a list of tests performed, see <u>Using EKM Path Diagnostics</u> on
page 183.

To enable Automatic EKM Path Diagnostics:

1 From the Web client, select **Setup > Encryption > System
Configuration**.

2 Select the **Automatic EKM Path Diagnostics** check box.

3 Select a test interval from the **Interval** drop-down list.

4 **Q-EKM Only:** From the **Test Warning Threshold** drop-down list,
select the number of consecutive, missed test intervals required
before the library generates a RAS ticket informing you that the test
could not be performed within the specified number of test intervals.
You can select "Off" or any value from 1 to 24. If you select "Off," the
library will never generate a RAS ticket, no matter how many tests
are missed. The default threshold is 3.

**Viewing and Changing
the Active Key Server**

The **Key Manager Status** screen shows you which encryption key server
is currently active, and allows you to change the active server. When you
change the active server, it means that the next key server operation and
all subsequent key server operations will be performed using the new
active server until that server fails or the key server settings are changed.

> **Note:** This feature is currently only available with KMIP Key Manager.

1 From the Web client, select **Tools > EKM Management > Server Status**.

The **Key Manager Status** screen appears. A list of all your connected EKM servers displays. The currently active server displays in bold green type with the word "(Active)" after it.

2 To choose a different server to be the active server, select that server's radio button and click **Apply**.

Viewing Tape Drive Encryption Settings

You can view the encryption settings in the following ways:

- **System Information Report** — To view encryption information on all key servers, partitions, and tape drives, select **Reports > System Information** from the Web client.

- **Library Configuration Report** — To view the encryption status of a selected tape drive or tape cartridge, select **Reports > Library Configuration** from the Web client and click a tape drive or slot. The encryption status is displayed in a pop-up status window.

- **Partition Encryption** — From the Web client, select **Setup > Encryption > Partition Configuration** to view and change the encryption settings of partitions. See Step 6: Configuring Partitions for Library Managed Encryption on page 180 for more details.

Performing Scalar Key Manager Functions on the Library

Once the SKM servers are set up, most SKM functions occur automatically without user action required. SKM provides some key management capability through the library Web client.

For a complete description and instructions for using these features, see the library Web client online help.

These functions are:

- Generating Data Encryption Keys on page 189

- Sharing Encrypted Tape Cartridges on page 192

- Exporting the Native Encryption Certificate on page 193

-
-
-
-
-

Generating Data Encryption Keys

Data encryption keys are generated in sets of a specified quantity (see the *Scalar Key Manager User's Guide* for more information).

The library tracks data encryption key usage and reminds you to generate more keys when needed. If you try to generate data encryption keys on an SKM server that already has sufficient unused data encryption keys, then it will not create more. You will receive a message to that effect on the library remote Web client.

> **Note:** Each library that you connect to an SKM server requires its own set of data encryption keys. Each library only pulls data encryption keys from the set that "belongs" to it. This means that an SKM server may contain several distinct sets of data encryption keys. When the data encryption keys for one library have all been used, then more keys must be generated.

You can generate data encryption keys in the following ways:

- Generating Data Encryption Keys at Initial Setup
- Generating Data Encryption Keys When 80% Depleted
- Generating Data Encryption Keys When 100% Depleted
- Manually Generating Data Encryption Keys

Generating Data Encryption Keys at Initial Setup

At initial setup, the library triggers each SKM server to generate a set of data encryption keys. The process is described in .

Generating Data Encryption Keys When 80% Depleted   When an SKM server has used 80 percent of the data encryption keys assigned to a

particular library, that library attempts to automatically generate data encryption keys on the SKM server. Both SKM servers must be running and operational in order for automatic key generation to succeed.

- **If automatic key generation succeeds,** a RAS ticket informs you the keys were generated and instructs you to back up both SKM server keystores as soon as possible.

- **If automatic key generation fails,** the library tries again every time a new key is requested, until the keys are 90 percent depleted. At that point, the library stops trying to auto-generate keys and issues a RAS ticket stating that you must manually generate keys. See Manually Generating Data Encryption Keys on page 190.

Generating Data Encryption Keys When 100% Depleted If an SKM server completely runs out of data encryption keys for a particular library, that library generates a RAS ticket, which states that you have run out of data encryption keys and that the library attempted to fail over to the other SKM server. If this happens, it is imperative that you manually generate a new set of data encryption keys on the depleted server immediately and then back up both SKM servers. See Manually Generating Data Encryption Keys on page 190.

Manually Generating Data Encryption Keys To manually generate data encryption keys, you need to temporarily disable library managed encryption on a partition, and then enable it again. Enabling library managed encryption on a partition triggers the library to check both SKM servers to see if new data encryption keys are needed. If so, it creates the keys.

Note: The data encryption key generation process takes approximately 15 minutes. You should not run any library or host-initiated operations on SKM partitions during key generation and backup.

Avoid manually generating keys on more than five libraries simultaneously as the key generation process is resource-intensive on the server. Generating keys manually on more than five libraries at once could result in a failure to complete the key generation operation, or interfere with key retrieval operations. If a failure does occur during key generation, wait 10 minutes, then try to start it again. The key generation process will resume from where the error was encountered.

To manually generate data encryption keys:

1 Make sure that both SKM servers are running and operational.

2 From the library's Web client, access the encryption partition configuration screen (**Setup > Encryption > Partition Configuration**).

3 Select an SKM partition configured for library managed encryption, and temporarily disable library managed encryption by changing the encryption method from **Enable Library Managed to Allow Application Managed**. *Remember which partition it is*, because you will be changing it back in a few minutes. Make sure to click **Apply**.

> **Caution:** When you change the partition's encryption method to **Allow Application Managed**, the data that was written to the tapes while the partition was configured for **Enable Library Managed** can no longer be read, until you change the partition back to **Enable Library Managed**. You will only be disabling for a short time, and then changing back to **Enable Library Managed** (just to trigger the key generation process) so this should have little effect, unless you forget to turn it back to **Enable Library Managed**.

4 Wait 3 minutes to allow the changes to complete.

5 Go back to the encryption partition configuration screen and change the partition back to **Enable Library Managed**. Again, make sure to apply the changes.

6 Wait for the process to complete before resuming library operations.

7 Back up both SKM servers. You must back up both SKM servers every time you generate new data encryption keys to protect your data in case of catastrophic server failure. See the *Scalar Key Manager User's Guide* for instructions on backing up the SKM servers.

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 an SKM server that is different than the server 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 a native encryption 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 native encryption certificate that belongs to the destination SKM server. (The two SKM servers in a server pair share the same native encryption certificate.) The native encryption certificate is saved as a file to a location specified by the administrator on a computer (see <u>Exporting the Native Encryption Certificate</u> on page 193).

  2 The destination administrator e-mails the native encryption certificate file to the source administrator.

  3 The source administrator saves the native encryption certificate file to a location on a computer, and then imports it onto the source SKM server (see <u>Importing Encryption Certificates</u> on page 194).

  4 The source administrator exports the data encryption keys, assigning the destination SKM server's native encryption certificate to wrap (encrypt) the keys. The file containing the wrapped encryption keys is saved to a location on a computer specified by the source administrator. See <u>Exporting Data Encryption Keys</u> on page 194.

  5 The source administrator e-mails the file containing the wrapped data encryption keys to the destination administrator.

6 The destination administrator saves the file containing the wrapped data encryption keys to a location on a computer, and then imports the keys onto the destination SKM server (see Importing Data Encryption Keys on page 196).

7 The destination library can now read the encrypted tapes.

For more information about the key servers and library managed encryption best practices, please refer to the *Scalar Key Manager User's Guide*.

Exporting the Native Encryption Certificate

To receive encryption keys from another SKM server, you must first send your SKM server's native encryption certificate to that server. The public key contained in the native encryption certificate will be used to wrap (encrypt) the encryption keys to protect them during transport to you.

Note:	This function is available to administrators and only applies to SKM servers. Since the native encryption certificate is the same for both servers in an SKM server pair, you may export it when only one SKM server is connected/operational.

To export an encryption certificate:

1 Before starting this process, read and follow the sequence of steps outlined in Sharing Encrypted Tape Cartridges on page 192.

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

3 Click **Apply** to export your SKM server's native encryption certificate.

4 Click **Close** to close the Progress Window.

5 In the **File Download** dialog box that displays, click **Save**.

6 In the **Save As** dialog box that opens, choose a location in which to save the file, then click **Save**.

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, you need to import the encryption certificate of the destination SKM server.

Note:	This function is available to administrators and only applies to SKM servers. Both SKM servers must be connected and operational in order to import encryption certificates.

To import encryption certificates:

1 Before starting this process, read and follow the sequence of steps outlined in <u>Sharing Encrypted Tape Cartridges</u> on page 192.

2 Receive the encryption certificate file from the destination SKM server administrator and save it to a known location on your computer.

3 From the **Tools** menu, select **EKM Management > Encryption Certificate > Import**.

4 Click **Browse** to locate the saved encryption certificate file.

5 Click **Open**.

6 Click **Apply** to import the certificate onto your SKM server.

Exporting Data Encryption Keys

SKM servers provide 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 (i.e., source), you need to export the encryption keys used to encrypt those tapes and send them to the destination server.

Note:	This function is available to administrators and only applies to SKM servers. Both SKM servers must be connected and operational in order to export data encryption keys.

> **Note:** **Missing/Changed Barcode Labels** — If a tape cartridge
> barcode label is missing, the key used to encrypt the tape will
> not be exported in an **Export Current** operation. If a tape
> cartridge barcode label is changed, the key used to encrypt
> the tape will not be exported in an **Export Current** or **Export
> Selective** operation. The keystore metadata pairs the data
> encryption key with the label that was present at the time of
> first encryption. If the label is lost or changed, the pairing is
> lost, and these export options will either export no key or
> possibly the wrong key. Encryption read/write operations are
> not affected by media barcode label and will continue to
> work correctly.

To export encryption keys:

1 Before starting this process, read and follow the sequence of steps outlined in <u>Sharing Encrypted Tape Cartridges</u> on page 192.

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

3 Assign the encryption certificate with which you will "wrap" (encrypt) the keys by selecting it from the **Certificate Name Used For Export** drop-down list. Choose the certificate that belongs to the server to which the keys will be imported.

> **Note:** The owner of that server should have sent you the
> certificate and you should have imported it (see <u>Sharing
> Encrypted Tape Cartridges</u> on page 192 and <u>Importing
> Encryption Certificates</u> on page 194). The drop-down list
> contains all of the encryption certificates that you have
> ever imported onto your SKM servers (indicated by the
> word "imported" in the list), as well as the certificate
> belonging to your SKM server pair (indicated by the word
> "native" in the list).

4 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 in the library performing this export. Also exports all keys that were imported onto the key server, via a "key import" operation, from any library.

- **Export Current** — Exports all the keys that were used to encrypt the tape cartridges that are currently in the library performing this export. This includes storage slots, I/E stations, and tape drives. If a tape cartridge is no longer in the library, the key used to encrypt the tape will not be exported. If a tape cartridge barcode label is missing or changed, the key used to encrypt the tape will not be exported.

- **Export Selective** — Exports only the key(s) 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. If a tape cartridge barcode label is changed, the key used to encrypt the tape will not be exported.

5 Click **Apply**.

All the exported keys are saved to a single encryption key file.

6 A **Save As** dialog box opens allowing you to save the encryption key file to a location on your computer. Choose a location and click **Save**.

Importing Data Encryption Keys

SKM servers provide 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 (i.e., destination).

Note:	This function is available to administrators and only applies to SKM servers. Both SKM servers must be connected and operational in order to import data encryption keys.

To import encryption keys:

1 Before starting this process, read and follow the sequence of steps outlined in <u>Sharing Encrypted Tape Cartridges</u> on page 192.

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 Click **Open**.

6 Click **Apply** to import the keys onto your SKM server.

7 Back up both SKM servers following the instructions in the SKM user's guide.

In case of an incomplete import, the library displays a message and generates a RAS ticket. For instructions on what to do if this happens, see

Accessing the SKM Server Logs

• The library can download the audit and error logs from the SKM servers. You should not need to retrieve these logs unless Quantum Support directs you to do so. You can download the logs to your computer or e-mail them to a recipient. In order to e-mail the logs, the library e-mail account must be configured (see "Configuring the Library E-mail Account" in the *Scalar i500 User's Guide*).

• The path to open the appropriate screen is as follows:

• From the Web client, select **Tools > EKM Management > Retrieve SKM Logs**.

Using the SKM Encryption Key Import Warning Log

This log lists the tape cartridges for which encryption keys failed the most recent encryption key import operation. 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 displays an "import warning" message and generates a RAS ticket that directs you to view this log to see which keys did not get imported.

For each key that failed the import, the log provides a message type that is either:

• **Error** — The key could not be imported.

• **Warning** — The key was imported, but the metadata update failed.

For each key that failed the import, the log provides one of the following message descriptions:

- **CRC Data Missing** — Error. Metadata is missing for the key. This means that the export file is corrupt. **Suggested Solution:** Export the key(s) for the listed tape cartridge(s) again, and then perform the import operation again.

- **CRC Check Failed** — Error. The CRC data does not match the key or key metadata. The export file is corrupt. **Suggested solution:** Try to import the same file again. If this fails, export the key(s) for the listed tape cartridge(s) again, and then perform the import operation again.

- **Import To Primary/Secondary Server Failed** — Error. The key import to the stated server failed (probably due to a network or other connection issue). If the key failed to import to the secondary server, it may have been imported successfully to the primary server. **Suggested solution:** Check network connections and perform the import operation again.

- **Key Metadata Update Failed (but key data was imported successfully)** — Warning. The key was imported, but the metadata update failed. You can access the key, but you cannot export it until it is actually used in an encryption operation on the library. **Suggested solution:** Use the key to read (decrypt) a tape. This marks the key as "used" and updates the metadata, which will allow you to export the key.

This log is only available if you are running SKM and have encryption key management licensed on the library.

The log file is cleared and created new for each import operation so that it shows only the key corruptions and import failures that occurred during the latest encryption key import attempt.

The path to open the appropriate screen is as follows:

- From the Web client, select **Reports > Log Viewer**.

FIPS-Certified Encryption Solution

FIPS (Federal Information Processing Standard) 140-2 is a U.S. government standard relating to computer security and encryption.

The Quantum Scalar i500 now offers a FIPS 140-2 Level 1 certified encryption solution composed of the Scalar Key Manager and HP LTO-5 or LTO-6 Fibre Channel tape drives in a Scalar i500 library. FIPS mode can be enabled on the HP LTO-5 or LTO-6 tape drives via the library user interface. Once in FIPS mode, all encryption key communication between the tape drive and the library controller is authenticated and encrypted.

Details about configuring FIPS mode include:

- Library firmware must be at version 600G or later.

- HP LTO-5 or LTO-6 FC tape drive firmware must be at the latest version qualified with the Scalar i500 library (see the *Scalar i500 Release Notes* for qualified firmware levels).

- An Encryption Key Management license must be installed on the library sufficient to cover the tape drive(s) on which you want to enable FIPS mode.

- A Storage Networking license must be installed on the library sufficient to cover the tape drive(s) on which you want to enable FIPS mode.

- FIPS mode is configured by partition. FIPS partitions must contain only HP LTO-5 FC or HP LTO-6 FC tape drives.

- The partition encryption method must be set to **Enable Library Managed** in order to set FIPS mode.

- FIPS mode is disabled by default.

- Ethernet connectivity is required for the tape drives on which you want to enable FIPS mode. For most libraries, this requires one or more Ethernet Expansion blades installed on the library, unless your library consists of a single 5U control module. For 5U libraries, you can connect your tape drives directly to the Ethernet ports on the library control blade (LCB). See Tape Drive Ethernet Connectivity and the Ethernet Expansion Blade on page 458.

• The library must be connected to Scalar Key Manager. Scalar Key Manager software must be at version 2.0 or later in order to be FIPS certified.

> **Caution:**   If the Ethernet Expansion blade fails and the attached tape drives have FIPS mode enabled, all encryption operations (encrypting, decrypting, key requests) on the attached tape drives will fail. If this happens, contact Quantum Support for a replacement Ethernet Expansion blade as soon as possible.

Configuring the Library for FIPS

To configure your library for FIPS, perform the following steps:

1 Upgrade library firmware to version 600G or later.

2 For all HP LTO-5 or LTO-6 FC tape drives that you plan to enable for FIPS, upgrade firmware to the latest version qualified with the Scalar i500 library (see the *Scalar i500 Release Notes* for qualified firmware levels).

3 Shut down the library.

4 Do one of the following:

If your library is...	Do this...
5U	Perform Cabling a 5U Library for Ethernet Connectivity on page 460.
14U or larger	Perform Cabling the Ethernet Expansion Blade on page 468.

5 Power on the library.

6 Install Storage Networking and Encryption Key Management licenses on the library, if they are not already installed.

7 Enable FIPS mode (see Enabling and Disabling FIPS Mode on HP LTO-5 and LTO-6 Tape Drives on page 201).

Enabling and Disabling FIPS Mode on HP LTO-5 and LTO-6 Tape Drives

To operate your HP LTO-5 or LTO-6 Fibre Channel tape drives to be compliant with FIPS, you must enable "FIPS mode." FIPS mode is configured by partition. You enable FIPS mode on a partition, which enables FIPS mode on all of the tape drives in the partition.

To change FIPS mode for a partition:
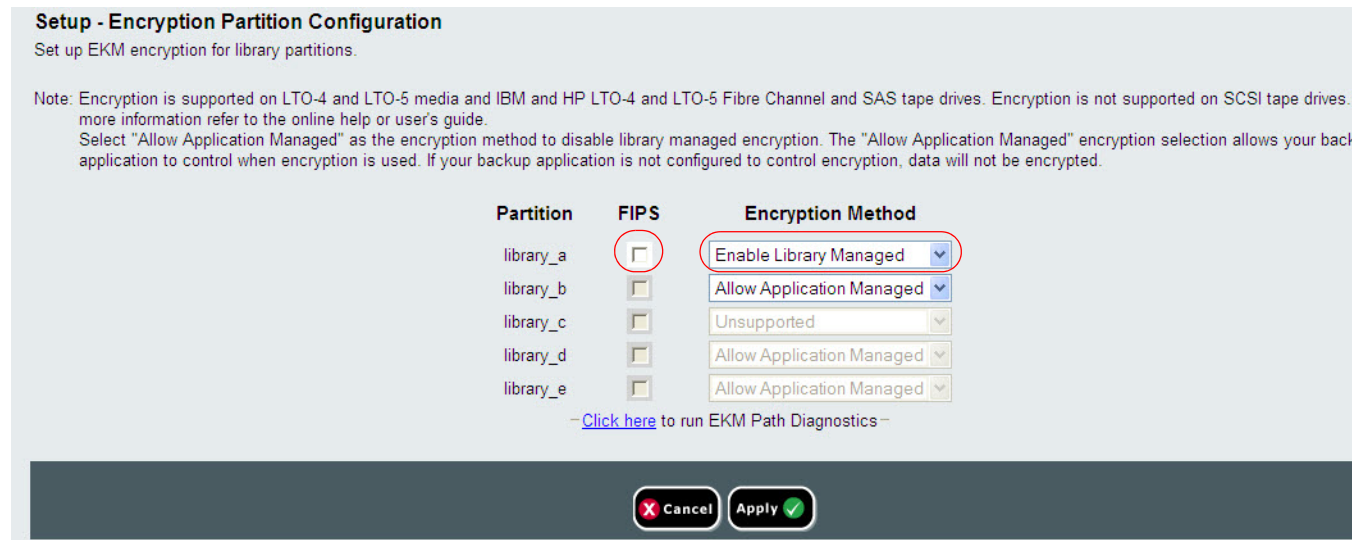
1 On the library web client, select **Setup > Encryption > Partition Configuration**.

The **Setup - Encryption Partition Configuration** page displays (see Figure 28 on page 201).

Change the Encryption Method of a partition to **Enable Library Managed**.

2 Select the **FIPS** check box to enable FIPS mode for the partition. Clear the **FIPS** check box to disable FIPS mode for the partition.

3 Click **Apply**.

Figure 28 Enabling FIPS Mode

Setup - Encryption Partition Configuration
Set up EKM encryption for library partitions.

Note: Encryption is supported on LTO-4 and LTO-5 media and IBM and HP LTO-4 and LTO-5 Fibre Channel and SAS tape drives. Encryption is not supported on SCSI tape drives.
more information refer to the online help or user's guide.
Select "Allow Application Managed" as the encryption method to disable library managed encryption. The "Allow Application Managed" encryption selection allows your back
application to control when encryption is used. If your backup application is not configured to control encryption, data will not be encrypted.

Partition	FIPS	Encryption Method
library_a	☐	Enable Library Managed
library_b	☐	Allow Application Managed
library_c	☐	Unsupported
library_d	☐	Allow Application Managed
library_e	☐	Allow Application Managed

– Click here to run EKM Path Diagnostics –

X Cancel   Apply ✓

**Viewing FIPS Status on
the Library**

There are three ways to view FIPS status on the library:

• The Partition Configuration screen **(Setup > Encryption > Partition
  Configuration)** shows which partitions are enabled for FIPS. All tape
  drives in FIPS partitions are enabled.

• The System Information Report (**Reports > System Information)**
  contains a **FIPS** column in the **Library Partitions** section. The column
  displays "Yes" if FIPS is enabled on the partition and "No" FIPS is
  disabled.

• The tape drive information pop-up screen on the Library
  Configuration Report (**Reports > Library Configuration**) contains a
  FIPS Enabled item. This item only displays when the tape drive is an
  HP LTO-5 or LTO-6 Fibre Channel tape drive. The item displays
  "Yes" when FIPS is enabled on the drive and "No" when FIPS is
  disabled.

Extended Data Lifecycle Management (EDLM) provides data protection and integrity checking by scanning your tape cartridges, providing results, and allowing StorNext® to migrate data from bad or suspect tapes. EDLM allows you to run manual scans on any tape cartridge in the library at any time, and performs automatic scans according to schedules and policies that you set up.

To use EDLM, you will set up one or more dedicated partitions to be used for scanning. These partitions are called "library managed" partitions because they are not accessible by hosts. You can manually scan a tape cartridge at any time, or you can set up automatic scanning schedules and policies. Scanning takes place using "EDLM scanning drives" which are different from regular tape drives. You cannot use regular tape drives to perform EDLM scans.

This section covers the following topics:

-

-

-

-

-

-

About EDLM

Details about EDLM are as follows:

- The EDLM feature requires an Extended Data Lifecycle Management license to be installed on the library. One license covers the entire library. See the *Scalar i500 User's Guide* for instructions on how to enable a license.

- Library firmware must be at code version 620G or later to use EDLM.

- You need Administrator privileges to configure EDLM and initiate manual tests.

- At least one dedicated library managed partition is required for the media scans. This library managed partition is accessible only by a library administrator. It is not presented to any other applications. The library managed partition is assigned its own dedicated resources and EDLM scanning is executed in the background. Cartridges are moved into EDLM-scanning drives residing in the EDLM library managed partition. After being scanned, cartridges are returned to their original locations. See Step 4: Creating the EDLM Library Managed Partition on page 213.

- You can scan cartridges manually at any time. See Running Manual EDLM Tests on page 224. You can also set up automatic media scanning policies by partition. Each partition can have its own unique set of media scanning and action policies. See Step 5: Setting Up Automatic EDLM Scanning Policies on Partitions on page 216.

- All types of tape cartridges (data, cleaning, diagnostic, and firmware update tapes) can be scanned manually. However, only data cartridges can be scanned automatically.

- If StorNext® Storage Manager is managing your partitions, you can use it in conjunction with EDLM to automatically copy data off of bad or suspect tapes or to trigger media scans. To use StorNext, you must separately install a SNAPI client plug-in. See Step 2: Installing the EDLM Plug-in for SNAPI on page 208.

- All media to be scanned must have a readable barcode label.

- All scans are performed in the order in which their requests were received. If there are too many scans for the available tape drives, scan requests are queued. **Exception**: Manual scans always go to the top of the queue, regardless of when they are scheduled.

- A tape may only be scheduled once in the queue. For example, if a tape is in the queue to be scanned per a particular policy, and a different policy attempts to schedule it for scan later in the queue, the scan requests will be combined and the tape will only be scanned once, at the earlier time, and for the longest scan length (quick, normal, or full).

- You cannot move media using the **Operations > Media > Move** command to or from an EDLM library managed partition.

- You cannot delete the last remaining EDLM library managed partition if a standard partition has automatic EDLM scan policies enabled.

- The maximum number of records returned for an EDLM scan is 500.

Details about the EDLM library managed partition include:

- You can have multiple EDLM library managed partitions in the library.

- All tape drives in the EDLM library managed partition must be "EDLM-scanning drives" (not standard tape drives) which must be purchased from Quantum. These EDLM-scanning drives are HP LTO-4 Fibre Channel or HP LTO-5 Fibre Channel tape drives. You can have both LTO-4 and LTO-5 EDLM-scanning drives in the same EDLM library managed partition.

- An EDLM library managed partition can support any number of EDLM-scanning drives (within the normal support of the physical library).

- All of the EDLM scanning drives in the EDLM library managed partition must be connected to a Fibre Channel I/O blade. Each FC I/O blade supports up to four tape drives. You can use multiple FC I/O blades to support the EDLM-scanning drives. It is recommended (although not required) that the FC I/O blade(s) used for EDLM scanning drives have only EDLM scanning drives attached, and recommended that the blade not be connected to a host. Otherwise, the host will have access to the EDLM drives. **For this reason, we strongly discourage using the same FC I/O blade for EDLM drives and host-connected 4 Gb/s SNW drives. If this must be done, the FC I/O blade must be "channel zoned" to prevent host access to the EDLM scanning drives.**

- Tape drives in the EDLM library managed partition will only be used for EDLM scanning purposes.

- An EDLM library managed partition can be composed of a mix of licensed and unlicensed slots. Unlicensed slots will be used first, but if the size of a newly configured EDLM partition exceeds the number of available unlicensed slots, then the empty licensed slots will be used.

- Standard tape drive cleaning policies apply to the tape drives in the EDLM library managed partition.

- You can set up EDLM scanning policies on the EDLM library managed partition.

- If you plan to use the EDLM partition to scan tapes encrypted using library managed encryption, you will need to configure this partition for library managed encryption, so that it can request the correct encryption keys from the encryption key servers. Without the proper encryption keys, the EDLM scanning drives cannot perform normal or full scans on encrypted tapes. Select **Setup > Encryption > Partition Configuration**.

Note: When a partition is configured for Q-EKM, scan types of Normal and Full cannot be selected.

- You cannot delete the last remaining EDLM partition if a standard partition has EDLM policies enabled. To disable EDLM scanning policies on a partition, select **None** for each of the following: **Scan upon import**, **Scan based on Tape Alert**, and **Use StorNext configuration**. In addition, set the normal and full scan time intervals to zero. For more information, see Step 5: Setting Up Automatic EDLM Scanning Policies on Partitions on page 216.

Cleaning for EDLM Drives

Cleaning for EDLM drives must be done through the library's manual cleaning feature or automatic cleaning feature. Simply inserting a cleaning tape into an EDLM drive will not initiate cleaning because EDLM drives are configured for a partial load, and the drive won't load the tape to clean the drive.

Incomplete EDLM Scans

In rare cases, various operational issues could prevent an EDLM scan from properly initiating. These instances will be indicated in individual EDLM scan result details as "I/O Blade Component Failure." This message does not necessarily mean there are hardware issues with the I/O blade or tape drive, but may indicate logical errors within operational software for these components.

If these indications are observed within individual EDLM scan result details, Quantum recommends power cycling I/O blades being utilized for EDLM scans using the remote user interface's **Setup > FC I/O Blade > FC I/O Blade Control** screen.

Please refer to the online help located on the **Setup > FC I/O Blade > FC I/O Blade Control** screen for further details on power cycling FC I/O blades.

> **Caution:** If data drives are connected, make sure to stop any running backups before power cycling blades.

Configuring EDLM

Configuring EDLM consists of the following steps:

- Step 1: Preparing the Library on page 208
- Step 2: Installing the EDLM Plug-in for SNAPI on page 208

Step 1: Preparing the Library

1 Upgrade library firmware to at least version 620G. If needed, contact Quantum Support to get the firmware.

2 Install EDLM-scanning drives in the library.

3 Connect each EDLM-scanning drive to one of the four initiator ports in a Fibre Channel I/O blade. If you have more than four EDLM-scanning drives, you will need to use more than one Fibre Channel I/O blade.

4 Log on as an administrator.

5 Install the Extended Data Lifecycle Management license on the library. See the *Scalar i500 User's Guide* or online help for instructions.

6 Recommended: It is a good idea to create a "known good tape cartridge" to have on hand in case you need to test an EDLM scanning drive. A "known good tape cartridge" means one that is fairly new, formatted, fully written, and that has a good cartridge memory (CM). This tape will provide data that is easily verifiable to help isolate media and drive issues.To purchase a "known good tape" contact Quantum Technical Support. See Testing Suspect EDLM Drives on page 235 for more information.

> **Note:** The default StorNext Storage Manager port number is 61776. If you changed the port on your server, be sure to type the new port number into this field.

Step 2: Installing the EDLM Plug-in for SNAPI

This step is optional. If StorNext Storage Manager is managing your partitions, you can use it in conjunction with EDLM to automatically copy data from bad or suspect tapes or to trigger media scans. If you are not using StorNext in conjunction with EDLM, skip this step.

In order to use StorNext for these purposes, you must first install the StorNext application programming interface (SNAPI) client plug-in on the library, and then configure the library to communicate with StorNext Storage Manager. The EDLM plug-in for SNAPI is available from Quantum.

To install the EDLM plug-in for SNAPI:

1 Confirm that the StorNext Storage Manager application managing your partition is supported by the Scalar i500 firmware. For a list of supported external applications and their corresponding plug-ins, see the *Scalar i500 Release Notes*.

2 Download the correct EDLM plug-in for SNAPI bundle as follows:

   a Go to the following Web site.

      http://www.quantum.com/ServiceandSupport/SoftwareandDocumentationDownloads/SI500/Index.aspx

   b Click the **Drivers** tab to view the available plug-ins.

   c Click the **Download** button for the plug-in you want to install. Download the file to an accessible location on your computer.

   The plug-in bundle is a .zip file containing the following files:

   • Client plug-in

   • End User/Open Source License Agreement

3 Extract the files from the .zip file.

4 Read the End User/Open Source License Agreement. Installation of the plug-in implies acceptance of the license agreement.

5 From the library Web client, select **Tools > EDLM > Manage Plug-ins**.

6 The **Tools - Manage EDLM Plug-ins** screen appears.

Figure 29 Installing the SNAPI
Plug-in
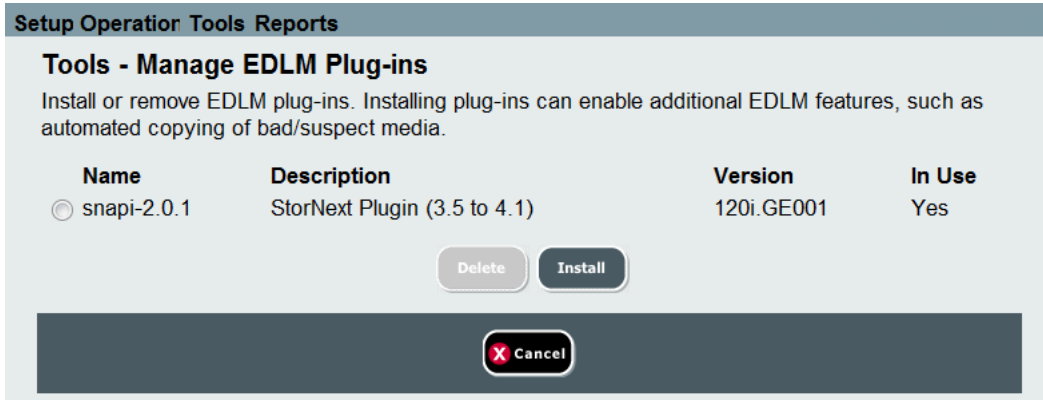
7 Click **Install**.

The **Tools - Manage EDLM Plug-ins screen** appears.

Figure 30 Installing the SNAPI
Plug-in
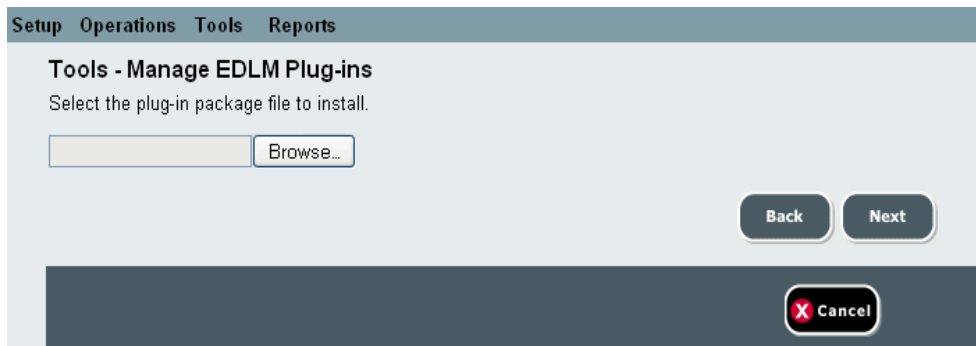
8 Click **Browse** to navigate to and select the EDLM plug-in for SNAPI
you downloaded earlier.

9 Click **Next**.

A confirmation screen appears.

10 Click **Install**.

The file is installed. When complete, a **Success** message appears.

11 Click **Close** to close the **Success** message.

Step 3: Configuring the StorNext Host Settings on the Library

This step is optional. If StorNext Storage Manager is managing your partitions, you can use it in conjunction with EDLM to automatically copy data from bad or suspect tapes or to trigger media scans. If you are not using StorNext in conjunction with EDLM, skip this step.

After installing the SNAPI client plug-in, you must configure the library to communicate with the StorNext Storage Manager host server.

1 From the Web client, select **Tools > EDLM > Configure StorNext Settings**.

The **Tools - EDLM StorNext Configuration** screen appears.

2 Click **Create**.

The **Tools - EDLM StorNext Configuration** entry screen appears.

Figure 31 StorNext Host Configuration

3 In the **Name** field, type a name that you will use to identify the StorNext Storage Manager server.

4 From the **API Client Plug-in** drop-down list, select the SNAPI client plug-in.

5 From the **Primary Host Address** field, type the IP address (or host name, if DNS is configured) of the primary StorNext Storage Manager server.

6 From the **Primary Host Port** field, accept the default or type the port number of the primary StorNext Storage Manager server.

> **Note:** The default StorNext Storage Manager port number is 61776. If you changed the port on your server, be sure to type the new port number into this field.

7 Optionally, type an IP address (or host name, if DNS is configured) for a secondary StorNext Storage Manager server in the **Secondary Host Address** field.

8 Optionally, accept the default or type a port number of a secondary StorNext Storage Manager server in the **Secondary Host Port** field.

> **Note:** The default StorNext Storage Manager port number is 61776. If you changed the port on your server, be sure to type the new port number into this field.

9 Click **Apply**.

The settings are configured. When complete, a **Success** message appears.

10 Click **Close** to close the **Success** message.

The main screen appears again with the server you just entered listed. There is a **Run** button in the **Diagnostics** column.

11 Click the **Run** button to test the settings you configured. If a **Failed** message appears, you can click the **Failed** link and a message box appears to help you troubleshoot. Make sure the IP addresses and port numbers you entered are correct, and that the plug-in is supported.

Figure 32 Testing the StorNext
Settings
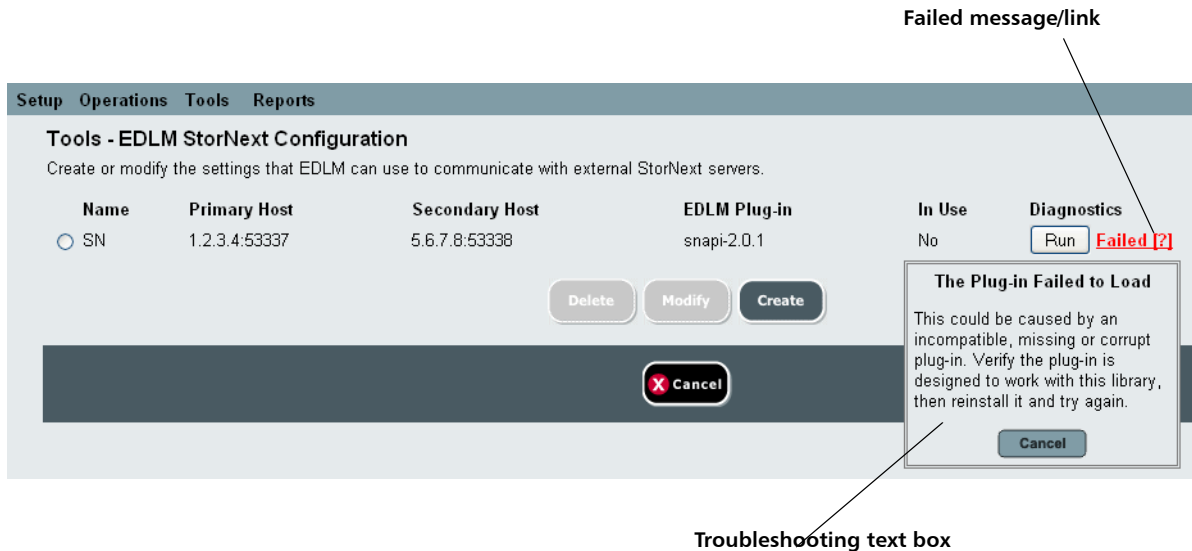
12 Once you have successfully configured StorNext host settings, you
can configure StorNext-related EDLM policies on partitions as
described in <u>Chapter 8, Step 5: Setting Up Automatic EDLM
Scanning Policies on Partitions</u>.

Step 4: Creating the EDLM Library Managed Partition

The EDLM library managed partition is a dedicated partition that you set
up in the library for scanning media with EDLM. This partition exists
solely for media scanning purposes and is not accessible to hosts or other
applications. Tape cartridges are moved into the EDLM library managed
partition and scanned using the tape drives residing in the EDLM library
managed partition. When the scan is complete, the cartridges are
returned to their original partitions.

> **Note:** If you plan to use this EDLM partition to scan tapes encrypted using library managed encryption, you will also need to configure this partition for library managed encryption, so that it can request the correct encryption keys from the encryption key servers. Without the proper encryption keys, the EDLM scanning drives cannot perform normal or full scans on encrypted tapes. Once you have created the partition, select **Setup > Encryption > Partition Configuration** and configure the partition for library managed encryption.

To create the EDLM library managed partition, do the following:

1 From the Web client, select **Setup > Partitions**.

2 Click **Create**.

The **Create Partition - Basic Settings** screen appears (see Figure 33).

Figure 33 Creating EDLM
Partitions

3 From the Select Partition Type drop-down list, choose **Library Managed (EDLM)**.

4 Type a name for the partition in the **Enter Name** text box.

5 Type in the number of storage slots to assign to the partition in the **Enter Number of Slots** text box.

> **Note:** The number in parentheses indicates the number of slots available for use in the partition. For standard partitions, the number equals the number of licensed slots available, and the default equals the total number of available slots. Since EDLM partitions can contain both unlicensed and licensed slots (using all unlicensed slots before using licensed slots), the number in parentheses equals the total number of licensed and unlicensed slots, and the default equals the number of unlicensed slots available. You can configure EDLM partitions to use zero slots if desired.

> **Note:** The **Select Emulation Type** and **Select Media Barcode Format** fields are not selectable when creating EDLM library managed partitions.

6 Select the drive(s) you want to add to the partition from the table. Only EDLM scanning drives appear in the list.

7 Click **Next**.

The **Create Partition - EDLM Policy Settings** screen appears (see Figure 34 on page 217).

8 If desired, set EDLM scanning policies on this EDLM library managed partition (go to Step 5: Setting Up Automatic EDLM Scanning Policies on Partitions on page 216).

9 If you do not wish to configure automatic EDLM scanning policies on the partition, click **Apply** to finish.

Step 5: Setting Up Automatic EDLM Scanning Policies on Partitions

You can set EDLM scanning policies on both standard partitions and on EDLM library managed partitions. Once configured, scanning takes place automatically per the policies. You can temporarily stop automatic scans on partitions by using the Pause feature (see Pausing EDLM Scans on Partitions on page 222).

1 Log on as an administrator.

2 From the Web client, select **Setup > Partitions**.

3 Click **Create** to create a new partition, or select a partition and click **Modify** to modify an existing partition.

4 When finished configuring the general settings, click **Next**.

The **Create Partition - EDLM Policy Settings** screen appears (see Figure 34 and Figure 35).

Note:	Fewer policies are available on EDLM library managed partitions because they are inaccessible to hosts.

Figure 34 EDLM Policy
Settings for EDLM Library
Managed Partitions

Figure 35 EDLM Policy
Settings for Standard Partitions

5 Set EDLM scanning policies on this partition. Table 8 describes the policies that you can set.

> **Note:** To disable EDLM scanning policies on a partition, select **None** for each of the following: **Scan upon import**, **Scan based on Tape Alert**, and **Use StorNext configuration**. In addition, set the normal and full scan time intervals to zero.

Table 8   EDLM Policy Settings
for Partitions

Setting	Description
General Settings	
Allow concurrent scans	Select the number of tape drives that this partition can use for EDLM scans at any one time. If you have several partitions that will use EDLM scanning drives, you can use this feature to divide the EDLM drive resources so that a single partition with a large number of scans to perform can never "hog" all of the resources and prevent other partitions from performing their scans in a timely manner.
	Choices are: Unlimited (default), 1, 2, 3, or 4. "Unlimited" means that this partition can use all available EDLM scanning drives concurrently.
Report media inaccessible	**When this check box is de-selected** (default), if a host requests a tape cartridge that is being scanned, the scan is cancelled and the tape cartridge is moved back to its original location to service the host request. The interrupted scan is not rescheduled. The EDLM report indicates the interruption or cancellation. This ensures that normal operations are not affected by EDLM scanning.
	When this check box is selected, if a host requests a tape cartridge while it is being scanned, the library responds to the host that the tape cartridge is inaccessible.
	Note: This feature is currently disabled. The library always reports media accessible to hosts (i.e., the box is de-selected and cannot be selected).

Setting	Description
Use StorNext Configuration	Select whether to use StorNext in conjunction with EDLM to perform certain EDLM operations; and, if so, which StorNext configuration to use. From the drop-down list, select **None** (default) or select one of the StorNext configurations you set up in <u>Step 3: Configuring the StorNext Host Settings on the Library</u> on page 211.
Scan Settings	
Scan upon import	Choose whether to scan tapes as soon as they are imported into this partition; and, if so, which type of scan to perform. This policy is disabled by default.

Scan Settings

Scan upon import — Choose whether to scan tapes as soon as they are imported into this partition; and, if so, which type of scan to perform. This policy is disabled by default.

Choices are:

- **None (default)** — Does not scan upon import.

- **Quick** — Does not scan the tape. Evaluates data from the cartridge memory (CM) only. Takes less than one minute per tape. Examples of when to use a quick scan:

  - When you first import previously used scratch tapes into the library.

  - When you import data cartridges that have been used in other backup and archival environments and need to do a quick check to determine whether the tape cartridge is nearing end of life, at end of life, or may have had issues reading or writing.

- **Normal** — Evaluates the cartridge memory (CM) and scans selected portions of the tape, focusing on areas most likely to indicate problems. Takes up to 20 minutes per tape. Examples of when to use a normal scan:

  - For tapes in frequent use within the library, with scanning triggered by drive-reported media Tape Alert events.

  - For tapes in frequent use within the library, with scanning being performed at regular time intervals.

- **Full** — Evaluates the cartridge memory (CM) and scans the entire tape. Can take more than 2 hours on a full tape. Example of when to use a full scan:

  - When tape cartridges are accessed infrequently and are used primarily for on site or offsite long-term data retention.

  - When tape cartridges with valuable data are introduced into the library and the state and condition of the tapes are unknown.

Setting	Description
Scan based on Tape Alert	Choose whether to scan tapes based on Tape Alert count; and, if so, which type of scan to perform (Quick, Normal, or Full, described above). Select **None** to disable this policy. This policy is disabled by default.
	When enabled, a tape will be scanned if the number of Tape Alerts reported for that cartridge exceeds the user-specified value in the **Tape Alert count** field, described in more detail below.
	The Tape Alerts included in the count are:
	• 01h (1)– Read Warning
	• 03h (3) – Hard Error
	• 04h (4) – Media
	• 05h (5) – Read Failure
	• 06h (6) – Write Failure
	• 12h (18) – Tape Directory Corrupted on Load
	• 33h (51) – Tape Directory Invalid on Unload
	• 34h (52) – Tape System Area Write Error
	• 35h (53) – Tape System Area Read Error
	• 37h (55) – Loading Failure
	• 3Bh (59) – WORM Medium Integrity Check Failed
Tape Alert count	Use this field in conjunction with the **Scan based on Tape Alert** policy. From the drop-down list, select the number of Tape Alerts allowed before a scan is performed.
Normal scan time interval	Scans a tape if the listed time interval since the last scan was performed has been exceeded. In the text box, type a time interval (in days) after which a scan will be performed. A value of zero (default) means the this policy is disabled.
Full scan time interval	**Note:** When deciding the interval, consider the number of tapes to be scanned in the entire library, as well as the type of scan to be performed. Full scans can take more than 2 hours on full tapes. Over-scheduling can cause delays or cause tapes not to be scanned as intended.

Setting	Description
Scan based on StorNext media suspect count	Only available if you selected **Use StorNext Configuration** above. The suspect count is a means by which StorNext Storage Manager determines when to stop writing data to tape. If you select this policy, a tape will be queued for EDLM testing when its suspect count threshold is reached. If the EDLM test indicates the tape is good, you can reset the suspect count on the StorNext application and continue to use the tape. For more information on suspect counts and resetting suspect counts, refer to your StorNext application's documentation.
Result Action Settings	
Disable RAS ticket for bad or suspect media	Select this check box if you wish to disable summary RAS tickets and RAS ticket e-mail notifications stating media is bad or suspect media based on the results of EDLM scans. By default, these summary RAS tickets are disabled (i.e., this check box is selected), because this information is available from the EDLM test results. **Note:** RAS tickets for specific drive and media issues found during EDLM scans will never be disabled. Only the summary results tickets and notifications (stating media is suspect or bad) can be enabled or disabled.
Initiate StorNext copy operation for	Only available if you selected **Use StorNext Configuration** above. Automatically requests StorNext Storage Manager to copy all data from a bad and/or suspect tape to another tape. From the drop-down list, you can choose to copy bad tapes, suspect tapes, or both. You can also choose **Disabled**, which disables the policy. This policy is disabled by default. A RAS ticket will be generated for each request to copy data indicating whether the request succeeds or fails.

6 Click **Apply** to finish.

Pausing EDLM Scans on Partitions

You can temporarily halt EDLM scanning in a partition but keep your EDLM policy selections intact so that you can re-enable them later. You might want to do this if you suspect a problem (for example, if it seems that too many tapes are being scanned, and library operations are being affected).

When you pause EDLM scans, tapes that are currently being scanned finish their scans, are unloaded from the tape drives, and are moved back to their original locations. No further tapes are scanned. Tapes in the queue remain queued. Once unpaused, tapes that would have been queued during the pause period are queued and scans resume as normal.

To pause automatic scanning, you must change the EDLM mode on a partition, as follows:

1 Log on as an administrator.

2 From the Web client, select **Operations > Partitions > Change Mode**.

The **Change Partition Mode** screen appears.

3 Under **EDLM Mode**, the **Current** column displays one of the following:

- Not Configured — EDLM policies have not been configured on the partition.

- Active — EDLM policies are configured and running.

- Paused — EDLM scanning is paused.

The **New** column contains an **Active/Paused** button. The button toggles between modes.

4 To change the mode from Active to Paused or from Paused to Active, click the button in the **New** column, and then click **Apply**.

The operation completes and, if successful, a Success message appears.

5 Click **Close** to close the Success message.

Running Manual EDLM Tests

You may wish to evaluate media outside of the automatic EDLM scanning policies. To do this, you can run a manual EDLM scan. Manual scans are given highest priority and go to the top of the scanning queue. As soon as an EDLM scanning drive has finished its current scan, it will accept the tape scheduled for a manual scan. Once all manual scans are finished, the scan queue continues as normal.

Manual EDLM scans can be run on any tape in the library, as long the following conditions are met:

- An EDLM license must be installed on the library.

- The EDLM library managed partition must be configured on the library (see Step 4: Creating the EDLM Library Managed Partition on page 213).

- The cartridge you want to scan must be readable by a tape drive in the EDLM library managed partition per standard LTO-gen-based backwards-compatibility limitations.

- The cartridge you want to scan must be labeled properly. Unlabeled media cannot be selected for manual scans.

- The cartridge can be located in any partition, including the EDLM library managed partition. However, the cartridge must not be located in an EDLM drive.

- If a tape is currently being scanned, you cannot select it for manual scanning.

To run a manual EDLM test, do the following:

1 Log on as an administrator.

2 Select **Tools > EDLM > Test Selection**.

The **Tools - EDLM Test Selection** screen appears.

3 From the **Partition** drop-down list, choose the partition that contains the tape(s) you want to scan.

4 From the **Scan type** drop-down list, choose the type of scan to perform (Quick, Normal, or Full). The default is Normal. For a description of these scan types, see the **Scan Settings** section of Table 8 on page 219.

5 If you want the test to continue on error, select the **Continue On Error** check box. By default, during normal and full scans, a cartridge memory (CM) test is performed first. If that fails, the rest of the scan (the tape test) is skipped and the test fails. When you select **Continue On Error**, the tape test is performed even if the CM test fails.

6 Select the tape(s) to scan from the table. To select all tapes listed, select the check box at the top of the check box column. To filter the displayed list, enter a barcode or portion of a barcode in the **Filter by barcode** field and click **Find**.

> **Note:** If you select a tape that is not supported by the EDLM scanning drives, once you click **Apply**, a dialog box message will appear stating, "You have selected to scan media that may not be supported by any of the EDLM drives installed in the library. If you continue, these scans may not complete successfully. Are you sure you want to do this?" If you continue, the tape will be queued for scan, but may fail.

7 Click **Apply**.

The test is queued. Once the test is queued, a **Success** message appears. This does not mean the test was run or that the tape passed the test, it just means that the test is queued.

> **Note:** Even though manually scheduled tests move directly to the top of the queue, it is possible that the tape will not be tested right away (if all EDLM drives are currently in the process of scanning tapes, they will finish their current scans before becoming available to perform the manually scheduled test).

8 Click **Close** to close the **Success** message.

9 To view the test results, select **Tools > EDLM > Test Results** (see Working With EDLM Test Results on page 226).

Working With EDLM Test Results

You can view the status of all your EDLM test sessions, including sessions that are queued but not started yet, in the EDLM Test Sessions List screen. You can stop, pause, resume, or delete test sessions. See Working with the EDLM Test Sessions List on page 227.

Each entry in the EDLM Test Sessions List screen presents an overview of a single EDLM test session. A test session includes all tapes in the library that were scheduled to be scanned at a particular point in time. Thus, a test session can include multiple tapes from different partitions.

• **Example 1:** You select 10 tapes on which to perform a manual scan. The test session includes 10 tapes.

- **Example 2:** Partition A has an automatic scan policy to scan tapes on import. You import a tape. Meanwhile, Partition B has an automatic scan policy to scan every 180 days. Ten tapes in that partition have reached the 180-day mark at the same time that you import the tape into Partition A. Because these automatic scans occur at the same time, the test session includes all 11 tapes from both partitions.

Within each test session, you view details about each tape that was scanned (see Viewing EDLM Session Report Details on page 229).

Working with the EDLM Test Sessions List

To view the status of EDLM test sessions (both automatic and manual), do the following:

1 Log on as an administrator.

2 From the Web client, select **Tools > EDLM > Test Results**.

The **Tools - EDLM Test Results** screen appears.

The table displays the set of media tests that have run based on the time range selected. Each row in the table presents an overview of a single EDLM test session. The table displays the following information about the test sessions:

Item	Description
Session ID	The session identifier, a unique number assigned to each test session that was run.
State	Pending, Complete, In Progress, Stopped, or Paused.
Start Time	The date and time the test session was started.
Finish Time	The date and time the test session completed.
Results	A summary of results for all media tested in the session. The reported values include the number of tapes scanned (in parentheses) for each result obtained. **Note:** To view results for individual tapes in the session, select a test session row and then click the **Details** button. Results are the following: • **Good** — The tape is good. • **Bad** — The tape is bad. • **Suspect** — The tape is possibly unreliable or defective. • **Untested** — The tape could not be fully scanned, for various reasons, including: incompatible media; cartridge could not be loaded; tape is encrypted but the data encryption key could not be obtained; drive not communicating with I/O blade, test was stopped. **Note:** Untested media do not initiate RAS tickets or EDLM media action policies (such as copying data from a bad or suspect tape). • **Not Completed** — The test has not completed yet.

3 From the **Select Time Range** drop-down list, select the range of time for test sessions that you want displayed. The time range is based on the start time of the test session. Choose one of the following:

- **Last Day** — Test sessions that were run in the last 24 hours.

- **Last Week** — Test sessions that were run in the last seven days.

- **Last Month** — Test sessions that were run in the last month.

- **All —** All test sessions that were run on the library. The storage limit is 5,000 media scans. When the limit is reached, old scan results are deleted as new scan results are added.

4 To work with a session, select a test session row and then click your desired option:

Option	Description
Stop	Stops a currently running test session. Once stopped, you cannot restart the test session. Any test results collected so far are listed. Tapes that did not complete testing as a result of being stopped show a test result of Untested.
Pause	Pauses a currently running test session. If a tape is currently being scanned, the scan will finish and the tape will be ejected and moved back to its original location. Tapes in the test session that have not been tested yet will remain queued.
Resume	Resumes a paused test session. Queued tapes are mounted and scanned.
Details	Displays the test report for the selected test session in a new window. See Viewing EDLM Session Report Details on page 229.
Delete	Deletes the selected test session from the list. Once deleted, you cannot retrieve the information again.

Viewing EDLM Session Report Details

To view details about a specific EDLM test session, do the following:

1 Go to the EDLM Test Results screen (**Tools > EDLM > Test Results**).

2 Select a row and then click the **Details** button.

The test results display in a new window.

Setup Operation Tools Reports

Tools - EDLM Test Results

The results of the session are indicated below. Select a row in the table to see a detailed report.

	Barcode	Test Result	Scan Type	Drive ID	Partition	State	Completed
⊙	8ST491L3	Suspect	Normal	HU173208L0	edlm_a	Complete	Mar 25, 2012 09:12:36 AM
○	000721L4	Suspect	Normal	HU173208L0	edlm_a	Complete	Mar 25, 2012 09:13:13 AM

◀ **Page:** 1 of 1 ▶   **Session Results: 1 - 2**

CM Scan Status:
Completed

CM Scan Analysis:
Drive Reported Tape Alert

Tape Scan Status:
Not run

Tape Scan Analysis:
N/A

[Back] [Refresh] [_____] [Send] [Save]

The top section of the screen lists each tape in the test session. The following information is reported:

Item	Description
Barcode	The media barcode identifier.
Test Result	The test result displays as one of the following: • **Good** — The tape is good. • **Bad** — The tape is bad. • **Suspect** — The tape is possibly unreliable or defective. • **Untested** — The tape could not be fully scanned, for various reasons, including: incompatible media; tape could not be loaded; tape is encrypted but the data encryption key could not be obtained; drive not communicating with I/O blade, test was stopped. **Note:** Untested media do not initiate RAS tickets or StorNext copy operations. • **Not Completed** — Test has not completed yet.
Scan Type	The type of test that was run: Quick, Normal, or Full.
Drive ID	The physical serial number of the tape drive that tested the tape.
Partition	The partition that the tape(s) being tested in the session belong to.
State	The current test status: Pending, In Progress, Completed, Stopped or Paused.
Completed	The date and time the test completed.

3 To view test details for a specific tape, select a row in the top section. Details about the test results display in the area below the table. The following details display:

Item	Description
CM Scan Status	One of the following: • **Complete** — Test is finished; however, the result may not be "good." You can also get this if the test was stopped. For details, see the CM Scan Analysis. • **Paused** • **Pending** • **Not Run** — For details see the CM Scan Analysis • **In Progress** • **Stopped**
CM Scan Analysis	One of the following: • **Good** • **N/A** • **Failed to receive CM data** • **CM hardware failure** • **Tape reached 99% of the manufacturer defined number of tape thread/load operations** • **Tape reached 99% of the manufacturer defined number of full tape capacity write operations** • **CM indicates uncorrected errors on the tape** • **Unable to load tape** • **Unable to unload tape** • **Tape not present** • **No compatible drive** • **I/O Blade Component Failure**

Item	Description
Tape Scan Status	One of the following: • **Complete** — Test is finished; however, the result may not be "good." For details see the CM Scan Analysis. • **Paused** • **Pending** • **Not Run** — For details, see the CM Scan Analysis. • **In Progress** • **Not Configured** — You requested a Quick Scan only so the tape was not scanned. • **Stopped**

Item	Description
Tape Scan Analysis	One of the following:
	• **Good**
	• **N/A**
	• **I/O Blade Component Failure**
	• **Failed to retrieve scan data**
	• **Unexpected EOD. Possibly corrupt CM**
	• **Unformatted tape**
	• **Failed to read tape data**
	• **Un-recovered read errors on the tape**
	• **Corrupt data format**
	• **Tape experienced a mechanical error**
	• **Tape performance is severely degraded**
	• **Unable to load tape**
	• **Unable to unload tape**
	• **Tape is a cleaning cartridge**
	• **CM fault detected**
	• **Unknown media type detected**
	• **Scan operation interrupted and ended**
	• **Drive does not report media presence**
	• **Tape is encrypted**
	• **Tape is blank**
	• **Block size exceeds maximum**
	• **Tape is a FUP tape**
	• **Drive CM read failed**

4 To send a copy of the test session report via e-mail, type an address in the **Send** field and click the **Send** button.

> **Note:** In order to send an e-mail, e-mail notifications must be set up on the library (**Setup > Notifications > E-mail Configuration**).

5 To update the screen with the current status, click **Refresh**.

Testing Suspect EDLM Drives

If an EDLM drive reports a suspicious number of errors within a given time period, it will be taken offline and not used for testing until brought back online manually. This operation allows testing the drive with a known-good tape cartridge to determine whether the problems detected by the drive are legitimate, or possibly due to a problem with the drive itself. If this occurs, the library will issue a RAS ticket directing you to test the tape drive.

To test the drive:

1 Select **Tools > Drive Operations**.

The **Tools - Drive Operations** screen opens.

4 To send a copy of the test session report via e-mail, type an address in the **Send** field and click the **Send** button.

> **Note:** In order to send an e-mail, e-mail notifications must be set up on the library (**Setup > Notifications > E-mail Configuration**).

5 To update the screen with the current status, click **Refresh**.

Testing Suspect EDLM Drives

If an EDLM drive reports a suspicious number of errors within a given time period, it will be taken offline and not used for testing until brought back online manually. This operation allows testing the drive with a known-good tape cartridge to determine whether the problems detected by the drive are legitimate, or possibly due to a problem with the drive itself. If this occurs, the library will issue a RAS ticket directing you to test the tape drive.

To test the drive:

1 Select **Tools > Drive Operations**.

The **Tools - Drive Operations** screen opens.

Setup   Operations   Tools   Reports

Tools - Drive Operations

Select the desired operation from the list below.

- ○ Update tape drive firmware using a firmware image file.
- ○ Retrieve tape drive log.
- ○ Retrieve tape drive sled log.
- ○ Clean tape drive.
- ○ Upload/remove tape drive firmware for autoleveling.
- ○ Force data path failover.
- ○ Force control path failover.
- ○ Perform EDLM drive test.

X Cancel   Next ▶

2 Select **Perform EDLM Drive Test** and click **Next**.

The **EDLM Drive Test** screen appears.
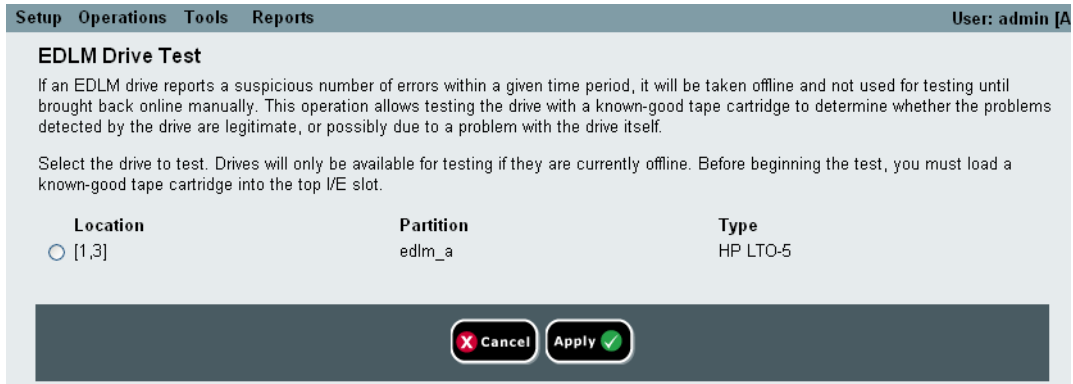
3 Place a known good tape cartridge into the top I/E station slot.

> **Note:** A "known good tape cartridge" means one that is fairly new, formatted, fully written, and that has a good cartridge memory (CM). It is a good idea to create one to have on hand for this type of operation.

4 Select the drive to test and click **Apply**.

The tape is tested using the known good tape cartridge. When the test completes, a **Success** or **Failure** message appears.

5 Do one of the following:

- **If the result is Success** — Manually bring the tape drive back online (**Tools > Drives > Change Mode**).

- **If the result is Failure** — If you used a known good tape, a failure generally means the drive has failed. View the RAS ticket details or contact Quantum Support for further analysis.

Running Your Library

This chapter explains how to access and operate your library. Most of the library functions described here can be found on the **Operations** menu.

> **Note:** The information in this chapter assumes you are using the Web client. Differences in functionality between the Web client and the operator panel are noted.

This chapter covers:

- [Powering on the Library](#)
- [Shutting Down, Powering Off, and Completely Removing Power](#)
- [Restarting the Library](#)
- [Logging In](#)
- [Logging Out](#)
- [Performing Media Operations](#)
- [About Cleaning Tape Drives](#)
- [About Tape Drive Operations](#)
- [Locking and Unlocking the I/E Stations](#)
- [Controlling FC I/O Blade Power](#)

Powering on the Library

To power on the library:

1 Connect all power cords to their electrical source.

2 Turn on each power supply using the switch on the rear of the power supply.

3 Press the power button located on the front door of the library's control module.

When you power on the library, the library performs a self-test to ensure that all of its parts are functioning properly. All tape drives and partitions are brought online.

Shutting Down, Powering Off, and Completely Removing Power

The **Shutdown** command shuts down the library's operating system and firmware. When performing a shutdown, the library finishes the current command and lowers the robot to the floor of the library.

Caution:	Always perform a shutdown before powering off the library or completely removing power from the library.

Before performing a shutdown, make sure the connected host applications are not sending commands to the library.

To power off the library: Perform the shutdown sequence and then press the power button on the front of the control module.

To completely remove power: Perform the shutdown sequence and power off the library. Then turn off the power switch on each power supply, located at the rear of the library. Finally, disconnect the power supply cables from their electrical source.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Operations > System Shutdown**.

- From the operator panel, select **Operations > Shutdown**.

Restarting the Library

The **Restart** command shuts down and restarts the library's operating system and firmware. When performing a restart, the library finishes the current command, then shuts down the library and restarts it. During the restart, the library brings all tape drives and partitions online and performs an inventory of cartridges, tape drives, and slots.

Before performing a restart, make sure the connected host applications are not sending commands to the library.

Restarting takes approximately 5 minutes for the control module and longer for the 14U and higher library configurations.

If the "Not Initialized" message appears on the operator panel after the restart process is complete, the library did not properly initialize. View the **All RAS Tickets** screen to find the problem that is preventing the library from properly initializing. See <u>Viewing RAS Tickets</u> on page 482.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Operations > System Shutdown**.

- From the operator panel, select **Operations > Shutdown**.

Logging In

All users, service users, and administrators must log in to the library to perform library functions or view library operations.

If you are logging in to the library for the first time using the default administrator account, type **admin** in the **User Name** text box and **password** in the **Password** text box.

After you log on for the first time, change the password for the default administrator account. Passwords are limited to 6–16 lower-case alphanumeric characters and can also include underscores (_), periods (.), hyphens (-), asterisks (*), and and the "at" symbol (**@**). For example: **pass_1**. For information on changing passwords, see Modifying Local User Accounts on page 98.

Note:	If you misplace the password for the default administrator account, contact Quantum Technical Support. For contact information, see Getting More Information or Help on page 8.

Logging In When LDAP or Kerberos is Enabled

When LDAP or Kerberos is enabled, the **Login** screen displays a **Remote Authentication** check box. Log in on either the operator panel or Web client as follows:

• Select the **Remote Authentication** check box to log in using a directory service user name and password.

• Clear the **Remote Authentication** check box to log in using a local user name and password.

For more information on LDAP, see Configuring LDAP on page 99.

For more information on Kerberos, see Configuring Kerberos on page 104.

Logging Out

Logging out secures the library from being accessed by unauthorized users. Log out whenever you have finished accessing the library through either the Web client or the operator panel.

From the Web client or the operator panel, you can click the **LOGOUT** button at the top right of the screen to log out. From the Web client, you can also select **Operations > Logout**.

Performing Media Operations

Administrators and users can use commands on the Web client and operator panel **Operations** menu to perform the following media operations:

- Import data cartridges into the library

- Export data cartridges from the library

- Move data cartridges between tape drives, I/E stations, and storage slots within a partition

- Import cleaning cartridges into the library (AutoClean is enabled)

- Export cleaning cartridges from the library (AutoClean is enabled)

- Load cartridges into tape drives

- Unload cartridges from tape drives

- Change the tape drive mode from online to offline and back as needed

In addition, administrators can:

- Clean tape drives manually, using the **Tools > Drive Mgmt > Clean Drive** command on the operator panel or **Tools > Drive Operations > Clean a tape drive** from the Web client.

The following topics provide an overview of these media operations. For step-by-step procedures, see the library's online Help. To access the online Help system, click the **Help** icon at the top right of the Web client or operator panel.

Note: The information and procedures in this user's guide apply specifically to the library Web client and the operator panel user interface, not to the host application. Performing media operations through the library user interface may affect your host application. See your host application documentation for information.

Importing Media

The Import Media operation allows you to use the I/E station to import data cartridges into the library. The library's scanner automatically reads the barcode on new cartridges imported into the library.

> **Note:** If your library has zero I/E station slots, you cannot import or export media. See [Configuring I/E Station Slots](#) on page 79.

This topic focuses on using the library user interface, not the host application, to import media. Using the library to import media may necessitate performing an inventory of the library with the host application. See your host application documentation for more information.

There are two ways to import tape cartridges via the library: with manual cartridge assignment enabled or disabled. Manual cartridge assignment is enabled on the library by default. For information on disabling/enabling this feature, see [Disabling/Enabling Manual Cartridge Assignment](#) on page 77.

This section contains the following sub-sections

- [Importing Media with Manual Cartridge Assignment Enabled](#) on page 243

- [Importing with Manual Cartridge Assignment Disabled](#) on page 244

- [Process for Importing Media](#) on page 244

The table below describes the differences in what you can do depending on manual cartridge assignment status:

Manual Cartridge Assignment	Cartridge Assignment in I/E Station	Is Importing Unassigned Media Allowed?
Enabled (default)	You are asked to assign cartridges to a partition immediately upon placing them in the I/E station. You may "cancel" out of this window without assigning them to a partition.	From operator panel: **NO** From Web client: **YES**
Disabled	You are not asked to assign cartridges to a partition and the cartridges remain unassigned until imported into the library.	From operator panel: **YES** From Web client: **YES**

Importing Media with Manual Cartridge Assignment Enabled

- When Manual Cartridge Assignment is enabled (default), once you load tape cartridges into the I/E station and close the I/E station door, the **Assign I/E** screen automatically appears on the operator panel. The **Assign I/E** screen prompts you to use the operator panel to assign the cartridges to a specific partition or to the system partition. The cartridges can be used only by the assigned partition. All of the cartridges you placed in the I/E station are assigned to the same partition that you selected.

- If you cancel out of the **Assign I/E** screen (or forget to assign the inserted cartridge to a partition), the cartridges remain unassigned until you either import them via the Web UI or open and close the I/E station so the **Assign I/E** screen displays again.

- You cannot import unassigned media into the library via the operator panel.

- You can import unassigned media into the library via the Web client. When importing cartridges via the Web client, all unassigned cartridges in the I/E station will be assigned to the same partition. However, only the cartridges you select will actually be moved into the library storage slots. The non-selected cartridges will remain in

the I/E station assigned to that partition until you import them into that partition. To import a previously assigned cartridge into a different partition, you must first remove that cartridge from the I/E station, place it in a different I/E station slot, and then import it into the desired partition.

• Unassigned cartridges are not visible to host applications.

Importing with Manual Cartridge Assignment Disabled

• Disabling manual cartridge assignment allows you to load several tape cartridges into the I/E station and assign them to different partitions.

• The **Assign I/E** screen does not appear on the operator panel. The cartridges in the I/E station are available for use by any partition, including the system partition. The cartridges in the I/E station remain unassigned until you import them into a partition (importing assigns them to the partition).

• You can import unassigned tape cartridges via the operator panel or the Web client. When importing unassigned tape cartridges, only the cartridges you actually import into a partition will be assigned to that partition. The rest of the cartridges will remain unassigned in the I/E station.

• Unassigned cartridges are visible to host applications and can be claimed by any host application on a first-come, first-served basis.

Process for Importing Media

You must have access to the library's I/E station and the operator panel to import cartridges.

If you have AutoClean enabled, you can also import cleaning cartridges into the library. For information, see Importing Cleaning Media on page 256. In addition, you can bulk load cartridges into the library rather than use the I/E station to import media. For information, see Bulk Loading on page 246.

Note: Once the import operation has started, do not interfere with the operation by opening and closing the I/E station door.

The process for importing cartridges includes the following steps:

1 Go to the front of the library and insert cartridges into the I/E station.

2 Close the I/E station door.

The **Assign I/E** screen appears on the operator panel if the **Manual Cartridge Assignment** setting is enabled on the operator panel **System Settings** screen (**Tools > System Settings**).

If the **Assign I/E** screen appears, do the following:

a Assign the cartridges to the appropriate partition by selecting a partition listed on the **Assign I/E** screen.

The partition button turns red after it has been selected.

> **Caution:** If you select the wrong partition, open the I/E station door. Move the cartridge to a different I/E station slot and close the I/E station door. The library will rescan the I/E station, and the **Assign I/E** screen will appear again.

b Select **Apply**.

If the selected partition is online, it will be taken offline before the import operation is performed, and brought back online after the operation is complete. If the library contains multiple partitions, the import operation will not affect operations in other partitions.

> **Note:** If the operation does not complete successfully, the partition remains offline until you turn it back online manually or restart the library (see Taking a Partition Online or Offline on page 76).

3 Use the **Import Media** screens on either the operator panel or the Web client to import the cartridges into the partition. Follow the on-screen prompts, or see the library's online Help for step-by-step procedures. To access the online Help system, click the **Help** icon at the top right of the Web client or operator panel user interface.

You need to provide the following information in the **Import Media** screens to import media:

- **Partition** — The partition into which you want to import the cartridges. The screen lists only the partitions to which you have been given access. The screen includes information about the partition mode (online or offline) and the number of empty slots in the partition. The number of cartridges you can import is limited to the number of empty slots.

- **Media** — The cartridges that you want to import.

> **Note:** You can filter the list of media by entering all or part of a barcode in the **Search** text box. Use an asterisk (*) to search with wildcards. You can also sort the list by clicking on columns with bold headings. For example, selecting the **Location** column heading sorts the list by location coordinates.

The paths to open the appropriate screens are as follows:

- **From the** Web client, select **Operations > Media > Import**.

- From the operator panel, select **Operations > Import Media**.

For step-by-step procedures, see the library's online Help. To access the online Help system, click the **Help** icon at the top right of the Web client or operator panel user interface.

Bulk Loading

Bulk loading is another way to load media into the library. If zero I/E station slots are configured, you will always need to bulk load cartridges into the library. If I/E station slots have been configured, you may want to perform an initial bulk load when you first start using your library. The library will perform an inventory after the bulk load is complete.

Before bulk loading, print out the Library Configuration report from the Web client to see how the physical slots of the library are configured. The report shows what slots are unavailable or configured as cleaning slots or as I/E station slots. For information on accessing the report, see <u>Viewing the Library Configuration Report</u> on page 268.

> **Caution:** Place cartridges in their appropriately configured slot location; for example, cleaning cartridges should not be placed in slots configured for storage.

When I/E station slots have been configured as I/E slots, the I/E station door is unlocked, and you can open the main access door to the library. When all I/E station slots are configured as storage, the I/E station door is always locked. You will not be able to open the main access door to bulk load tape cartridges into the library without first unlocking the I/E station door. If possible, bulk load the library before configuring the I/E station slots as storage. Otherwise, unlock the I/E station door. For information on locking and unlocking the I/E stations, see Locking and Unlocking the I/E Stations on page 262. For information on configuring I/E station slots, see Configuring I/E Station Slots on page 79.

To perform an initial bulk load, open the access door and manually insert directly into storage slots as many cartridges as you plan to use. The cartridges will not go in all the way if they are inserted incorrectly.

Note:	A small number of physical storage slots are inaccessible to the robot and should not be used for any tape cartridges. These slots appear as unavailable in the Library Configuration report. For detailed information on these slots, see Unused Slots on page 247.

Note:	When you open the main access door to load tape cartridges into the library, the library will automatically generate a Reliability, Availability, and Serviceability (RAS) ticket, alerting you to the fact that the door was opened. For information on resolving a RAS ticket, see About RAS Tickets on page 481.

After the initial bulk load, you can use the **Import Media** screen to add cartridges without interrupting library operations, as long as I/E station slots have been configured. For more information, see Importing Media on page 242.

Unused Slots

Each library configuration contains a limited number of slots that are not accessible to the robot. The slot counts in this user's guide do not include these unusable slots.

In any library configuration, the picker cannot access the bottom slot in each column in the lowest module in the stack due to the fact that there is

not enough clearance at the bottom of the library for the robotic picker. When bulk loading the library, do not insert storage or cleaning tapes into the bottom row of the lowest module in the library configuration.

Moving Media

Once media has been imported into the library, you can use the Move Media operation to move a single data cartridge between tape drives and slots within a partition.

> **Note:** If your library has zero I/E station slots, you cannot move cartridges to and from the I/E station. See <u>Configuring I/E Station Slots</u> on page 79.

This topic focuses on using the library user interface, not the host application, to move media. Using the library to move media may necessitate performing an inventory of the library with the host application. See your host application documentation for more information.

Details on using the library to move media include:

- If the partition is online, it will be taken offline before the move is performed and brought back online after the move is complete. You will be asked to confirm that you want to take the partition offline.

> **Note:** If the operation does not complete successfully, the partition remains offline until you turn it back online manually or restart the library (see <u>Taking a Partition Online or Offline</u> on page 76).

- You can select only the partitions to which you have been given access.

- You can only move media within one partition at a time.

You need to provide the following information in the user interface to move media:

- **Partition** — Lists the partitions that you have permission to access.

- **Selected Media** — The single cartridge that you want to move.

- **Selected Destination** — The location to which you want to move the cartridge.

> **Note:** You can filter the list of media by entering all or part of a
> barcode in the **Search** text box. Use an asterisk (*) to search
> with wildcards. You can also sort the list by clicking on
> columns with bold headings. For example, selecting the
> **Location** column heading sorts the list by location coordinates.

- The paths to open the appropriate screens are as follows:

- From the Web client, select **Operations > Media > Move**.

- From the operator panel, select **Operations > Move Media**.

For step-by-step procedures, see the library's online Help. To access the
online Help system, click the **Help** icon at the top right of the Web client or
operator panel user interface.

Exporting Media

The Export Media operation enables you to export data cartridges from
storage slots to empty I/E station slots for removal from the library.

> **Note:** If your library has zero I/E station slots, you cannot import or
> export media. See <u>Configuring I/E Station Slots</u> on page 79.

This topic focuses on using the library user interface, not the host
application, to export media. Using the library to export media may
necessitate performing an inventory of the library with the host
application. Also, if the host application has issued a prevent media
removal command, you will not be able to use the library user interface to
export media. See your host application documentation for more
information.

If you have AutoClean enabled, you can also export cleaning cartridges.
For information, see <u>Exporting Cleaning Media</u> on page 258.

> **Note:** Once the export operation has started, do not interfere with
> the operation by opening and closing the I/E station door.

> **Caution:** Some host applications may fail import/export operations when the I/E station contains cartridges that are assigned to another partition. Move cartridges from the I/E station as soon as possible to avoid possible conflicts with the other partitions.

Details on exporting cartridges include:

- If the partition is online, it will be taken offline before the export operation is performed and brought back online after the operation is complete. You will be asked to confirm that you want to take the partition offline.

  > **Note:** If the operation does not complete successfully, the partition remains offline until you turn it back online manually or restart the library (see Taking a Partition Online or Offline on page 76).

- You can select only the partitions to which you have been given access.

- You can only export cartridges if empty I/E station slots are available.

- You must have access to the library's I/E station and the operator panel to import cleaning cartridges.

You need to provide the following information in the **Export Media** screens to export media:

- **Partition** — The partition from which you want to export cartridges. The screens include information about the partition mode (online or offline) and the number of empty I/E station slots. The number of cartridges you can export is limited to the number of empty slots.

- **Media** — The tape cartridges that you want to export.

> **Note:** You can filter the list of media by entering all or part of a barcode in the **Search** text box. Use an asterisk (*) to search with wildcards. You can also sort the list by clicking on columns with bold headings. For example, selecting the **Location** column heading sorts the list by location coordinates.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Operations > Media > Export**.

- From the operator panel, select **Operations > Export Media**.

For step-by-step procedures, see the library's online Help. To access the online Help system, click the **Help** icon at the top right of the Web client or operator panel user interface.

Loading Tape Drives

The Load Drive operation enables you to load a cartridge from a storage slot into a tape drive. The storage slot and tape drive must be assigned to the same partition.

This topic focuses on using the library user interface, not the host application, to load tape drives. Using the library to load tape drives may necessitate performing an inventory with the host application. See your host application documentation for more information.

Details on loading tape drives include:

- If the partition is online, it will be taken offline before the load operation is performed and brought back online after the operation is complete. You will be asked to confirm that you want to take the partition offline.

> **Note:** If the operation does not complete successfully, the partition remains offline until you turn it back online manually or restart the library (see Taking a Partition Online or Offline on page 76).

- You can select only partitions to which you have been given access.

- Default tape drive locations are highlighted if the barcode field is empty or the field is cleared.

You need to provide the following information in the **Load Drive** screens to load tape cartridges into tape drives:

- **Partition** — The partition containing the cartridge you want to load into a tape drive. The screens include information about the partition mode (online or offline).

- **Media** — The tape cartridges that you want to move.

> **Note:** You can filter the list of media by entering all or part of a
> barcode in the **Search** text box. Use an asterisk (*) to search
> with wildcards. You can also sort the list by clicking on
> columns with bold headings. For example, selecting the
> **Location** column heading sorts the list by location coordinates.

The paths to open the appropriate screens are as follows:

• From the Web client, select **Operations > Drive > Load**.

• From the operator panel, select **Operations > Load Drive**.

For step-by-step procedures, see the library's online Help. To access the
online Help system, click the **Help** icon at the top right of the Web client or
operator panel user interface.

Unloading Tape Drives

The Unload Drive operation allows you to unload a cartridge from a tape
drive to a storage slot. The storage slot and tape drive must be assigned to
the same partition.

This topic focuses on using the library user interface, not the host
application, to unload tape drives. Using the library to unload tape drives
may necessitate performing an inventory with the host application. See
your host application documentation for more information.

Details about unloading tape drives include:

• Only drives with media loaded appear on the screen.

• You can select only partitions to which you have been given access.

• If the affected partition is online, it will be taken offline before the
unload operation is performed, and brought back online after it is
complete.

> **Note:** If the operation does not complete successfully, the
> partition remains offline until you turn it back online
> manually or restart the library (see Taking a Partition
> Online or Offline on page 76).

You need to provide the following information in the **Unload Drive**
screens to unload tape cartridges from tape drives:

- **Partition —** The partition containing the tape drive that you want to unload. The screens include information about the partition mode (online or offline).

- **Tape drive —** The tape drive that contains the cartridge that you want to unload.

Note:	You can sort the list of tape drives by clicking on columns with bold headings. For example, selecting the **Location** column heading sorts the list by location coordinates.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Operations > Drive > Unload**.

- From the operator panel, select **Operations > Unload Drive**.

For step-by-step procedures, see the library's online Help. To access the online Help system, click the **Help** icon at the top right of the Web client or operator panel user interface.

Taking a Tape Drive Online or Offline

There are two tape drive modes: online and offline.

- **Online** — Tape drive is available for use. This is the normal operating mode for the tape drive.

- **Offline** — Tape drive is offline to the host application and is not available for cartridge load and unload (move) operations initiated by the host application, but it remains available for Web client or operator panel initiated move commands.

Note:	If a cartridge is already in the tape drive when you take the tape drive offline, then the host can still read and write data on the tape.

Some operations require that the tape drive be offline. You can take a tape drive offline rather than the entire library or partition so as to minimize disruption of library operations.

This topic focuses on using the library user interface, not the host application, to change the tape drive mode. Using the library to change tape drive mode may affect the host application. See your host application documentation for more information.

Details on changing the tape drive mode include:

- The default tape drive mode is online.

- You can select only tape drives in partitions to which you have been given access.

- The **Online/Offline** buttons toggle between modes.

- Once taken offline, tape drives remain offline until they are turned online again, or the library is restarted. Restarting the library will bring all offline tape drives back online.

> **Note:** If you change the mode of a control path tape drive to offline, a caution dialog appears asking you to confirm the mode change. For information on control path tape drives, see <u>Working With Control Paths</u> on page 86.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Operations > Drive > Change Mode**.

- From the operator panel, select **Operations > Change Drive Mode**.

For step-by-step procedures, see the library's online Help. To access the online Help system, click the **Help** icon at the top right of the Web client or operator panel user interface.

About Cleaning Tape Drives

Library tape drives require occasional cleaning. Cleaning cartridges are used to remove accumulated residue from each tape drive's read/write head.

The library supports two methods for cleaning tape drives with cleaning cartridges: AutoClean and Manual.

AutoClean — Configuring one or more dedicated cleaning slots automatically enables AutoClean. Cleaning cartridges are stored in the designated cleaning slots. When a tape drive needs cleaning, it notifies the library, and the library automatically cleans the tape drive using a cleaning cartridge loaded in a cleaning slot. Automatic cleaning is

integrated into routine library operations. The host application requests the library to move a tape cartridge. If the tape drive performing the operation needs cleaning, the library will perform the move operation and then automatically clean the tape drive with a cleaning cartridge before informing the host application that the move operation is complete.

When a cleaning cartridge has expired, a RAS ticket informs the user to export the expired tape from the library. If more cleaning cartridges are present, the next cleaning cartridge will be used for the next cleaning request. If no more cleaning cartridges are available, a RAS ticket will inform the user that the tape drive needs cleaning and that a cleaning tape needs to be imported.

Only administrators can configure cleaning slots, thus enabling AutoClean. When AutoClean is enabled, the library allows you to import and export cleaning media through the I/E Station.

For information on configuring cleaning slots, see Configuring Cleaning Slots on page 78. For information on importing and exporting cleaning media, see Importing Cleaning Media on page 256 and Exporting Cleaning Media on page 258.

> **Note:** Cleaning slots are not visible to the host application. To choose host-based cleaning, do not configure any cleaning slots, and configure your host application to manage cleaning tape drives. Configuring cleaning slots on the library may affect the host application. See your host application documentation for information.

Manual Cleaning — When a tape drive needs cleaning, it notifies the library. If the library's AutoClean feature is not enabled (no cleaning slots have been configured), the library generates a RAS ticket informing the user that the tape drive needs cleaning. Administrators can clean tape drives manually at any time, using commands on the operator panel or Web client. For more information, see Manually Cleaning Tape Drives on page 260.

Enabling AutoClean

To enable AutoClean, an administrator must configure at least one cleaning slot in the library. For information on configuring cleaning slots, see Configuring Cleaning Slots on page 78. For a description of AutoClean, see About Cleaning Tape Drives on page 254.

Viewing the Cleaning Count

The cleaning count is the number of times a cleaning cartridge has been used to clean a tape drive. Knowing this can help you decide when to replace a cleaning cartridge. The cleaning count is now listed in two locations:

- Library Configuration Report (from the Web client, select **Reports > Library Configuration**)

- Export Cleaning Media screen (from the Web client, select **Operations > Cleaning Media > Export**)

Using Valid Cleaning Media

The preferred method of labeling a cleaning cartridge is to have **CLN** or **CLNU** as the prefix on the label. Any cartridge detected with a **CLN** or **CLNU** prefix will be considered a universal cleaning cartridge, regardless of any media identification extension. Cartridges containing a media identification of **C1**, **C2**, **C3**, **C4**, **C5**, and **CU** will be considered cleaning cartridges and will be tracked and treated as if the media label contained the prefix **CLN** or **CLNU**.

Importing Cleaning Media

When AutoClean is enabled (at least one cleaning slot has been configured), you can use the Import Cleaning Media operation to import cleaning cartridges from the I/E station to designated cleaning slots. For information on configuring cleaning slots, see Configuring Cleaning Slots on page 78. For a description of AutoClean, see About Cleaning Tape Drives on page 254.

When manual cartridge assignment is enabled (the default setting), you cannot import cartridges via the operator panel until you have assigned them to a specific partition or to the system partition. Cleaning cartridges should always be assigned to the system partition. Assigning cleaning cartridges to the system partition makes them available to all partitions in the library. For more information about manual cartridge assignment, see Importing Media on page 242 and Disabling/Enabling Manual Cartridge Assignment on page 77.

You must have access to the library's I/E station and the operator panel to import cleaning cartridges.

> **Caution:** Some host applications may fail import/export operations when the I/E station contains cartridges that are assigned to another partition. Move cartridges from the I/E station as soon as possible to avoid possible conflicts with the other partitions.

> **Note:** If your library has zero I/E station slots, you cannot import or export cleaning media. See <u>Configuring I/E Station Slots</u> on page 79.

> **Note:** Once the import operation has started, do not interfere with the operation by opening and closing the I/E station door.

The process for importing cleaning cartridges includes the following steps:

1 Go to the front of the library and insert the cartridges into the I/E station.

> **Note:** Do not insert cartridges into the I/E station during the restart process.

2 Close the I/E station door.

The **Assign I/E** screen appears on the operator panel if the **Manual Cartridge Assignment** setting is enabled on the operator panel **System Settings** screen (**Tools > System Settings**).

If the **Assign I/E** screen appears, do the following:

a On the **Assign I/E** screen, select **System**.

The **System** button turns red after it is selected. Selecting **System** assigns the cartridge to the physical library and not to a specific partition.

b Select **Apply**.

3 Use the **Import Cleaning Media** screen on either the operator panel or the Web client to import the cleaning cartridges into the library. Follow the on-screen prompts, or see the library's online Help for

step-by-step procedures. To access the online Help system, click the **Help** icon at the top right of the Web client or operator panel user interface.

You need to provide the following information in the **Import Cleaning Media** screens to import media:

- **Media** — the cleaning cartridges that you want to import.

The screen includes information about the number of empty cleaning slots in the library. The number of cleaning cartridges you can import is limited to the number of empty cleaning slots.

Note:	You can filter the list of media by entering all or part of a barcode in the **Search** text box. Use an asterisk (*) to search with wildcards. You can also sort the list by clicking on columns with bold headings. For example, selecting the **Location** column heading sorts the list by location coordinates.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Operations > Cleaning Media > Import**.
- From the operator panel, select **Operations > Import Cleaning Media**.

Exporting Cleaning Media

When AutoClean is enabled, you can use the Export Cleaning Media operation to export one or more cleaning cartridges from dedicated cleaning slots to the I/E station for removal from the library. You may need to export expired cleaning cartridges or free up cleaning slots for data storage.

After exporting cleaning cartridges, you can reduce the number of configured cleaning slots. The extra slots become available for use as storage slots. For information on configuring cleaning slots, see Configuring Cleaning Slots on page 78. For a description of AutoClean, see About Cleaning Tape Drives on page 254.

Caution:	Some host applications may fail import/export operations when the I/E station contains cartridges that are assigned to another partition. Move cartridges from the I/E station as soon as possible to avoid possible conflicts with the other partitions.

> **Note:** If your library has zero I/E station slots, you cannot import or export cleaning media. See Configuring I/E Station Slots on page 73.

> **Note:** Once the export operation has started, do not interfere with the operation by opening and closing the I/E station door.

Details on exporting cleaning cartridges include:

- You must have access to the library's I/E station and the operator panel to export cleaning cartridges.

- You can only export cartridges if empty I/E station slots are available.

You need to provide the following information in the **Export Cleaning Media** screens to export cleaning media:

- **Media —** The tape cartridges that you want to export.

The screen includes information about the number of empty I/E station slots in the library. The number of cleaning cartridges you can export is limited to the number of empty I/E station slots. The screen also displays the cleaning status (usable/expired) and cleaning count (the number of times the cartridge was used to clean a tape drive) for each cleaning cartridge in the library.

> **Note:** You can filter the list of media by entering all or part of a barcode in the **Search** text box. Use an asterisk (*) to search with wildcards. You can also sort the list by clicking on columns with bold headings. For example, selecting the **Location** column heading sorts the list by location coordinates.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Operations > Cleaning Media > Export**.

- From the operator panel, select **Operations > Export Cleaning Media**.

For step-by-step procedures, see the library's online Help. To access the online Help system, click the **Help** icon at the top right of the Web client or operator panel user interface.

Manually Cleaning Tape Drives

The **Clean Drive** screens allow administrators to manually clean tape drives.

Note:	Be sure to unload the tape drive before attempting to clean it. If the tape drive is loaded with a cartridge, it will not available for this operation.

If you have at least one cleaning slot configured (see Configuring Cleaning Slots on page 78), and you are using the Web client, you can choose to use a cleaning tape from either a configured cleaning slot or the topmost I/E station slot. If two or more cleaning slots are configured and have cleaning tapes in them, the library chooses which cleaning tape to use. If you have zero cleaning slots configured, or if you are using the operator panel, you must use a cleaning tape in the topmost I/E station slot. You are prompted to insert a cleaning cartridge in the appropriate slot and select the tape drive you want to clean. The library then takes the associated partition offline, moves the cleaning cartridge from the I/E station slot to the designated tape drive, and cleans the tape drive. You will be asked to confirm that you want to take the partition offline.

When the operation is complete, the library moves the cleaning cartridge back to the I/E station slot and takes the partition back online.

Note:	If the operation does not complete successfully, the partition remains offline until you turn it back online manually or restart the library (see Taking a Partition Online or Offline on page 76).

Note:	If your library has zero I/E station slots, you will not be able to manually clean tape drives. See Configuring I/E Station Slots on page 79.

For step-by-step procedures, see the library's online Help. To access the online Help system, click the **Help** icon at the top right of the Web client or operator panel user interface.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Tools > Drive Operations > Clean a tape drive**.

- From the operator panel, select **Tools > Drive Mgmt > Clean drive**.

About Tape Drive Operations

You can perform the following tape drive operations:

- Upgrade tape drive firmware using a firmware image file. For more information, see <u>Using an Image File to Upgrade Tape Drive Firmware</u> on page 282.

- Retrieve tape drive logs. Tape drive logs can be retrieved from any tape drive installed in the library. For more information, see <u>Retrieving Tape Drive Logs</u> on page 495.

- Retrieve tape drive sled logs. Tape drive sled logs can be retrieved from any sled installed in the library. For more information, see <u>Retrieving Tape Drive Sled Logs</u> on page 496.

- Clean tape drives. Tape drive can be cleaned manually at any time. For more information, see <u>About Cleaning Tape Drives</u> on page 254.

- Upload/remove tape drive firmware for autoleveling. Available only for FC tape drives connected to an FC I/O blade. For more information, see <u>Autoleveling Tape Drive Firmware</u> on page 283.

- Reset tape drives. Resetting a tape drive power cycles the tape drive while the tape drive remains in the drive sled in the library. For more information, see <u>Drive Reset</u> on page 514.

- Force data path failover. For use with a Storage Networking license and HP LTO-5 tape drives. See <u>Forcing Data Path Failover</u> on page 158.

Locking and Unlocking the I/E Stations

Each control module and expansion module has an I/E station door with multiple open and close sensors. A secondary door located behind the I/E station door acts as a redundant indicator as to whether the I/E station is opened or closed. When you are finished accessing the I/E station, make sure the station door is fully closed.

Administrators can use this operation to lock or unlock the doors for all I/E stations that are configured as I/E station slots. If all I/E station slots are configured as storage, this operation unlocks the control module I/E station only.

> **Note:**   Some host applications use a command to lock and unlock I/E station doors. This command usually cannot be overridden by the library. Use the host application to lock or unlock I/E station doors if this occurs. Using the library lock/unlock operation may affect the host application. See your host application documentation for information.

There are three 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" 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.

- If the I/E station slots are configured as storage slots, the door is always locked. When all I/E station slots are configured as storage slots, you can use the Locking and Unlocking I/E station operation to unlock the I/E station in the control module. When the I/E station is unlocked, you can open the main access door on the control module. This, in turn, unlocks all remaining I/E stations in the library, allowing you to access all remaining access doors in the library.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Operations > I/E Station**.
- From the operator panel, select **Operations > Lock/Unlock I/E Station**.

Controlling FC I/O Blade Power

Administrators can turn on, turn off, or power cycle individual FC I/O blades in the library. Turning off or power cycling the FC I/O blade will cause a temporary loss of communication with connected hosts. The screen will display a warning message about the communication loss and ask you to confirm that you want to proceed.

The **Setup - Blade Control** screen allows you to perform the following operations on the selected FC I/O blades:

On the Web client:

- Click **On** to turn on the FC I/O blade.
- Click **Off** to turn off the FC I/O blade.
- Click **Cycle** to power cycle the FC I/O blade. It takes approximately 3 minutes to power cycle a blade.

On the operator panel, select the option you want:

- Power Cycle Blade
- Power On Blade
- Power Off Blade

Note:	This operation should not be performed concurrently by multiple administrators logged in from different locations. You can access the appropriate screens, but you cannot apply changes while another administrator is performing the same operation.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Setup > I/O Blades > Blade Control**.

- From the operator panel, select **Setup > I/O Blades > Blade Control**.

Getting Information – Logs and Reports

This chapter describes how to find information about your library.

From the operator panel, you can find system information in the **About Scalar i500** screen (**Tools > About Library**). From the Web client, you can find information in the **Reports** and **Tools** menus.

> **Note:** Users without administrator privileges can view only certain reports. See <u>User Privileges</u> on page 50 for information about user privileges.

This chapter covers:

- <u>Viewing Information About the Scalar i500</u>
- <u>Viewing the System Information Report</u>
- <u>Viewing the Library Configuration Report</u>
- <u>Viewing the Network Settings Report</u>
- <u>Viewing Logged-in Users</u>
- <u>Viewing the All Slots Report</u>
- <u>Viewing, Saving, and E-mailing Library Logs</u>
- <u>Viewing FC I/O Blade Information</u>
- <u>Viewing FC I/O Blade Port Information</u>

Viewing Information About the Scalar i500

The **About** screen gives you a quick glance at your library settings.

From the Web client, you can view the **About Scalar i500**report, which provides the following information about the library:

- Serial Number
- Firmware Version Number

From the operator panel, the **About** screen provides the following information about the library:

- Library name
- State
- Serial number
- System firmware version number
- Date and time of last firmware update
- Current date and time

From the operator panel **About** screen, you can also navigate to other screens for detailed information about:

- the network (IP addresses)
- tape drives
- partitions

The paths to open the appropriate screens are as follows:

- From the Web client, select **Reports > About > Scalar i500**.
- From the operator panel, select **Tools > About Library**.

Viewing the System Information Report

The System Information Report contains information on the following library settings:

- **Date and time** — current date, time, and time zone settings

- **Physical library** — host name, Internet Protocol (IP) address(es), serial number, firmware version, board support package (BSP) level, the date the BSP was last updated, and robot firmware version.

- **Encryption** (this section displays only if encryption key management is licensed and configured on the library) — key server type; encryption software version; SSL connection (enabled/disabled); primary host (primary key server IP address or host name), primary key server port number; primary key server serial number; secondary host (secondary key server IP address or host name); secondary key server port number; secondary key server serial number.

- **Library Partitions** — name, serial number, control path, mode, encryption method, encryption system type, number of slots, number of media, number of tape drives, and whether FIPS is configured for each partition.

- **Tape drives —** location coordinates, vendor name, model, type, physical serial number (P-SN), logical serial number (L-SN), firmware level, sled boot version, sled application version, encryption method, and whether the tape drive is connected to an I/O blade.

- **FC I/O blades** — if the library contains FC I/O blades, this table lists the location coordinates, World Wide Node Name (WWNN), firmware level, and ready status.

- **EE blades** — if the library contains Ethernet Expansion blades, this table lists the location coordinates and status.

The path to open the report from the Web client is **Reports > System Information**.

Viewing the Library Configuration Report

The Library Configuration Report is a dynamic representation of the physical locations of various library resources, including tape drives, slots, partitions, and modules.

Each partition's slots are displayed in a unique color, indicated in the legend. I/E station slots, cleaning slots, and unavailable slots are also displayed in unique colors. A black triangle in the upper left corner of a slot indicates media is present in the slot. A red triangle indicates media is present but the media barcode label is unreadable. A "**c**" in a tape drive indicates the drive is the control path for the partition.

By default, the Library Configuration Report displays the coordinates for all licensed slots that are assigned to a partition. To view all library slot coordinates, click **Show ALL coordinates**. To display the barcodes for all imported cartridges, click **Show Barcodes**.

shows an example of the Library Configuration Report.

Figure 36 Library Configuration
Report
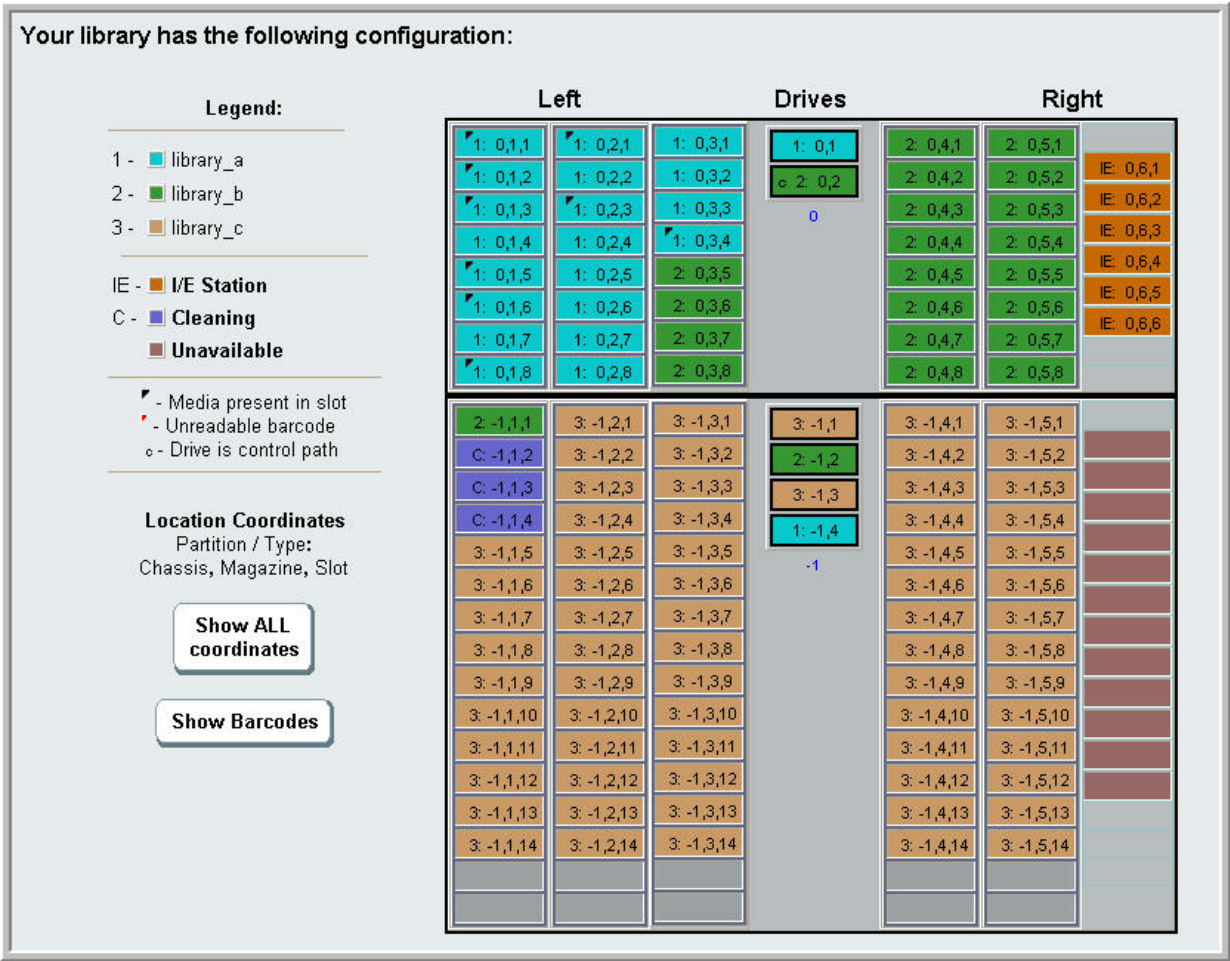
Use the report to view detailed information on the following resources. Click on the item you want to view and the information appears in a box to the right of the library diagram.

- **Tape drives** — Depending on the interface type, the information provided may not include all of the following: interface type, tape drive type, ready state, mode (online/offline), assigned partition name, location coordinates, media barcode ("No_Label" means unreadable barcode), media type, element address, vendor, model,

physical SN, logical SN, World Wide Node Name (WWNN), World Wide Port Name (WWPN), loop ID, topology request, speed request, actual topology, actual speed, maximum speed, active port (if the drive has more than one FC port), SNW licenses (displays which Storage Networking features the tape drive is using, if any; see Chapter 6, Storage Networking), SCSI ID, SAS address, tape drive firmware level, control path status, and encryption method of each tape drive.

> **Note:** The library configuration report lists the native device identifier as reported by the tape drive. HP tape drives always report SCSI as the native device identifier, even if they are Fibre Channel or SAS. For example, if you have HP L TO-4 Fibre Channel or SAS drives, they will be listed in the report as HP LTO-4 SCSI drives.

- **Slots** — Type, assigned partition name (storage and import/export [I/E] station slots only), location coordinates, barcode (storage and I/E station slots only), media type, element address, encryption method, get count, get retries, put count, and put retries. If the slot is a cleaning slot, the cleaning status (usable/expired) and cleaning count (the number of times the cartridge was used to clean a tape drive) are also displayed. For more details about slot data, see Viewing the All Slots Report on page 272.

- **Partitions** — Name, online status, emulation type, barcode policy, number of total tape drives in the partition, number of active tape drives partition, total media, mounted media, total slots, full slots, total I/E stations, full I/E stations, and encryption method of each partition.

- **Modules (Chassis)** — Manufacturer, model type, and serial number of each module.

You can print the report by clicking on the printer icon in the report window.

The path to open the report from the Web client is **Reports > Library Configuration**.

Viewing the Network Settings Report

The Network Setings Report provides information on the following library network settings:

- **Network** — host name, primary DNS, alternate DNS.

- **IPv4 Settings** — Dynamic Host Configuration Protocol (DHCP) enabled/disabled, IP address, gateway address, and net mask.

- **IPv6 Settings** (if IPv6 is enabled) — DHCP enabled/disabled, Stateless enabled/disabled, Static enabled/disabled, network prefix, gateway, and all IPv6 addresses.

- **SSL** — SSL, port, and cipher of the library.

- **SMI-S** — access and state enabled/disabled settings of the library.

  - **Access**: Indicates whether the SMI-S port for SMI-S traffic to the library (port 5988) is enabled or disabled. You can change the setting via the operator panel, **Tools > Security** menu. The default setting is enabled.

  - **State**: Indicates whether allowing SMI-S to run on the library is enabled or disabled. You can change this setting on the operator panel, **Tools > System Settings**. The default is disabled.

- **SNMP** — access enabled/disabled, V1 enabled/disabled, V2 enabled/disabled, V3 enabled/disabled, algorithm, encryption enabled/disabled, and port.

- **SNMP-Traps** — IP addresses and ports.

The path to open the report from the Web client is **Reports > Network Settings**.

Viewing Logged-in Users

The Logged-in User's Report report contains information about the users that are currently logged into the library. The report contains the following information:

- **User name** — Name of logged-in user.

- **Role name** — Privilege level of logged-in user (for example, **Admin** for administrator, **User** for non-administrator, non-service user).

- **Login date and time** — Date and time the user logged into the library.

- **Last activity date and time** — Date and time the user last logged into the library.

- **Login location** — IP address or host name of the system being used to access the system.

- **Management interface** — User interface being used to access the system (Web client or operator panel).

The path to open the report from the Web client is **Reports > Logged in Users**.

Viewing the All Slots Report

The All Slots Report contains information on all slots that are currently assigned to a partition and all I/E slots. A maximum of 20 responses displays per page. You can scroll between the pages using the page arrows at the bottom left of the screen. The report contains the following information about each slot:

- **Slot type** — Drive, I/E station, cleaning, or storage slot.

- **Barcode** — Barcode number of the cartridge installed in the slot (no barcode number means the slot is empty).

- **Partition** — The partition that owns the slot.

- **Location** — Location coordinates of the slot. (For a description of location coordinates, see <u>Understanding the Location Coordinates</u> on page 32.)

- **Element Address** — Element address of the slot.

- **Encryption** — The encryption state of the media in the slot. In order for the library to know the encryption state, the tape must have been placed into an encryption-capable tape drive in the library. The encryption-capable tape drive reads and records the encryption state of the tape, and the encryption state displays as "Encrypted" or "Not Encrypted." If the tape was not placed into an encryption-capable tape drive in the library, or if the slot is empty, the encryption state displays as "Unknown."

- **Get Count** — The number of times the picker successfully removed a tape from the slot.

- **Get Retries** — The number of times the picker had to perform a recovery operation to remove a tape from the slot.

- **Put Count** — The number of times the picker successfully placed a tape into the slot.

- **Put Retries** — The number of times the picker had to perform a recovery operation to place a tape into the slot.

> **Note:** "Get" and "put" counts and retries are counted from the beginning of library use to the present. If the LCB compact flash card is replaced, the count starts over at zero.

The path to open the report from the Web client is **Reports > All Slots**.

Viewing, Saving, and E-mailing Library Logs

The library collects specific information in log files that you can view onscreen, save to your computer, or e-mail to a recipient. The following library logs are available:

- **Installation Verification Test Summary Log** — This log is saved each time you run the Installation Verification Test (IVT). The log saves only the information from the most recently run test. If you run the

test again, the new information overwrites the previous information. This option presents the summary log. For more information, see <u>Using the Installation Verification Test</u> on page 509.

- **Installation Verification Test Detailed Log**— This log is saved each time you run the Installation Verification Test (IVT). The log saves only the information from the most recently run test. If you run the test again, the new information overwrites the previous information. This option presents the detailed log. For more information, see <u>Using the Installation Verification Test</u> on page 509.

- **Command History Log** — Available only if you are using FC I/O blades. When you select this report, you choose the FC I/O blade and device for which you want to run the report. The **Blade** menu lists all FC I/O blades installed in the library (if more than one are installed). The **Devices** menu lists the devices associated with the selected FC I/O blade. The report shows all commands from the selected device to the selected blade. When the log file reaches its maximum size, the oldest information is replaced as new information is added.

- **Cleaning Log** — Shows all cleanings that have been performed in the library since firmware version 520G was installed. When the log reaches its maximum size, the oldest information is replaced as new information is added. The comma-separated values (csv) file provides the following information:

  Date Time (date and time); Barcode (barcode of the cleaning cartridge); Tape (location coordinates of the cleaning cartridge); Drive (location coordinates of the tape drive that was cleaned); Status (pass/fail); Return Code (service use only), Cleaning Type (Manual, Auto, MoveMedium), Expired ("Invalid" if the tape is expired or a data tape was improperly used to clean; "-" if not applicable); Usage Count ("N/A" if the cleaning did not complete); Reserved.

- **Slot Position Log** — Shows current information for all slots in the library. The comma-separated values (csv) file provides the following information for each slot:

  Date and Time, Slot Type (Picker, Drive, Storage, or IE), Object Present? (Y, N), Location Coordinates, X Position, Y Position, Angle Position, X Calibration Offset, Y Calibration Offset.

- **RAS Tickets Log** — Records all RAS tickets for the library. When the log file reaches its maximum size, the oldest information is replaced as new information is added.

- **Media Security Log** — Lists media that have been completely removed from the library. This log is only available if you have an Advanced Reporting license installed on the library (see <u>Obtaining and Installing a License Key</u> on page 88), and you have enabled the library to collect data for the log file. For more information about this log and how to enable the library to collect data for the log, see <u>Configuring and Viewing the Media Security Log</u> on page 143.

- **Media Usage Log** — Lists information regarding data written and read on the medium and lists statistics pertaining to soft and hard read and write errors. This log is only available if you have an Advanced Reporting license installed on the library (see <u>Obtaining and Installing a License Key</u> on page 88). For more information about the information displayed in this log, see <u>Viewing the Media Usage Log</u> on page 144.

- **SKM Encryption Key Import Warning Log** — Lists keys that failed the most recent data key import operation. This log is only available if you are running Scalar Key Manager (SKM). For detailed information about this log, see <u>Using the SKM Encryption Key Import Warning Log</u> on page 197.

The path to open the report from the Web client is **Reports > Log Viewer**.

Viewing FC I/O Blade Information

Administrators can view information about all the FC I/O blades installed in the library. The **Tools - Blade Information** screen lists the following FC I/O blade information:

- **Location**—Library location coordinates of the blade: [module,blade#], where blade# is 1 for the top blade in the module and 2 for the bottom blade in the module.

- **Firmware Version**—Firmware version of the blade (part of the library firmware).

- **Serial Number**— Serial number of the blade.

- **WWNN**—World Wide Node Name of the blade.

- **CCL** — Command control LUN.
- **Status/State** — The status of the blade can be: Ready, Not Ready, Auto Level Failed, Auto Leveling Booting, and Unknown.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Tools > I/O Blade Info**.
- From the operator panel, select **Tools > Blade Info**.

Viewing FC I/O Blade Port Information

Administrators can view information about all the FC I/O blades installed in the library. The **Tools - Blade Port Information** screen lists the following port information for each FC I/O blade:

- **Port number** — The port number: 1–6.
- **WWPN** — World Wide Port Name of the port.
- **Status** — The status of the blade: Config wait, Loop init, Login, Ready, Lost Sync, Error, Re-Init, Non part, and Failed.
- **Actual Speed** — Negotiated speed of the port: 1 Gb/s, 2 Gb/s, or 4 Gb/s. If the port is not in a ready state, "N/A" displays.
- **Actual Loop ID** — Negotiated loop ID of the port: 0–125. On the Web client, if the port connection type is Point to Point, or if the port is not in a ready state, "N/A" displays. On the operator panel, if the port is not in a ready state, "N/A" displays.
- **Requested Speed** — Requested speed of the port: Auto, 1 Gb/s, 2 Gb/s, 4 Gb/s, or 8 Gb/s (Web client only).
- **Requested Loop ID** — Requested loop ID of the port: Auto or 0–125 (Web client only).
- **Framesize** — Framesize setting of the port: 528, 1024, or 2048.
- **Mode** — Mode of the port: Public or Private.
- **Role** — Role of the port: Target (ports 1–2) or Initiator (ports 3–6).
- **Connection** — Connection type of the port: Loop, Point to Point, or Loop Preferred.

For information about configuring FC I/O blade ports, see <u>Configuring FC I/O Blade Ports</u> on page 110.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Tools > I/O Blade Port Info**.

- From the operator panel, select **Tools > Blade Info > Port Info**.

Updating Library and Tape Drive Firmware

There are two types of firmware that can be upgraded on the library: library firmware (including drive sled firmware) and tape drive firmware. There may be times when you will need to upgrade your library and tape drive firmware as directed by Quantum Support.

You can find release notes, upgrade instructions, and a listing of the latest version of firmware on the Quantum Web site at: http://www.quantum.com/ServiceandSupport/SoftwareandDocumentationDownloads/SI500/Index.aspx.

You need to contact Quantum Support directly to receive the firmware itself. Before loading firmware, check the release notes to make sure that it is compatible with your library and tape drives.

This chapter covers:

- Upgrading Library Firmware
- Upgrading Tape Drive Firmware
- Autoleveling Tape Drive Firmware

Upgrading Library Firmware

The library firmware upgrade operation allows you to upgrade library firmware using the Web client. Upgrading library firmware can take up to an hour for large configurations. Contact Quantum Support for a copy of the latest firmware. Download the file to your computer hard drive. Library firmware comes bundled with tape drive firmware, firmware upgrade instructions, and release notes. Verify with the release notes or Quantum Support that you are updating the library with the correct version of firmware. For technical support see Getting More Information or Help on page 8.

Library firmware version 200G.GSxxx and 210G.GSxxx (SP1) support library configurations of up to 14U. Library firmware 300G.GSxxx (I1) supports library configurations up to 23U. Library firmware versions 320G.GSxxx (SP3) and higher support library configurations up to 41U. Make sure you are running the appropriate firmware version to support the size of your library. It is recommended that you use the most current version of firmware regardless of library size.

- To determine the latest version of library firmware, refer to the release notes or check the Quantum Web site at: http://www.quantum.com/ServiceandSupport/SoftwareandDocumentationDownloads/SI500/Index.aspx.

- To find out the latest version of tape drive firmware, refer to the release notes.

Release notes and instructions for upgrading library and tape drive firmware can be found here: http://www.quantum.com/ServiceandSupport/SoftwareandDocumentationDownloads/SI500/Index.aspx.

It is recommended that you resolve and close all open RAS tickets before upgrading library firmware. If Auto-Ticket Closure is enabled, all open RAS tickets will be closed during the reboot which occurs after firmware is upgraded (see Closing RAS Tickets Automatically on page 485).

Saving the current library configuration before you upgrade library firmware is recommended in case the upgrade fails. After you have upgraded the firmware, save the library configuration again. For more information, see Saving and Restoring the Library Configuration on page 488.

It is also a good idea to capture a library snapshot information before making any significant change to your system such as upgrading library firmware. Technical support personnel can, if necessary, use the snapshot file to troubleshoot the library. For more information, see Capturing Snapshots of Library Information on page 485.

Caution:	If you are currently running library firmware version 320G.GS004 or 400G.GS006, you must first install and run the Library Service Utility before upgrading firmware. If you do not first run the Library Service Utility, then the firmware upgrade may not complete successfully. The Library Service Utility and installation instructions are located in the ".zip" file that contains the firmware download files.
	If you are currently running library firmware prior to version 320G.GS004, do not upgrade to version 320G.GS004 or 400G.GS006, but instead upgrade to the latest version. You will not need to run the Library Service Utility.

Note:	If you downgrade from one major firmware version to an earlier major version, library configuration settings will be reset to the factory defaults. You can restore the other configurable items using a configuration file that was saved when the earlier version of library firmware was installed on the library, or you can reconfigure your library's settings. For more information, see Saving and Restoring the Library Configuration on page 488.

Note:	If you are running firmware version 400G or higher and want to downgrade, the following restrictions apply:
	• If your library is Quantum branded, you can downgrade to version 400G or higher (there is no lower version of Quantum-branded firmware).
	• If your library is ADIC branded and has FC I/O blades installed, you can downgrade to version 400G or higher. Firmware versions 320G and lower do not support FC I/O blades. If your library does not have FC I/O blades, you can downgrade to a lower version of firmware.

> **Note:** If your library is running firmware version 600G or later, you can only downgrade library firmware to version 410G or later. If you need to downgrade to a version earlier than 410G, contact Quantum Support for assistance.

> **Note:** If you purchased your library after October 15, 2008, you cannot downgrade library firmware to below version 520G.

> **Note:** This operation should not be performed concurrently by multiple administrators. You can access the screen, but you cannot apply changes while another administrator is performing the same operation.

> **Note:** The library automatically restarts after the firmware upgrade is complete. Before logging into the library, clear the Web browser cache. See your Web browser's documentation for instructions on how to clear the cache.

You can find instructions on updating library firmware on the Quantum Website. You can also find step-by-step instructions in your library's online Help. To access the online Help system, click the **Help** icon at the top right of the Web client or operator panel user interface.

You cannot upgrade library firmware from the operator panel. The path to open the appropriate screen is as follows:

- From the Web client, select **Tools > Update Library Firmware**.

Upgrading Tape Drive Firmware

You can use the Web client to upgrade one or more tape drives in your library with an image file obtained from Quantum Support.

Using an Image File to Upgrade Tape Drive Firmware

The Web client allows you to upgrade tape drive firmware using a firmware image file. The firmware upgrade can take up to 40 minutes (less if the upgrade is performed using FC I/O blades).

Tape drive firmware is available from Quantum Support. Verify with the release notes or Quantum Technical Support that you are updating the tape drives with the correct version of firmware.

Details on using an image file to upgrade tape drive firmware include:

- The library allows you to upgrade firmware on multiple tape drives at one time. Upgrade firmware on all tape drives of the same interface type at the same time to make sure that all drives are at the same firmware level. Having different levels of drive firmware in the library is not recommended.

- Each tape drive interface type requires unique firmware. The image file must contain the appropriate SCSI, FC, or Serial Attached SCSI (SAS) firmware image for the corresponding SCSI, FC or SAS drive type.

- The tape drive and associated partition are automatically taken offline during the operation and brought back online when the operation completes. You will be asked to confirm that you want to take the tape drive and partition offline.

> **Note:** If the operation does not complete successfully, the partition remains offline until you turn it back online manually or restart the library (see Taking a Partition Online or Offline on page 76).

Instructions for upgrading tape drive firmware can be found in the online help and at: http://www.quantum.com/ServiceandSupport/SoftwareandDocumentationDownloads/SI500/Index.aspx.. You can also find step-by-step instructions in your library's online Help. To access the online Help system, click the **Help** icon at the top right of the Web client or operator panel user interface.

> **Caution:** Since tape drives restart after a firmware upgrade, make sure that cartridges are not loaded in the applicable tape drives before upgrading firmware.

Caution:	Do not turn off power to the library during the upgrade process. Turning off power to the library during the upgrade can cause problems with the library.

Note:	This operation should not be performed concurrently by multiple administrators. You can access the appropriate screens, but you cannot apply changes while another administrator is performing the same operation.

You cannot upgrade tape drive firmware with an image file from the operator panel. The path to the appropriate screen is as follows:

- From the Web client, select **Tools > Drive Operations**.

Downgrading IBM LTO-4 Tape Drive Firmware

IBM LTO-4 drive brick firmware PGA3 (82FB) and newer contain special security restrictions that prevent downgrading this firmware to previous versions that are not FIPS-compliant [for example, PGA1 (77BE)].

If you need to downgrade LTO-4 tape drive firmware from level 82FB or higher to level 77BE or lower, contact Quantum Technical Support for instructions and assistance.

Autoleveling Tape Drive Firmware

The autoleveling feature enables you to automatically upgrade firmware on all FC tape drives that are connected to the FC I/O blades or Ethernet Expansion blades. This allows you to keep all FC tape drives of the same type (for example, LTO-5) at the same firmware level. Tape drive firmware is checked whenever a tape drive is reset, such as when the library is power cycled or restarted, or whenever a tape drive is added or replaced. If the firmware does not match, the tape drive firmware is autoleveled.

FC tape drives must be connected to an FC I/O blade or an Ethernet Expansion blade to participate in autoleveling operations. The library does not support autoleveling FC tape drives connected directly to an FC

host or switch. In addition, the library does not support autoleveling SCSI or SAS tape drives.

To enable autoleveling, you must upload a firmware image file to the library. If you have multiple versions of FC tape drives installed in your library (for example, LTO-4 and LTO-5), you must upload a unique firmware image file for each version. You can also delete a firmware image file when you no longer want to autolevel tape drive firmware.

Uploading Tape Drive Firmware Used in Autoleveling

Before uploading tape drive firmware, verify with published release notes or Quantum Support that you are uploading the correct version of firmware. For contact information, see <u>Getting More Information or Help</u> on page 8.

You must have access to a tape drive firmware image file to enable autoleveling. Tape drive firmware is available from Quantum Support.

It is not necessary to delete an old version of firmware before uploading a new version. The new version of firmware overwrites the old version.

You can find step-by-step instructions in your library's online Help. To access the online Help system, click the **Help** icon at the top right of the Web client or operator panel user interface.

You cannot upload tape drive firmware from the operator panel. The path to the appropriate screen is as follows:

- From the Web client, select **Tools > Drive Operations > Upload/remove tape drive firmware for autoleveling**.

Deleting Tape Drive Firmware Used in Autoleveling

The library allows you to delete a firmware image file if you no longer want to autolevel tape drive firmware. In addition, you might want to delete a firmware image file if your library no longer contains a specific version of tape drives. For example, if you replace all LTO-3 tape drives with LTO-4 tape drives, you no longer need the LTO-3 firmware.

You can find step-by-step instructions in your library's online Help. To access the online Help system, click the **Help** icon at the top right of the Web client or operator panel user interface.

You cannot upload tape drive firmware from the operator panel. The
path to the appropriate screen is as follows:

• From the Web client, select **Tools > Drive Operations > Upload/remove
tape drive firmware for autoleveling**.

Chapter 12
Installing, Removing, and Replacing

This chapter describes how to add, remove, and replace hardware within your library. Adding, removing, or replacing library components may require you to power off the entire library. There are a few components, however, that you can service without powering off the library, such as replacing tape drives. Instead, you may only need to take a specific partition offline, or you may not need to impact the status of the library at all.

Warning:	All libraries taller than 14U must be installed in a rack having a main protective earthing (grounding) terminal, and power must be supplied via an industrial plug and socket-outlet and/or an appliance coupler complying with IEC 60309 (or an equivalent national standard) and having a protective earth (ground) conductor with a cross sectional area of at least 1.5 mm^2 (14 AWG). To ensure proper airflow and access space, allow 60 cm (24 inches) in the front and back of the library.

Warning:	Under no circumstances should a rack be moved while loaded with one or more modules.

> **Warning:** Without tape drives, tape cartridges, or power supplies, a control module weighs approximately 60 lbs (27.2 kg). An expansion module, without tape drives, tape cartridges, or power supplies, exceeds 65 lbs (29.5 kg).
>
> To avoid serious injury, at least two people are required to safely lift the modules.

This chapter covers:

- Taking the Library Online/Offline
- Cabling the Library
    - Specific Instructions for LTO-5 and LTO-6 Tape Drives
    - Cabling Libraries With SCSI Tape Drives
    - Cabling Libraries With SAS Tape Drives
    - Cabling Libraries With Fibre Channel Tape Drives Connected Directly to a Host or Switch
    - Cabling Libraries With Fibre Channel Tape Drives Connected to Fibre Channel I/O Blades
    - Recommended Library Cabling for FC I/O Blades
    - Managing Ethernet Cables
- Cable Management Guidelines
- Installing a Stand-Alone 5U Control Module
- Installing a New Multi-Module Library Configuration
- Adding Expansion Modules to an Existing Library
- Preparing to Remove or Replace a Module
- Permanently Removing Expansion Modules From an Existing Library
- Replacing the Control Module
- Replacing an Expansion Module
- Removing and Replacing the Library Control Blade and LCB Compact Flash Card
- Adding, Removing, and Replacing Power Supplies
- Installing the Library in a Rack

Taking the Library Online/Offline

An online library allows a host application to fully control library operations. Taking a library offline switches library control to the user interfaces and limits host application command requests.

Taking a Library Online

To take an entire library online, take all of its partitions online.

1 Using the library's operator panel, select **Operations > Change Partition Mode**; or, using the Web client, select **Operations > Partitions > Change Mode**.

2 For each partition that you want to take online, click **Online**.

3 Click **Apply**.

Taking a Library Offline

To take an entire library offline, take all of its partitions offline.

1 Using the library's operator panel, select **Operations > Change Partition Mode**; or, using the Web client, select **Operations > Partitions > Change Mode**.

2 For each partition that you want to take offline, click **Offline**.

3 Click **Apply**.

Cabling the Library

Use the following cabling procedure appropriate for your drive type.

Specific Instructions for LTO-5 and LTO-6 Tape Drives

The library handles the Ethernet and Fibre Channel data ports on LTO-5 and LTO-6 tape drives differently depending on the tape drive. See Figure 37, Figure 38, and Figure 39 for details.

> **Caution:** LTO-5 Fibre Channel tape drives can be configured for speeds of up to 8 GB per second and support auto-negotiation to 8 Gb/s, 4 Gb/s, and 2 Gb/s. If they are configured for 8 Gb/s, you should connect them directly to a host or switch and not to an FC I/O blade, because the FC I/O blade only allows speeds up to 4 Gb/s. If you connect an LTO-5 Fibre Channel tape drive to an FC I/O blade, the speed will autonegotiate to 4 Gb/s (see Setting Tape Drive Parameters on page 83). Speeds less than 2 Gb/s are not supported.

> **Caution:** If you enable data path failover, control path failover, or host access control, do not connect the tape drive to an FC I/O blade.

> **Caution:** Do not connect a tape drive to both an FC I/O blade and an Ethernet Expansion blade.

Figure 37 HP LTO-5 Dual Port
Fibre Channel Tape Drive
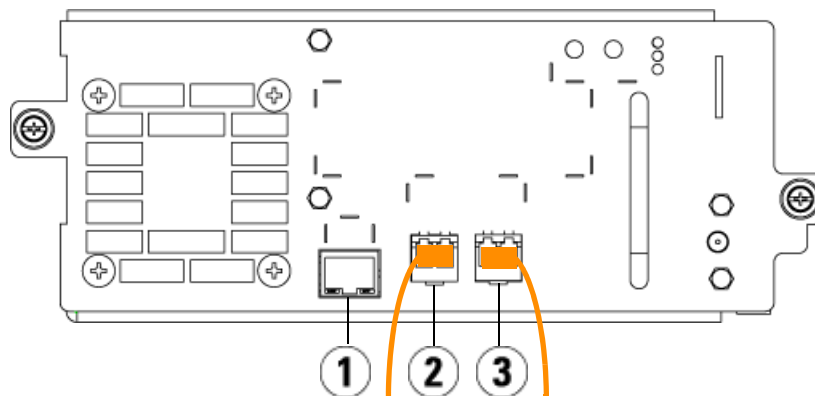
1 Ethernet port — Use for Ethernet
connectivity in conjunction with
FIPS.

2 Fibre Channel port 1 — Default
data port. If you are only using one
port, use this port.

3 Fibre Channel port 2 — Default
failover port (for use with data
path failover).

Figure 38 HP LTO-5 Single
Port SAS Tape Drive
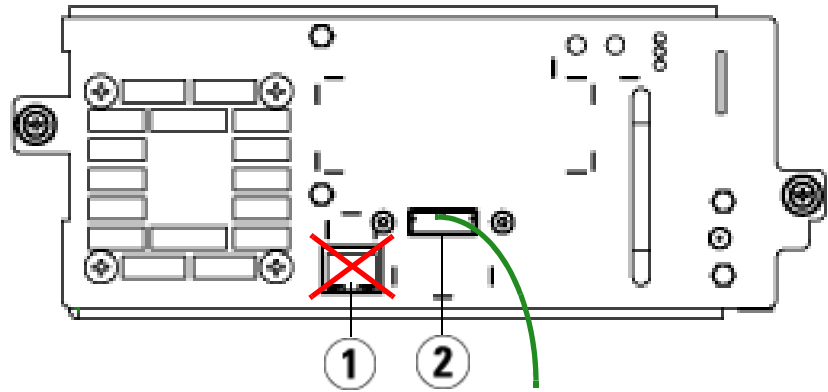
1	Ethernet port - do not use
2	SAS port - use this port

Figure 39 IBM LTO-5 Single
Port Fibre Channel Tape Drive
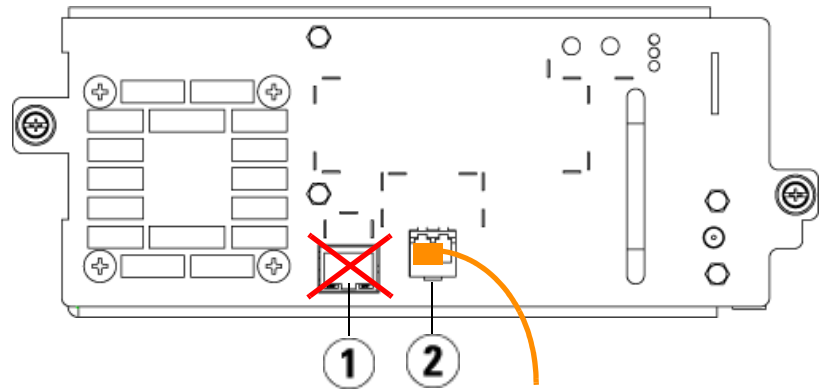
1	Ethernet port - do not use
2	Fibre Channel port - use this port

**Cabling Libraries With
SCSI Tape Drives**

Use this procedure, along with <u>Figure 40</u> and <u>Figure 41</u>, if you are
installing a library that includes SCSI tape drives:

> **Warning:** All libraries taller than 14U must be installed in a rack
> having a main protective earthing (grounding) terminal,
> and power must be supplied via an industrial plug and
> socket-outlet and/or an appliance coupler complying with
> IEC 60309 (or an equivalent national standard) and having
> a protective earth (ground) conductor with a cross
> sectional area of at least 1.5 mm^2 (14 AWG).
>
> To ensure proper airflow and access space, Allow 60 cm
> (24 inches) in the front and back of the library.

Figure 40 Stand-Alone 5U
Control Module SCSI Cabling
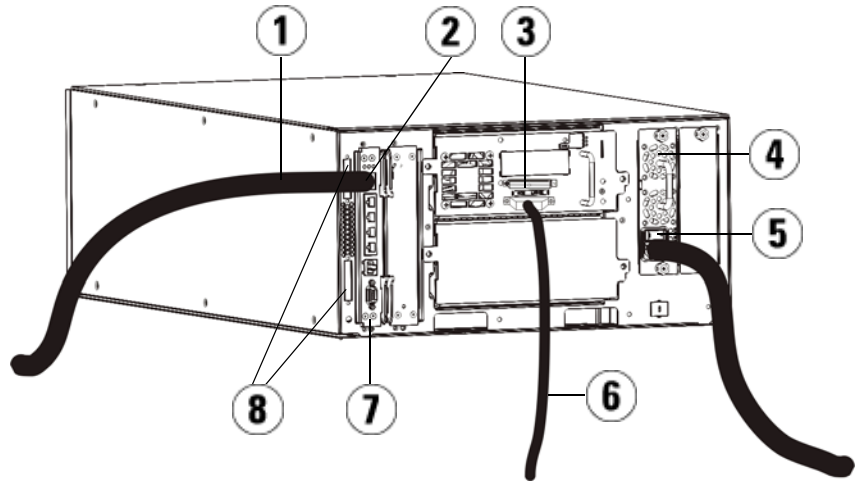
1	Ethernet cable to customer network
2	GB Ethernet port
3	SCSI terminator
4	Power supply
5	Rear power switch
6	SCSI cable to host
7	Library control blade
8	Module terminators

Figure 41 Multi-Module SCSI
Cabling
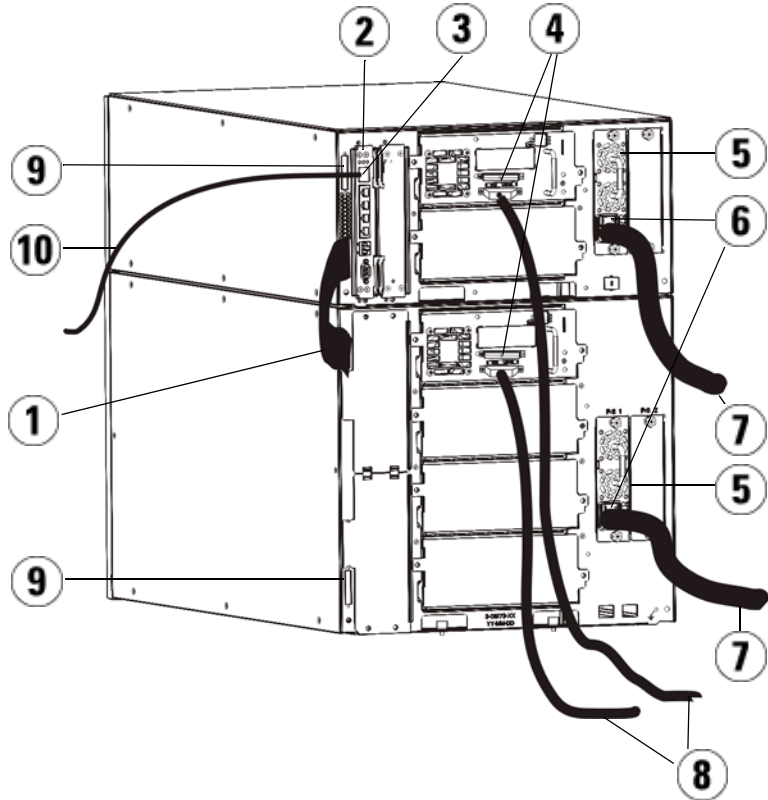
1   Module-to-module cable

2   Library control blade

3   GB Ethernet port

4   SCSI terminator

5   Power supply

6   Rear power switch

7   Power cords

8   SCSI cables to host

9   Module terminators

10 Ethernet cable to customer network

1 If your library is larger than 14U, install it in a rack. See <u>Installing the Library in a Rack</u> on page 417 for instructions. The instructions include procedures for removing and replacing tape drives.

2 Connect the SCSI cables to the tape drives. There are two recommended ways to cable SCSI tape drives: one tape drive per SCSI bus or two tape drives per SCSI bus (see <u>Figure 42</u>).

> **Note:** To avoid possible performance issues, do not connect more than two SCSI drives per SCSI bus.

> **Caution:** The library supports a maximum cable length of 12 meters (including internal wiring) for Ultra 160 SCSI and Ultra 320 SCSI cables.

To connect one tape drive per SCSI bus:

a Use a SCSI cable to connect the bottom port of the tape drive to your host.

b Use a SCSI terminator to terminate the top port of the tape drive.

To connect two tape drives per SCSI bus:

a Connect one end of the SCSI cable to the top SCSI port of the bottom tape drive. Then connect the other end of the cable to the bottom SCSI port of the tape drive above. The SCSI cable connecting the two tape drives should be at least 30 cm in length.

b Use another SCSI cable to connect the bottom tape drive of the SCSI bus to your host.

c Use a SCSI terminator to terminate the top tape drive of the SCSI bus.

Figure 42 Cabling One or Two
Tape Drives Per SCSI Bus

One tape
drive per
SCSI bus

Two tape
drives per
SCSI bus
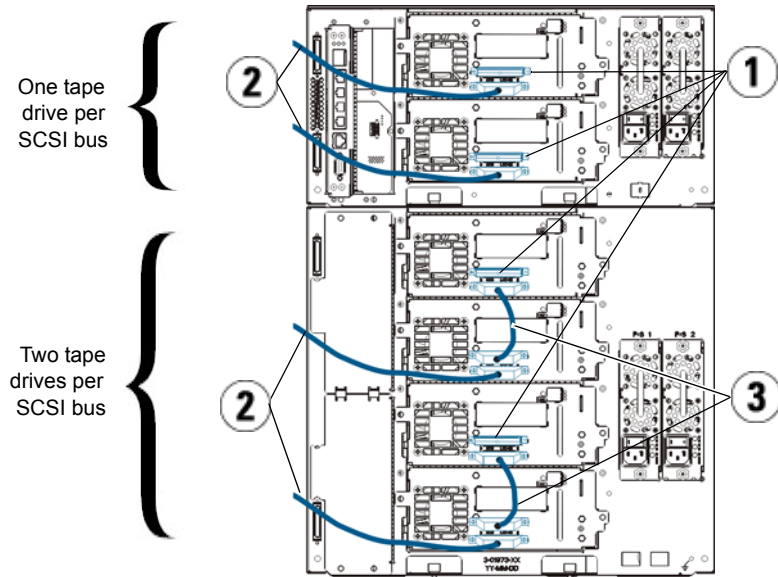
1	SCSI terminator
2	SCSI drive-to-host cable
3	SCSI cable connecting two SCSI tape drives

3 Connect the module terminators.

> **Caution:** The module terminator is not the same as a SCSI terminator. Using a SCSI terminator instead of a module terminator will damage the library.

a Using the module terminators, terminate the top and bottom modules in the library stack. Install one module terminator in the top terminator connector on the topmost module and one in the bottom terminator connector on the bottommost module.

If your library configuration consists of a single module, place module terminators in the module's top and bottom module terminator connector.

b If you need to add expansion modules to the control module, remove the module terminator from the control module terminator connection that is closest to the expansion module.

c Replace the module terminator in the expansion module in the terminator connection that is furthest from the control module.

4 Connect the module-to-module cable from the control module to the expansion module.

5 Connect your Ethernet cable to the Gigabit (GB) Ethernet port on the library control blade (LCB) for remote access to the library via the Web client.

6 Connect a power cord to the outlet on the power supply on the rear of the library.

There should always be a power cord connected to the power supply on the control module. If redundant power supplies are used, connect a power cord to each of the additional power supply outlets.

7 Power on the library.

    a Turn on the rear power switch of each of the power supplies.

    b Turn on the front power button.

    c Power up the host system.

8 Verify communication with all devices on the bus.

9 Configure the library using the commands on the operator panel. See configuration information in <u>Configuring Your Library</u> on page 52.

Cabling Libraries With SAS Tape Drives

Each SAS tape drive should be connected directly to the host bus adapter (HBA) using one SAS cable. The LTO-4 and LTO-5 SAS tape drives in the Scalar i500 library use the SFF-8088 type SAS connector. The connector needed on the host end of the cable depends on the type of Host Bus Adapter (HBA) being used.

> **Caution:**   Quantum sells both SAS-1 and SAS-2 tape drives. SAS-2 technology and the SAS-2 standard allow for increased connection speed and greater cable lengths when compared to SAS-1. Quantum recommends the use of Quantum-qualified cables when using SAS tape drives. Quantum engineers and qualifies cables specifically to be compatible with the tape library SAS connection architecture.

The library does not support daisy-chaining SAS cables. The library does not support the use of SAS expander devices or cables at this time.

Use this procedure, along with Figure 43 and Figure 44, to connect SAS cables directly to the host.

> **Warning:**   All libraries taller than 14U must be installed in a rack having a main protective earthing (grounding) terminal, and power must be supplied via an industrial plug and socket-outlet and/or an appliance coupler complying with IEC 60309 (or an equivalent national standard) and having a protective earth (ground) conductor with a cross sectional area of at least 1.5 mm^2 (14 AWG).
>
> To ensure proper airflow and access space, Allow 60 cm (24 inches) in the front and back of the library.

Figure 43 Stand-Alone Control
Module SAS Cabling
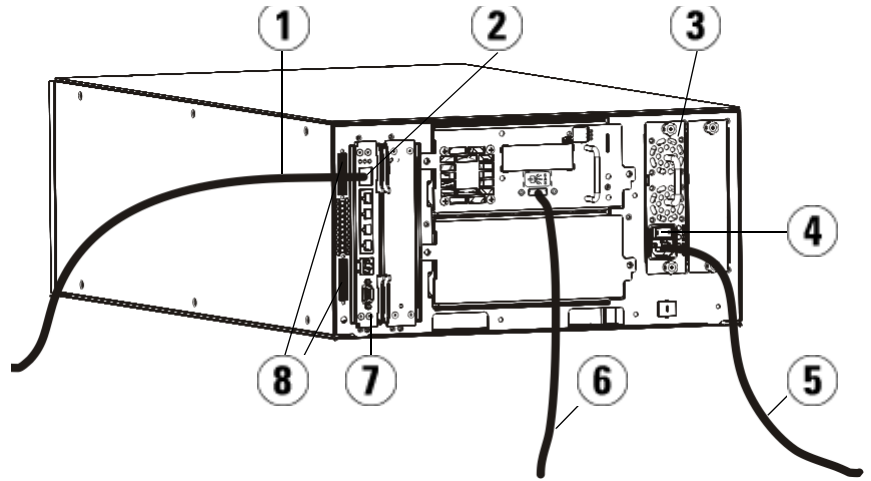
1	Ethernet cable to network
2	GB Ethernet port
3	Power supply
4	Rear power switch
5	Power cord
6	SAS cable to host
7	Library control blade
8	Module terminators

Figure 44 Multi-Module SAS
Cabling
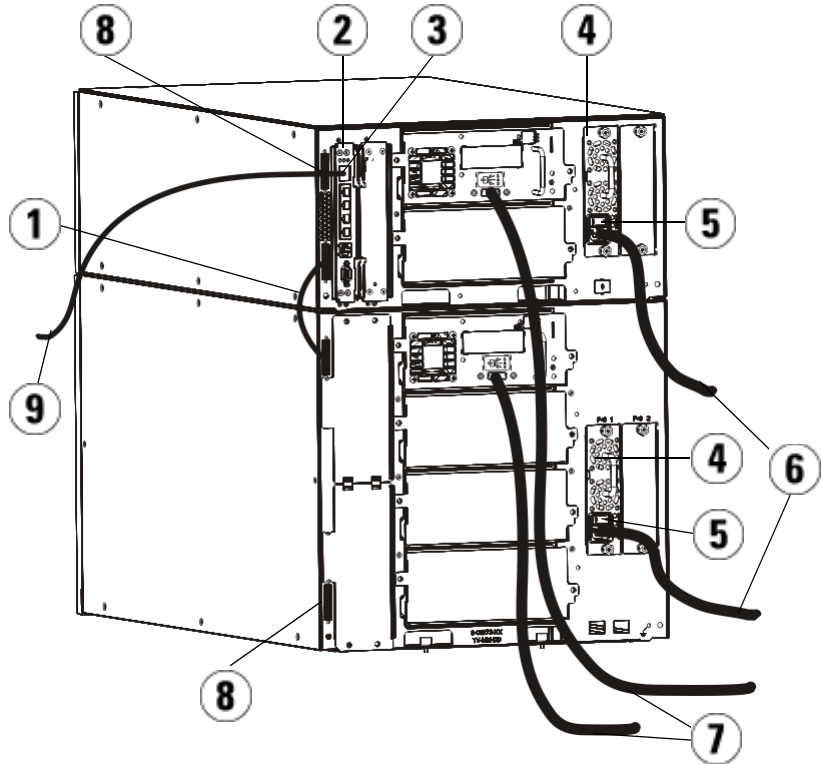
1   Module-to-module cable

2   Library control blade

3   GB Ethernet port

4   Power supply

5   Rear power switch

6   Power cords

7   SAS cables to host

8   Module terminators

9   Ethernet cable to network

1 If your library is larger than 14U, install it in a rack. See <u>Installing the</u> <u>Library in a Rack</u> on page 417 for instructions. The instructions include procedures for removing and replacing tape drives.

2 Connect one end of the SAS cable to the tape drive. Connect the other end of the SAS cable to the host.

3 If your library configuration consists of a single module, place module terminators in the module's top and bottom module terminator connectors.

Caution:	The module terminator is not the same as a SCSI terminator. Using a SCSI terminator instead of a module terminator will damage the library.

4 If the library consists of more than one module, connect the modules together as follows:

Caution:	The module terminator is not the same as a SCSI terminator. Using a SCSI terminator instead of a module terminator will damage the library.

   a Using the module terminators, terminate the top and bottom modules in the library stack. Install one module terminator in the top terminator connector on the topmost module and one in the bottom terminator connector on the bottommost module.

   b If you need to add expansion modules to the control module, remove the module terminator from the control module terminator connection that is closest to the expansion module.

   c Replace the module terminator in the expansion module in the terminator connection that is furthest from the control module.

   d Connect the module-to-module cable from the control module to the expansion module.

5 Connect your Ethernet cable to the Gigabit (GB) Ethernet port on the library control blade (LCB) for remote access to the library via the Web client.

6 Connect a power cord to the outlet on the power supply on the rear of the library.

There should always be a power cord connected to the power supply on the control module. If redundant power supplies are used, connect a power cord to each of the additional power supply outlets.

7 Plug the power cord into a nearby AC power source.

8 Power on the library.

   a Turn on the rear power switch of each of the power supplies.

   b Turn on the front power button.

   c Power up the host system.

9 Verify communication with all devices on the bus.

10 Configure the library using the commands on the operator panel. See configuration information in <u>Configuring Your Library</u> on page 52.

Cabling Libraries With Fibre Channel Tape Drives Connected Directly to a Host or Switch

Use this procedure, along with <u>Figure 45</u> and <u>Figure 46</u>, if you are installing a library that includes FC tape drives that are connected directly to a host or switch.

Figure 45 Stand-Alone Control
Module Fibre Channel Cabling
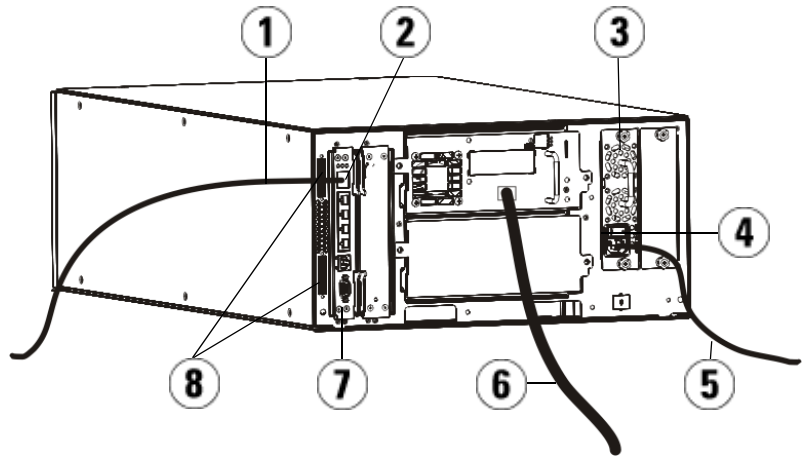
1	Ethernet cable to customer network
2	GB Ethernet port
3	Power supply
4	Rear power switch
5	Power cord
6	Fibre cable to host
7	Library control blade (LCB)
8	Module terminators

Figure 46 Multi-Module Fibre
Channel Cabling
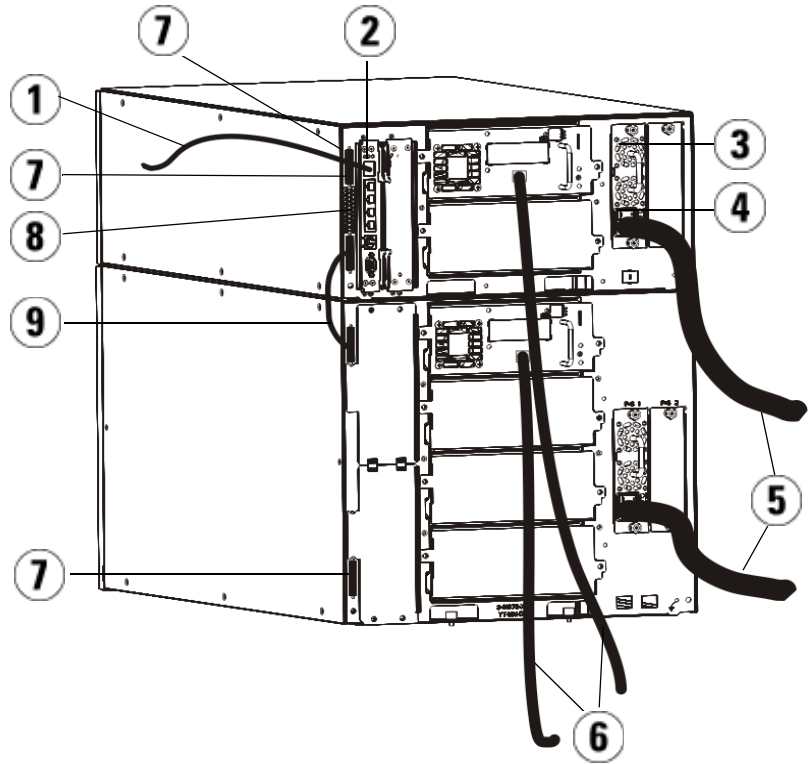
1	Ethernet cable to network
2	GB Ethernet port
3	Power supply
4	Rear power switch
5	Power cords
6	Fibre cables to host
7	Module terminators
8	Library control blade (LCB)
9	Module-to-module cable

> **Warning:** All libraries taller than 14U must be installed in a rack
> having a main protective earthing (grounding) terminal,
> and power must be supplied via an industrial plug and
> socket-outlet and/or an appliance coupler complying with
> IEC 60309 (or an equivalent national standard) and having
> a protective earth (ground) conductor with a cross
> sectional area of at least 1.5 mm^2 (14 AWG).
>
> To ensure proper airflow and access space, Allow 60 cm
> (24 inches) in the front and back of the library.

> **Note:** Pay attention to where the operator panel is positioned in the
> rack for optimum usability.

1 If your library is larger than 14U, install it in a rack.

See <u>Installing the Library in a Rack</u> on page 417 for instructions. The
instructions include procedures for removing and replacing tape
drives.

2 Connect the fibre cables to the tape drives.

    a Attach one end of the fibre cable to the fibre port on each tape
       drive.

    b Attach the other end of the cable to the host or switch.

> **Note:** The fibre cable can be connected from the tape drive to a
> switch rather than a host.

3 Connect the module terminators.

> **Caution:** The module terminator is not the same as a SCSI
> terminator. Using a SCSI terminator instead of a
> module terminator will damage the library.

    a Using the module terminators, terminate the top and bottom modules in the library stack. Install one module terminator in the top terminator connector on the topmost module and one in the bottom terminator connector on the bottommost module.

       If your library configuration consists of a single module, place module terminators in the module's top and bottom module terminator connectors.

    b If you need to add expansion modules to the control module, remove the module terminator from the control module terminator connection that is closest to the expansion module.

    c Replace the module terminator in the expansion module terminator connection furthest from the control module.

4 Connect the module-to-module cable from the control module to the expansion module.

5 Connect your Ethernet cable to the Gigabit (GB) Ethernet port on the Library Control Blade (LCB) for remote access to the library via the Web client.

**6** Connect a power cord to the outlet on the power supply on the rear of the library.

   There should always be a power cord connected to the power supply on the control module. If redundant power supplies are used, connect a power cord to each of the additional power supply outlets.

7 Power on the library.

    a Turn on the rear power switch of each of the power supplies.

    b Turn on the front power switch.

    c Power up the host system.

8 Verify communication with all devices on the bus.

Configure the library using the commands on the operator panel. See configuration information in <u>Configuring Your Library</u> on page 52.

Cabling Libraries With Fibre Channel Tape Drives Connected to Fibre Channel I/O Blades

These instructions explain how to install the FC cables that connect the FC drives to the FC I/O blades. The FC I/O blades support connections to LTO-2, LTO-3, LTO-4, LTO-5 and LTO-6 drives.

> **Caution:** LTO-5 Fibre Channel tape drives can be configured for speeds of up to 8 GB per second and support auto-negotiation to 8 Gb/s, 4 Gb/s, and 2 Gb/s. If they are configured for 8 Gb/s, you should connect them directly to a host or switch and not to an FC I/O blade, because the FC I/O blade only allows speeds up to 4 Gb/s. If you connect an LTO-5 Fibre Channel tape drive to an FC I/O blade, the speed will autonegotiate to 4 Gb/s (see Setting Tape Drive Parameters on page 83). Speeds less than 2 Gb/s are not supported.

For information on installing FC I/O blades, see Adding, Removing, and Replacing FC I/O Blades on page 443.

Cabling may be affected by partitioning or zoning changes made as part of configuration. When cabling to drives, ensure that they are cabled to the correct hosts for the defined partitions. If the FC I/O blades have active channel zoning, ensure that the drives are attached to ports that are accessible to the defined zone. For information on partitioning, configuring FC I/O blade ports, channel zoning, and host mapping, see Chapter 3, Configuring Your Library.

Details about cabling FC I/O blades include:

- Each expansion module can support up to two FC I/O blades. A maximum of four FC I/O blades can be present in any library configuration. A maximum of four FC drives can be connected to one FC I/O blade.

- Ports 1 and 2 on each FC I/O blade are reserved for connection to hosts. Ports 1 and 2 are always in target mode. The other four ports (3, 4, 5 and 6) are always in initiator mode. See Figure 47.

- Ideally, an installed tape drive should be cabled to a port on the nearest FC I/O blade to eliminate the need to manage excessively long cables. The nearest FC I/O blade is usually located in the same expansion module as the tape drive.

> **Note:** See Cable Management Guidelines on page 316 for best-
> practice guidelines for cabling a library.

Figure 47 FC I/O Blade
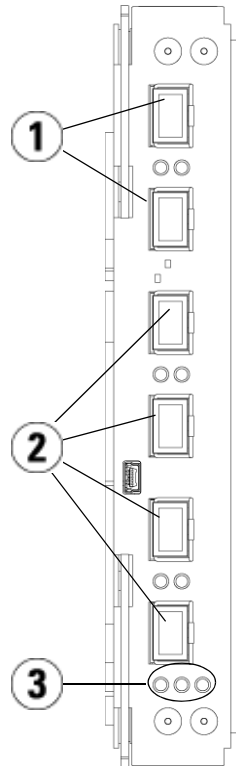
1   Target ports 1 and 2 to host(s)

2   Initiator ports 3 – 6 to drives

3   LEDs (blue, amber, green)

Use the following procedure, along with Figure 48, if you are installing a
library that includes FC tape drives that are connected to FC I/O blades.

Figure 48 FC With I/O Blade
Cabling
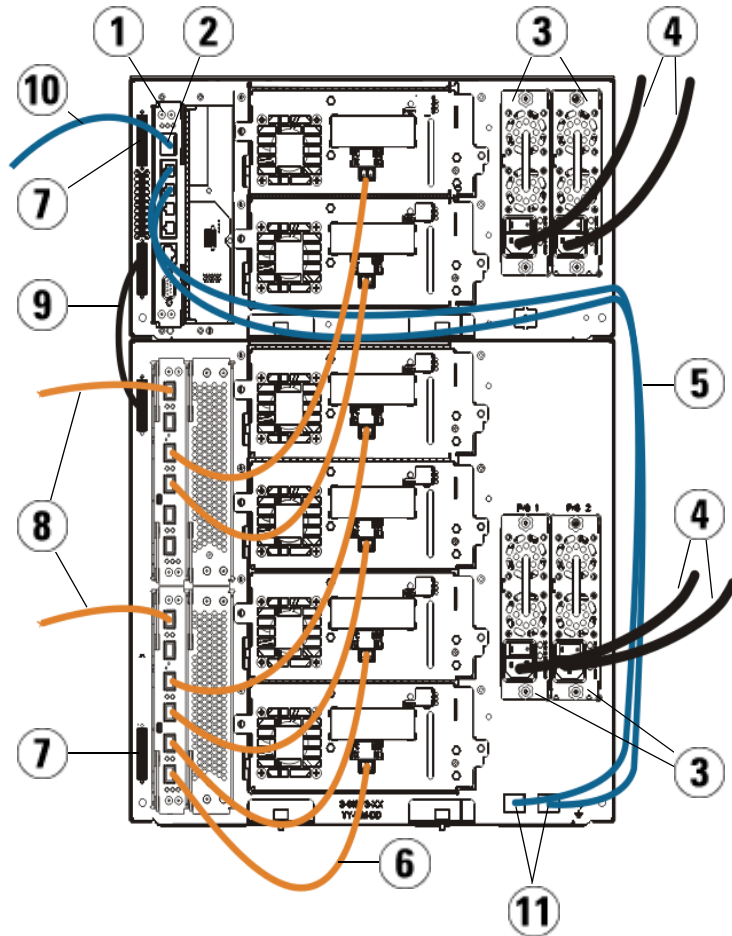
	1	Library control blade (LCB)	7	Module terminator
	2	GB Ethernet port	8	FC cable to host
	3	Power supplies	9	Module-to-module cable
	4	Power cords	10	Ethernet cable to network
	5	Ethernet cables from LCB to expansion module (one per FC I/O blade)	11	UPPER and LOWER Ethernet ports
	6	FC cable from FC I/O blade to tape drive		

Required tools: None

1 If your library is larger than 14U, install it in a rack. See <u>Installing the Library in a Rack</u> on page 417 for instructions. The instructions include procedures for removing and replacing tape drives.

Warning: All libraries taller than 14U must be installed in a rack having a main protective earthing (grounding) terminal, and power must be supplied via an industrial plug and socket-outlet and/or an appliance coupler complying with IEC 60309 (or an equivalent national standard) and having a protective earth (ground) conductor with a cross sectional area of at least 1.5 mm^2 (14 AWG).

To ensure proper airflow and access space, Allow 60 cm (24 inches) in the front and back of the library.

Note: Pay attention to where the operator panel is positioned in the rack for optimum usability.

---

2 For each FC I/O blade installed in an expansion module, connect the expansion module containing the FC I/O blade(s) to a port in the Ethernet hub on the LCB:

Note: Without these Ethernet cables connected, the FC I/O blades will not work.

---

a If the FC I/O blade is installed in the bottom bay of the expansion module, connect one end of an Ethernet cable to the Ethernet port labeled **LOWER** in the lower right corner of the expansion module. Connect the other end of the cable to a port in the Ethernet hub on the LCB.

b If the FC I/O blade is installed in the upper bay of the expansion module, connect one end of an Ethernet cable to the Ethernet port labeled **UPPER** in the lower right corner of the expansion module. Connect the other end of the cable to a port in the Ethernet hub on the LCB.

c Follow the instructions in <u>Cable Management Guidelines</u> on page 316 for best practices in routing the Ethernet cables.

3 Remove and discard the necessary number of the black rubber protective covers from the ports on the FC I/O blades.

4 Carefully unwrap the FC cables and remove the two white plastic protective caps from each end of the cable.

Caution: FC cables will be damaged if they are bent at more than a four-inch arc.

---

5 Connect the FC cable to one of the following initiator ports on the FC I/O blade: 3, 4, 5, or 6. When you choose the port, take into account the location of any other tape drives that you plan to connect to the same FC I/O blade. See Cable Management Guidelines on page 316 for best-practice guidelines for cabling a library.

6 Insert the other end of the FC cable into the FC port on the FC tape drive.

7 Repeat the above steps for each FC drive you want to connect to the FC I/O blade. Do not connect any of these FC cables to ports 1 or 2 on the FC I/O blade.

8 Connect the host(s) to ports 1 and/or 2 on the FC I/O blade.

9 Install the module terminators.

Caution: The module terminator is not the same as a SCSI terminator. Using a SCSI terminator instead of a module terminator will damage the library.

---

   a Using the module terminators, terminate the top and bottom modules in the library stack. Install one module terminator in the top terminator connector on the topmost module and one in the bottom terminator connector on the bottommost module.

     If your library configuration consists of a single module, place module terminators in the module's top and bottom module terminator connectors.

   b If you need to add expansion modules to the control module, remove the module terminator from the control module terminator connection that is closest to the expansion module.

   c Replace the module terminator in the expansion module terminator connection furthest from the control module.

10 Connect the module-to-module cable from the control module to the expansion module.

11 Connect an Ethernet cable to the Gigabit (GB) Ethernet port on the Library Control Blade (LCB) for remote access to the library via the Web client.

12 Connect a power cord to the outlet on the power supply on the rear of the library.

There should always be a power cord connected to the power supply on the control module. If redundant power supplies are used, connect a power cord to each of the additional power supply outlets.

13 Power on the library.

   a Turn on the rear power switch of each of the power supplies.

   b Turn on the front power button.

   c Power up the host system.

14 Verify communication with all devices on the bus.

15 Configure the library using the commands on the operator panel. See configuration information in

Recommended Library Cabling for FC I/O Blades

Fibre optic cables connect Fibre Channel tape drives to FC I/O blades and FC I/O blades to a Storage Area Network (SAN) fabric or host. Correctly managing these cables on the rear of the library can prevent damage to the cables and Fibre Channel ports and ensure optimal data throughput.
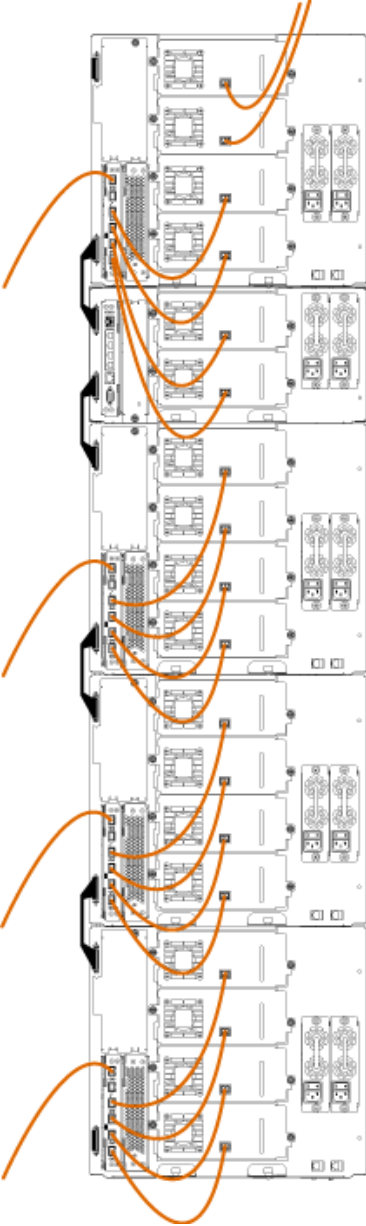
Note:	This section applies to libraries containing Fibre Channel tape drives, which are connected to a host or a Fibre Channel switch using an FC I/O blade. For tape drives that are directly attached to a host or a SAN switch, follow standard fibre optic cable handling best practices.

Ideally, an installed tape drive should be cabled to a port on the nearest FC I/O blade to eliminate the need to manage excessively long cables. The nearest FC I/O blade is usually located in the same expansion module as the tape drive.

You will need to provide fibre cables long enough to connect a host or a SAN switch to a target port on an FC I/O blade.

It is important to consider how drives are assigned to partitions when cabling tape drives and hosts to an FC I/O blade. If you want a host to be able to communicate with a tape drive that is assigned to a particular partition, both the drive and the host that has access to the partition should communicate through the same FC I/O blade.

The following table provides an example of a 41U library with FC I/O blade-attached tape drives. The information next to the image shows each tape drive and the FC I/O blade and port to which each tape drive is connected.

Recommended Cabling With FC I/O Blades In Maximum Capacity Library	Tape Drive	FC I/O Blade	FC I/O Blade Port
	[1,1]	N/A (direct attached)	
	[1,2]	N/A (direct attached)	
	[1,3]	[1,2]	Port 3
	[1,4]	[1,2]	Port 4
	[0,1]	[1,2]	Port 5
	[0,2]	[1,2]	Port 6
	[-1,1]	[-1,2]	Port 3
	[-1,2]	[-1,2]	Port 4
	[-1,3]	[-1,2]	Port 5
	[-1,4]	[-1,2]	Port 6
	[-2,-1]	[-2,-2]	Port 3
	[-2,-2]	[-2,-2]	Port 4
	[-2,-3]	[-2,-2]	Port 5
	[-2,-4]	[-2,-2]	Port 6
	[-3,1]	[-3,2]	Port 3
	[-3,2]	[-3,2]	Port 4
	[-3,3]	[-3,2]	Port 5
	[-3,4]	[-3,2]	Port 6
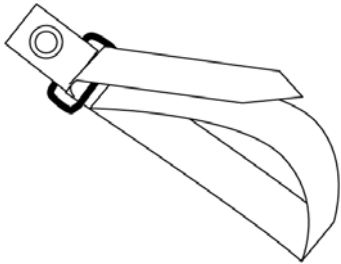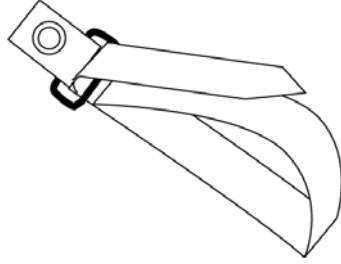
Cable Management Guidelines
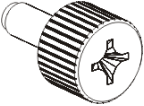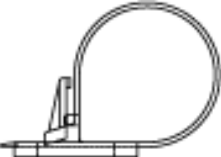
As the library expands to support larger configurations, it is important to restrain and organize cables and power cords on the rear of the library. Doing so ensures that the rear of the library remains accessible and reduces the possibility that cables become damaged.

Use this section to find cable management guidelines and best practices for power cords and Ethernet cables. Use the equipment specified in the Cable Management Kit section below.

Cable Management Kit

If you purchase a Fibre Channel I/O blade or an Ethernet Expansion blade, you will receive a cable management kit with all the equipment necessary to perform these procedures. You can also order the cable management kit from http://shop.quantum.com. The color of the straps matches the color of the cords they are designed to secure.

Component	Description	Quantity
	Black hook-and-loop fastener — Secures power cords to expansion modules.	1
	Blue hook-and-loop fastener —Secures Ethernet cables to expansion modules.	1

Component	Description	Quantity
	Push-in clip — to secure hook-and-loop fasteners to expansion modules.	2
	M5 thumbscrew — For older library models without drilled holes for push-in clips. The M5 thumbscrew attaches hook-and-loop fasteners to the M5 threaded hole on the lower right of any module chassis.	2
	Push-in wire saddle cable clamp — Secures Ethernet cables to the control module.	2
	Adhesive-backed wire saddle cable clamp — For older library models without drilled holes for push-in wire saddle clamps. The adhesive-backed wire saddle clamp secures Ethernet cables to the control module.	2

Managing Power Cords

Power cord management is important especially for the larger, expanded library configurations. A 41U library with redundant power (the maximum configuration) may contain as many as 10 power supply units with 10 power cords to manage.

To organize power cords on the rear of the library, mount a black hook-and-loop fastener to each module and then secure the power cords with the fastener.

Power cords and power cord hook-and-loop fasteners that are shipped with the library are black in color.

You can apply the following procedure to any library that contains at least one expansion module.

To secure a power cord to the library frame:

1 Facing the rear of the library, locate a specific hole that is drilled into the back of the expansion module for the hook-and-loop fastener. This hole is located on the rear of the library, about three inches from the top of the expansion module near the right side of the library chassis. Refer to the illustration below to locate this hole.

> **Note:** If your module chassis does not have the drilled hole, use an M5 thumbscrew to attach the black hook-and-loop fastener to the nearest available M5 threaded hole on the lower right of any module chassis.

2 Insert a push rivet into the rivet hole on the black hook-and-loop fastener. The head of the rivet should be on the same side of the fastener as the plastic loop.

3 Firmly press the push rivet through the hole in the expansion module described above. The hook-and-loop fastener should now be secured to the library chassis.

4 Plug the power cord into a power supply unit closest to the hook-and-loop fastener.

5 Determine how much cord length you need to reach and easily plug into the AC power source. Do not plug the cord into power source until you are ready to power on the library.

6 If there is excess power cord, loop the excess cord into a bundle in the shape of a figure-eight. The bundle should be small enough to hold comfortably with one hand, or about eight inches in length.

7 Wrap the bundle with the hook-and-loop fastener. Thread the strap through the plastic loop and tighten the strap around the bundled cord. Secure the strap by pressing it down.

The power cord is now secured to the expansion module. Repeat these steps to secure other power cords, if necessary. Bundle adjacent power cords together using the same hook-and-loop fastener.

Once complete, power cord management for a 41U library should look similar to

Figure 49 Power Cord
Management
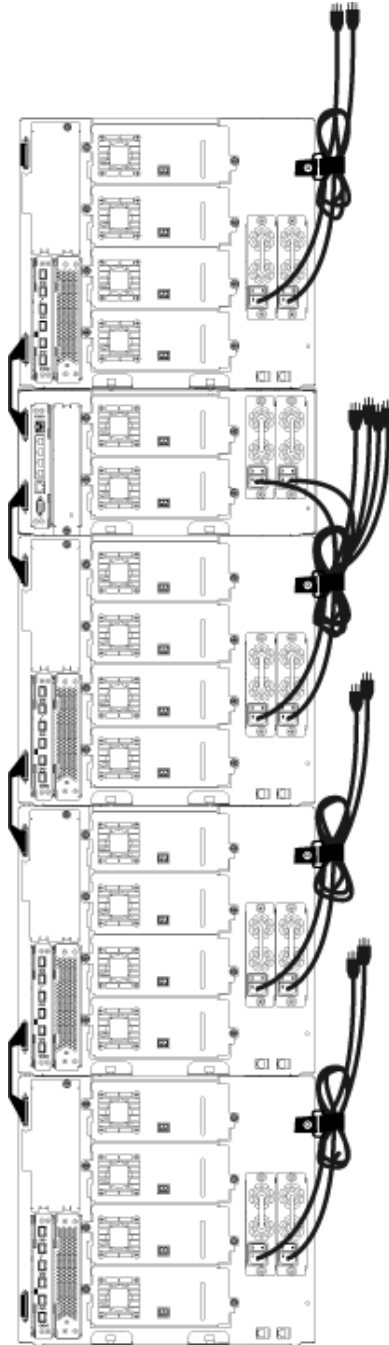
Managing Ethernet Cables

A Scalar i500 library with FC I/O blades or Ethernet Expansion blades uses external Ethernet cables on the rear of the library to provide connectivity between the LCB in the control module and an expansion module. The upper and lower FC I/O blade/Ethernet Expansion blade bays within an expansion module each have a corresponding Ethernet port on the back of the module. Running an Ethernet cable between this port and one of the Ethernet hub ports on the LCB establishes Ethernet connectivity between the blade and the LCB.

The LCB provides ports for up to four Ethernet cables on its internal Ethernet hub. This allows the library to support a total of four FC I/O blades and/or Ethernet Expansion blades.

To organize Ethernet cables on the rear of the library, mount two wire saddles on the control module to route the Ethernet cable(s) to the right side of the library. Mount a blue hook-and-loop fastener to each module and then secure the Ethernet cables with the fastener.

Ethernet cables and Ethernet hook-and-loop straps that are shipped with the library are blue in color.

Apply the following procedure to any library that contains at least one expansion module and at least one FC I/O blade or Ethernet Expansion blade.

To secure an Ethernet cable to the library frame using a cable tie:

1 Facing the rear of the library, install the two push-in wire saddle cable clamps onto the control module chassis. Push the rivet of one clip into the hole drilled into the cover plate located to the right of the LCB. Push the rivet of the other clip into the hole located near the extreme right side of the library, below the control module's power supplies. See <u>Figure 50</u> on page 322 for the locations of these holes.

> | **Note:** | If your control module chassis does not have the drilled holes, use the adhesive -backed wire saddle cable clamps in the location shown in <u>Figure 50</u>. |
> |---|---|

2 Locate a specific hole that is drilled into the back of the expansion module for the hook-and-loop strap. This hole is located on the rear of the library, about three inches from the bottom of the expansion module on the right side of the frame back plane. See <u>Figure 50</u> on page 322 for the location of this hole.

> **Note:** If your module chassis does not have the drilled hole, use an M5 thumbscrew to attach the black hook-and-loop fastener to the nearest available M5 threaded hole on the lower right of any module chassis.

3 Insert a push rivet into the rivet hole on the blue hook-and-loop fastener. The head of the rivet should be on the same side of the fastener as the plastic loop.

4 Firmly press the push rivet through the hole in the expansion module described above. The hook-and-loop fastener should now be secured to the library chassis.

5 Plug the one end of the Ethernet cable into one of the four Ethernet hub ports on the LCB.

6 Plug the other end of the Ethernet cable into the appropriate port on the expansion module.

If the FC I/O blade is installed in the module's upper I/O blade bay, plug the cable into the Ethernet port labeled **UPPER**. If the FC I/O blade or Ethernet Expansion blade is installed in the module's lower I/O blade bay, plug the cable into the Ethernet port labeled **LOWER**.

7 Open the wire saddle nearest the LCB, place the Ethernet cable inside, and snap the wire saddle shut.

8 Repeat for the other wire saddle.

9 If there is excess Ethernet cable, loop the excess cable into a bundle in the shape of a figure-eight. The bundle should be small enough to hold comfortably with one hand, or about six inches in length.

10 Wrap the bundle with the hook-and-loop fastener. Thread the strap through the plastic loop and tighten the strap around the bundled cable. Secure the strap by pressing it down.

The Ethernet cable is now secured to the expansion module. Repeat these steps to secure other Ethernet cables, if necessary.

Once complete, the Ethernet cabling for a 41U library containing four FC I/O blades should appear similar to .

Figure 50 Ethernet Cable
Management
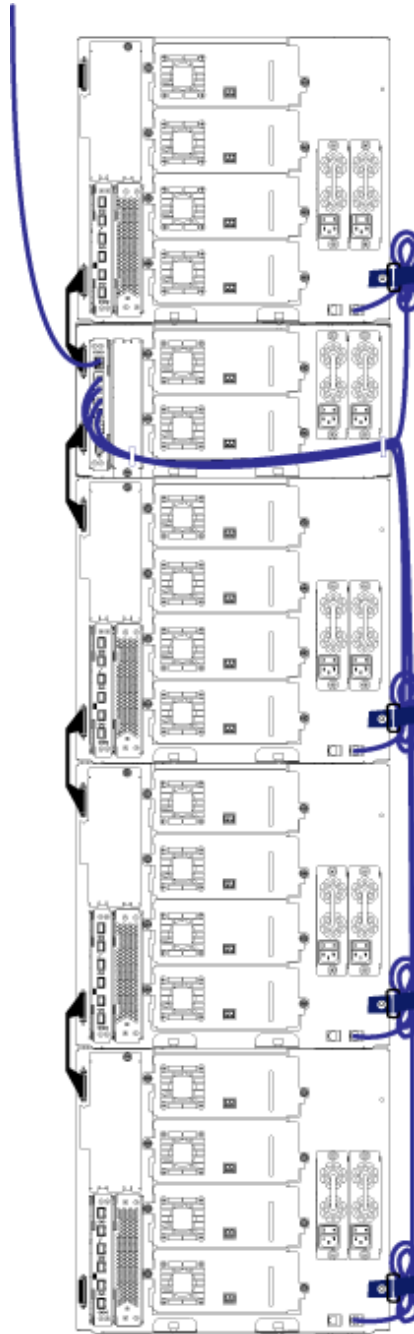
Figure 51 shows how a 41U library with FC I/O blades installed would appear with power, Ethernet, and fibre cables installed and managed according to these guidelines.

Figure 51 Cable Management, All Cables, FC I/O Blades Installed
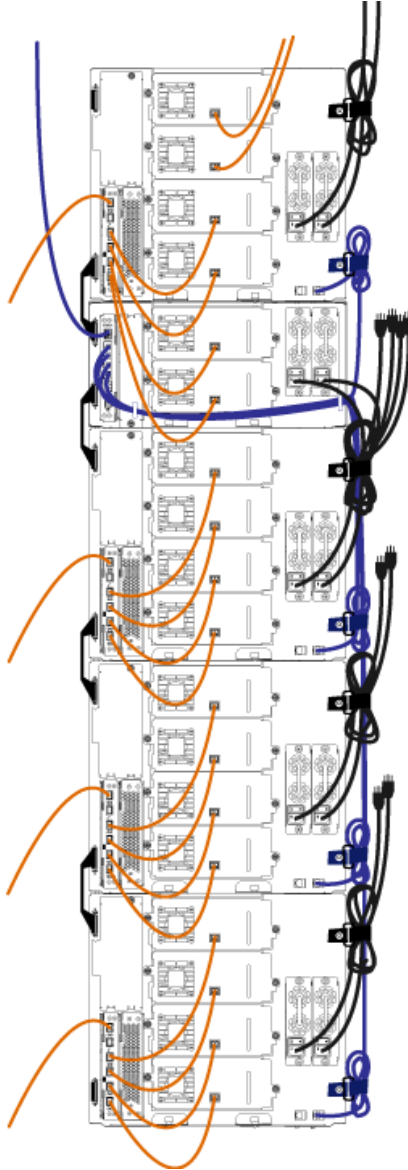
Figure 52 shows how a 41U library with Ethernet Expansion blades installed would appear with power, Ethernet, and fibre cables installed and managed according to these guidelines.

Figure 52 Cable Management, All Cables, Ethernet Expansion Blades Installed
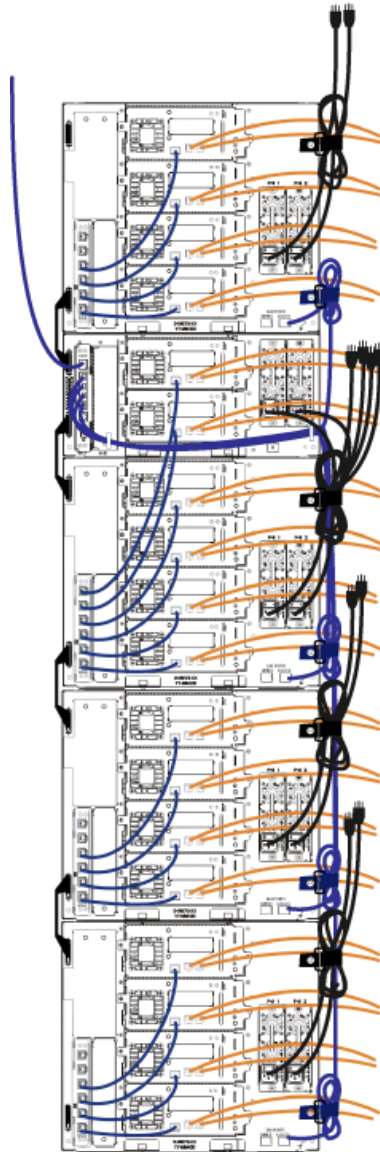
Installing a Stand-Alone 5U Control Module

Required tools: None

Use this procedure to install a 5U library configuration:

1 Prepare the rack to hold modules, if you want to install your library in a rack. See <u>Installing the Library in a Rack</u> on page 417 for instructions on installing a rack-mount kit.

2 Make sure all tape drives have been removed from the control module. See <u>Adding, Removing, and Replacing Tape Drives</u> on page 438 for instructions on removing tape drives.

3 Make sure all power supplies have been removed from the control module. See <u>Adding, Removing, and Replacing Power Supplies</u> on page 414 for instructions on removing power supplies.

4 Open the library's I/E station door and access door. Lift the control module and place it in the desired location.

5 If you are placing the control module in a rack, use the rack ears to fasten the control module to the rack. For instructions, see <u>Installing the Bottom Module in the Rack</u> on page 427.

6 If not already installed, install the library control blade (LCB) in the control module. See <u>Removing and Replacing the Library Control Blade and LCB Compact Flash Card</u> on page 402 for instructions on installing the LCB.

7 Add the tape drives to the module.

8 Install the power supplies. See <u>Adding, Removing, and Replacing Power Supplies</u> on page 414 for instructions on installing power supplies.

9 Close the library's I/E station door and access door.

10 Connect all power cords and network data cables. See <u>Cabling the Library</u> on page 289.

11 Install module terminators in the top and bottom module terminator connectors. See <u>Cabling the Library</u> on page 289 for information on installing the module terminators.

12 Power on the library.

13 Configure the library using the operator panel Setup Wizard.

14 Add the tape cartridges to the library using the I/E station.

15 If your host application inventories the location of each tape cartridge in the library, open the host application and re-inventory to sync the logical inventory with the physical inventory of the library.

Installing a New Multi-Module Library Configuration

Use this procedure for installing a new multi-module library. A multi-module library contains a control module and up to four expansion modules.

There are no restrictions on where the control module can be installed in the library configuration. However, the recommended placement of the control module for library configurations up to 32U is on top of all installed 9U expansion modules. The recommended placement of the control module for 41U library configurations is on top of three 9U expansion modules and below the top expansion module.
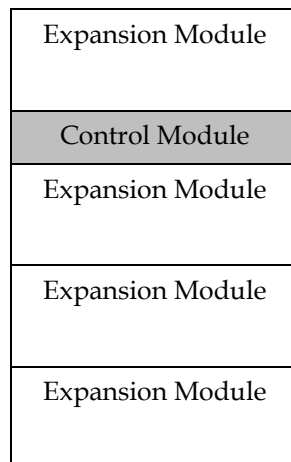
| Expansion Module |
| Control Module |
| Expansion Module |
| Expansion Module |
| Expansion Module |

> **Warning:** All libraries taller than 14U must be installed in a rack having a main protective earthing (grounding) terminal, and power must be supplied via an industrial plug and socket-outlet and/or an appliance coupler complying with IEC 60309 (or an equivalent national standard) and having a protective earth (ground) conductor with a cross sectional area of at least 1.5 mm^2 (14 AWG).
>
> To ensure proper airflow and access space, Allow 60 cm (24 inches) in the front and back of the library.

Preparing to Install a Multi-Module Library

Required tools:

- Phillips #2 screwdriver, for removing and replacing the top cover plate
- T10 TORX screwdriver, for removing and replacing the bottom cover plate

1 Prepare the rack to hold modules, if you want to install your library in a rack. See Installing the Library in a Rack on page 417 for instructions on installing a rackmount kit.

2 Make sure all tape drives have been removed from all of the modules you plan to install. See Adding, Removing, and Replacing Tape Drives on page 438 for instructions on removing tape drives.

3 Make sure all power supplies have been removed from all of the modules you plan to install. See Adding, Removing, and Replacing Power Supplies on page 414 for instructions on removing power supplies.

4 Park the robot assembly in the control module. Before unstacking the library, the robot assembly must be placed in the control module.

   a Open the I/E station and access doors of each module.

   b Using your hands, gently lift the robot assembly into the control module. The robot assembly should glide slowly and with some resistance.

> **Caution:** Support the robot assembly by holding onto the broad metal X-axis plate. Lifting the robot by the thin metal rod will bend the rod. Lifting the robot by the black plastic picker body can damage the robot.

c After raising the robot assembly to the approximate middle of the control module, hold it in place with one hand and, using your other hand, move the parking tab in a counter-clockwise direction until it stops in the "parked" position. The metal parking tab is located at the bottom of column 1.

d Gently lower the robot assembly to rest on the parking tab.

| 1 | Parking tab in "parked" position |

5 Remove and replace the cover plates, if appropriate. When removing the cover plate, ensure that you do not remove the y-home flag screw as shown in Figure 53 on page 330.

> **Caution:** Before removing the control module's bottom cover plate, the robot assembly must be parked as described in Step 4 above.

Figure 53 Cover plate with y-
home flag
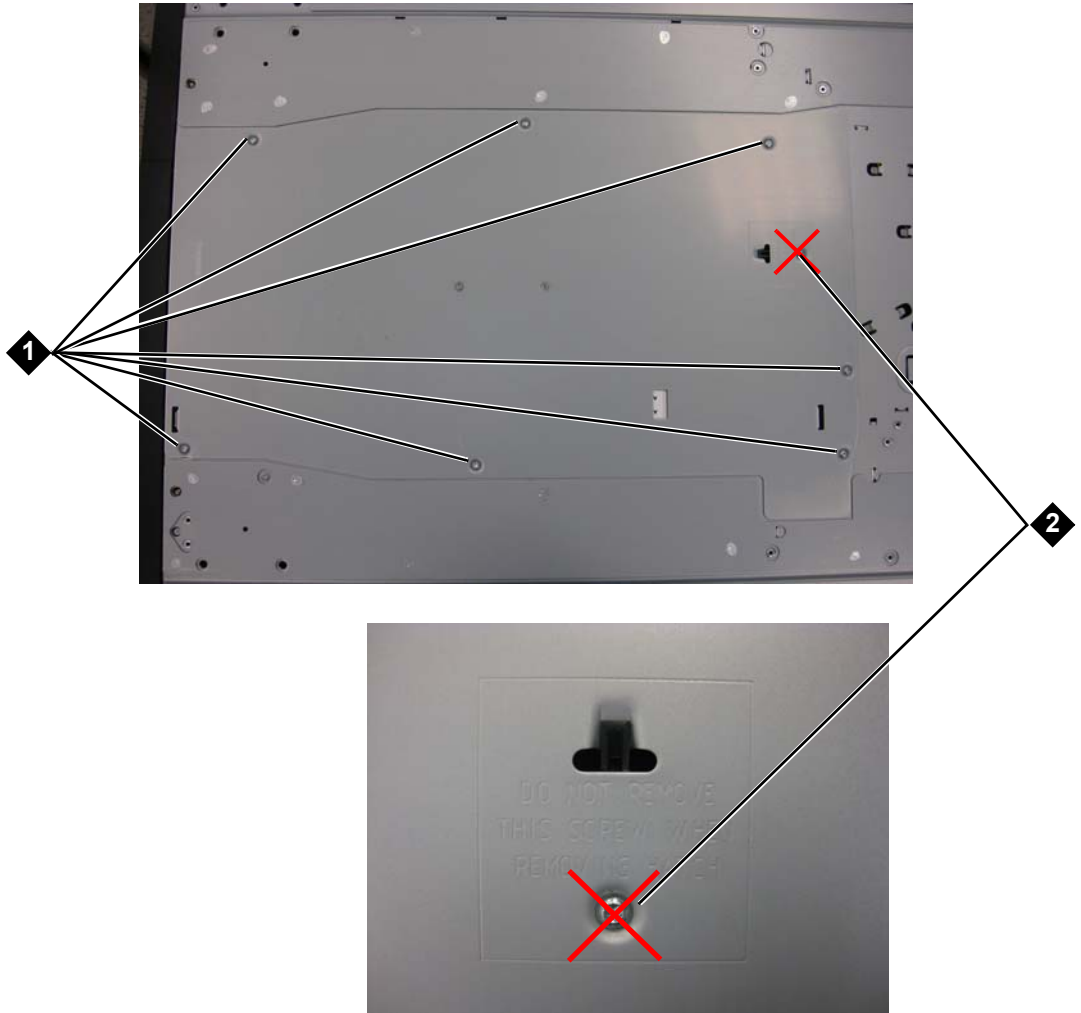
1	screws to remove
2	y-home flag screw - do not remove

a If you plan to stack the control module at the top of the library, and if an expansion module will be located below it, remove the control module's bottom cover plate and the expansion module's top plate.

b If you plan to stack the control module between expansion modules, remove both the top and bottom plates of the control module. Also remove the top plate of the expansion module located below the control module and the bottom plate of the expansion module located above the control module.

c If you plan to stack the control module at the bottom of the library, and if an expansion module will be located above it, remove the control module's top plate and the expansion module's bottom plate.

Figure 54 Recommended
Module Locations

5U	14U	23U	32U	41U
				cover plate
			cover plate	Expansion Module
		cover plate	Control Module	Control Module
	cover plate	Control Module	Expansion Module	Expansion Module
cover plate	Control Module	Expansion Module	Expansion Module	Expansion Module
Control Module	Expansion Module	Expansion Module	Expansion Module	Expansion Module
cover plate	cover plate	cover plate	cover plate	cover plate

**Installing the Expansion
Module**

Install the expansion module as follows:

1 Open the expansion module's access door and raise the guide pin by
pulling it up and turning it slightly as if it were a screw. Otherwise,
the guide pin may scratch the front doors of the module on which
you are stacking.
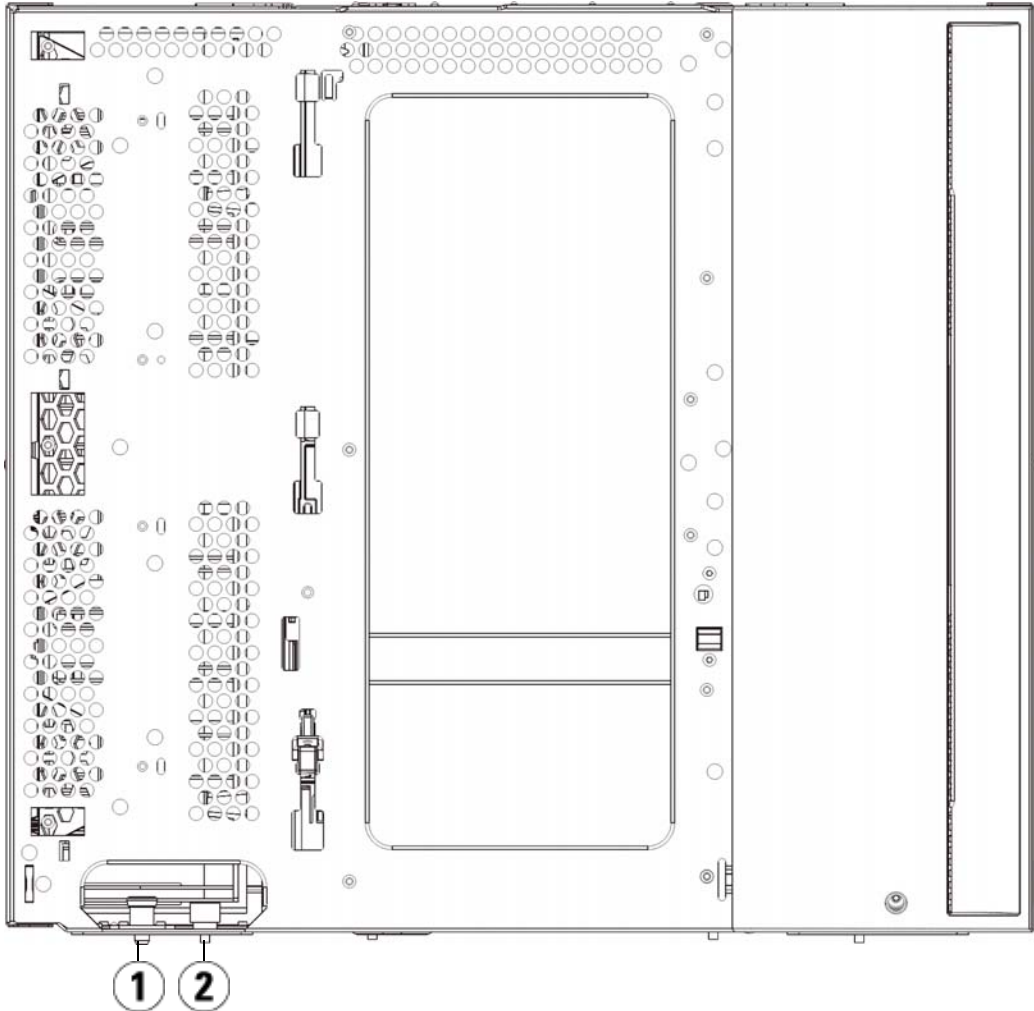
| 1 | Guide pin |
| 2 | Thumbscrew |

2 Lift the new expansion module and, from the front of the library, place it in the desired location.

3 If stacking the expansion module on top of another module, secure the two modules together by tightening the two thumbscrews at the base of the front of the module and the two thumbscrews located at the base of the back of the module. Then lower the module's guide pin (located at the base of the front of the module) by turning it and pushing it down.

4 Tighten all thumbscrews located at the base of the front and back of the modules.

5 Fasten the module to the rack with rack ears. See Installing the Library in a Rack on page 417 for information on installing a rackmount kit.

6 If stacking the expansion module on top of another module, engage the Y-rails of the new module in your library configuration. Ensure that the Y-rails are properly aligned and the thumbscrews are tightened.

1	Front Y-rail
2	Rear Y-rail
3	Y-rail (this end up)
4	Squeeze here to release

a From the front of the library, open the I/E station and access doors of the expansion module. Squeeze the handle of the Y-rail release mechanism, lift it out of its locked position, and slide it downward as far as it will go.

b From the back of the library, find the rear Y-rail release mechanism, which is located in the interior of the right side of the module. Squeeze the handle of the Y-rail release mechanism, lift it out of its locked position, and slide it downward as far as it will go.

Caution:	Check to make sure that there is no gap between the top and bottom Y-rails on both the front and back of the library. If a gap exists, the library cannot mechanically initialize.

Doing this aligns the Y-rails with the Y-rails of the module beneath it.

Figure 55 Y-Rail in Unlocked, Functional Position
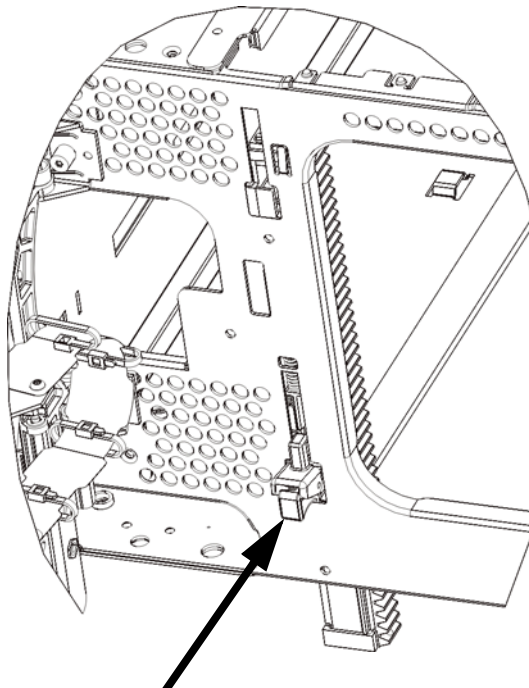
7 Repeat these steps for each expansion module you are installing.

Installing the Control Module

Install the 5U control module as follows:

1 Open the control module's I/E station door and access door.

2 Lift the control module and place it in the desired location.

3 If stacking the control module on top of another module, secure the two modules together by tightening the two thumbscrews at the base of the front of the module and the two thumbscrews located at the base of the back of the module. Then lower the module's guide pin (located at the base of the front of the module) by turning it and pushing it down.

4 Tighten all thumbscrews located at the base of the front and back of the modules.

5 Use the rack ears to fasten the control module to the rack.

6 If not already installed, install the library control blade (LCB) in the control module. See Removing and Replacing the Library Control Blade and LCB Compact Flash Card on page 402 for instructions on installing the LCB.

Preparing to Use the Multi-Module Library

Prepare the library for use as follows:

1 Unpark the robot assembly.

   a Gently raise the robot assembly so that it no longer rests on the parking tab.

> **Caution:** Support the robot assembly by holding onto the broad metal X-axis plate. Lifting the robot by the thin metal rod will bend the rod. Lifting the robot by the black plastic picker body can damage the robot.

   b With your free hand, move the parking tab in a clockwise direction until it stops in the "unparked" position. When in the correct position, the parking tab is removed completely from the interior of the module and will not accidentally swing into the path of the robot.

   c Gently release the robot assembly. It will lower to the bottom module of the library.

| 1 | Parking tab in "unparked" position |

2 Close the library's I/E station and access doors.

3 Add the tape drives to the modules. For details, see Adding, Removing, and Replacing Tape Drives on page 438.

4 If your library contains FC I/O blades, install both the I/O blades and the accompanying fan blades in the expansion module. For details, see and Adding, Removing, and Replacing the FC I/O Fan Blade on page 454.

5 Add the power supplies.For details, see <u>Adding, Removing, and Replacing Power Supplies</u> on page 414.

6 Connect all power cords, network data cables, and module-to-module cables. Make sure the module terminators are installed at the top and bottom of the stack of modules. For cabling instructions, see <u>Cabling the Library</u> on page 289.

7 Power on the library. For libraries larger than a 14U, boot time may take 15-20 minutes.

8 Configure the library using the **Setup Wizard** that appears on the operator panel interface.

9 Add the tape cartridges to the library's modules using the I/E station commands from the operator panel or Web client.

10 Open the host application and reinventory in order to synchronize its logical inventory with the physical inventory of the library.

Adding Expansion Modules to an Existing Library

Adding expansion modules to the library increases the number of data cartridges available within the library system. These instructions explain how to add an expansion module to an existing library.

Note:	The maximum number of expansion modules supported in a library depends on the level of firmware the library is running. The latest firmware must be installed on the library if you are upgrading from a 5U or 14U configuration to a larger configuration. The latest firmware can be found at <u>www.quantum.com/support</u>. See <u>Updating Library and Tape Drive Firmware</u> on page 278 for more information.

There are some configuration settings to take into account when adding an expansion module to an existing library.

• All COD licenses remain the same. If the current license key does not cover the expanded capacity, you will need a new license key to use the newly available slots.

- Partition, I/E station slot, and cleaning slot assignments do not change; however, unassigned slots may change location.

- Modifying partitions can cause the storage slots to be scattered throughout the library.

- I/E station slots in the new module(s) are assigned as data storage slots. You can reconfigure these slots as I/E station slots after the expansion module has been added to the library.

A library can use up to four expansion modules to a maximum height of 41U.

There are no restrictions on where the control module can be installed in the library configuration. However, the recommended placement of the control module for library configurations up to 32U is on top of all installed expansion modules. The recommended placement of the control module for 41U library configurations is on top of three expansion modules and below the top expansion module.

When adding additional expansion modules to an existing library configuration, the recommended placement of the new expansion module is at the bottom of the existing library configuration (except for the 41U, where recommended placement is on top). Installing the new expansion module at the bottom of the existing library configuration will logically assign slot numbering within the library.

Expansion Module
Control Module
Expansion Module
Expansion Module
Expansion Module

Warning:	All libraries taller than 14U must be installed in a rack having a main protective earthing (grounding) terminal, and power must be supplied via an industrial plug and socket-outlet and/or an appliance coupler complying with IEC 60309 (or an equivalent national standard) and having a protective earth (ground) conductor with a cross sectional area of at least 1.5 mm^2 (14 AWG).
	To ensure proper airflow and access space, Allow 60 cm (24 inches) in the front and back of the library.

Warning:	Without tape drives, tape cartridges, or power supplies, a 5U control module weighs approximately 60 lbs (27.2 kg). A 9U expansion module, without tape drives, tape cartridges, or power supplies, exceeds 65 lbs (29.5 kg).
	To avoid serious injury, at least two people are required to safely lift the modules.

Preparing to Install an Additional Expansion Module

Prepare to install an additional expansion module as follows:

Warning:	Without tape drives, tape cartridges, or power supplies, a 5U control module weighs approximately 60 lbs (27.2 kg). A 9U expansion module, without tape drives, tape cartridges, or power supplies, exceeds 65 lbs (29.5 kg).
	To avoid serious injury, at least two people are required to safely lift the modules.

Caution:	If the library contains a partition that spans modules, and you plan to install the new expansion module between those modules, you must delete the partition before adding the new module, and re-create the partition after installing the module.

Required tools:

- Phillips #2 screwdriver, for removing and replacing the top cover plate

- T10 TORX screwdriver, for removing and replacing the bottom cover plate

You need to unstack the library to install the new expansion module at the bottom of the new library configuration.

1 Upgrade the library firmware to a level that can support the number of modules you are adding. See Updating Library and Tape Drive Firmware on page 278 for information on upgrading firmware.

2 If you have a partition that spans modules, and you plan to add the new expansion module between those modules, you must delete the partition before adding the new module (see Deleting Partitions on page 74).

3 Remove all tape cartridges from the library using the import and export commands of the operator panel or Web client.

4 Power off the library.

5 Disconnect all power cords, network data cables, and module-to-module cables from all of the modules.

> **Note:** You should label all cables before you remove them so you can later reconnect them to their proper locations.

6 Park the robot assembly in the control module. Before unstacking the library, the robot assembly must be placed in the control module.

   a Open the I/E station and access doors of each module.

   b Using your hands, gently lift the robot assembly into the control module. The robot assembly should glide slowly and with some resistance.

> **Caution:** Support the robot assembly by holding onto the broad metal X-axis plate. Lifting the robot by the thin metal rod will bend the rod. Lifting the robot by the black plastic picker body can damage the robot.

c After raising the robot assembly to the approximate middle of the control module, hold it in place with one hand and, using your other hand, move the parking tab in a counter-clockwise direction until it stops in the "parked" position. The metal parking tab is located at the bottom of column 1.

d Gently lower the robot assembly to rest on the parking tab.

1	Parking tab in "parked" position

7 Remove all power supplies from each module.

8 Remove all tape drives from each module.

Unstacking the Existing Modules

Unstack the modules as follows:

1 Starting with the topmost module of your library, open the I/E station and access doors.

> **Caution:** Before unstacking the modules, the robot assembly must be parked as described in [Preparing to Install an Additional Expansion Module](#) above.

2 If your current configuration already uses an expansion module, disengage the Y-rails so the modules can be safely unstacked.

   a From the front of the library, find the Y-rail release mechanism, which is located on the left side of the module. Squeeze the handle of the Y-rail release mechanism, lift it, and release it so that it locks into place.

   b From the rear of the library, find the rear Y-rail release mechanism located in the interior of the right side of the module. Squeeze the handle of the Y-rail release mechanism, lift it, and release it so that it locks into place.

> **Note:** The rear Y-rail is impossible to lift up with the tape drives installed.
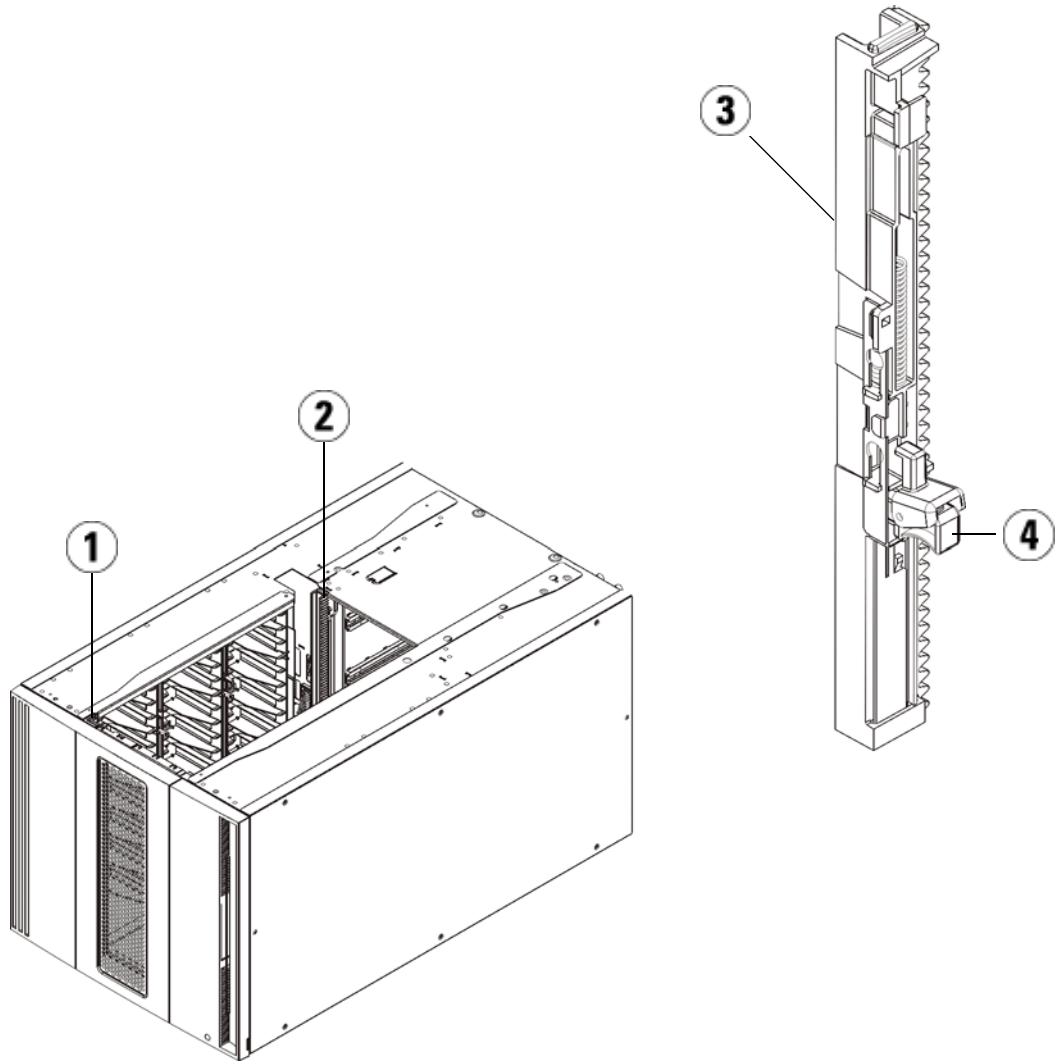
1 Front Y-rail

2 Rear Y-rail

3 Y-rail (this end up)

4 Squeeze here to release

3 Remove the rack ears that fasten the module to the rack.

4 Loosen the thumbscrews located at the base of the front and rear of the module.
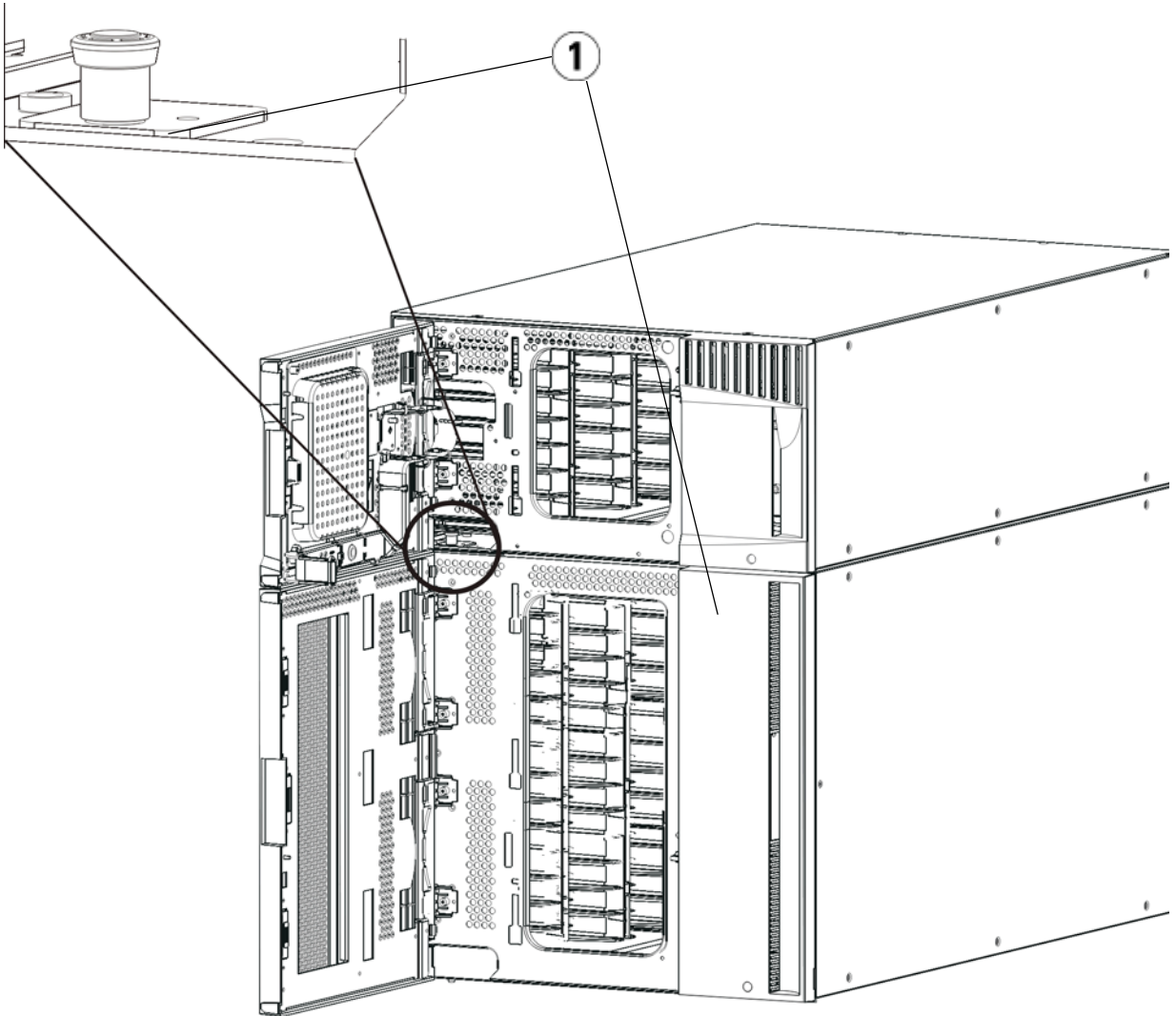
1   Thumbscrews (behind doors)

5 Open the module's access door and raise the guide pin by pulling it up and turning it slightly as if it were a screw. Otherwise, the guide pin may scratch the front doors of the module beneath it.
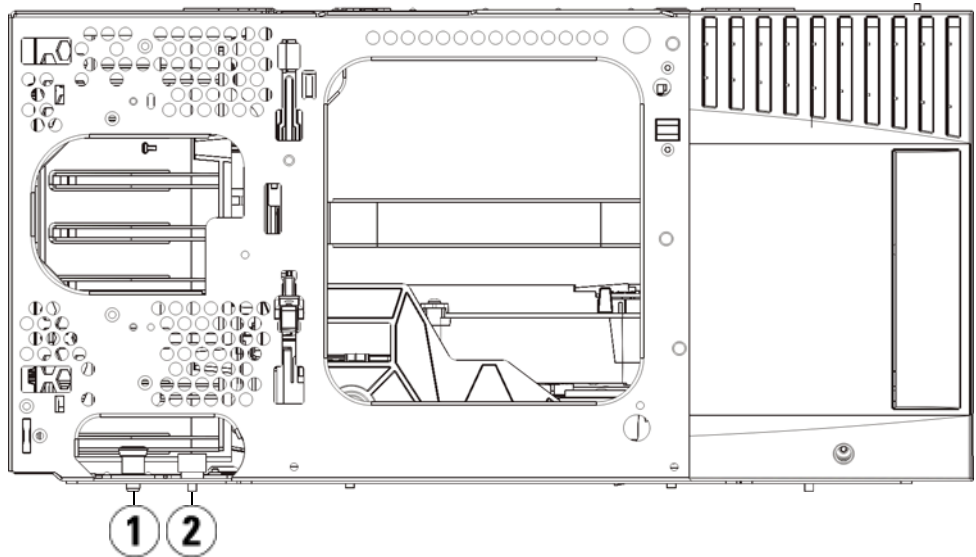
| 1 | Guide pin |
| 2 | Thumbscrew |

6 From the front of the library, slide the entire module toward you and lift it off of the module below it.

7 Repeat these steps for each module that you need to remove.

Installing the New 9U Expansion Module

Install the new 9U expansion module as follows:

1 Prepare the rack to hold modules, if you want to install your library in a rack. See <u>Installing the Library in a Rack</u> on page 417 for instructions on installing a rackmount kit.

2 Remove and replace the cover plates, if appropriate.

> **Caution:** Before removing the control module's bottom cover plate, the robot assembly must be parked as described in <u>Preparing to Install an Additional Expansion Module</u> above.

    a If you plan to stack the control module at the top of the library, and if an expansion module will be located below it, remove the control module's bottom cover plate and the expansion module's top plate.

    b If you plan to stack the control module between expansion modules, remove both the top and bottom plates of the control module. Also remove the top plate of the expansion module, located below the control module, and the bottom plate of the expansion module, located above the control module.

    c If you plan to stack the control module at the bottom of the library, and if an expansion module will be located above it, remove the control module's top plate and the expansion module's bottom plate.

Figure 56 Cover Plate Location
After Adding an Expansion
Module

5U	14U	23U	32U	41U
				cover plate
			cover plate	**NEW** Expansion Module*
		cover plate	Control Module	Control Module
	cover plate	Control Module	Expansion Module	Expansion Module
cover plate	Control Module	Expansion Module	Expansion Module	Expansion Module
Control Module	**NEW** Expansion Module*	**NEW** Expansion Module*	**NEW** Expansion Module*	Expansion Module
cover plate	cover plate	cover plate	cover plate	cover plate

* Recommended location for adding an expansion module.

3 Open the expansion module's access door and raise the guide pin by pulling it up and turning it slightly as if it were a screw. Otherwise, the guide pin may scratch the front doors of the module on which you are stacking it.
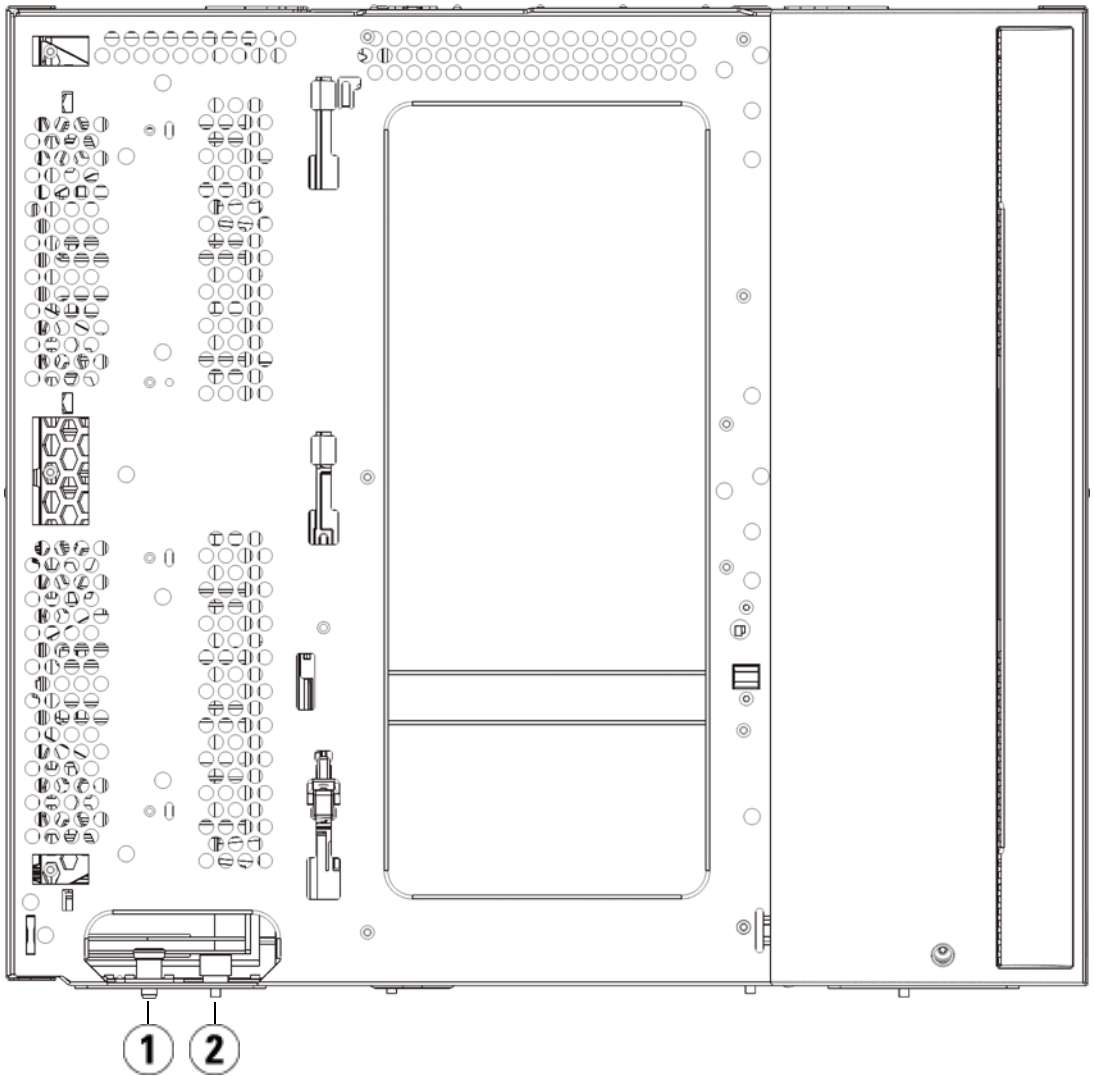
1	Guide pin
2	Thumbscrew

4 Lift the new expansion module and, from the front of the library, place it in the desired location.

5 If there is already a module installed, secure the two modules together by tightening the two thumbscrews at the base of the front of the module and the two thumbscrews located at the base of the back of the module. Then lower the module's guide pin (located at the base of the front of the module) by turning it and pushing it down.

6 Tighten all thumbscrews located at the base of the front and back of the modules.

7 Fasten the module to the rack with rack ears.

8 Engage the Y-rails of the new module in your library configuration. Ensure that the Y-rails are properly aligned and the thumbscrews are tightened.
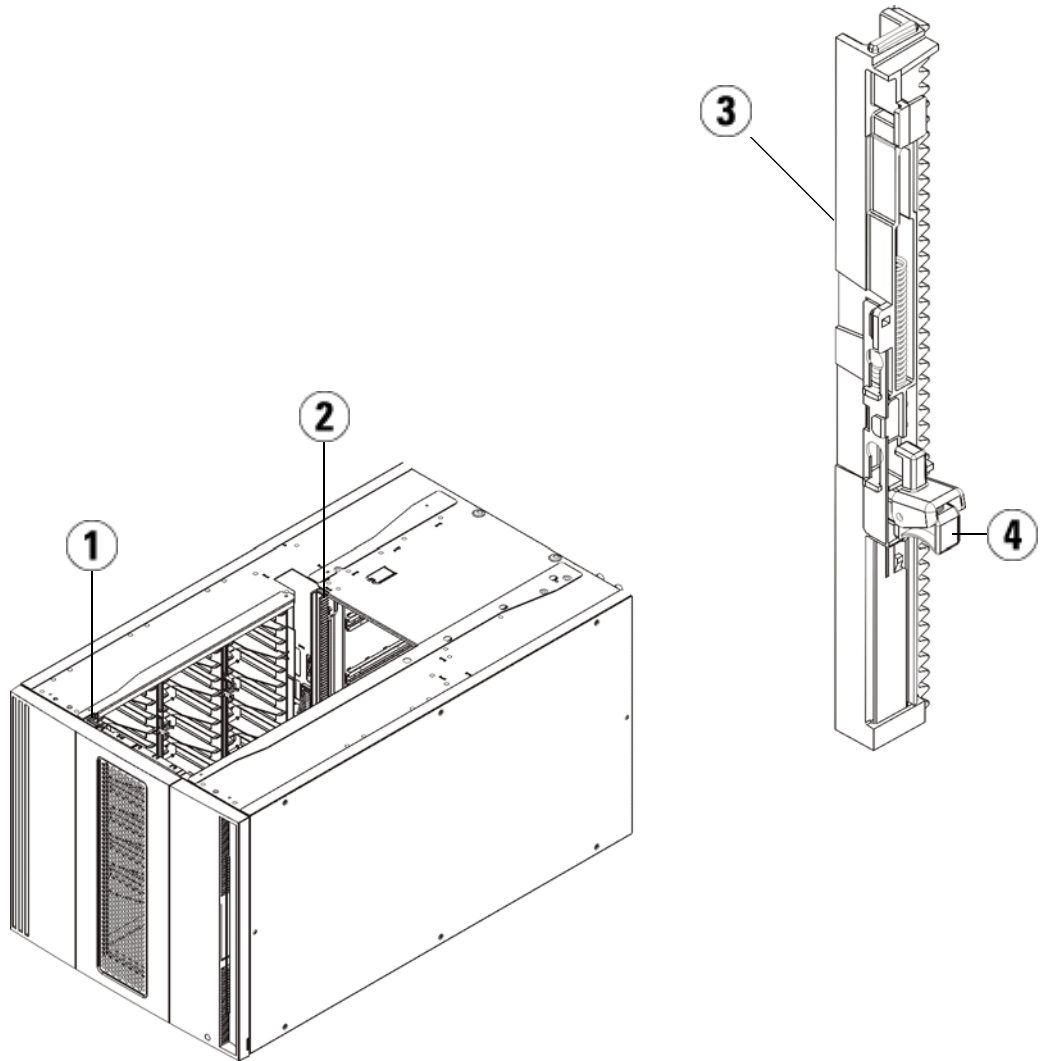
1   Front Y-rail

2   Rear Y-rail

3   Y-rail (this end up)

4   Squeeze here to release

   a From the front of the library, open the I/E station and access doors of the expansion module.

   b Squeeze the handle of the Y-rail release mechanism, lift it out of its locked position, and slide it downward as far as it will go.

   c From the back of the library, find the rear Y-rail release mechanism, which is located in the interior of the right side of the module. Squeeze the handle of the Y-rail release mechanism, lift it out of its locked position, and slide it downward as far as it will go.

      Doing this aligns the Y-rails with the Y-rails of the module beneath it.

Caution:	Check to make sure that there is no gap between the top and bottom Y-rails on both the front and back of the library. If a gap exists, the library cannot mechanically initialize.
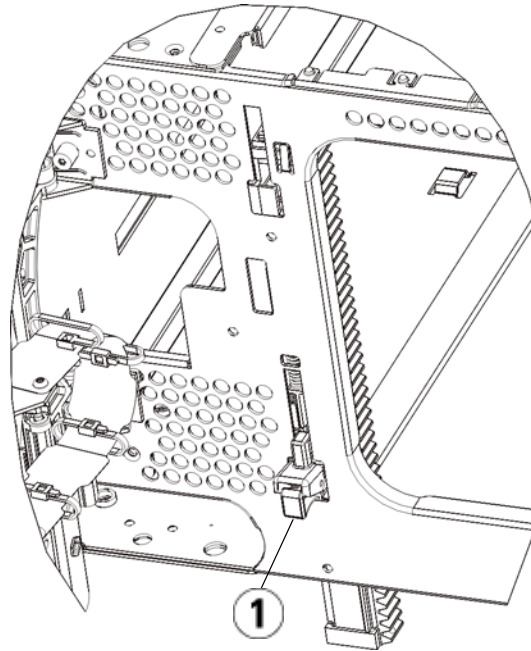
1	Y-rail in unlocked, functional position

9 Repeat these steps for each module you need to re-install in the library configuration.

Preparing to Use the Library

Prepare to use the library as follows:

1 Add the tape drives to the modules. For details, see <u>Adding, Removing, and Replacing Tape Drives</u> on page 438.

2 Add the power supplies. For details, see <u>Adding, Removing, and Replacing Power Supplies</u> on page 414.

3 Add the LCB to the control module. For details, see <u>Removing and Replacing the Library Control Blade and LCB Compact Flash Card</u> on page 402.

4 If your library contains FC I/O blades, install both the I/O blades and the accompanying fan blades in the expansion module. For details, see <u>Adding, Removing, and Replacing FC I/O Blades</u> on page 443 and <u>Adding, Removing, and Replacing the FC I/O Fan Blade</u> on page 454.

5 Unpark the robot assembly.

   a Gently raise the robot assembly so that it no longer rests on the parking tab.

Caution:	Support the robot assembly by holding onto the broad metal X-axis plate. Lifting the robot by the thin metal rod will bend the rod. Lifting the robot by the black plastic picker body can damage the robot.

   b With your free hand, move the parking tab in a clockwise direction until it stops in the "unparked" position. When in the correct position, the parking tab is removed completely from the interior of the module and will not accidentally swing into the path of the robot.

   c Gently release the robot assembly. It will lower to the bottom module of the library.

1   Parking tab in "unparked" position

6 Connect all power cords, network data cables, and module-to-
module cables. Make sure the module terminators are installed at the
top and bottom of the stack of modules. For cabling instructions, see
Cabling the Library on page 289.

7 Power on the library.

8 Reconfigure the library, including applying the new COD license
key, using the operator panel or Web client.

9 Recreate any partitions you deleted prior to installing the module.

10 Add the tape cartridges to the library's modules using the I/E station commands from the operator panel or Web client.

11 Open the host application and reinventory in order to synchronize its logical inventory with the physical inventory of the library. Due to the way the library logically addresses its tape drives and slots internally, adding an expansion module will change the element addresses, and this can affect proper communication to a controlling host. See <u>Understanding Logical Element Addressing</u> on page 35. Because of this, you must refresh the configuration of any backup application that manages the library to reflect the adjusted positions. In addition, you may need to reboot the host server(s) or rescan the bus to detect the changes.

Preparing to Remove or Replace a Module

Follow the instructions in this section before performing any of the following procedures:

- <u>Permanently Removing Expansion Modules From an Existing Library</u> on page 364
- <u>Replacing the Control Module</u> on page 376
- <u>Replacing an Expansion Module</u> on page 388

Caution:	**If a control module is replaced,** all library configuration data will be invalidated and requires a new library configuration. Follow the instructions below to completely export all tape cartridges and completely delete all logical partition configuration and cleaning slot assignments.

Caution:	**If an expansion module is removed or replaced**, you must follow the steps below to modify or delete all the affected partitions before removing the module. Recreate the partitions after the removal or replacement is complete.

Required tools:

- Phillips #2 screwdriver, for removing and replacing the top cover plate

- T10 TORX screwdriver, for removing and replacing the bottom cover plate

Instructions:

1   View your library's current configuration before removing or replacing any library modules to determine which partitions may be affected, which tape cartridges belong to which partition, and whether cleaning slots are configured within the library module you are removing or replacing. See <u>Viewing the Library Configuration Report</u> on page 268.

For example, in <u>Figure 57</u>, the following library configuration may be observed. Note that there are three partitions configured. All three partitions share six I/E elements in the control module. The library is configured for automatic cleaning and has three cleaning slots configured in the expansion module.

- Library_a configured all storage elements in the control module, and has one drive configured in the control module, and one drive configured in the expansion module.

- Library_b configured most storage elements in the control module, but references its last storage element in the expansion module. This partition has one drive configured in the control module and one drive configured in the expansion module.

- Library_c configured all storage elements in the expansion module, and also configured two drives in this expansion module.

Figure 57 Library Configuration
Example 1
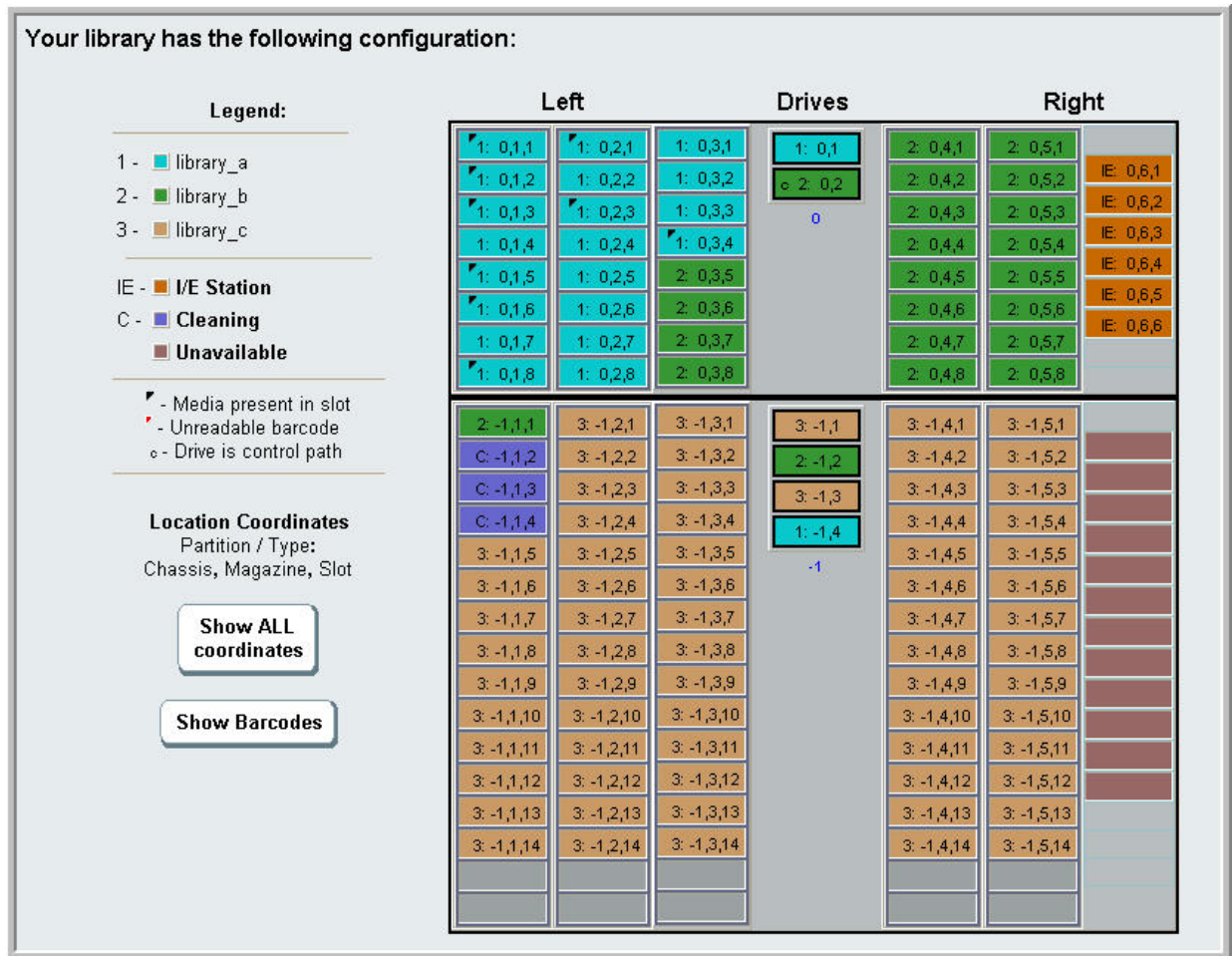
2 If cleaning slots are configured for automatic, library–initiated cleaning operations, export all affected cleaning media from the elements contained within the module you are removing or replacing. See Exporting Cleaning Media on page 258.

3 If cleaning slots are affected and all cleaning media has been exported from the module you are removing or replacing, reduce or delete the cleaning slots so that cleaning slots are no longer configured within the module you are removing or replacing. You

can designate new cleaning slots after the module has been removed or replaced. See <u>Configuring Cleaning Slots</u> on page 78.

4 If the module you are removing or replacing contains tape drives, make sure that none of the tape drives have media mounted. See <u>Unloading Tape Drives</u> on page 252.

5 If the module you are removing or replacing contains I/E slots, remove all media from the affected I/E slots and store them separately for each partition so you can import them back into the same partition once the module removal or replacement is complete.

6 If one or more partitions reference any storage slots within the module you are removing or replacing, export all tape cartridges from the affected partitions and keep the exported cartridges separated by partition, so you can import them back into the same partition once the module removal or replacement is complete. See <u>Exporting Media</u> on page 249.

Caution:	The library will not be able to locate tape cartridges that are removed from one partition and returned to a different partition. The tape cartridges must be returned to the same partition from which they were removed.

7 If a partition references storage slots within the module you are removing or replacing, delete such partition. You can create new partitions after modules have been removed or replaced. See <u>Working With Partitions</u> on page 68.

> **Note:** If the last elements of a partition reside in the module you are removing or replacing, you may be able to modify the partition instead of deleting it. (See Understanding Logical Element Addressing on page 35 for more information on how the library logically addresses tape drives and slots.) In that case, you would 1) export those tape cartridges that reside in the module you are removing or replacing, and 2) modify the partition, instead of deleting it, so that the partition no longer references any storage or drive elements within the module you are removing or replacing. See Modifying Partitions on page 73.
>
> **For example**, in Figure 58, after exporting all affected tape cartridges from the module you are removing, the cleaning slots are deleted, then Library_c is completely deleted, and Library_b is modified to reduce its storage slot count by one, as this deletes the storage slot reference in the expansion module. No storage element modifications are required for Library_a.

Figure 58 Library Configuration
Example 2

8 If a partition references tape drives within the module you are
removing or replacing, modify any affected partition by removing
the referenced drive elements from the partition. See <u>Modifying
Partitions</u> on page 73.

For example, in <u>Figure 57</u> on page 358, all partitions reference drives
in the expansion modules. In <u>Figure 58</u> on page 361, Library_c was
deleted, as well as its drive references in the expansion module.

Library_a and Library_b still require partition modifications to remove the drive reference and hereby free the expansion module of all partition resource references.

9 If you are removing or replacing an expansion module, set the number of I/E station slots to six. You can reconfigure I/E station slots after the module removal or replacement is complete. See

10 Power off the library.

11 Disconnect all power cords, network data cables, and module-to-module cables from each module you will be removing.

> **Note:** You should label all cables before you remove them so you can later reconnect them to their proper locations.

12 Park the robot assembly in the control module. Before unstacking the library, the robot assembly must be placed in the control module.

   a Open the I/E station and access doors of each module.

   b Using your hands, gently lift the robot assembly into the control module. The robot assembly should glide slowly and with some resistance.

> **Caution:** Support the robot assembly by holding onto the broad metal X-axis plate. Lifting the robot by the thin metal rod will bend the rod. Lifting the robot by the black plastic picker body can damage the robot.

   c After raising the robot assembly to the approximate middle of the control module, hold it in place with one hand and, using your other hand, move the parking tab in a counter-clockwise direction until it stops in the "parked" position. The metal parking tab is located at the bottom of column 1.

   d Gently lower the robot assembly to rest on the parking tab.

| 1 | Parking tab in "parked" position |

13 Remove all power supplies from each module that you intend to remove. For details, see <u>Adding, Removing, and Replacing Power Supplies</u> on page 414.

14 Remove all tape drives from each module that you intend to remove. If you are going to replace the module, label the drives with their locations so you can re-install them in the same locations later. For details, see <u>Adding, Removing, and Replacing Tape Drives</u> on page 438.

15 If the module you are removing or replacing contains FC I/O blades, remove both the I/O blades and the accompanying fan blades from the expansion module. For details, see Adding, Removing, and Replacing FC I/O Blades on page 443 and Adding, Removing, and Replacing the FC I/O Fan Blade on page 454.

16 Before removing a module, you must first remove all expansion modules (if any) positioned above it. Disconnect all power cords, network data cables, and module-to-module cables from the module you are removing or replacing and all modules located above it. Then remove the modules.

Warning:	Without tape drives, tape cartridges, or power supplies, a control module weighs approximately 60 lbs (27.2 kg). An expansion module, without tape drives, tape cartridges, or power supplies, exceeds 65 lbs (29.5 kg).
	To avoid serious injury, at least two people are required to safely lift the modules.

Note:	If the library is installed in a rack, you need to perform additional steps to remove modules from and place modules into the rack. See Installing the Library in a Rack on page 417 for more information.

Permanently Removing Expansion Modules From an Existing Library

These instructions explain how to permanently remove an expansion module from the library.

There are some configuration settings to take into account when removing an expansion module from an existing library.

- COD licenses remain the same. After the expansion module is removed, there may be more slots licensed than are available. Only the available slots appear on the **License** screen.

• All resources in the removed module(s) are removed. A partition with all resources in the removed module(s) will be present with no slots or drives. This partition can only be deleted.

Warning:	All libraries taller than 14U must be installed in a rack having a main protective earthing (grounding) terminal, and power must be supplied via an industrial plug and socket-outlet and/or an appliance coupler complying with IEC 60309 (or an equivalent national standard) and having a protective earth (ground) conductor with a cross sectional area of at least 1.5 mm^2 (14 AWG).

To ensure proper airflow and access space, Allow 60 cm (24 inches) in the front and back of the library. |

Warning:	Without tape drives, tape cartridges, or power supplies, a 5U control module weighs approximately 60 lbs (27.2 kg). A 9U expansion module, without tape drives, tape cartridges, or power supplies, exceeds 65 lbs (29.5 kg).

To avoid serious injury, at least two people are required to safely lift the modules. |

Removing the Expansion Module

To remove the expansion module:

1 Before removing a module, follow the instructions in <u>Preparing to Remove or Replace a Module</u> on page 356.

2 For each module that you plan to remove, open the I/E station and access doors of each module.

Caution:	Before unstacking the modules, the robot assembly must be parked as described in <u>Preparing to Remove or Replace a Module</u> on page 356.

3 Disengage the Y-rails so the modules can be unstacked safely.

1	Front Y-rail
2	Rear Y-rail
3	Y-rail (this end up)
4	Squeeze here to release

a From the front of the library, find the Y-rail release mechanism, which is located on the left side of the control module. Squeeze the handle of the Y-rail release mechanism, lift it, and release it so that it locks into place.

b From the rear of the library, find the rear Y-rail release mechanism located in the interior of the right side of the module. Squeeze the handle of the Y-rail release mechanism, lift it, and release it so that it locks into place.

1	Y-rail in locked, non-functional position

4 Remove the rack ears that fasten the module to the rack. See Installing the Library in a Rack on page 417 for detailed instructions on using the rack ears.

5 Loosen the thumbscrews located at the base of the front of the module.

| 1 | Thumbscrews (behind doors) |

6 Loosen the two thumbscrews located at the base of the back of the module.

7 Open the module's access door and raise the guide pin by pulling it up and turning it slightly as if it were a screw. Otherwise, the guide pin may scratch the front doors of the module beneath it.

8 From the front of the library, slide the entire module toward you and lift it off of the module below it.

9 Repeat these procedures for each module that you intend to remove.

10 Remove and replace the cover plates, if appropriate (see Figure 59).

Caution: Before removing the control module's bottom cover plate, the robot assembly must be parked as described in Preparing to Remove or Replace a Module on page 356.

---

a If you plan to stack the control module at the top of the library, and if an expansion module will be located below it, remove the control module's bottom cover plate and the expansion module's top plate.

b If you plan to stack the control module between expansion modules, remove both the top and bottom plates of the control module. Also remove the top plate of the expansion module located below the control module and the bottom plate of the expansion module located above the control module.

c If you plan to stack the control module at the bottom of the library, and if an expansion module will be located above it, remove the control module's top plate and the expansion module's bottom plate.

Figure 59 Cover Plate Location
After Removing an Expansion
Module

5U	14U	23U	32U
			cover plate
		cover plate	Control Module
	cover plate	Control Module	Expansion Module
cover plate	Control Module	Expansion Module	Expansion Module
Control Module	Expansion Module	Expansion Module	Expansion Module
cover plate	cover plate	cover plate	cover plate

Preparing to Use the New Library Configuration

Prepare to use the new library configuration as follows:

1 Ensure that the Y-rails are properly aligned and the thumbscrews are tightened.

1	Front Y-rail
2	Rear Y-rail
3	Y-rail (this end up)
4	Squeeze here to release

a From the front of the library, open the I/E station and access doors of the expansion module. Squeeze the handle of the Y-rail release mechanism, lift it out of its locked position, and slide it downward as far as it will go.

b From the back of the library, find the rear Y-rail release mechanism, which is located in the interior of the right side of the module. Squeeze the handle of the Y-rail release mechanism, lift it out of its locked position, and slide it downward as far as it will go.

Doing this aligns the Y-rails with the Y-rails of the module beneath it.

Caution:	Check to make sure that there is no gap between the top and bottom Y-rails on both the front and back of the library. If a gap exists, the library cannot mechanically initialize.

1	Y-rail in unlocked, functional position

2 Add the tape drives to the modules. For details, see Adding, Removing, and Replacing Tape Drives on page 438.

3 Add the power supplies. For details, see Adding, Removing, and Replacing Power Supplies on page 414.

4 If your library contains FC I/O blades, install both the I/O blades and the accompanying fan blades in the expansion module. For details, see Adding, Removing, and Replacing FC I/O Blades on page 443 and Adding, Removing, and Replacing the FC I/O Fan Blade on page 454.

5 Unpark the robot assembly.

   a Gently raise the robot assembly so that it no longer rests on the parking tab.

Caution: Support the robot assembly by holding onto the broad metal X-axis plate. Lifting the robot by the thin metal rod will bend the rod. Lifting the robot by the black plastic picker body can damage the robot.

b With your free hand, move the parking tab in a clockwise direction until it stops in the "unparked" position. When in the correct position, the parking tab is removed completely from the interior of the module and will not accidentally swing into the path of the robot.

c Gently release the robot assembly. It will lower to the bottom module of the library.

1   Parking tab in "unparked" position

6 Close the library's I/E station and access doors.

7 Connect all power cords, network data cables, and module-to-module cables. Make sure the module terminators are installed at the top and bottom of the stack of modules. For cabling instructions, see Cabling the Library on page 289.

8 Power on the library.

9 Re-create and/or modify partitions, cleaning slots, and I/E station slots as desired.

10 Import tape cartridges to the correct library partitions as needed.

11 Save the library configuration (see <u>Saving the Library Configuration</u> on page 489.

12 If the host application inventories the location of each tape cartridge in the library, open the host application and reinventory in order to sync its logical inventory with the physical inventory of the library. Due to the way the library logically addresses its tape drives and slots internally, permanently removing an expansion module from the library will change the element addresses, and this can affect proper communication to a controlling host. See <u>Understanding Logical Element Addressing</u> on page 35. Because of this, you must refresh the configuration of any backup application that manages the library to reflect the adjusted positions. In addition, you may need to reboot the host server(s) or rescan the bus to detect the changes.

Replacing the Control Module

These instructions explain how to remove a control module and replace it with a control module field replaceable unit (FRU). You may need to replace the control module if its chassis is severely damaged. Typically, however, only certain customer replaceable units (CRUs) or FRUs within the control module need to be replaced.

There are some configuration settings to take into account when replacing the control module.

- If you have applied one or more license keys to the original control module, you will need to replace each license key and apply it to the new control module. For more information, see <u>Obtaining and Installing a License Key</u> on page 88.

- A partition with all resources in the removed module will be present with no slots or drives. This partition can only be deleted.

There are no restrictions on where the control module can be installed in the library configuration. However, the recommended placement of the control module for library configurations up to 32U is on top of all installed expansion modules. The recommended placement of the control

module for 41U library configurations is on top of three expansion modules and below the top expansion module.

Removing the Control Module

1 Before removing a module, follow the instructions in Preparing to Remove or Replace a Module on page 356.

2 Starting with the topmost module of your library, open the I/E station and access doors of the module.

Caution:	Before unstacking the modules, the robot assembly must be parked as described in Preparing to Remove or Replace a Module on page 356.

3 Disengage the Y-rails so the modules can be safely unstacked.

a From the front of the library, find the Y-rail release mechanism, which is located on the left side of the module. Squeeze the handle of the Y-rail release mechanism, lift it, and release it so that it locks into place.

b From the rear of the library, find the rear Y-rail release mechanism located in the interior of the right side of the module. Squeeze the handle of the Y-rail release mechanism, lift it, and release it so that it locks into place.

Note:	The rear Y-rail is impossible to lift up with the tape drives installed.

1	Front Y-rail
2	Rear Y-rail
3	Y-rail (this end up)
4	Squeeze here to release

4 Remove the rack ears that fasten the module to the rack.

5 Loosen the thumbscrews located at the base of the front and rear of the module.
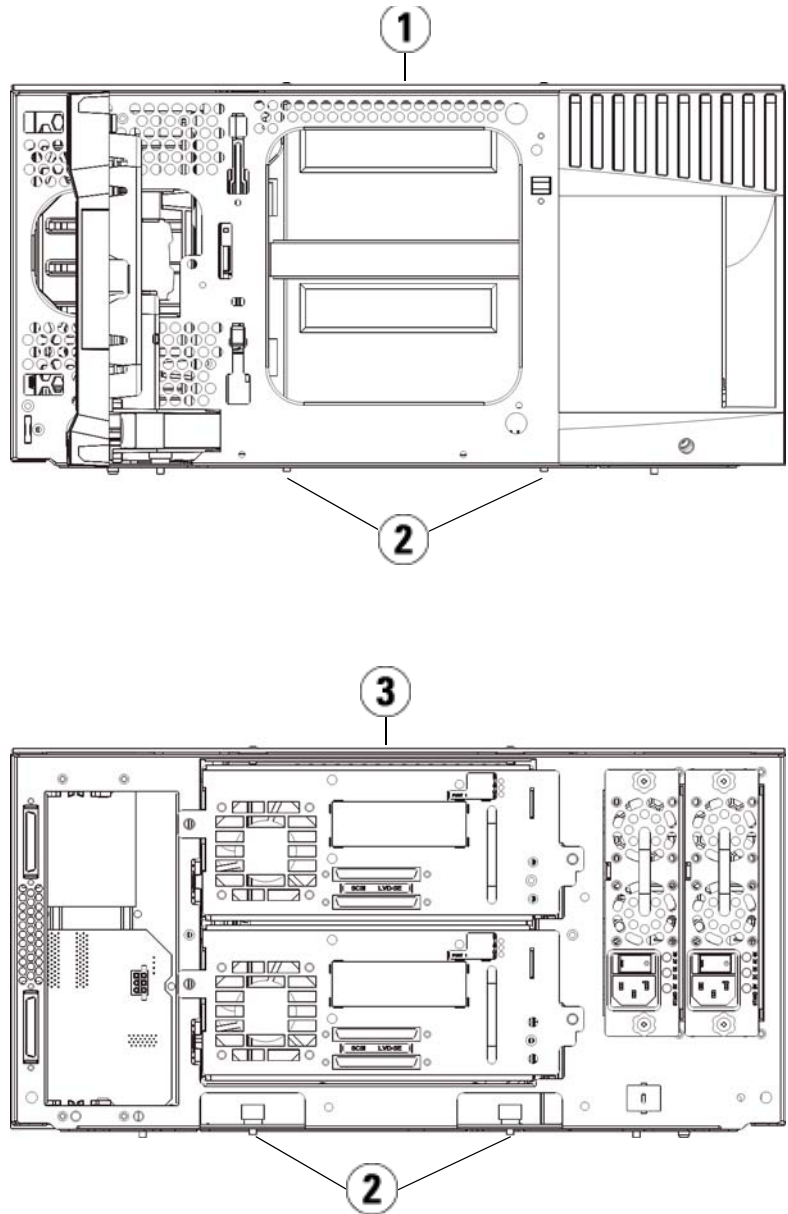
1   Control module (front)

2   Thumbscrews

3   Control module (rear)

6 Open the module's access door and raise the guide pin by pulling it up and turning it slightly as if it were a screw. Otherwise, the guide pin may scratch the front doors of the module beneath it.
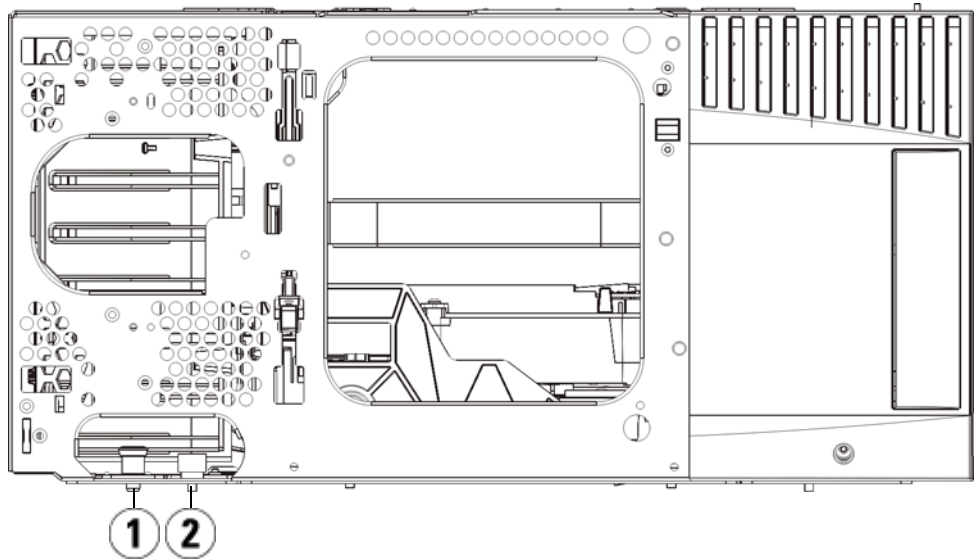
1	Guide pin
2	Thumbscrew

7 Slide the entire module toward you and lift it off of the module below it.

Replacing the Control Module

1 If not already removed, remove the tape drives and power supplies from the control module you are replacing.

2 Using the Phillips #2 screwdriver (for the top cover plate) and the T10 TORX screwdriver (for the bottom cover plate), remove the new control module plates from the top and bottom of the module, as necessary.

> **Caution:** Before removing the control module's bottom cover
> plate, the robot assembly must be parked as described
> in <u>Preparing to Remove or Replace a Module</u> on
> page 356.

a If your library consists of only the control module, do not remove
the plates.

b If you plan to stack the control module at the top of the library,
and if an expansion module is located below it, remove the
control module's bottom cover plate.

c If you plan to stack the control module in the middle of the
library, remove both the top and bottom cover plates.

d If you plan to stack the control module at the bottom of the
library, and if an expansion module is located above it, remove
the control module's top cover plate.

3 Remove the LCB from the removed control module and set it aside.

The LCB stores information about the library's contents and
configuration, so you will probably want to install this LCB (or
possibly just the LCB compact flash card) in the new control module.
For details about removing the LCB, see <u>Removing and Replacing the
Library Control Blade and LCB Compact Flash Card</u> on page 402.

> **Note:** If you plan to stack the control module on top of a 9U
> expansion module, be sure to park the robot in the control
> module first.

4 If the library configuration includes expansion modules below the
control module, install them in the library now.

5 Install the new control module in the library. Lift the control module
and, from the front of the library, place it in the desired location.

Place the control module on top of the expansion module and slide it
to the rear of the unit. A small notch on the bottom of the control
module aligns it with the top of the 9U expansion module.

6 Use rack ears to fasten the control module on top of a 9U expansion
module.

7 If you placed the control module on top of an expansion module, secure the two modules by tightening the two thumbscrews at the base of the *front* of the module and the two thumbscrews located at the base of the *back* of the module. Then lower the module's guide pin (located at the base of the front of the module) by turning it and pushing it down.

8 Stack all expansion modules (if any) in their original positions above the control module. Use rack ears to fasten the modules to the rack.Then tighten all thumbscrews located at the base of the front and back of the modules.

9 Engage the Y-rails. Tighten the thumbscrews and lower the guide pin. Doing this aligns the Y-rail with the Y-rail of the module beneath it.

   a From the front of the library, open the I/E station and access doors of the control module. Squeeze the handle of the Y-rail release mechanism, lift it out of its locked position, and slide it downward as far as it will go.
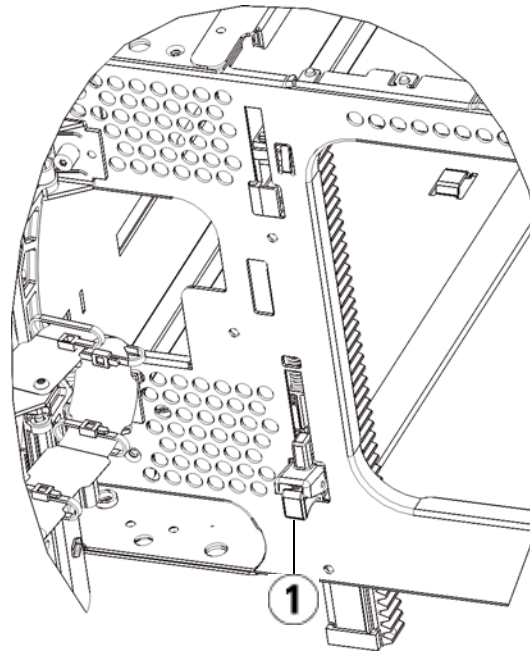
| 1 | Y-rail in unlocked, functional position |

b From the back of the library, find the rear Y-rail release
mechanism, which is located in the interior of the right side of the
module. Squeeze the handle of the Y-rail release mechanism, lift
it out of its locked position, and slide it downward as far as it will
go.

10 Unpark the robot assembly.

a Gently raise the robot assembly so that it no longer rests on the
parking tab.

| **Caution:** | Support the robot assembly by holding onto the broad metal X-axis plate. Lifting the robot by the thin metal rod will bend the rod. Lifting the robot by the black plastic picker body can damage the robot. |

b With your free hand, move the parking tab in a clockwise direction until it stops in the "unparked" position. When in the correct position, the parking tab is removed completely from the interior of the module and will not accidentally swing into the path of the robot.

c Gently release the robot assembly. It will lower to the bottom module of the library.

| 1 | Parking tab in "unparked" position |

**Preparing to Use the
Control Module**

1   Close the library's I/E station and access doors.

2   Add the tape drives to the modules. For details, see <u>Adding,
    Removing, and Replacing Tape Drives</u> on page 438.

3   Add the power supplies. For details, see <u>Adding, Removing, and
    Replacing Power Supplies</u> on page 414.

4   Install the LCB or compact flash card from the removed control
    module in the new control module. For details, see <u>Removing and
    Replacing the Library Control Blade and LCB Compact Flash Card</u> on
    page 402.

5   Connect all power cords, network data cables, and module-to-
    module cables. Make sure the module terminators are installed in
    their previous positions at the top and bottom of the stack of
    modules. For cabling instructions, see <u>Cabling the Library</u> on
    page 289.

6   Power on the library.

7   Re-create and/or modify partitions, cleaning slots, and I/E station
    slots as desired.

8   Import tape cartridges into the correct partitions as needed.

9   Save the library configuration (see <u>Saving the Library Configuration</u>
    on page 489.

10 If the host application inventories the location of each tape cartridge
    in the library, open the host application and reinventory in order to
    sync its logical inventory with the physical inventory of the library.
    Due to the way the library logically addresses its tape drives and slots
    internally, replacing a control module may change the element
    addresses, and this can affect proper communication to a controlling
    host. See <u>Understanding Logical Element Addressing</u> on page 35.
    Because of this, you must refresh the configuration of any backup
    application that manages the library to reflect the adjusted positions.
    In addition, you may need to reboot the host server(s) or rescan the
    bus to detect the changes.

Special Instructions for Replacing a Control Module in a Library Running SKM

If your library is running SKM, you must you run a special script on the SKM server after you replace the control module. The script will correct the library serial number associations in the key server database and allow you to export used SKM encryption keys via the Web client correctly. For instructions, refer to the chapter titled "Updating the SKM Keystore After Replacing a Library Control Module" in the *Scalar Key Manager 2.0 User's Guide*.

When running the script, you will need to enter the serial numbers of both the non-functioning control module as well as the serial number of the new replacement control module. Before you send the control module back to Quantum, record the serial numbers so you can provide them when required. If you have already returned the failed control module to Quantum, contact Quantum Support to obtain its serial number.

Locating the Serial Number on the Scalar i500

On the Scalar i500, the serial number label is located inside the control module, on the horizontal bar at the back of the library. To see the label, open the front door. See <u>Figure 4</u> for location and <u>Figure 61</u> for an example.

The serial number is listed first. The serial number is all of the characters following the "%SN" on the serial number label. Do not enter the "%SN" characters when typing the serial number into the SKM command line.

Figure 60 Scalar i500 Serial
Number Label On Control
Module Seen Through Open
Front Door
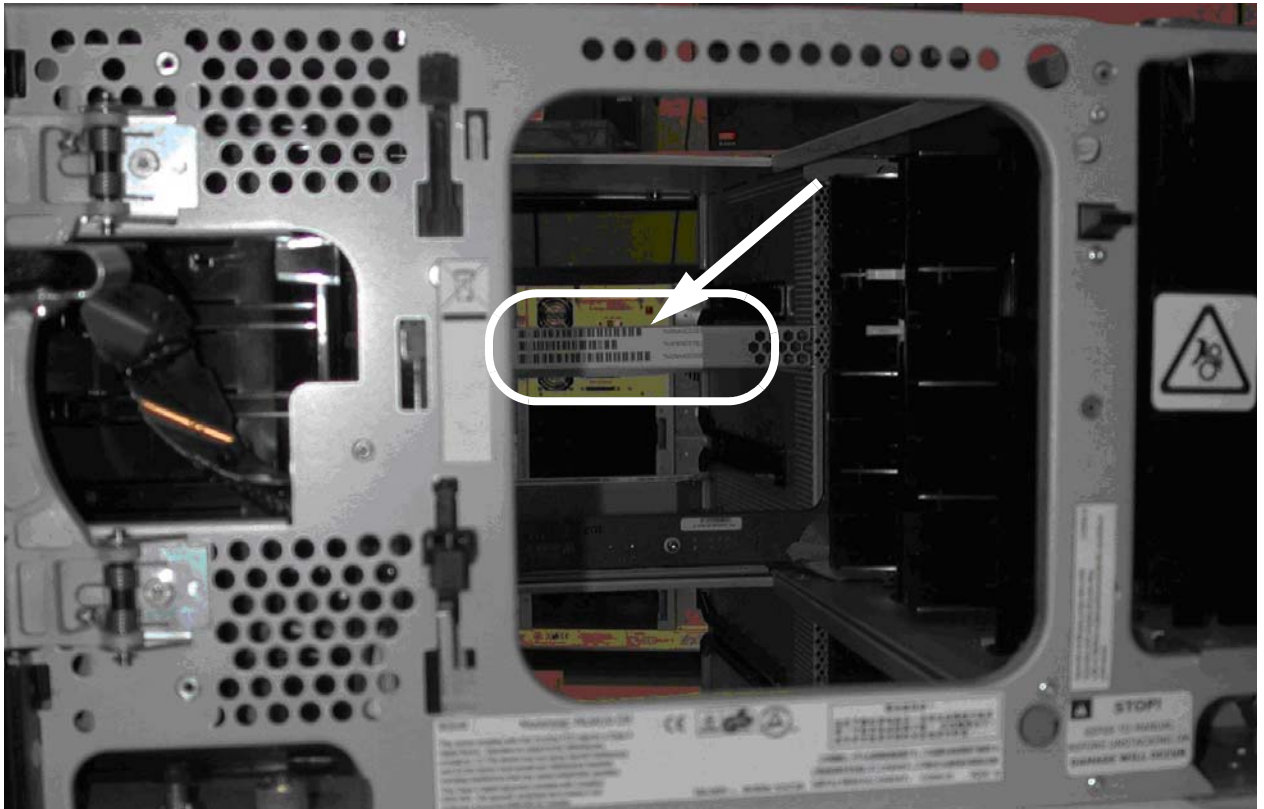
Figure 61 Scalar i500
SN/WWN Label

You can also find the serial number on the library as follows:

- **Operator panel** — Select **Tools > About Library**.

- **Web client** — Select **Reports > System Information**. The serial number is in the **Physical Library** table in the **Serial Number** column.

Replacing an Expansion Module

These instructions explain how to remove and replace an expansion module. You may need to replace the expansion module if its chassis is severely damaged.

A library can use up to four expansion modules to a maximum height of 41U.

There are some configuration settings to take into account when removing and replacing an expansion module.

- COD licenses remain the same. After the expansion module is removed, there may be more slots licensed than are available. Only the available slots appear on the **License** screen.

- All resources in the removed module(s) are removed. A partition with all resources in the removed module(s) will be present with no slots or drives. This partition can only be deleted.

> **Note:** The maximum number of expansion modules supported in a library depends on the level of firmware the library is running. See Updating Library and Tape Drive Firmware on page 278 for more information.

Warning: All libraries taller than 14U must be installed in a rack having a main protective earthing (grounding) terminal, and power must be supplied via an industrial plug and socket-outlet and/or an appliance coupler complying with IEC 60309 (or an equivalent national standard) and having a protective earth (ground) conductor with a cross sectional area of at least 1.5 mm^2 (14 AWG).

To ensure proper airflow and access space, Allow 60 cm (24 inches) in the front and back of the library.

Warning: Without tape drives, tape cartridges, or power supplies, a control module weighs approximately 60 lbs (27.2 kg). An expansion module, without tape drives, tape cartridges, or power supplies, exceeds 65 lbs (29.5 kg).

To avoid serious injury, at least two people are required to safely lift the modules.

**Removing the 9U
Expansion Module**

1 Before removing the module, follow the instructions in <u>Preparing to
Remove or Replace a Module</u> on page 356.

2 Starting with the topmost module of your library, open the I/E
station and access doors of each module.

Caution:	Before unstacking the modules, the robot assembly must be parked as described in <u>Preparing to Remove or Replace a Module</u> on page 356.

3 Disengage the Y-rails so the modules can be unstacked safely.

1	Front Y-rail
2	Rear Y-rail
3	Y-rail (this end up)
4	Squeeze here to release

     a From the front of the library, find the Y-rail release mechanism, which is located on the left side of the control module. Squeeze the handle of the Y-rail release mechanism, lift it, and release it so that it locks into place.

1	Y-rail in locked, non-functional position

     b From the rear of the library, find the rear Y-rail release mechanism located in the interior of the right side of the module. Squeeze the handle of the Y-rail release mechanism, lift it, and release it so that it locks into place.

4 Remove the rack ears that fasten the module to the rack. See <u>Installing the Library in a Rack</u> on page 417 for detailed instructions on using the rack ears.

5 Loosen the thumbscrews located at the base of the front of the module.

| 1 | Thumbscrews (behind doors) |

6 Loosen the two thumbscrews located at the base of the back of the module.

7 Open the module's access door and raise the guide pin by pulling it up and turning it slightly as if it were a screw. Otherwise, the guide pin may scratch the front doors of the module beneath it.

8 From the front of the library, slide the entire module toward you and lift it off of the module below it.

9 Repeat these procedures for each module that you need to remove.

10 Remove and replace the cover plates, if appropriate.

> **Caution:** Before removing the control module's bottom cover plate, the robot assembly must be parked as described in <u>Preparing to Remove or Replace a Module</u> on page 356.

a If you plan to stack the control module at the top of the library, and if a 9U expansion module will be located below it, remove the control module's bottom cover plate and the 9U expansion module's top plate.

b If you plan to stack the control module between 9U expansion modules, remove both the top and bottom plates of the control module. Also remove the top plate of the 9U expansion module located below the control module and the bottom plate of the 9U expansion module located above the control module.

c If you plan to stack the control module at the bottom of the library, and if a 9U expansion module will be located above it, remove the control module's top plate and the 9U expansion module's bottom plate.

Replacing the 9U Expansion Module

1 Remove all tape drives from the expansion module that you are adding. See <u>Adding, Removing, and Replacing Tape Drives</u> on page 438 for instructions on removing tape drives.

2 Remove the power supplies from the expansion module that you are adding. See <u>Adding, Removing, and Replacing Power Supplies</u> on page 414 for instructions on removing power supplies.

3 Open the expansion module's access door and raise the guide pin by pulling it up and turning it slightly as if it were a screw. Otherwise, the guide pin may scratch the front doors of the module on which you are stacking it.
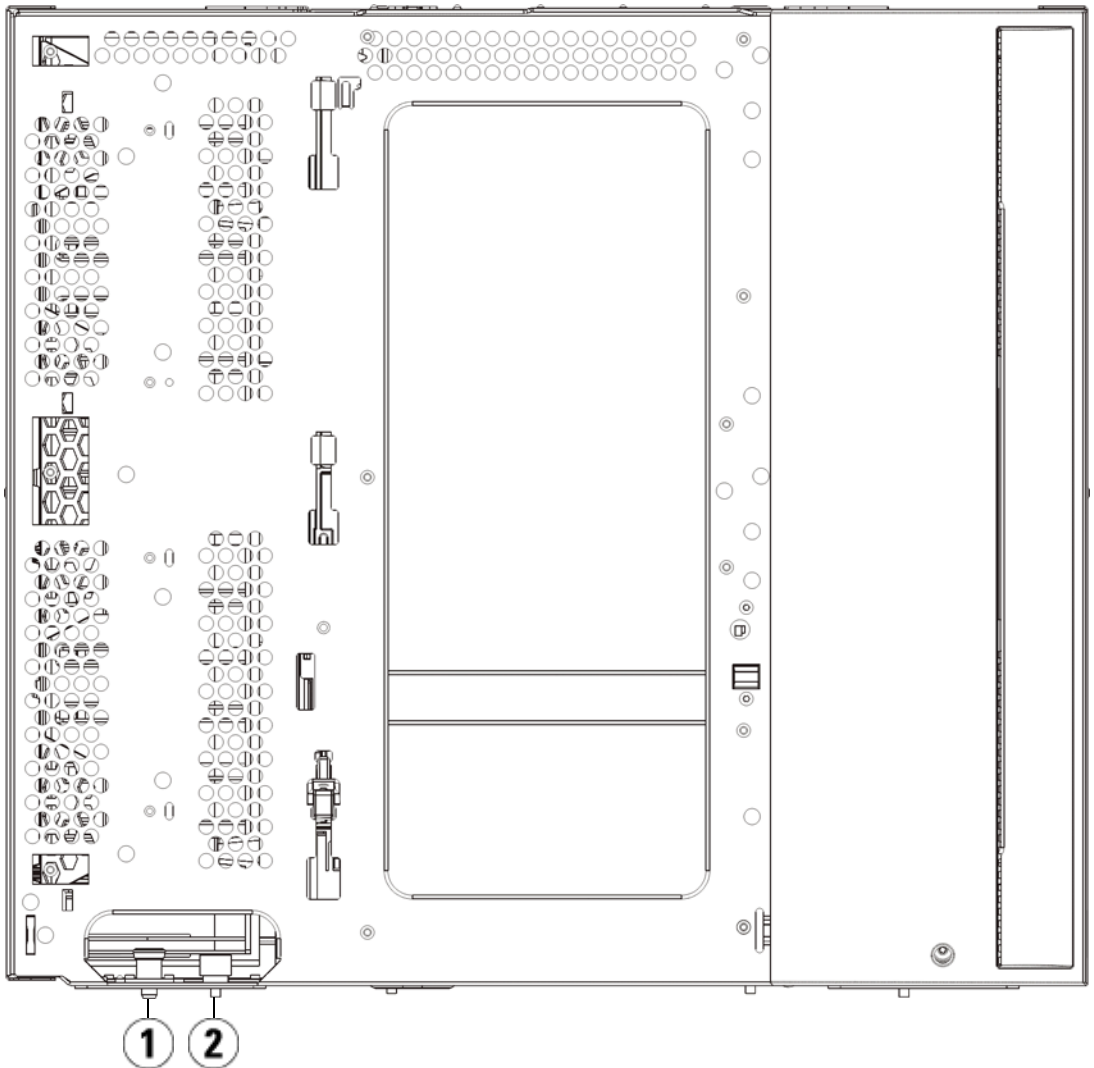
1	Guide pin
2	Thumbscrew

4 Lift the new expansion module and, from the front of the library, place it in the desired location.

5 Fasten the module to the rack with rack ears.

6 Secure the two modules together by tightening the two thumbscrews at the base of the front of the module and the two thumbscrews located at the base of the back of the module. Then lower the module's guide pin (located at the base of the front of the module) by turning it and pushing it down.

7 Tighten all thumbscrews located at the base of the front and back of the modules.

8 Engage the Y-rails of each module in your library configuration. Ensure that the Y-rails are properly aligned and the thumbscrews are tightened.

1	Front Y-rail
2	Rear Y-rail
3	Y-rail (this end up)
4	Squeeze here to release

a From the front of the library, open the I/E station and access doors of the expansion module. Squeeze the handle of the Y-rail release mechanism, lift it out of its locked position, and slide it downward as far as it will go.

| 1 | Y-rail in unlocked, functional position |

b From the back of the library, find the rear Y-rail release mechanism, which is located in the interior of the right side of the module. Squeeze the handle of the Y-rail release mechanism, lift it out of its locked position, and slide it downward as far as it will go.

Doing this aligns the Y-rails with the Y-rails of the module beneath it.

> **Caution:** Check to make sure that there is no gap between the top and bottom Y-rails on both the front and back of the library. If a gap exists, the library cannot mechanically initialize.

9 Unpark the robot assembly.

    a Gently raise the robot assembly so that it no longer rests on the parking tab.

> **Caution:** Support the robot assembly by holding onto the broad metal X-axis plate. Lifting the robot by the thin metal rod will bend the rod. Lifting the robot by the black plastic picker body can damage the robot.

    b With your free hand, move the parking tab in a clockwise direction until it stops in the "unparked" position. When in the correct position, the parking tab is removed completely from the interior of the module and will not accidentally swing into the path of the robot.

    c Gently release the robot assembly. It will lower to the bottom module of the library.

| 1 | Parking tab in "unparked" position |

Preparing to Use the 9U Expansion Module

1 Close the library's I/E station and access doors.

2 Add the tape drives to the modules. For details, see <u>Adding, Removing, and Replacing Tape Drives</u> on page 438.

3 Add the power supplies. For details, see <u>Adding, Removing, and Replacing Power Supplies</u> on page 414.

4 If your library contains FC I/O blades, install both the I/O blades and the accompanying fan blades in the expansion module. For details, see <u>Adding, Removing, and Replacing FC I/O Blades</u> on page 443 and <u>Adding, Removing, and Replacing the FC I/O Fan Blade</u> on page 454.

5 Connect all power cords, network data cables, and module-to-module cables. Make sure the module terminators are installed at the top and bottom of the stack of modules. For cabling instructions, see <u>Cabling the Library</u> on page 289.

6 Power on the library.

7 Re-create partitions, cleaning slots, and I/E station slots as desired.

8 Import tape cartridges to the correct partitions as needed.

9 Save the library configuration (see <u>Saving the Library Configuration</u> on page 489.

10 If the host application inventories the location of each tape cartridge in the library, open the host application and reinventory in order to sync its logical inventory with the physical inventory of the library.

Removing and Replacing the Library Control Blade and LCB Compact Flash Card

The library control blade (LCB) manages the entire library, including the operator panel and robot, and is responsible for running system tests to ensure that the library is functioning properly.

The LCB compact flash card contains important information about your library configuration. If you replace the compact flash card, then you need to reconfigure your library. You have two options:

- Replacing the LCB/Compact Flash Card or Compact Flash Card Only
- Replacing the LCB Only

Contact Quantum Support to determine which component(s) you need to replace and which set of instructions to follow.

Replacing the LCB/Compact Flash Card or Compact Flash Card Only

Contact Quantum Support to help you determine whether to replace the LCB and compact flash card together, or to replace just the compact flash card. The instructions for both options are nearly identical, except that for a compact flash card-only replacement, you will reuse the existing LCB and replace only the compact flash card within it. You will still need to upgrade firmware as described below.

Equipment Required

- Ethernet Cable.
- Host PC or laptop connected to the Scalar i500 library.
- Current Scalar i500 library firmware file saved to your host PC or laptop. Contact Quantum Support for the firmware, if needed.Latest library configuration saved on PC or laptop.

Instructions

The Compact Flash Card is new and has never been initialized. It contains only a minimal level of library firmware which allows the library to boot up and display an Upgrade Notification message. Once you install the LCB/compact flash card, you will need to upgrade firmware and reconfigure your network settings.

> **Note:**   Do not separate the old compact flash card from the library control blade (unless you are replacing the compact flash card only). Return the old LCB/compact flash card as a pair to Quantum.

1 If possible, save the library configuration (see <u>Saving the Library Configuration</u> on page 489).

2 Power off the library.

3 Disconnect all cables from the existing LCB. You may want to label each cable that is connected to the existing LCB to make sure that you can correctly reconnect them to the new LCB.

4 Remove the existing LCB from the library.

To remove the existing LCB, release both of the LCB latch hooks and, using the latch hooks as handles, pull the entire LCB toward you.
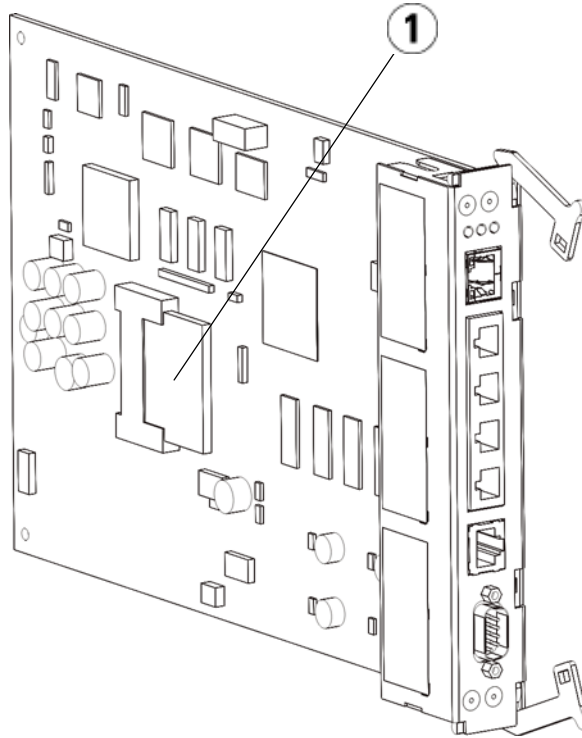
1	LCB compact flash card

5 If the new LCB and compact flash card came in discrete packages, insert the new compact flash card into the new LCB (or, if replacing the compact flash card only, remove the existing compact flash card and install the new one in the existing LCB).

6 Insert the new LCB into the vacant LCB slot on the back of the library.

When inserting the new LCB into the slot, be sure that the LCB LEDs are located at the top of the blade, and that the latch hooks are on the right side of the blade.

When sliding the new LCB into the slot, there should be no resistance.

> **Caution:** Do not force the LCB into the slot or damage may occur.

7 After inserting the new LCB, secure it by depressing both of the LCB latch hooks into the blade. The LCB will fit snugly into its slot.

8 Reconnect all cables to the new LCB.

9 Power on the library.

The green power light on the front panel turns on. The screen may remain dark for up to 5 minutes. Then an "Initialization In Progress" screen displays. The initialization process can take up to 30 minutes depending on library configuration.

> **Caution:** From this point forward until the process is complete, do NOT remove power from the library! Doing so may cause failure and cause LCB to become unusable.

When initialization is complete, the screen will display "Upgrade Notification: Compact Flash Replacement" screen shown below.
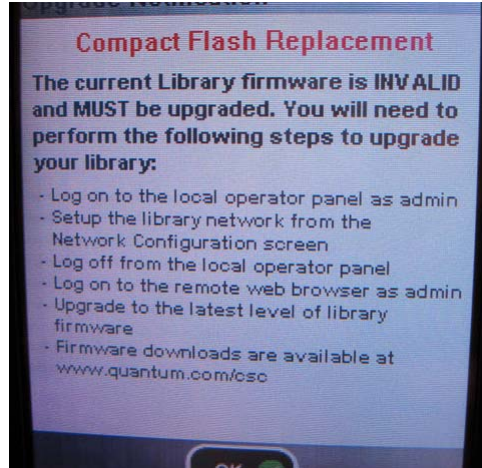
10 Click **OK**.

The login screen appears.

11 Enter the following default user name and password:

- User name: **admin**

- Password: **password**

12 Press **OK**.

The Enable IPv6 screen appears.
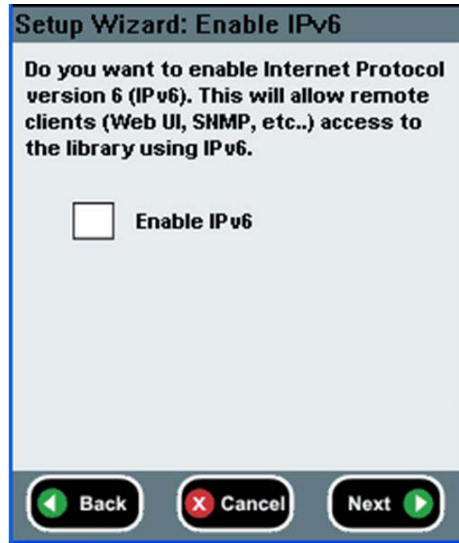
13 Select the **Enable IPv6** check box if you are required to use IPv6 or leave the check box blank to not enable it.

14 Press **Next**.

The Network Configuration screen appears. The system defaults to DHCP. For IPv4 only, you can deselect the DHCP option and assign a static IP address. You cannot assign a static IP address for IPv6.

Setup Wizard: Network Configuration

Your library has the following name and network settings. You can edit these settings or accept them.

Library Name: [   ]

Network Settings:

Use DHCP: (●)

_____OR_____

IP Address: [   ]

Subnet Mask: [   ]

Def. Gateway: [   ]

(Back)   (X Cancel)   (Apply ✓)

15 Accept the default settings by pressing **Apply**, or make any changes to the network settings, and then press **Apply**.

The progress window displays a "Success" message when complete.

16 Press **Close**.

The next screen lists one or more IP addresses assigned to the library.

17 Write down the IP addresses. You will need them to log in from your Web browser.

18 Click **Close**.

The system logs you out and you return to the login screen.

Caution:	The installation is NOT complete at this point. Install current library firmware following the steps below. Firmware Installation can take up to 1 hour to complete. DO NOT remove power from the library during this process.

19 Open a Web browser on the host PC and type the following in the address bar:

http://<ipaddress>/

where **ipaddress** is one of the IP addresses assigned to the library that you wrote down earlier.

A screen appears, displaying the current version of library firmware.
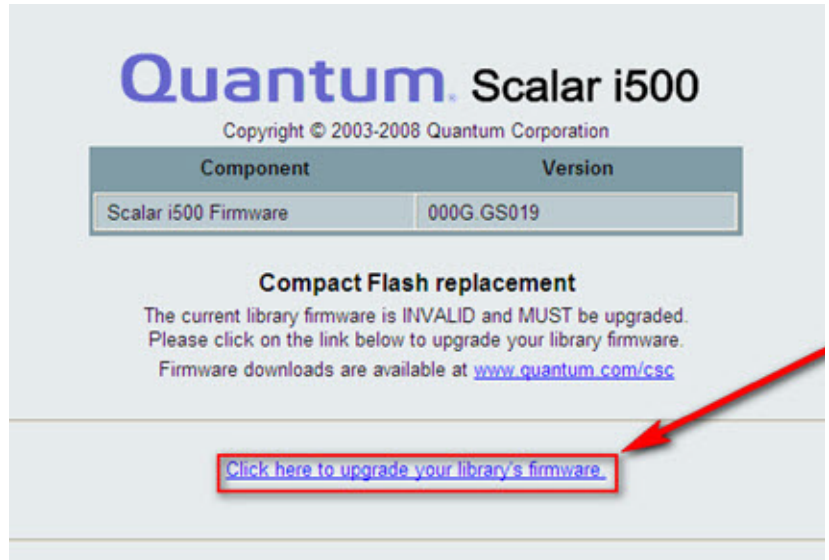
20 Click the **Click here to upgrade your library's firmware** link.

The Tools - Update Library Firmware screen appears.
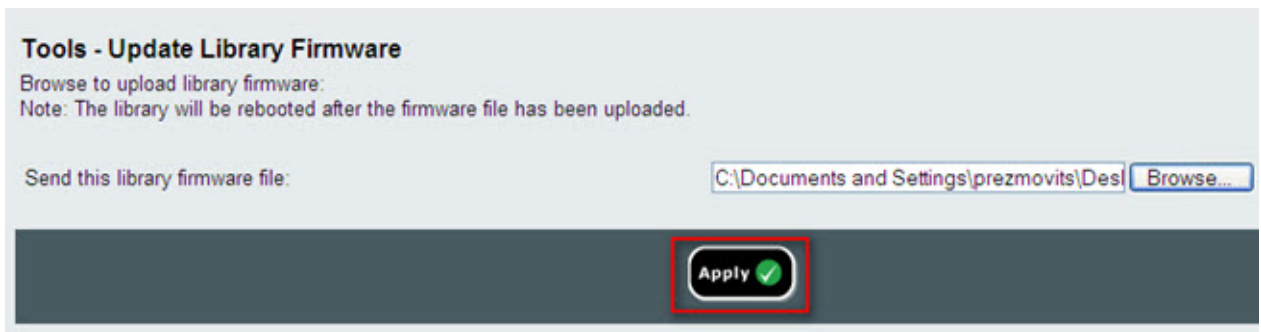
21 Click **Browse** to retrieve the .tgz firmware file from the location on your computer, then click **Apply**.

A dialog box appears asking you to confirm it is OK to reboot the library.

22 Click **OK**.

The screen displays "WORKING" in the Progress Window.

Once the Firmware has been transferred from the computer to the library the login screen appears.

Caution:	The appearance of the login screen on the Web browser does NOT mean the firmware upgrade has completed on the library; it is just an indication that the firmware image has been moved to the LCB/compact flash card. A 14U library with six tape drives installed can take up to 50 minutes to complete this process. Actual time may vary. You will not be able to log in until the firmware upgrade is complete.

Caution:	Do NOT remove power from the library while the firmware is upgrading.

The library operator panel may display the following "upgrade in progress" message; or it may blank out or change multiple times during the firmware upgrade process.

23 When the firmware upgrade is complete, the login screen appears on the operator panel.

24 Enter the following default user name and password:

- User name: **admin**

- Password: **password**

25 Press **OK**.

The Setup Wizard screen appears.

> **Note:** At this point the Scalar i500 Library is set up with factory default settings.

26 Reconfigure your library settings as they were before.

> **Caution:** Contact Quantum Support before restoring the configuration. In general, it is recommended that you use the setup wizard to manually reconfigure the library. It is not recommended to use the "restore configuration" tool to restore the previous settings. Doing so will completely reinstall the former library firmware level and potentially any defective configuration settings encountered prior to installing the new LCB/compact flash card combo. If you do restore a previous configuration and downrev firmware, you will need to install the latest version of firmware again.

Replacing the LCB Only

These instructions explain how to replace the LCB while reusing the existing LCB compact flash card.

Required tools: None

1 Power off the library.

2 Access the back of the library and locate the existing LCB.

3 Disconnect all cables from the existing LCB. You may want to label each cable that is connected to the existing LCB to make sure that you can correctly reconnect them to the new LCB.

4 Remove the existing LCB from the library.

To remove the existing LCB, release both of the LCB latch hooks and, using the latch hooks as handles, pull the entire LCB toward you.

5 Remove the existing LCB compact flash card from the existing LCB.
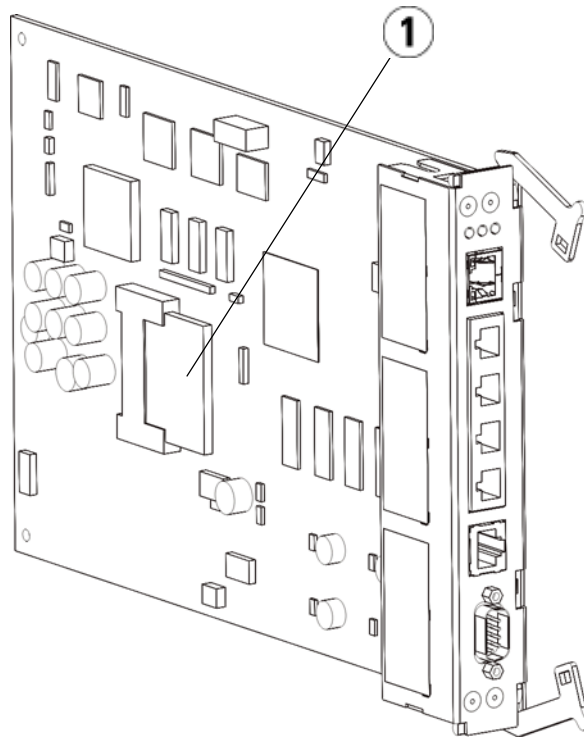
1   LCB compact flash card

6 Insert the existing LCB compact flash card into the new LCB.

7 Insert the new LCB (with existing LCB compact flash card) into the vacant LCB slot on the back of the library.

When inserting the new LCB into the slot, be sure that the LCB LEDs are located at the top of the blade, and that the latch hooks are on the right side of the blade.

When sliding the new LCB into the slot, there should be no resistance.

| **Caution:**	Do not force the LCB into the slot or damage may occur.

8 After inserting the new LCB, secure it into the control module by depressing both of the LCB latch hooks into the blade. The LCB will fit snugly into its slot.

9 Reconnect all cables to the new LCB.

10 Power on the library.

The green power light on the front panel turns on. The screen may remain dark for up to 5 minutes. Then an "Initialization In Progress" screen displays.

11 Check the status of the LCB LEDs. All of its LEDs (blue, amber, and green) should be solidly lit for a short period of time.

Adding, Removing, and Replacing Power Supplies

Library power is controlled at the individual power supplies and at the front panel of the library. The switch on the rear of each power supply shuts down power at the input of the individual power supplies. The switch on the front of the control module provides power to all control module and 9U expansion module power supplies. You can also turn off library power using the Web client, if necessary.

Adding a Redundant Power Supply

These instructions explain how to add a second (redundant) power supply to a module. You may need to add a redundant power supply to the library to make sure that the library does not go down (and become inaccessible) if its original power supply happens to fail. The library automatically uses the redundant power supply if the first power supply fails for any reason.

> **Note:** The control module and each expansion module with drives must use at least one power supply. You can add a redundant power supply to each module.
>
> Installing one power supply in one module and another power supply in another module does not provide redundant power; the two power supplies must reside within the same module.

Required tools: None

1 Save the library configuration (see <u>Saving the Library Configuration</u> on page 489).

2 Locate the vacant power supply slot and remove the cover plate. Save the cover plate in case the redundant power supply needs to be removed at a later date.

3 Insert the new power supply into the vacant slot.

4 When inserting the power supply, make sure that you insert it correctly with its on/off switch located at the bottom of the supply, below the handle. The power supply must be level to slide in smoothly.

5 Tighten the power supply's thumbscrews to secure the power supply to the library module.

6 Plug in the power supply cord.

7 Turn on the power supply's power, using the switch on the rear of the power supply.

8 Check the status of the power supply's LEDs. The top green LED and the blue LED should be solidly lit.

9 Power on the library.

10 Check the status of the power supply's LEDs. The two green LEDs should be solidly lit, and the blue LED should be off.

Permanently Removing a Redundant Power Supply

These instructions explain how to remove a redundant power supply from the control module. You may need to remove the second power supply if it is no longer necessary for the library.

Required tools: None

1 Save the library configuration (see <u>Saving the Library Configuration</u> on page 489).

2 Access the back of the library, and locate the power supply that you want to replace.

3 Turn off the power supply's power, using the switch on the rear of the power supply.

4 Disconnect the power supply cord from the power supply and from its source.

5 Loosen the power supply's thumbscrews.

6 Remove the power supply by gripping the power supply handle and pulling it toward you.

7 Install a cover plate over the vacant power supply slot.

Removing and Replacing a Power Supply

These instructions explain how to remove a power supply and replace it with a new one. You may need to replace a power supply if there are problems with one that is currently in use.

If the library has a redundant power supply, you can replace the power supply without powering off the library. If the library has only one power supply, you must power off the library before performing this procedure.

Required tools: None

1 Save the library configuration (see <u>Saving the Library Configuration</u> on page 489).

2 If the library does not use a second (redundant) power supply, power off the library.

3 Access the back of the library, and locate the power supply that you want to replace.

4 Turn off the power supply's power, using the switch on the rear of the power supply.

5 Disconnect the power supply's power cord.

6 Loosen the power supply's thumbscrews.

7 Remove the power supply by gripping the power supply handle and pulling it toward you.

8 Insert the new power supply into the vacant power supply slot.

When inserting the power supply, make sure that you insert it correctly with its on/off switch located at the bottom of the supply, below the handle. The power supply must be level to slide in smoothly.

9 Tighten the power supply's thumbscrews to secure the power supply to the library module.

10 Reconnect the power supply's power cord.

11 Turn on the power supply's power.

12 Check the status of the power supply's LEDs. The top green LED and the blue LED should be solidly lit.

13 Power on the library.

14 Check the status of the power supply's LEDs. The two green LEDs should be solidly lit, and the blue LED should be off.

Installing the Library in a Rack

All Scalar i500 libraries taller than 14U must be installed in a rack. The rack secures the bottom module, and all other modules are then secured to the bottom module.

The rackmount kit secures your library within a rack. These instructions explain how to install your stand-alone library into a rack and how to install additional modules into an existing rack.

Installing the modules into the rack requires at least two people.

Warning:	All libraries taller than 14U must be installed in a rack having a main protective earthing (grounding) terminal, and power must be supplied via an industrial plug and socket-outlet and/or an appliance coupler complying with IEC 60309 (or an equivalent national standard) and having a protective earth (ground) conductor with a cross sectional area of at least 1.5 mm^2 (14 AWG). To ensure proper airflow and access space, Allow 60 cm (24 inches) in the front and back of the library.

Warning:	Under no circumstances should a rack be moved while loaded with one or more modules.

> **Warning:** Without tape drives, tape cartridges, or power supplies, a control module weighs approximately 60 lbs (27.2 kg). An expansion module, without tape drives, tape cartridges, or power supplies, exceeds 65 lbs (29.5 kg).
>
> To avoid serious injury, at least two people are required to safely lift the modules.

> **Note:** The rackmount kit cannot be used with every type of rack. Racks with threaded rails or unique hole spacing, for example, may not support the rackmount kit. In addition, the rack must have rail spacing (front to rear) of between 605 mm (23.8 in.) and 770 mm (30.3 in.).
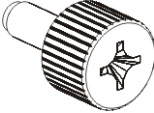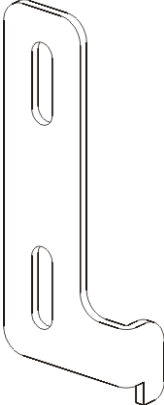
Preparing for Installation

Required tools: None

1 Before beginning installation, verify the contents of the rackmount kit (see Table 9) and the rack ear kit (see Table 10).

- You only need one rackmount kit per library. The rackmount kit allows you to secure the bottom module in the rack. It includes rack ears for additional security.

- You need one rack ear kit for each additional module. Each rack ear kit contains the supplies to install right and left rack ears on one module.

- You must install one set of rack ears for each module in the rack.

Table 9 Rackmount Kit Contents

Component	Description	Quantity
	Small ferrule — Used in racks with round holes	10 (8 required; 2 spares)

Component	Description	Quantity
	Large ferrule — Used in racks with square holes	10 (8 required; 2 spares)
	Thumbnut — Secures the rack shelves to the rack	8
	M5 thumbscrew — Secures the rack ears	4
	Rack ear, left — Holds the modules in the rack	1
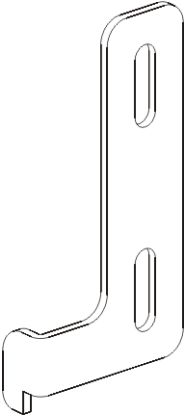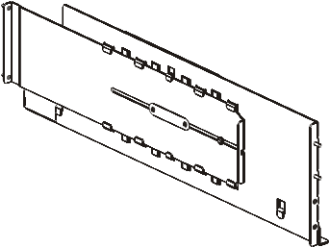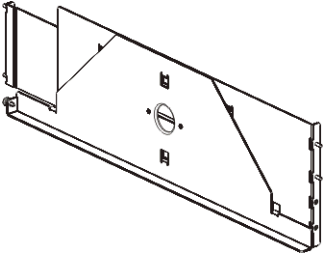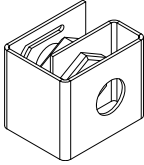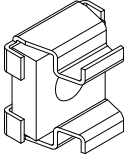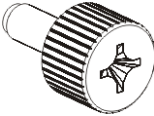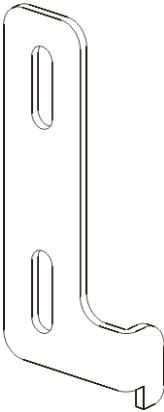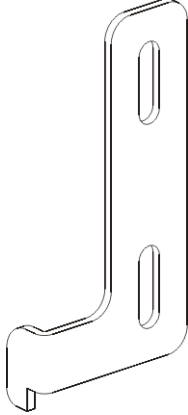
Component	Description	Quantity
	Rack ear, right — Holds the modules in the rack	1
	Rack shelf, left — Secures the modules in the rack	1
	Rack shelf, right— Secures the modules in the rack	1

Table 10   Rack Ear Kit
Contents

Component	Description	Quantity Required
	Nut clip — Used in racks with square holes	4
	Cage nut — Used in racks with round holes	4
	M5 thumbscrew — Secures the rack ears	4
	Rack ear, left — Holds the modules in the rack	1

Component	Description	Quantity Required
	Rack ear, right — Holds the modules in the rack	1

2 Remove all rack hardware that may interfere with the installation of the rackmount kit and the modules that you plan to add to the rack.

3 Consider removing the front and back doors of the rack to obtain full access to the mounting holes and other areas of the rack.

4 Determine the type of rack in which you plan to install the rackmount kit. Different racks require different rackmount parts. Although the rackmount kit contains many parts, the parts you use depend on your rack's mounting holes.

   a If the rack has round mounting holes, use the small ferrules and the nut clips.

   b If the rack has square mounting holes, use the large ferrules and the cage nuts.

   c If the rack has threaded (tapped M6) holes, do not use the ferrules, nut clips, or cage nuts.

5 Determine where in your rack you want to install the rackmount shelves.

   Consider installing the shelves at a height that puts the base of the control module anywhere between the 28U-32U alignment markers, which is usually a comfortable height for reading the operator panel. Remember, the control module can be placed anywhere within the

library configuration above, below, or between any expansion modules. However, for recommended configuration, see <u>Installing a New Multi-Module Library Configuration</u> on page 326.

Installing the Rackmount Shelves

Required parts: Rackmount shelves, (8) ferrules, (8) thumbnuts

1 If the rackmount shelves are extended, collapse them to their smallest size. It is easier to fit and position the shelves within the rack when the shelves are compact.

> **Note:** Extending the shelves can be difficult, but they are designed to be resized by hand. Do not use tools to resize the shelves, and never take them apart.

2 Place a ferrule on the end of each stud, and screw it on completely. The larger side of the ferrule should face the rack shelf, and the tapered end should face out. Be sure to use the proper size ferrule as described in <u>Preparing for Installation</u> on page 418.
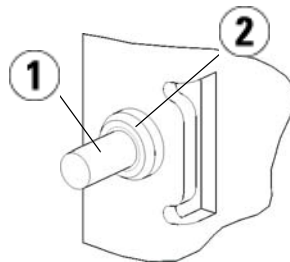
1   Stud
2   Ferrule

3 Install the rackmount shelves into the rack so that they are level with one another.

   a Install the shelf's rear studs in the rack's rear mounting holes.
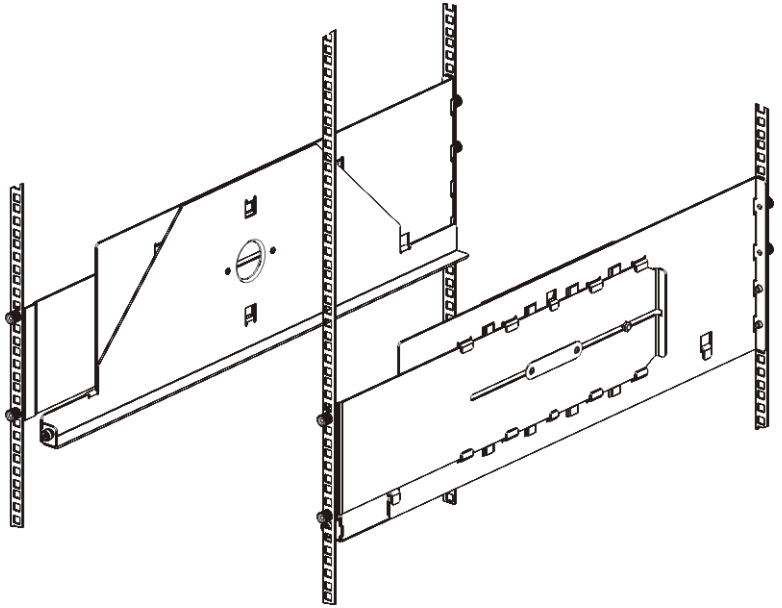
   b Position the shelf to the appropriate side of the rack (right or left) and align the shelf at the desired height.

   c Insert the shelf's rear studs into the rack's rear mounting holes.

   d Fasten a thumbnut to the end of each stud. Secure the rack tightly, so that the ferrule fits snugly within the hole in the rack.

   e Next, install the shelf's front studs in the rack's front mounting holes.
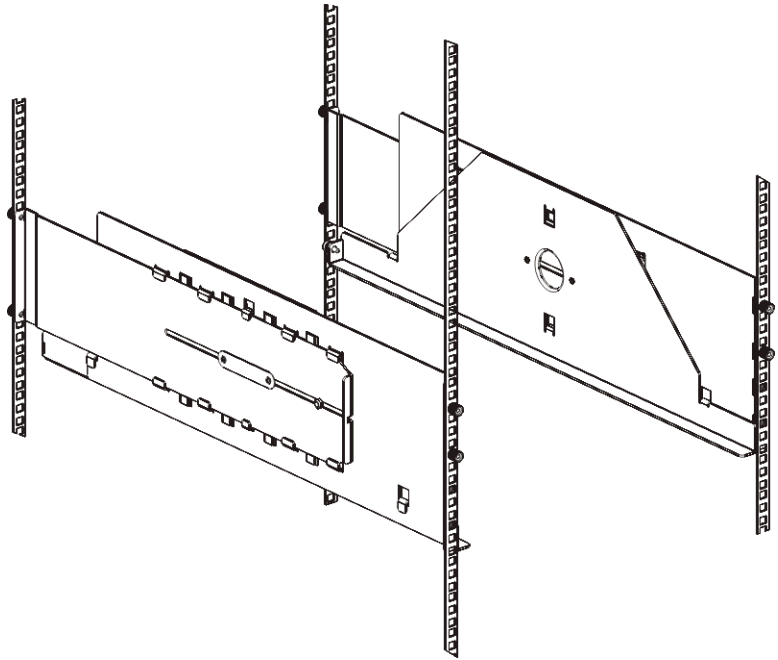
    f If the studs do not reach the mounting holes, pull the front of the shelf toward you to extend it to the necessary length. Hold the base of the shelf with one hand, and pull the extensible part of the shelf with your other hand.

> **Note:** Extending the shelves can be difficult, but they are designed to be resized by hand. Do not use tools to resize the shelves, and never take them apart.

    g Insert the shelf's front studs into the rack's front mounting holes.

    h Fasten a thumbnut to the end of each stud. Secure the rack tightly, so that the ferrule fits snugly within the hole in the rack.

4 Visually make sure that both shelves are level, and that they are aligned properly within the rack.

5 Make sure that all thumbnuts are fastened tightly. Some thumbnuts may have loosened during installation.

**Preparing Modules for
Rack Installation**

1 Power off your library and disconnect all power cords, network data
cables, and module-to-module cables.

2 Remove all tape cartridges, tape drives, power supplies, and all cords
and cables from the library modules. The modules are much easier to
lift into the rack without the additional weight of the tape drives.

Warning:	Without tape drives, tape cartridges, or power supplies, a control module weighs approximately 60 lbs (27.2 kg). An expansion module, without tape drives, tape cartridges, or power supplies, exceeds 65 lbs (29.5 kg).
	To avoid serious injury, at least two people are required to safely lift the modules.

3 Park the robot assembly in the control module. (Regardless of which
module you are installing, the robot must be parked in the control
module before you begin moving the modules into the rack.)

a Open the I/E station and access doors of each module.

b Using your hands, gently lift the robot assembly into the control
module. The robot assembly should glide slowly and with some
resistance.

Caution:	Support the robot assembly by holding onto the broad metal X-axis plate. Lifting the robot by the thin metal rod will bend the rod. Lifting the robot by the black plastic picker body can damage the robot.

c After raising the robot assembly to the approximate middle of the
control module, hold it in place with one hand and, using your
other hand, move the parking tab in a counter-clockwise
direction until it stops in the "parked" position. The metal
parking tab is located at the bottom of column 1.

d Gently lower the robot assembly to rest on the parking tab.

1	Parking tab in "parked" position

Installing the Bottom Module in the Rack

Required parts: Rack ears, (4) M5 thumbscrews

Explanation of parts: Each rack ear contains two elongated holes, enabling you to fasten it to the rack (using the M5 thumbscrews) in the most accessible mounting holes.

1 Place the desired module (whichever module you want to be the bottom module of the library) onto the rack-mount shelves. From the front of the rack, lift the module onto the shelf and gently slide it into the rack. Slide the module to the back of the rack, so that the front of the module is flush with the mounting holes.

2 From the back of the rack, secure the module to the rack-mount shelves by tightening the two silver thumbscrews that are attached to the rear of the rack-mount shelves.

3 Install the right rack ear. At the front of the library:

   a Open the I/E station door. At the lower right corner of the module is a vertical slot. Insert the hinge of the right rack ear into the slot and then position the holes of the rack ear flush with the rack rail.
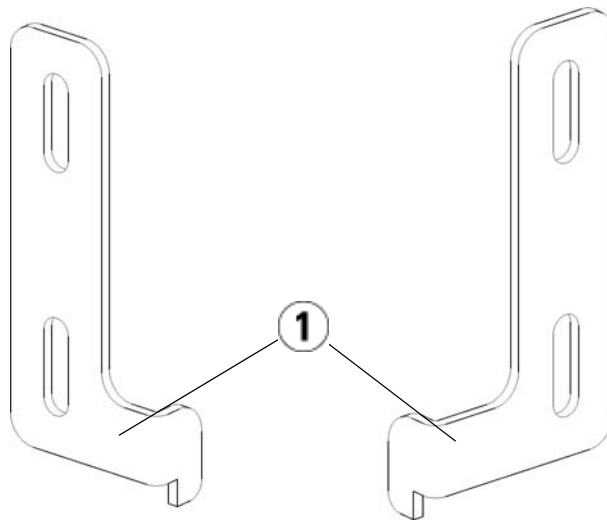
1	Hinge of rack ears

   b Using two M5 thumbscrews, fasten the rack ear to the rack. The thumbscrews should thread through the holes in the rack shelves and fasten completely and evenly.
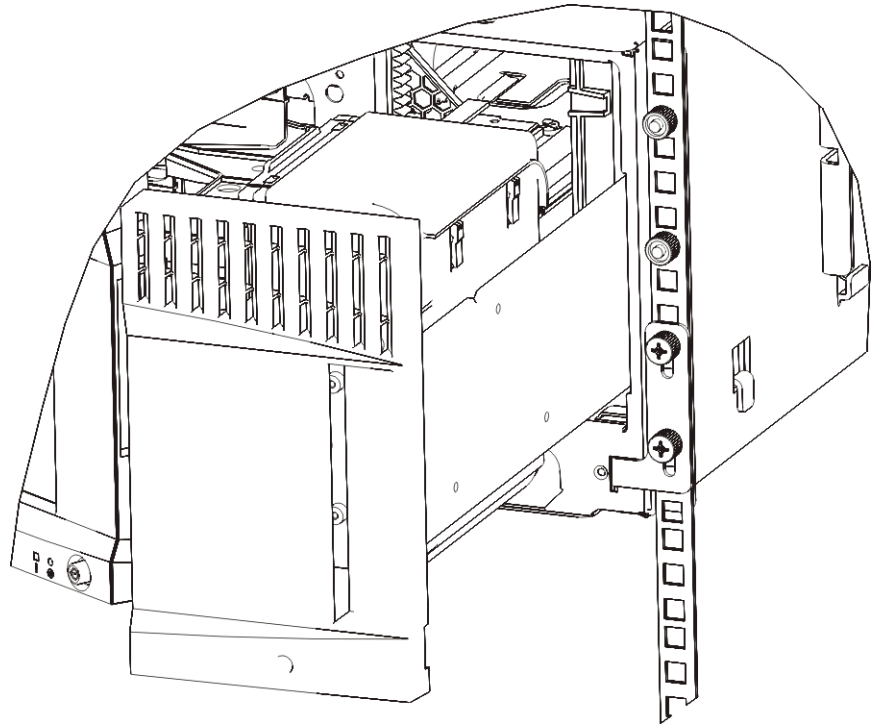
4 Install the left rack ear.

    a With the I/E station door open, open the left door (the access
door) of the module and locate the slot in the lower left corner of
the module. (The flexible door hinge allows the door to be pulled
away from the module, providing access to the slot.)

> **Note:** You may need to pull the door toward you in order to
> access the slot.

    b Install the left rack ear in the same manner as the right rack ear.

    c Using two M5 thumbscrews, fasten the rack ear to the rack. The
thumbscrews should thread through the holes in the rack shelves
and fasten completely and evenly.
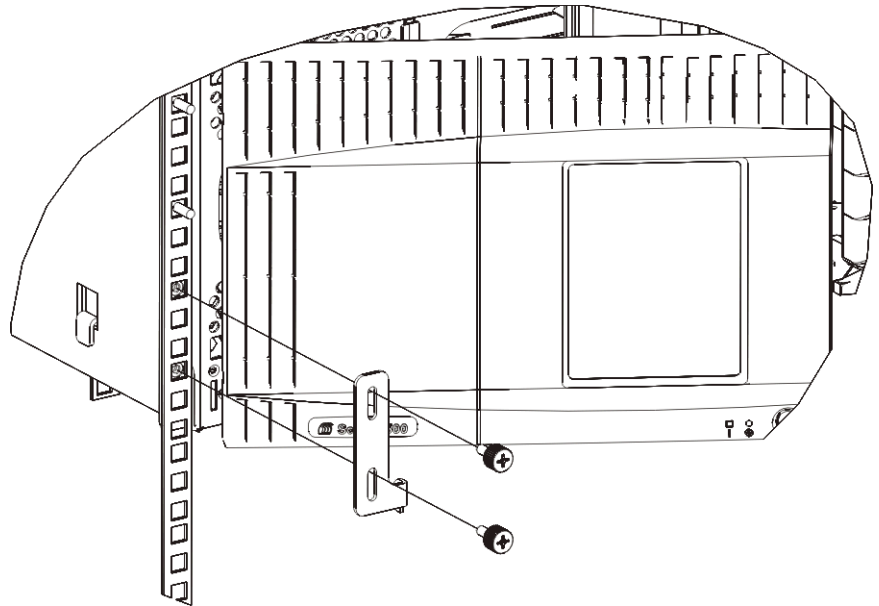
5 If you are only installing one module (a control module5U Library Control Module), unpark the robot assembly now. For instructions, see step 1 on page 336. If you are installing more modules, proceed to the next step and do not unpark the robot assembly yet.

6 Close the module's doors.

7 Install the remaining modules of your library (if any), following the instructions in <u>Installing Additional Modules Into the Rack</u> on page 431.

8 Reinstall the tape drives, power supplies, and tape cartridges in the library.

9 Cable your library as necessary, following the instructions provided in <u>Cabling the Library</u> on page 289.

10 Power on the library.

Installing Additional Modules Into the Rack

All modules that you add to the rack must be positioned above the module that you previously installed, since the bottom module must be secured to the rackmount shelves (unless you decide to uninstall the entire library from the rack and reconfigure it).

Required parts: Rack ears, (4) M5 thumbscrews, (4) nut clips or (4) cage nuts

Explanation of parts: Each rack ear contains two elongated holes, enabling you to fasten it to the rack (using the M5 thumbscrews and either the nut clips or cage nuts) using the most accessible mounting holes.

1 If you are installing a module above a module that currently has a top cover, remove the top cover. Similarly, if the module you are installing has a bottom cover, remove the bottom cover before installing the module above another module in the rack. You need to make sure the library is "hollow" all the way through with just one bottom cover on the lowest module and one top cover on the top module. See Installing the New 9U Expansion Module on page 347.

2 Determine where in the rack to install the nut clips (or cage nuts).

> **Note:** Consider using the following method to determine where to install the nut clips (or cage nuts) rather than adding the module to the rack first. If you add the module to the rack first, installing the nut clips (or cage nuts) can be difficult because rack space has become restricted.

a If you are adding a module above a previously racked expansion module, count nine full units from the location of the expansion module's rack ears, and prepare to install the nut clip (or cage nut) to that location on the rack.

For example, if the expansion module's rack ears are located at 1U and 2U, then the nut clips (or cage nuts) should be installed at 10U and 11U.

Next, determine which holes you must use within the 10U and 11U markers. Notice that each rack unit (U), as delineated by the alignment markers in the rack, contains three mounting holes. If you are adding a module anywhere above the control module, position the nut clip (or cage nut) at the middle hole in that unit. If you are adding a module anywhere below the control module, position the nut clip (or cage nut) at the upper hole in that unit.

   b If you are adding a module directly above a previously racked
   control module, count five full units from the location of the
   control module's rack ears, and prepare to install the nut clip (or
   cage nut) to that location on the rack.

   For example, if the control module's rack ears are located at 1U
   and 2U, then the nut clips (or cage nuts) should be installed at 6U
   and 7U.

   Next, determine which holes you must use within the 6U and 7U
   markers. Notice that each rack unit, as delineated by the
   alignment markers in the rack, contains three mounting holes. If
   you are adding a module anywhere above the control module,
   position the nut clip (or cage nut) at the middle hole in that unit.
   If you are adding a module anywhere below the control module,
   position the nut clip (or cage nut) at the upper hole in that unit.

3 Install the nut clips (or cage nuts) to the desired location in the rack.

   Installing nut clips:

   a Hold the nut clip so that its semi-circle design faces outside the
   rack.

   b Push the nut clip onto the rack's mounting holes so that the nut is
   behind the rack's holes. (After the nut clip is installed, you can
   slide it up and down the mounting holes, if necessary.)

   Installing cage nuts:

   a Hold the cage nut so that its hinges face outside the rack, and so
   that its hinges clasp the upper and lower portions of the square
   hole.

   b Place the cage nut in the desired hole. Insert one hinge in the hole
   first, then pinch the cage nut and push it into the hole until it
   snaps into place. (You may want to use a screwdriver to help
   push the hinge into the hole.)

4 Prepare the module to be stacked in the rack.

   a Power off the module and disconnect all power cords, network
   data cables, and module-to-module cables.

   b Consider removing all tape drives from the module. Modules are
   much easier to lift into the rack without the additional weight of
   the tape drives.

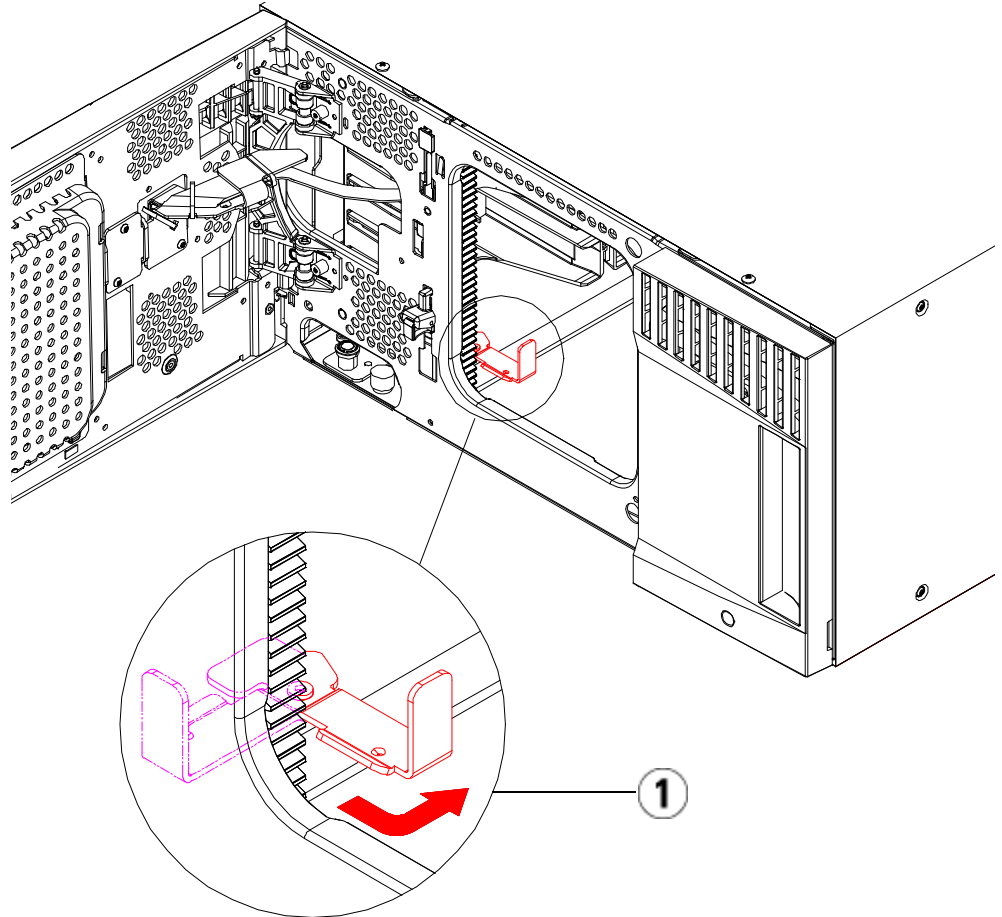   **c** Open the module's access door and raise the guide pin by pulling it up and turning it slightly as if it were a screw. Otherwise, the guide pin may scratch the front doors of the module on which you are stacking it.
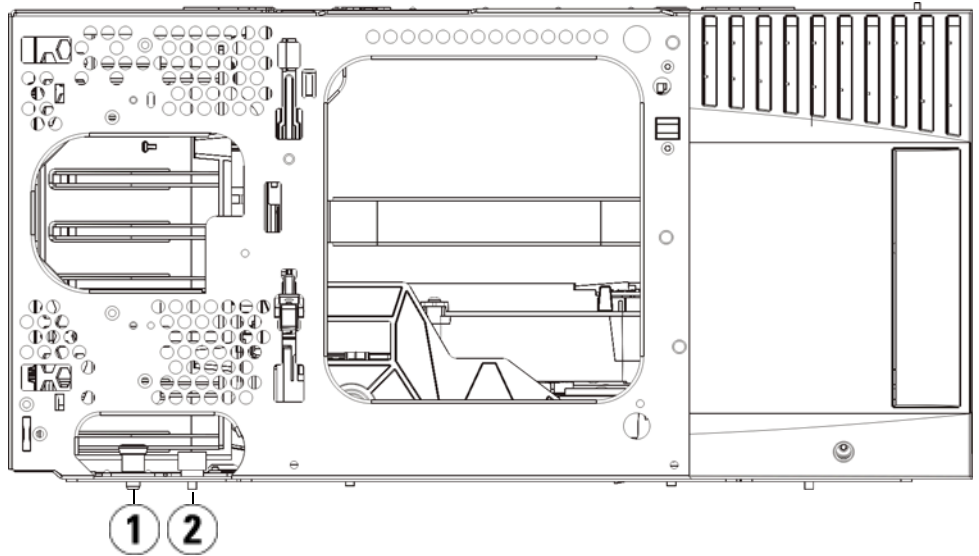
1	Guide pin
2	Thumbscrew

5 Lift the module, align it so that it is parallel with the module below it, and slide it into place.

6 Lower the module's guide pin by turning it and pushing it down.

7 Secure the module to the module beneath it by tightening the thumbscrews located at the base of the front and back of the module. Press down the thumbscrew, and then tighten it.
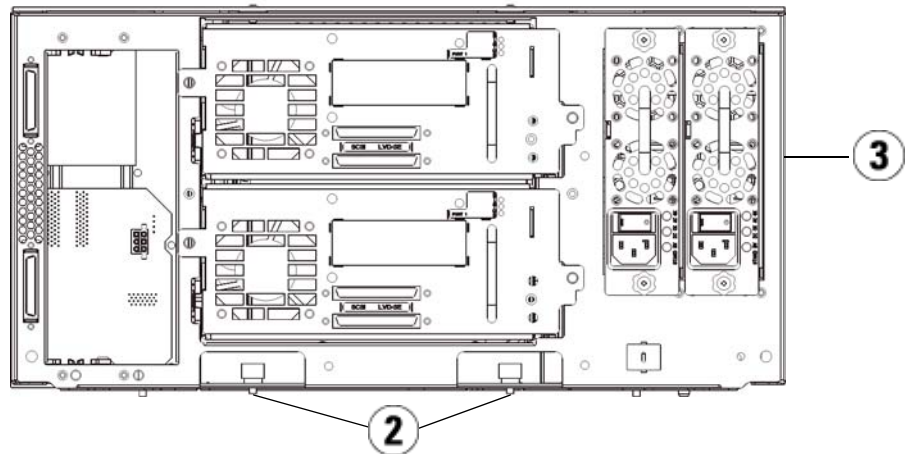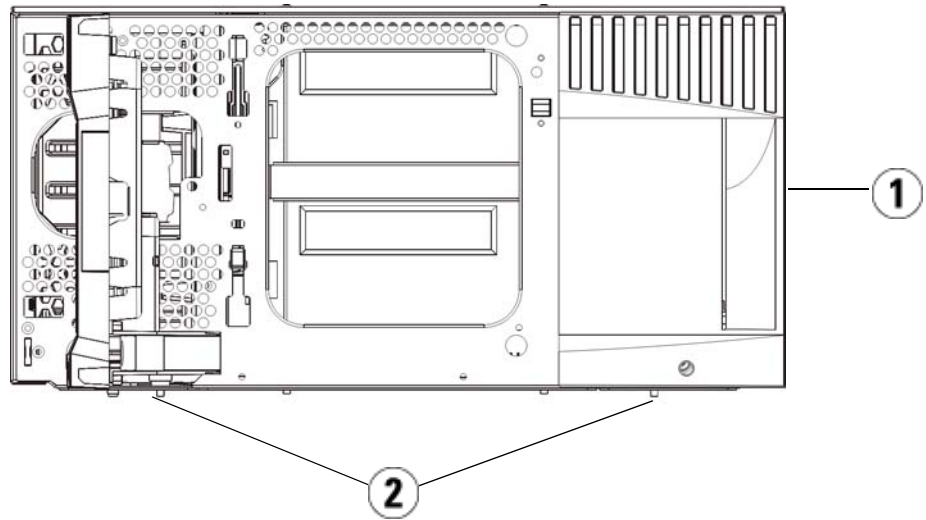
1	Control module (front)
2	Thumbscrews
3	Control module (rear)

8 Install the right rack ear. At the front of the library:

  a Open the I/E station door. At the lower right corner of the module is a vertical slot. Insert the hinge of the right rack ear into the slot and then position the holes of the rack ear flush with the rack rail.
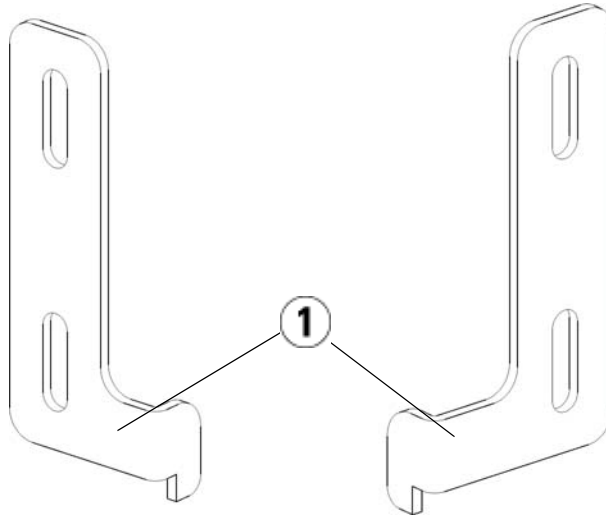
1	Hinge of rack ears

  b Using two M5 thumbscrews, fasten the rack ear to the rack. The thumbscrews should thread through the nut clips (or cage nuts) and fasten completely and evenly.
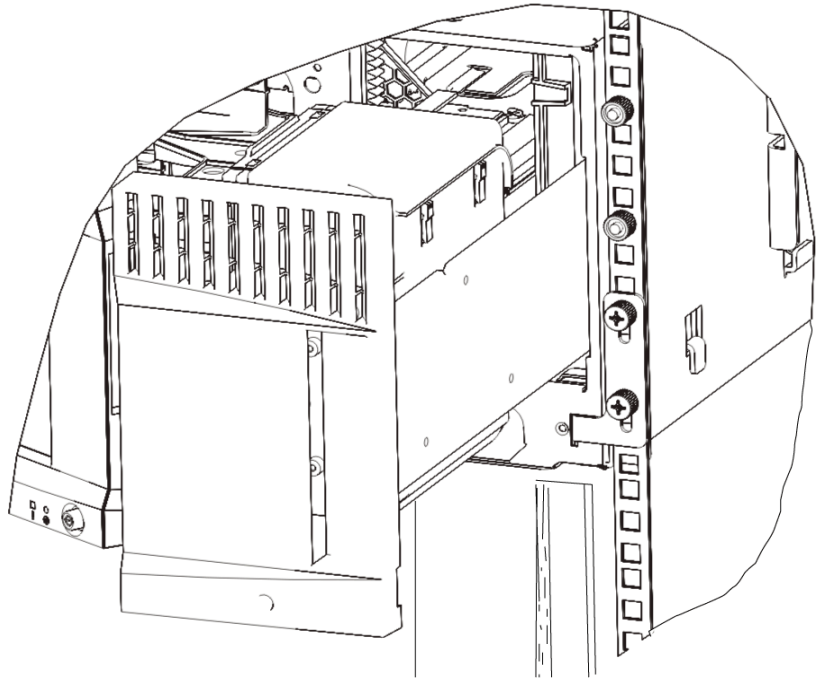
9 Install the left rack ear.

    a With the I/E station door open, open the left door (the access door) of the module and pull the door toward you in order to access the slot located in the lower left corner of the module. (The flexible door hinge allows the door to be pulled away from the module, providing access to the slot.)

> **Note:**   You may need to pull the door toward you in order to access the slot.

    b Install the left rack ear in the same manner as the right rack ear.

    c Using two M5 thumbscrews, fasten the rack ear to the rack. The thumbscrews should thread through the nut clips (or cage nuts) and fasten completely and evenly.
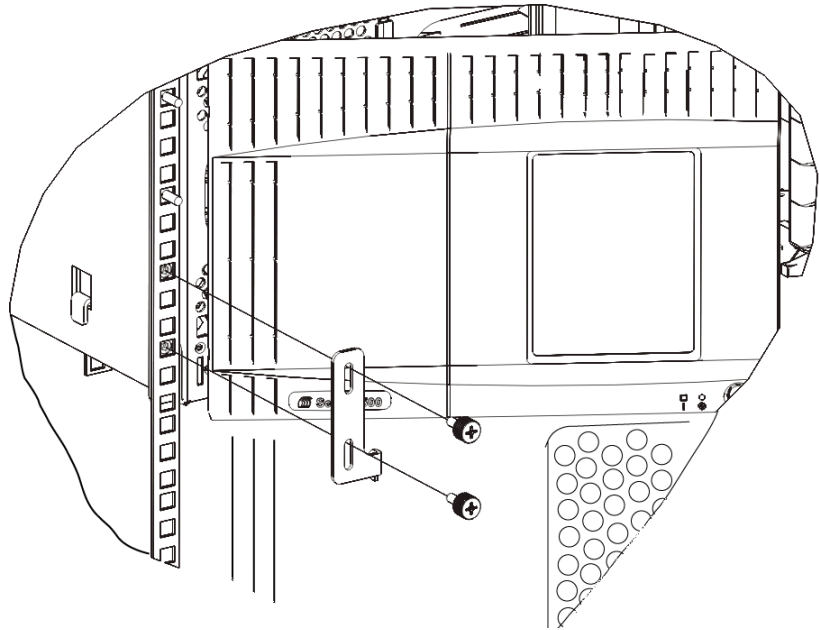
10 Close the module's doors.

11 Reinstall the tape drives to the library.

12 Cable your library as necessary, following the instructions provided
in <u>Cabling the Library</u> on page 289.

13 Power on the library.

Adding, Removing, and Replacing Tape Drives

The tape drive always resides in a universal drive sled (UDS), and together they are effectively one unit. If you order a new or replacement tape drive, it will already be installed in a sled.

> **Note:** If you are installing multiple tape drives with the library powered on, follow the special instructions in the note in below.

Adding a Tape Drive

These instructions explain how to add a tape drive to your library. You can add a tape drive while the library is powered on.

Required tools: None

1 Save the library configuration (see).

2 Detach the tape drive slot's cover plate. Loosen the cover plate's thumbscrews and remove the plate.

   Store the cover plate in a separate cabinet. If you later decide to remove the tape drive, you will need to reinstall the cover plate.

3 Insert the tape drive into the drive slot. Using the guide rails on both the tape drive and in the tape drive slot, slowly slide the tape drive into the slot. The tape drive must be level to slide in smoothly.

> **Note:** **Special Instructions for Installing Multiple Tape Drives:**
> If you are installing multiple tape drives with the library powered on, do not push the drive in all the way yet. Instead, push it in almost all the way, leaving it out approximately 3 inches so that it does not connect with the library's backplane. Then partially insert all of the other new tape drives in the same manner. When all the new tape drives are partially inserted, push them all the way in at the same time.

4 Tighten the tape drive's thumbscrews to secure the tape drive to the module.

The thumbscrews must be aligned with the module's screw holes. If they are not aligned, the tape drive was not inserted correctly.

5 Power on the library (if it is not powered on already).

6 If the green LED is solidly lit for three seconds and then blinks twice, wait 10-15 minutes while the universal drive sled (UDS) firmware upgrades.

There are two types of firmware related to the tape drive: firmware for the tape drive itself, and firmware for the UDS that surrounds the tape drive. The UDS firmware is part of the library firmware. The library automatically upgrades the UDS firmware if the firmware on the newly inserted UDS is different than the library's current UDS firmware. Firmware downloads may take about 15 minutes.

7 Connect the host interface cables to the tape drive.

8 Take the tape drive online.

    a From the **Operations** menu, select **Drive > Change Mode**.

       The **Change Drive Mode** screen appears.

    b Locate the tape drive that you want to take online.

    c In the **New** column, click **Offline** to change the button status to **Online**.

9 Check the tape drive's LEDs to make sure that the drive functions correctly (see Tape Drive LEDs on page 505. If the blue or amber LED stays on solid, reseat the tape drive.

10 Add the new tape drive to an appropriate partition. You cannot use the tape drive until it is assigned to a partition.

11 If necessary, upgrade tape drive firmware by following the instructions provided in Updating Library and Tape Drive Firmware on page 278. The library can use the tape drive immediately after the firmware is upgraded.

12 Due to the way the library logically addresses its tape drives internally (see Understanding Logical Element Addressing on page 35), adding a tape drive to the library may change the tape drive ordering, and this can affect proper communication to a controlling host. Because of this, you must refresh the configuration of any backup application that manages the library to reflect the

adjusted tape drive positions and the presence of the new drive. In addition, you may need to reboot the host server(s) or rescan the bus to detect the changes.

Permanently Removing a Tape Drive

These instructions explain how to remove a tape drive that you do not intend to replace with another one. You may want to permanently remove a tape drive from your library if you are decreasing the size of your SAN or reducing the number of partitions in your library.

You can remove a tape drive while the library is powered on. Do not, however, remove a tape drive that is currently in use.

Required tools: None

1 Prepare host applications for tape drive removal.

2 Save the library configuration.

3 If there is a tape cartridge in the target tape drive, use the Web client to unload it.

4 Using the Web client, delete the partition that uses the target tape drive. Then re-create the partition, if desired, using another tape drive.

5 Disconnect the host interface cables from the tape drive that you want to remove.

6 From the back of the library, loosen the tape drive's thumbscrews.

7 Remove the tape drive by gripping the tape drive handle and pulling the entire tape drive toward you.

8 Install a cover plate over the vacant tape drive slot.

If you cannot find a cover plate, contact Quantum Support to order one. It is important that all vacant slots have a cover plate to keep unwanted materials out of the library.

> **Warning:** Running the library without a cover plate can be dangerous. Doing so also causes the library to run at a reduced speed.

9 Due to the way the library logically addresses its tape drives internally (see Understanding Logical Element Addressing on page 35), permanently removing a tape drive from the library may

change the tape drive ordering, and this can affect proper communication to a controlling host. Because of this, you must refresh the configuration of any backup application that manages the library to reflect the adjusted tape drive positions and the presence of the new drive. In addition, you may need to reboot the host server(s) or rescan the bus to detect the changes.

Removing and Replacing a Tape Drive

These instructions explain how to remove a tape drive and replace it with a new one. You may need to replace a tape drive if you are experiencing problems with one that is currently in use.

You can remove a tape drive while the library is powered on. Do not, however, remove a tape drive that is currently in use.

The new tape drive replaces the old tape drive in the partition. You do not need to delete the old tape drive or add the new tape drive to the partition, unless the replacement tape drive is of a different type (generation, interface, or vendor) than the original. If the original tape drive is in a partition, and the replacement tape drive is of a different type, the library generates a RAS ticket will not activate the tape drive. If this happens, you must either replace the tape drive with one of the same type, or delete the old tape drive from the partition and then add the new tape drive to the partition (see <u>Modifying Partitions</u> on page 73).

Required tools: None

 1 Prepare host applications for tape drive removal.

 2 Save the library configuration.

 3 If there is a cartridge in the tape drive, use the Web client to unload it.

 4 Using the Web client, take the tape drive offline. When the tape drive is ready for removal, its blue LED will be solidly lit.

   a From the **Operations** menu, select **Drive > Change Mode**.

      The **Change Drive Mode** screen appears.

   b Locate the tape drive that you want to take offline.

   c In the **New** column, click **Online** to change the mode to **Offline**.

 5 Disconnect the host interface cables from the tape drive that you want to remove.

 6 From the back of the library, loosen the tape drive's thumbscrews.

7 Remove the tape drive by gripping the tape drive handle and pulling the entire tape drive toward you.

8 Add the new tape drive in the vacant slot. Using the guide rails on both the tape drive and the tape drive slot, slowly slide the tape drive into the slot. The tape drive must be level to slide in smoothly.

9 Tighten the tape drive's thumbscrews to secure the tape drive to the module.

The thumbscrews must be aligned with the module's screw holes. If they are not aligned, the tape drive was not inserted correctly.

10 Power on the library (if itis not powered on already) and wait for initialization to complete.

11 If the green LED is solidly lit for three seconds and then blinks twice, wait 10-15 minutes while the universal drive sled (UDS) firmware upgrades.

There are two types of firmware related to the tape drive: firmware for the tape drive itself, and firmware for the UDS that surrounds the tape drive. The UDS firmware is part of the library firmware. The library automatically upgrades the UDS firmware if the firmware on the newly inserted UDS is different than the library's current UDS firmware. Firmware downloads may take about 15 minutes.

12 Connect the host interface cables to the tape drive.

13 Take the tape drive online.

    a From the **Operations** menu, select **Drive > Change Mode**.

       The **Change Drive Mode** screen appears.

    b Locate the tape drive that you want to take online.

    c In the **New** column, click **Offline** to change the mode to **Online**.

14 Check the tape drive's LEDs to make sure that the drive functions correctly (see Tape Drive LEDs on page 505. If the blue or amber LED stays on solid, reseat the tape drive.

15 If necessary, upgrade tape drive firmware by following the instructions provided in the Updating Library and Tape Drive Firmware on page 278. The library can use the tape drive immediately after the tape drive firmware is upgraded.

16 When swapping out a tape drive, if the **Logical SN Addressing** feature is enabled, the library reports a logical tape drive serial number to the host that remains with the slot, so a replacement tape drive in the

same slot reports the same logical serial number and the host recognizes it immediately (see Tape Drive Logical SN Addressing on page 127). If **Logical SN Addressing** is disabled, the library reports the actual tape drive serial number to the host, so a swapped tape drive will not be registered by the host unless you refresh the configuration of any backup application that manages the library. In addition, you may need to reboot the host server(s) or rescan the bus to detect the changes.

Adding, Removing, and Replacing FC I/O Blades

This section describes adding, removing, and replacing FC I/O blades. The FC I/O blades support connections to LTO-2, LTO-3, LTO-4, LTO-5 and LTO-6 FC drives.

Caution:	If you are adding a new FC I/O blade or completely removing an FC I/O blade, be sure to read Working With Control Paths on page 86. If you do not configure control paths correctly, you will experience communication problems with tape drives and media changer devices (partitions).

Details about FC I/O blades include:

- You must be running 400-level code or above in order to use FC I/O blades.

- Each expansion module can support up to two FC I/O blades.

- A maximum of four FC I/O blades can be present in any library configuration.

- A maximum of four FC drives can be connected to one FC I/O blade.

- FC I/O blades cannot be installed in control modules. However, FC tape drives in the control module can be connected to FC I/O blades in an expansion module.

- Each FC I/O blade is accompanied by a fan blade that cools the FC I/O blade. The fan blade is installed to the right of the FC I/O blade in the expansion module. Each expansion module has four bays and can accommodate two FC I/O blades and two fan blades. <u>Figure 62</u> shows the FC I/O blade and fan blade installed in the expansion module. For instructions on installing the fan blade, see <u>Adding, Removing, and Replacing the FC I/O Fan Blade</u> on page 454.

- The recommended order of installing the FC I/O blade and fan blade in any expansion module is starting from the bottom two bays and moving up.

Figure 62 FC I/O Blade and
Fan Blade Bays in an
Expansion Module
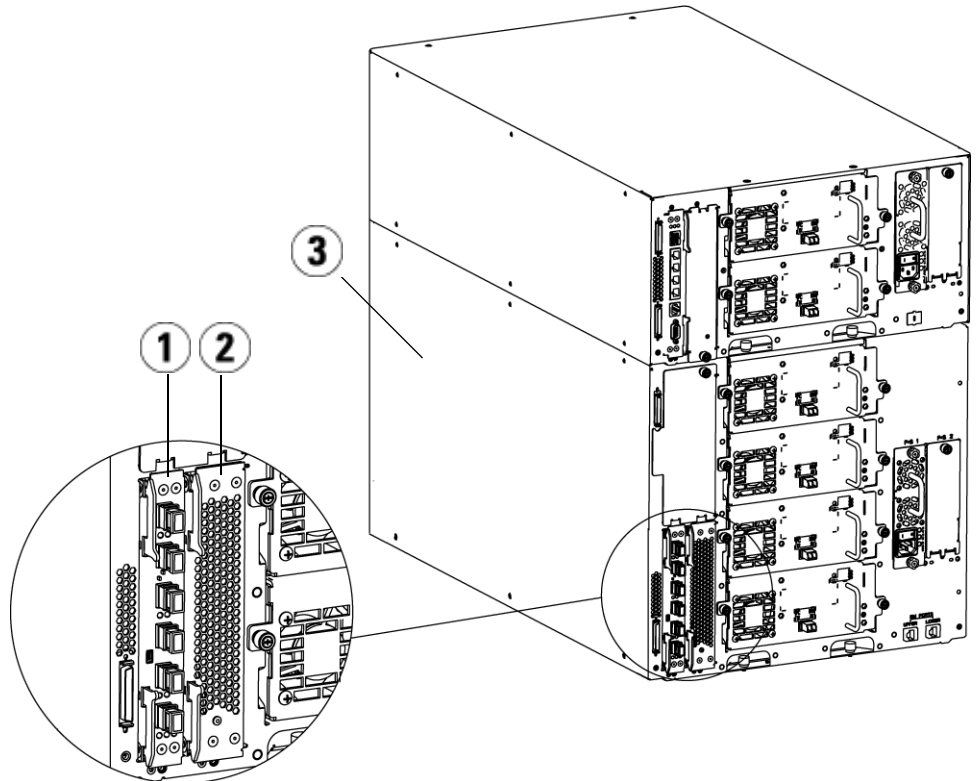
1	FC I/O blade
2	Fan blade
3	Expansion module

**Read This First:
Complete Installation
Steps**

When installing an FC I/O blade, you must follow the installation steps in this order or communication with the FC I/O blade and tape drives in the library will not work properly.

Caution:	If you are adding a new FC I/O blade or completely removing an FC I/O blade, be sure to read Working With Control Paths on page 86. If you do not configure control paths correctly, you will experience communication problems with tape drives and media changer devices (partitions).

You may perform the following steps with the library powered on.

1 Ensure you are running 400-level firmware or above.

2 Save the library configuration (see Saving the Library Configuration on page 489).

3 Connect the Ethernet cable from the Library Control Blade to the expansion module(s). For each FC I/O blade installed in an expansion module, connect the expansion module containing the FC I/O blade(s) to a port in the Ethernet hub on the LCB (see Figure 48 on page 310).

Caution:	If the Ethernet cable between the LCB and the expansion module is not connected when power is applied to the blade, the blade will hang in the "Booting" state.

• If the FC I/O blade is installed in the bottom bay of the expansion module, connect one end of an Ethernet cable to the Ethernet port labeled **LOWER** in the lower right corner of the expansion module. Connect the other end of the cable to a port in the Ethernet hub on the LCB.

• If the FC I/O blade is installed in the upper bay of the expansion module, connect one end of an Ethernet cable to the Ethernet port labeled **UPPER** in the lower right corner of the expansion module. Connect the other end of the cable to a port in the Ethernet hub on the LCB.

4 Remove the control path from tape drives that you plan to connect to an FC I/O blade. You must not allow an FC tape drive to serve as control path if it is connected to an FC I/O blade. If you do, the

control path will be filtered out by the I/O blade and will not be visible to the host. If a Fibre Channel tape drive is currently serving as the control path for a partition and you plan to connect that tape drive to an FC I/O blade, you must remove the control path from that tape drive. To remove the control path from a tape drive:

a Select **Setup > Control Path** from the operator panel or the Web client.

b If you have more than one partition, select the appropriate partition and click **Next**.

c Clear the control path selection on any FC tape drive that you plan to connect to an FC I/O blade.

5 Add or replace the fan blade(s) following the instructions in <u>Adding, Removing, and Replacing the FC I/O Fan Blade</u> on page 454. The fan blade is required to prevent overheating of the FC I/O blade.

6 Add or replace the FC I/O blade(s) following the instructions in <u>Adding an FC I/O Blade</u> on page 448 or <u>Replacing an FC I/O Blade</u> on page 453. If you are installing two FC I/O blades in an expansion module, install the lower one first.

7 Make sure cover plates are installed over any unused bays in the expansion module.

8 Connect the library and tape drive cables to the FC I/O blade (see <u>Figure 48</u> on page 310). See also <u>Recommended Library Cabling for FC I/O Blades</u> on page 313.

9 Configure/reconfigure library partitions if needed (from the Web client, select **Setup > Partitions**).

10 Configure control paths if needed. The library assigns control paths for new partitions when they are created. Ensure that each partition has only one control path. Ensure that you do not select an FC tape drive as the control path if it is connected to an FC I/O blade. See <u>Working With Control Paths</u> on page 86 for more important information about control paths. To modify the control path, select **Setup > Control Path** from the operator panel or Web client.

11 Configure host mapping (optional). If you have more than one FC I/O blade in the library, each FC I/O blade will present each partition that does not have a tape drive as the control path as a target device to the host. Thus the host may see the same partition multiple times. To minimize confusion, you should configure host mapping so that each host sees each device only once. For more information, see

the Host Mapping - Overview on page 116 and Configuring Host Mapping on page 118. To configure host mapping:

    a From the operator panel or Web client, select **Setup > FC I/O Blades > FC I/O Blade Control** and enable host mapping.

    b From the operator panel or Web client, select **Setup > FC I/O Blades > Host Mapping**.

12 Configure host port failover on the FC I/O blade (optional). From the Web client, select **Setup > FC I/O Blades > Host Port Failover**. To enable host port failover, you must configure target ports 1 and 2 on the FC I/O blade as point-to-point connections (**Setup > FC I/O Blades > Port Configuration**). For more information, see Configuring FC Host Port Failover on page 119.

13 Save the library configuration (see Saving the Library Configuration on page 489).

Adding an FC I/O Blade

These instructions explain how to add an FC I/O blade to your library. You can add an FC I/O blade while the library is powered on.

Required tools: None

1 Access the back of the expansion module.

> **Note:** The recommended order of installing the FC I/O blade and fan blade in an expansion module is starting from the bottom bay and moving up.

2 Remove the cover plate from the appropriate bay.

3 Press up and out to open the latch hooks on each side of the FC I/O blade.
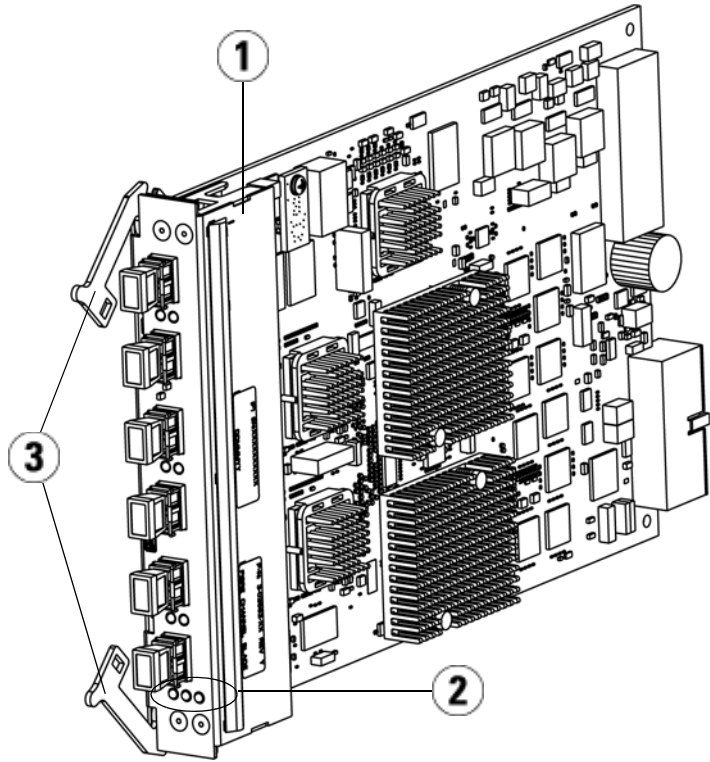
1	FC I/O blade
2	LEDs
3	Latch hooks, open

4 Carefully align the FC I/O blade with the guide slots in the bay. The status LEDs must be at the bottom.

> **Caution:** Forcing the blade into the bay can cause the pins to bend.

5 Evenly apply pressure to both sides of the blade and slide it into the expansion module until the latch hooks begin to move toward the middle of the blade. Push the latch hooks toward the middle of the

blade and into the locked position. You will feel the blade pins connect with the expansion module's backplane as the blade locks into place.

> **Note:** The LEDs for the FC I/O blade are on the bottom of the blade when the blade is correctly installed in the expansion module.

6 Remove the necessary number of the black rubber protective covers from the ports on the FC I/O blades when you are ready to cable the blade.
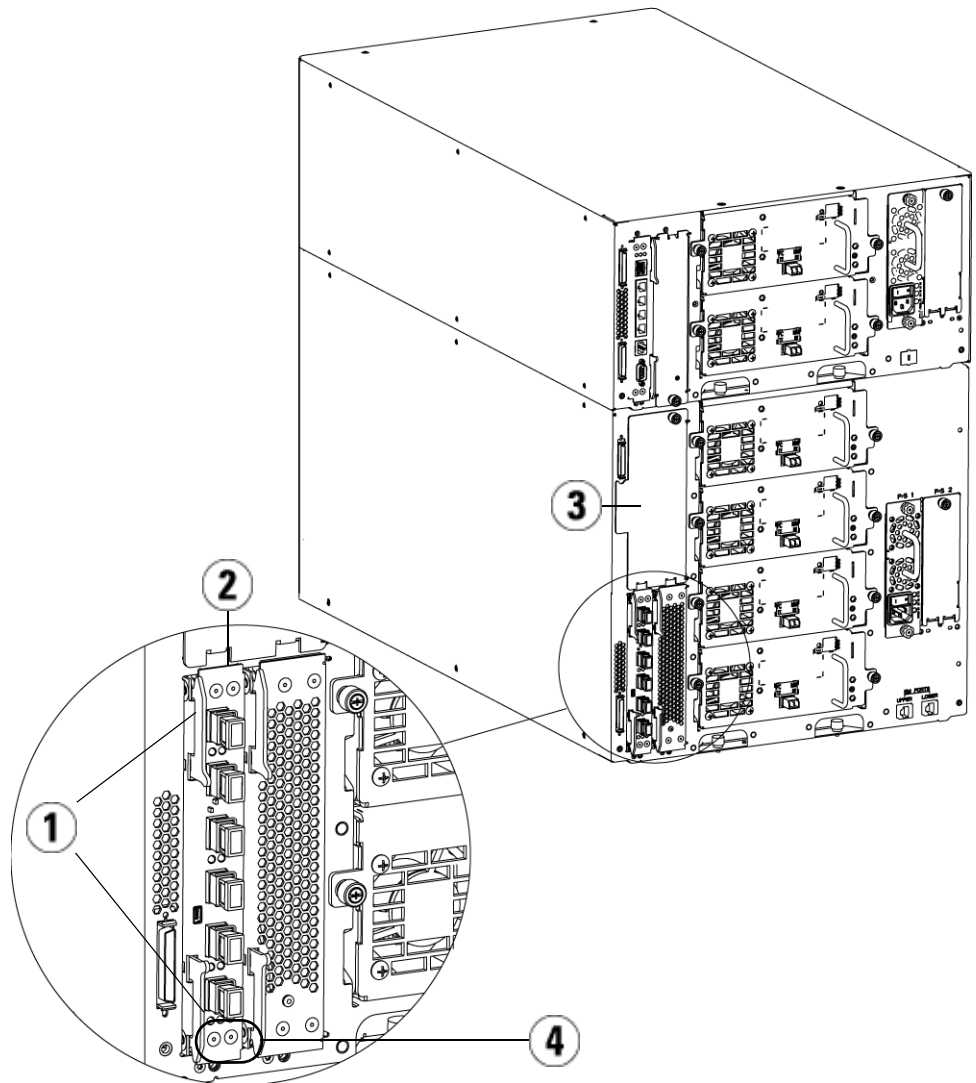
1   Latch hooks, locked

2   FC I/O blade

3   Cover plate on empty bay

4   FC I/O blade LEDs

7 Make sure cover plates are installed over any unused bays in the expansion module.

> **Caution:** Bays that are not populated with blades must contain a cover plate. If the cover plate is not installed, FC I/O blade temperature errors will occur.

8 Cable the library as described in <u>Cabling Libraries With Fibre Channel Tape Drives Connected to Fibre Channel I/O Blades</u> on page 308.

9 Save the library configuration (see <u>Saving the Library Configuration</u> on page 489).

Removing an FC I/O Blade

These instructions explain how to remove an FC I/O blade from your library. You can remove an FC I/O blade while the library is powered on.

> **Note:** The library will generate a RAS ticket when you remove the I/O blade. If you do not want the library to generate a RAS ticket, you can power down the I/O blade before removing it. See <u>Controlling FC I/O Blade Power</u> on page 263.

Required tools: None

1 Access the back of the expansion module containing the FC I/O blade.

2 Tag and disconnect all FC cables from the FC I/O blade.

> **Caution:** Handle the FC cables with care. They will be damaged if they are bent at more than a four inch arc.

3 Lift the latch hooks out of the locked position and push them up. You will feel the FC I/O blade unplug from the expansion module's backplane.

4 Continue lifting on the latch hooks until the blade is totally unplugged from the backplane.

5 Slide the FC I/O blade out of the expansion module.

6 Make sure cover plates are installed over any unused bays in the expansion module.

7 If you are permanently removing the FC I/O blade, you will need to configure the library to stop monitoring the FC I/O blade (see Permanently Removing FC I/O Blades on page 497).

8 Save the library configuration (see Saving the Library Configuration on page 489).

Replacing an FC I/O Blade

These instructions explain how to replace an FC I/O blade in your library. You can remove and replace a FC I/O blade while the library is powered on.

> **Note:** The library will generate a RAS ticket when you remove the FC I/O blade. If you do not want the library to generate a RAS ticket, you can power down the FC I/O blade before removing it. See Controlling FC I/O Blade Power on page 263.

Required tools: None

1 Access the back of the expansion module.

2 If you have not already done so, remove the old FC I/O blade, following the directions in Removing an FC I/O Blade on page 452.

3 Press up and out to open the latch hooks on each side of the replacement FC I/O blade.

4 Carefully align the FC I/O blade with the guide slots in the bay. The status LEDs must be at the bottom.

> **Caution:** Forcing the blade into the bay can cause the pins to bend.

5 Evenly apply pressure to both sides of the blade and slide it into the expansion module until the latch hooks begin to move towards the middle of the blade. Push the latch hooks towards the middle of the blade and into the locked position. You will feel the blade pins connect with the expansion module's backplane as the blade locks into place.

> **Note:**   The LEDs for the FC I/O blade are on the bottom of the blade when the blade is correctly installed in the expansion module.

6   Remove and discard the necessary number of the black rubber protective covers from the ports on the FC I/O blades.

7   Reconnect the FC cables to the appropriate FC ports on the FC I/O blade.

> **Caution:**   Fibre optical cables will be damaged if they are bent at more than a four-inch arc.

8   Save the library configuration (see <u>Saving the Library Configuration</u> on page 489).

> **Note:**   After you replace the FC I/O blade, the library ensures that the FC I/O blade is loaded with the proper firmware. This firmware is based on the currently installed level of library firmware. If the autoleveling process fails, the FC I/O blade becomes inoperable and the library creates a ticket to report the issue. For information about LED behaviors on blades during autoleveling operations, see <u>Blade Status LEDs</u> on page 500.

Adding, Removing, and Replacing the FC I/O Fan Blade

Each FC I/O blade is cooled by a fan blade. The fan blade is always installed in the bay to the right of the FC I/O blade. Each expansion module has four bays and can accommodate two FC I/O blades and two fan blades.

The recommended order of installing the FC I/O blade and fan in the expansion module is starting from the bottom two bays and moving up.

Figure 62 on page 445 shows the FC I/O blade and I/O fan blade installed side-by-side in the expansion module.

Adding an FC I/O Fan Blade

These instructions explain how to add an FC I/O fan blade to your library. You can add an FC I/O fan blade while the library is powered on.

Required tools: None

1 Access the back of the expansion module.

2 Remove the cover plate from blade bay to the right of the bay for the FC I/O blade.

> **Note:** The recommended order of installing the FC I/O blade and fan blade in an expansion module is starting from the bottom two bays and moving up.

3 Press up and out to open the latch hooks on each side of the FC I/O fan blade. The LED must be at the bottom of the blade.
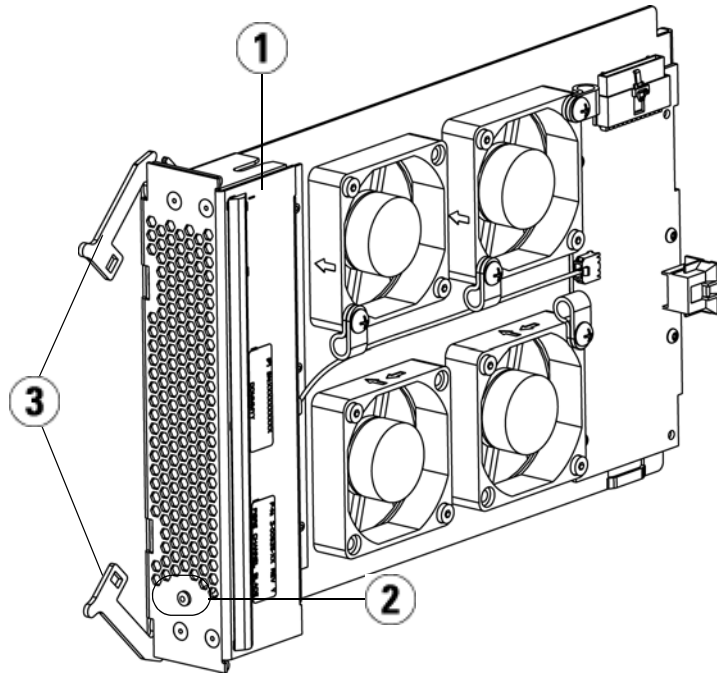
1	Fan blade
2	LED
3	Latch hooks, open

> **Caution:**   Forcing the blade into the bay can cause the pins to bend.

4 Evenly apply pressure to both sides of the fan blade and slide it into the expansion module until the latch hooks begin to move towards the middle of the blade. Push the latch hooks towards the middle of the blade and into the locked position. You will feel the blade pins connect with the expansion module's backplane as the blade locks into place.

> **Note:** The LED for the FC I/O fan blade is on the bottom of the blade when the blade is correctly installed in the expansion module.

5 Save the library configuration (see <u>Saving the Library Configuration</u> on page 489).

Removing an FC I/O Fan Blade

These instructions explain how to remove an FC I/O blade from your library. You can remove an FC I/O fan blade while the library is powered on.

> **Caution:** Do not permanently remove an FC I/O fan blade unless you also permanently remove the FC I/O blade to which it is associated.

Required tools: None

1 Access the back of the expansion module containing the FC I/O fan blade.

2 Lift the latch hooks out of the locked position and push them up. You will feel the FC I/O fan blade unplug from the expansion module's backplane.

3 Continue lifting on the latch hooks until the blade is totally unplugged from the backplane.

4 Slide the FC I/O fan blade out of the expansion module.

5 If you are permanently removing the FC I/O fan blade, place a cover on the empty bay.

6 Save the library configuration (see <u>Saving the Library Configuration</u> on page 489).

Replacing an FC I/O Fan Blade

These instructions explain how to replace an FC I/O fan blade in your library. You can remove and replace an FC I/O fan blade while the library is powered on.

Required tools: None

1 Access the back of the expansion module.

2 If you have not already done so, remove the old I/O fan blade, following the directions in <u>Removing an FC I/O Fan Blade</u> on page 457.

3 Press up and out to open the latch hooks on each side of the replacement I/O fan blade.

4 Carefully align the FC I/O fan blade with the guide slots in the bay. The status LED must be at the bottom.

> **Caution:**   Forcing the blade into the bay can cause the pins to bend.

5 Evenly apply pressure to both ends of the FC I/O fan blade and slide it into the expansion module until the latch hooks begin to move towards the middle of the blade. As you push in on the blade, you will feel the blade pins connect with the expansion module's backplane.

6 Push the latch hooks into the locked position.

7 Save the library configuration (see <u>Saving the Library Configuration</u> on page 489).

Tape Drive Ethernet Connectivity and the Ethernet Expansion Blade

LTO-5 and LTO-6 FC tape drives enable you to use tape drive Ethernet connectivity for FIPS-certified key exchanges, tape drive log collection, tape drive firmware updates, and tape drive firmware autoleveling via Ethernet instead of via internal serial communication. This speeds up operations and provides the security required for FIPS-certified key exchanges. 5U libraries can access tape drive Ethernet connectivity directly via the library control blade. For libraries greater than 5U, Quantum provides the Ethernet Expansion blade, which facilitates direct

Ethernet connectivity between HP LTO-5 and LTO-6 Fibre Channel tape drives and the library's internal Ethernet via the library control blade.

Details about tape drive Ethernet connectivity and the Ethernet Expansion blade include:

- Library firmware must be at version 600G or later.

- HP LTO-5 FC or HP LTO-6 FC tape drive firmware must be at the latest version qualified with the Scalar i500 library (see the *Scalar i500 Release Notes* for qualified firmware levels).

- An Encryption Key Management license must be installed on the library sufficient to cover all the tape drives you intend to use for Ethernet operations.

- A Storage Networking license must be installed on the library sufficient to cover all the tape drives you intend to use for Ethernet operations.

- 5U libraries do not support an Ethernet Expansion blade. For 5U libraries, connect the HP LTO-5 FC or HP LTO-6 FC tape drive to one of the internal Ethernet ports on the library control blade (see).

- In libraries that are greater than 5U, it is recommended that all HP LTO-5 FC or HP LTO-6 FC tape drives be connected to an Ethernet Expansion blade. The Ethernet Expansion blade is provided as part of your FIPS-compliant solution when you purchase 8 Gb Storage Networking tape drives.

- The Ethernet Expansion blade is not in the data path and does not affect tape drive control paths.

- Each Ethernet Expansion blade has six Ethernet ports to allow you to attach up to six HP LTO-5 FC or HP LTO-6 FC tape drives. Do not attach tape drives of any other type to the Ethernet Expansion blade.

- Do not connect the Ethernet Expansion blade to an external Ethernet source. The Ethernet Expansion blade is for internal Ethernet connectivity within the library.

- The Ethernet Expansion blade must be installed in the bottom left vertical bay in an expansion module. The empty bay to the right of the Ethernet Expansion blade must be covered by a cover plate.

- Libraries may contain both Ethernet Expansion blades and FC I/O blades.

- You may not connect a tape drive to both an Ethernet Expansion blade and an FC I/O blade.

- You are limited to a maximum of four blades per library (Ethernet Expansion blades and FC I/O blades), in any combination.

- If the tape drive Ethernet connection or an Ethernet Expansion blade fails, you will not be able to perform encryption operations on any connected tape drives that have FIPS mode enabled. You will still be able to collect tape drive logs and update tape drive firmware via internal serial communication.

> **Caution:** If the Ethernet Expansion blade or Ethernet connectivity fails and the attached tape drives have FIPS mode enabled, all encryption operations (encrypting, decrypting, key requests) on the attached tape drives will fail. These operations will NOT automatically continue over internal serial communication. If this happens, contact Quantum Support for a replacement Ethernet Expansion blade as soon as possible.

Cabling a 5U Library for Ethernet Connectivity

In a 5U library:

1 Upgrade library firmware to version 600G or later.

2 Upgrade tape drive firmware on all HP LTO-5 FC or HP LTO-6 FC tape drives that you plan to connect via Ethernet to the latest version qualified with the Scalar i500 library (see the *Scalar i500 Release Notes* for qualified firmware levels).

3 Shut down the library.

4 Connect the tape drives to one of the four internal Ethernet ports on the library control blade (LCB) using Ethernet cables (see Figure 63).

> **Note:** This figure and subsequent figures show two cables, but only one cable is used unless you are using data path failover.

5 Power on the library.

Figure 63 Ethernet
Connectivity on 5U Libraries
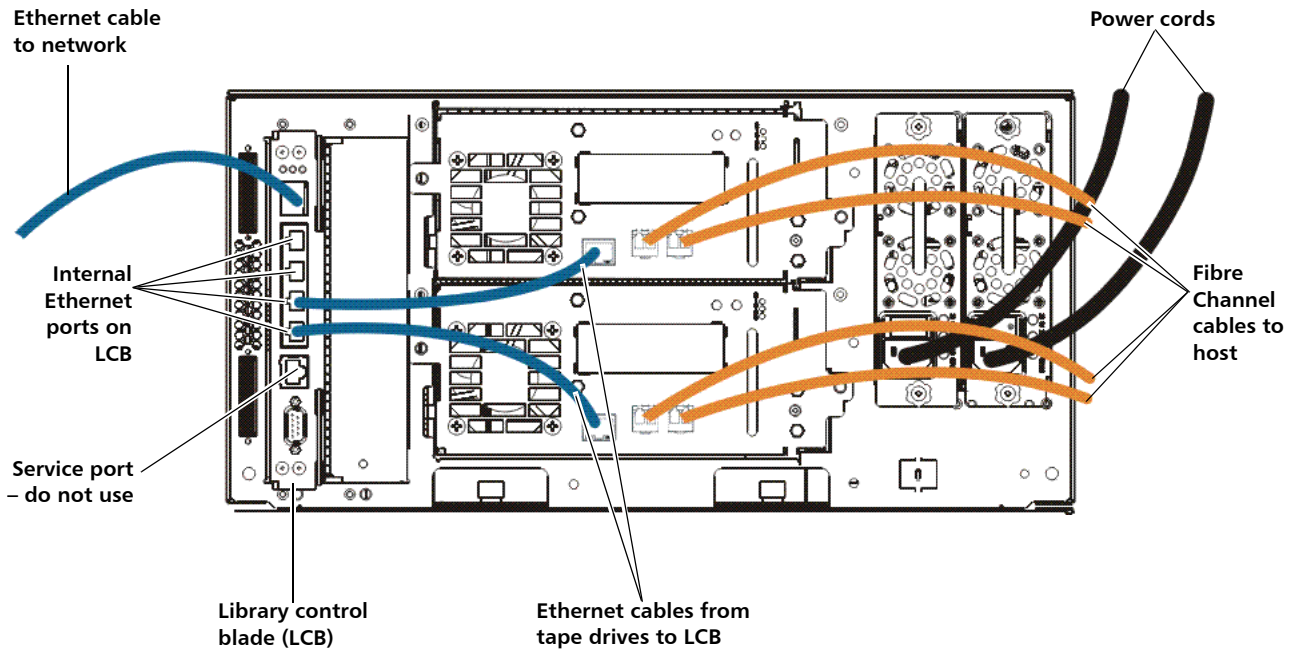
Ethernet cable to network

Power cords

Internal Ethernet ports on LCB

Service port – do not use

Library control blade (LCB)

Ethernet cables from tape drives to LCB

Fibre Channel cables to host

Installing the Ethernet Expansion Blade

The Ethernet Expansion blade must be installed in the bottom left vertical bay in an expansion module. The empty bay to the right of the Ethernet Expansion blade must be covered by a cover plate.

Equipment Required

- Ethernet Expansion blade
- Cover plate
- Ethernet cables (one for each tape drive that you will connect to the Ethernet Expansion blade), plus an extra one per Ethernet Expansion blade, to connect the LCB to the expansion module in which the Ethernet Expansion blade is installed.

Tools Required

None

Instructions

1 Upgrade library firmware to version 600G or later.

2 Upgrade tape drive firmware on all HP LTO-5 FC or HP LTO-6 FC tape drives that you plan to connect to the Ethernet Expansion blade to the latest version qualified with the Scalar i500 library (see the *Scalar i500 Release Notes* for qualified firmware levels).

3 Optional – Save the library configuration (see the *Scalar i500 User's Guide* for instructions).

4 Shut down the library.

5 For every expansion module that will contain an Ethernet Expansion blade, connect a standard Ethernet cable from one of the four internal Ethernet ports on the library control blade (LCB) to the Ethernet port marked "LOWER" located on the bottom right of the expansion module in which the Ethernet Expansion blade is installed. There are two ports, marked "UPPER" and "LOWER." Since the Ethernet Expansion blade must be installed in the lower bay of the expansion module, you must use the Ethernet port marked "LOWER." The "LOWER" port is on the right. See <u>Figure 64</u>.

Figure 64 Connecting the
Library Control Blade to the
Expansion Module Via Ethernet

**Ethernet cable to
network**

**Internal Ethernet
ports on LCB**

**Ethernet cable to
expansion module**

Cover plates

**Fibre
Channel
cables to
host**

3-09973-XX
YY-MM-DD

EM PORTS
UPPER   LOWER

**"UPPER" port. Do not
use for Ethernet
Expansion blades.**

**"LOWER" port connected via
Ethernet cable to LCB**
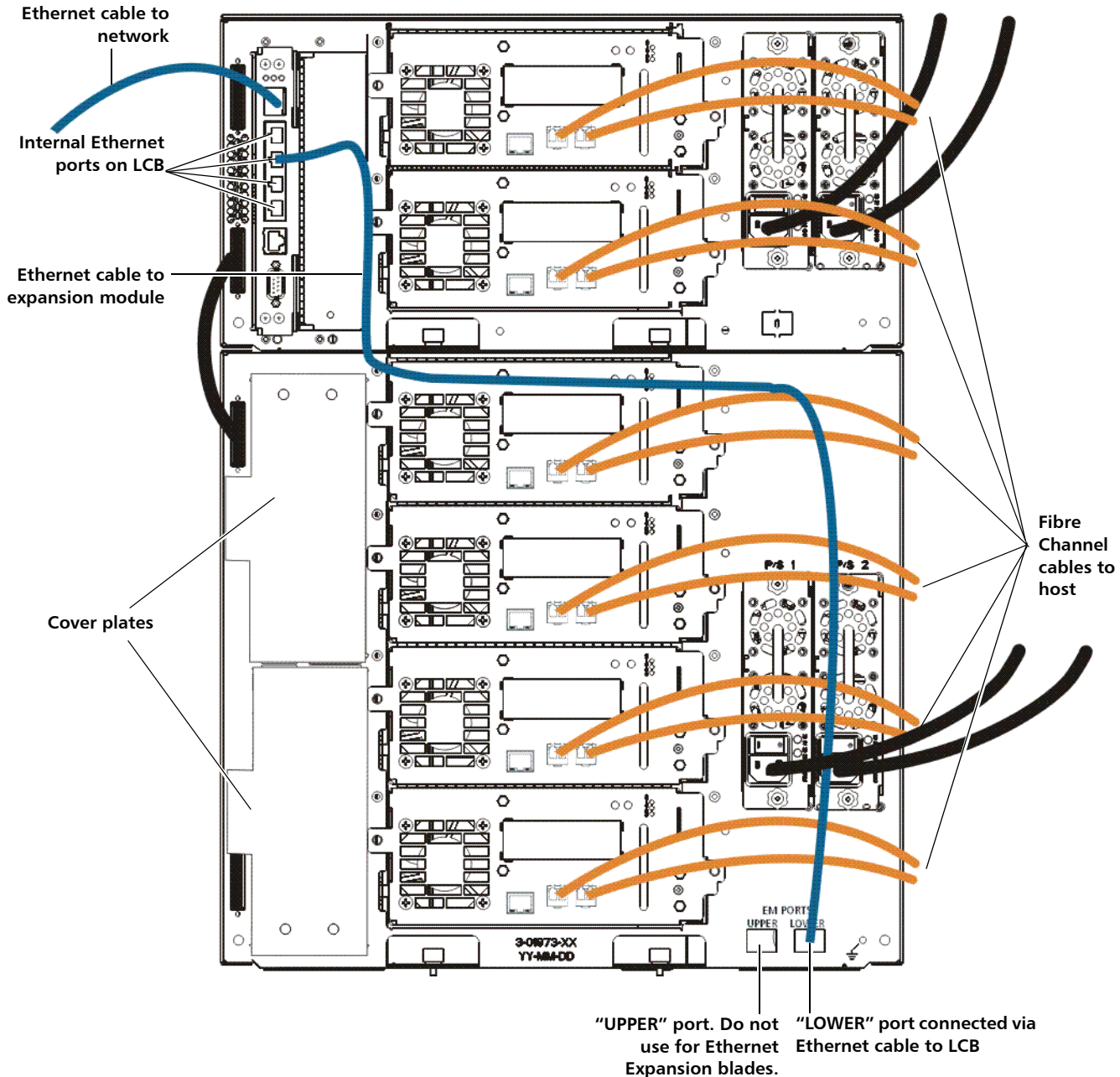
6 Prepare the library for Ethernet Expansion blade installation. The Ethernet Expansion blade must be installed in the bottom left bay of an expansion module.

- In some cases, this may require removal or relocation of an FC I/O blade and its accompanying fan blade.

- Remove the cover plate covering the two bottom left slots. To remove the cover plate, unscrew the two captive thumbscrews securing the cover plate and pull outward on the plate. Save the cover plate in case you need to use it later.

7 Remove the new Ethernet Expansion blade from the protective anti-static bag.

8 Press up and out to open the latch hooks on each side of the blade. Hold the Ethernet Expansion blade upright with the latch hooks on the left side, and the status LEDs at the bottom (see Figure 65).

Figure 65 Ethernet Expansion
Blade
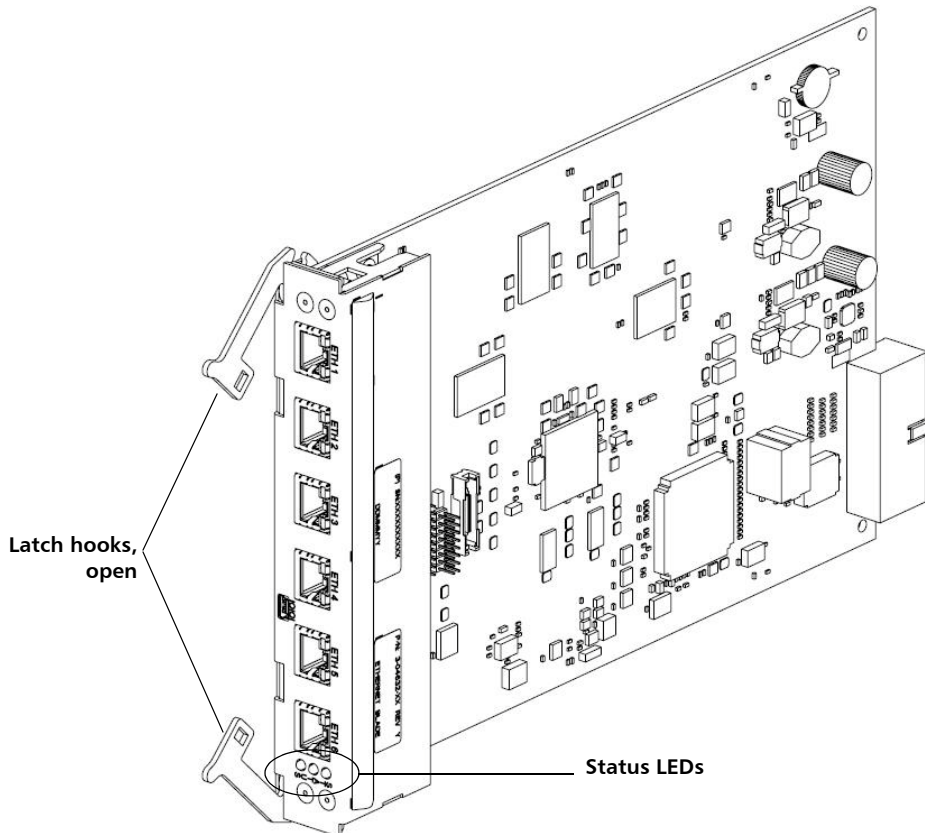
9 Carefully align the Ethernet Expansion blade with the guide slots in the bay.

> **Caution:**   Forcing the blade into the bay can cause the pins to bend.

10 Evenly apply pressure to both sides of the blade and slide it into the expansion module until the latch hooks begin to move toward the middle of the blade. Push the latch hooks toward the middle of the blade and into the locked position. You will feel the blade pins connect with the expansion module's backplane as the blade locks into place.

11 Observe the status LEDs on the Ethernet Expansion blade. The blue
LED should blink once every 10 seconds, indicating the blade is
powered on. The green LED should blink once per second, indicating
the blade's processor is working normally. The amber LED should be
off.

12 Install a cover plate over the empty bay to the right of the Ethernet
Expansion blade.

Caution:	If the cover plate next to an Ethernet Expansion blade is not installed, Ethernet Expansion blade temperature errors will occur.

Figure 66 Installing the
Ethernet Expansion Blade

**Double-
wide cover
plate**

**Ethernet
Expansion blade** **Cover
plate**

**Latch
hooks,
closed**
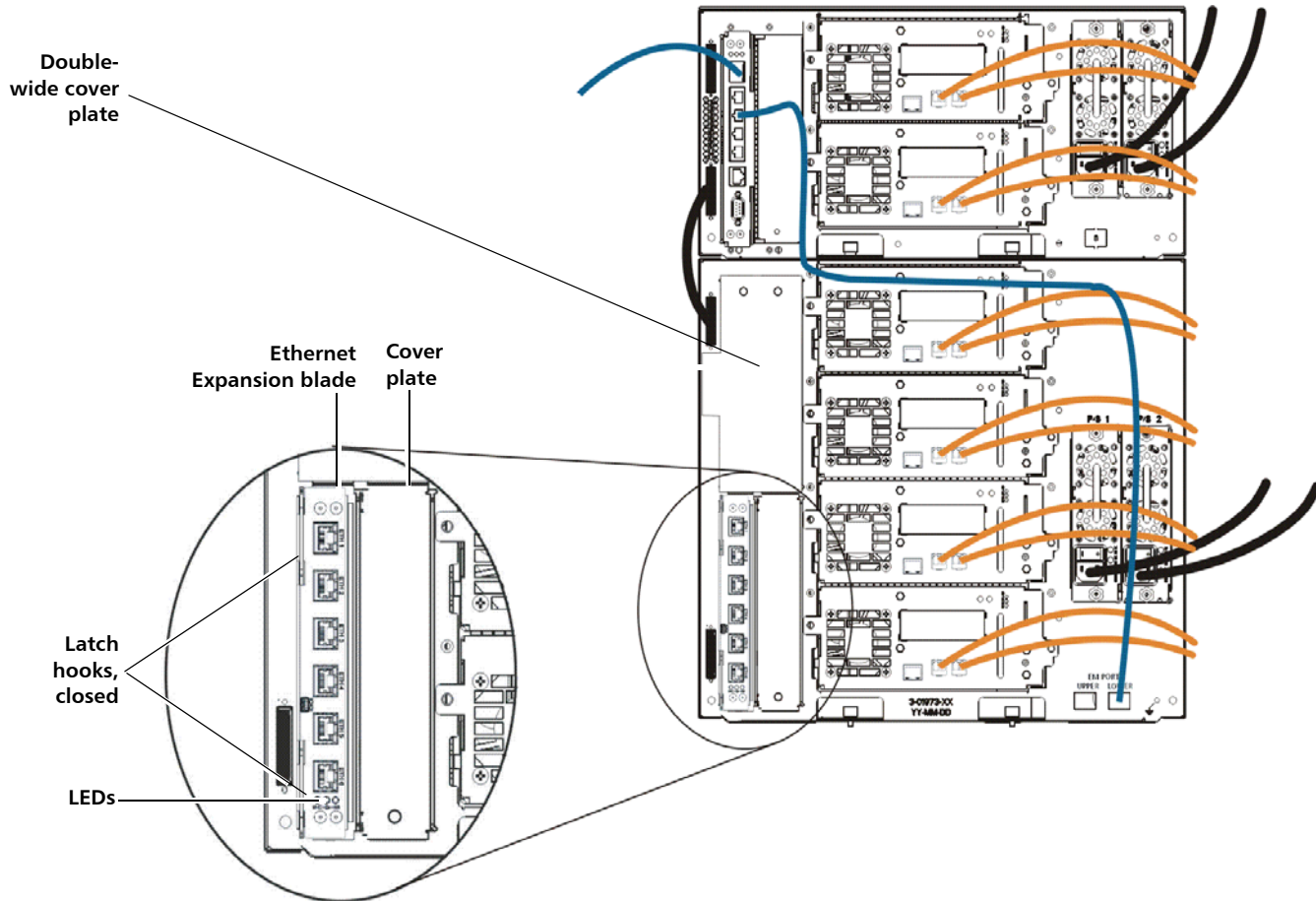
LEDs

13 Cable the Ethernet Expansion blade (see <u>Cabling the Ethernet
Expansion Blade</u> on page 468).

14 Power on the library.

15 Verify the Ethernet Expansion blade is in the "Ready" state using one
of these methods:

- Check the LEDs on the Ethernet Expansion blade. The green LED
should blink once per second, the blue LED should blink once
every 10 seconds, and the amber LED should be off.

- Use the library Web client:

  a Select **Tools > Diagnostics** to enter library diagnostics.

  b A message warns you that entering diagnostics will log out all other users of the same or lower privilege level.

  c Click **OK** to agree to log all other users out.

  d The diagnostics menu bar displays.

  e Select **Drives > EE Blade Control**.

  f A message warns you that power cycling an Ethernet Expansion blade may cause key exchange failures if FIPS is enabled.

  g Click **OK** to proceed.

  h The **Diagnostics - Ethernet Expansion Blade Control** screen displays (see Figure 68 on page 473).

  i Check the **Status** column for the Ethernet Expansion blade to be sure it says "Ready."

16 Save the library configuration (see the library user's guide for instructions).

Cabling the Ethernet Expansion Blade

Cable the library and Ethernet Expansion blade as follows (see Figure 67 on page 470).

- In a 14U and higher library, it is recommended that you do not connect HP LTO-5 FC tape drives to the library control blade (LCB). Instead, you should connect the tape drives to an Ethernet Expansion blade using normal Ethernet cables.

- The Ethernet Expansion blade must be installed in the lower left slot of the expansion module. A cover plate must cover the slot next to the Ethernet Expansion blade. See Figure 67

- For every expansion module that contains an Ethernet Expansion blade, make sure a standard Ethernet cable is connected from one of the four internal Ethernet ports on the library control blade (LCB) to the Ethernet port marked "LOWER" located on the bottom right of the expansion module in which the Ethernet Expansion blade is installed. There are two ports, marked "UPPER" and "LOWER." Since the Ethernet Expansion blade must be installed in the lower bay of the expansion module, you must use the port marked "LOWER." The "LOWER" port is on the right. See Figure 67. You must do this BEFORE placing the Ethernet Expansion blade into the library as per

the instructions in [Installing the Ethernet Expansion Blade](#) on page 461.

- Tape drives connected to an Ethernet Expansion blade must not be connected to an FC I/O blade. Instead, connect them to a host or switch.

Figure 67 Ethernet
Connectivity on 14U and Higher
Libraries

**Ethernet cable to
network**

**Internal Ethernet
ports on LCB**

Cover plate

**Ethernet
Expansion blade
with six Ethernet
ports, connected
to tape drives via
Ethernet cables**

**Power
cables**

**Fibre
Channel
cables to
host**

**Power
cables**

Cover plate

**"UPPER" port. Do not use for
Ethernet Expansion blades.**

**"LOWER" port connected via
Ethernet cable to LCB**

Ethernet cable to network

Internal Ethernet ports on LCB

Power cables

Cover plate

Ethernet Expansion blade with six Ethernet ports, connected to tape drives via Ethernet cables

Fibre Channel cables to host

Ethernet Expansion blade with six Ethernet ports, connected to tape drives via Ethernet cables

Power cables

Cover plate

"UPPER" port. Do not use for Ethernet Expansion blades.

"LOWER" port connected via Ethernet cable to LCB

**Permanently Removing
or Relocating an Ethernet
Expansion Blade**

Library firmware monitors all Ethernet Expansion blades after they are installed in the library. Once an Ethernet Expansion blade is installed, the library expects the blade to be in the same installed location after every power cycle.

If an Ethernet Expansion blade is permanently removed from the library or relocated within the library, the library firmware must be configured to stop monitoring the EE blade. If this is not done and the library continues to monitor a removed EE blade, RAS tickets could be generated.

> **Note:** You do not need to configure the library to stop monitoring an Ethernet Expansion blade if you are replacing a failed Ethernet Expansion blade with a new Ethernet Expansion blade in the same location (see Replacing an Ethernet Expansion Blade in the Same Location on page 474).

1 If you are underline permanently removing the Ethernet Expansion blade, disable FIPS mode on all Ethernet Expansion blade-connected tape drives FIRST before you remove the Ethernet Expansion blade. To disable FIPS mode, the tape drives must be Ethernet connected to allow the tape drives to reconfigure. See Enabling and Disabling FIPS Mode on HP LTO-5 and LTO-6 Tape Drives on page 201.

2 Remove the Ethernet Expansion blade from the library's configuration as follows:

    a On the library web client, select **Tools > Diagnostics** to enter library diagnostics.

    A message warns you that entering diagnostics will log out all other users of the same or lower privilege level.

    b Click **OK** to agree to log all other users out.

    The diagnostics menu bar displays.

    c Select **Drives > EE Blade Control**.

    The **Diagnostics - Ethernet Expansion Blade Control** screen displays (see Figure 68).

Figure 68 Ethernet 27
Ethernet Expansion Blade Control
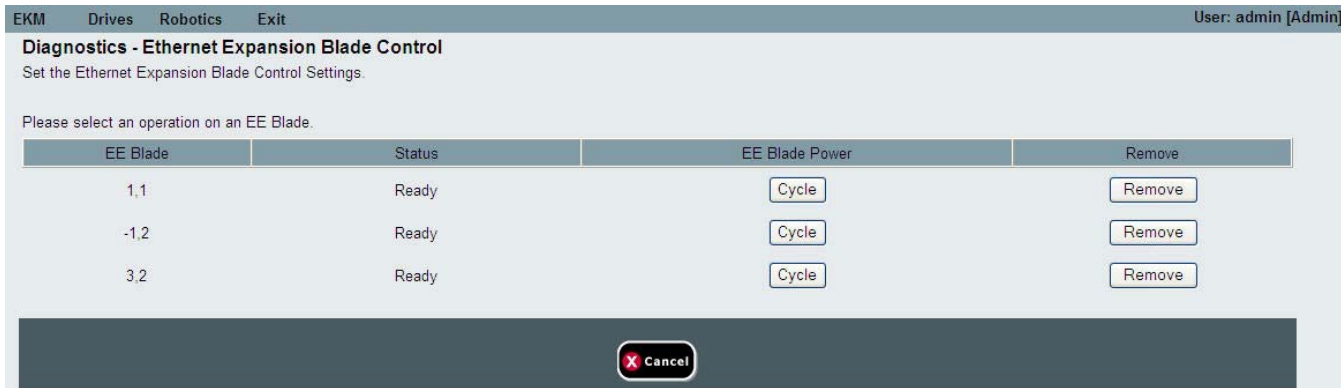
d Click the **Remove** button corresponding to the Ethernet
Expansion blade you want to remove.

> **Note:** Removing an Ethernet Expansion blade may cause
> key exchange failures if FIPS is enabled. A message
> warns you about the possible failures and asks you to
> confirm that you want to proceed.

3 Click **OK** to proceed or **Cancel** to cancel the operation without
removing the Ethernet Expansion blade.

4 Disconnect the Ethernet cables from the Ethernet Expansion blade.

5 Lift the latch hooks out of the lock position and push them up (see
Figure 65 on page 465). You will feel the blade unplug from the
library's backplane.

6 Continue lifting on the latch hooks until the Ethernet Expansion
blade is totally unplugged from the backplane.

7 Slide the Ethernet Expansion blade out of the bay.

8 Remove the cover plate from the bay to the right of the Ethernet
Expansion blade. Install the original double-wide cover plate over
both bays. This is required for cooling and dust reduction. If you
need a cover plate, contact Quantum.

9 Save the library configuration (see the library user's guide for
instructions).

Replacing an Ethernet Expansion Blade in the Same Location

If you are replacing an Ethernet Expansion blade in the same location, you do not need to perform a "remove" operation via the web client as you would if you were permanently removing or relocating the Ethernet Expansion blade.

1 Disconnect the Ethernet cables from the Ethernet Expansion blade.

2 Lift the latch hooks out of the lock position and push them up (see Figure 65 on page 465). You will feel the blade unplug from the library's backplane.

3 Continue lifting on the latch hooks until the Ethernet Expansion blade is totally unplugged from the library's backplane.

4 Slide the Ethernet Expansion blade out of the bay.

5 Install the new Ethernet Expansion blade (see Installing the Ethernet Expansion Blade on page 461).

6 Save the library configuration (see the library user's guide for instructions).

Power Cycling the Ethernet Expansion Blade

Administrators can power cycle individual Ethernet Expansion blades in the library. You might want to power cycle an individual Ethernet Expansion blade when troubleshooting, such as when resolving a Reliability, Availability, and Serviceability (RAS) ticket. You can only power cycle the Ethernet Expansion blade from the Web client.

To power cycle an Ethernet Expansion blade:

1 On the Web client, select **Tools > Diagnostics** to enter library diagnostics.

A message warns you that entering diagnostics will log out all other users of the same or lower privilege level.

2 Click **OK** to agree to log all other users out.

The diagnostics menu bar displays.

3 Select **Drives > EE Blade Control**.

4 Click **OK** to proceed.

The **Diagnostics - Ethernet Expansion Blade Control** screen displays (see Figure 68 on page 473).

5 Click the **Cycle** button corresponding to the Ethernet Expansion blade you want to power cycle.

It takes approximately 1 minute to power cycle an Ethernet Expansion blade. The status displays as "Booting" during the power cycle.

Viewing Ethernet Connectivity

There are two places on the library Web client which tell you whether tape drives are connected via Ethernet (either via an Ethernet Expansion blade or connected directly to the library control blade). These two places are:

• Tools > Drive Operations > Update tape drive firmware using a firmware image file

• Tools > Drive Operations > Retrieve Tape Drive Log

The tape drive table in each of these screens has a column called **Ethernet Connected**. If the tape drive is connected via Ethernet, the tape drive IP address will be listed in the column. If the tape drive is Ethernet capable but not connected, the column displays "No." If the tape drive is not Ethernet capable, the column displays "N/A."

You can also view the location coordinates and Ethernet Expansion blade status in the library System Information Report:

• **Reports > System Information**

Ethernet Expansion Blade Status LEDs

The status LEDs for the Ethernet Expansion blade are located at the bottom of the Ethernet Expansion blade below ETH 6 (see).

Figure 69 Ethernet Expansion
Blade LEDs

Port LED status

Ethernet Expansion blade
status LEDs
- Left = Blue
- Middle = Amber
- Right = Green
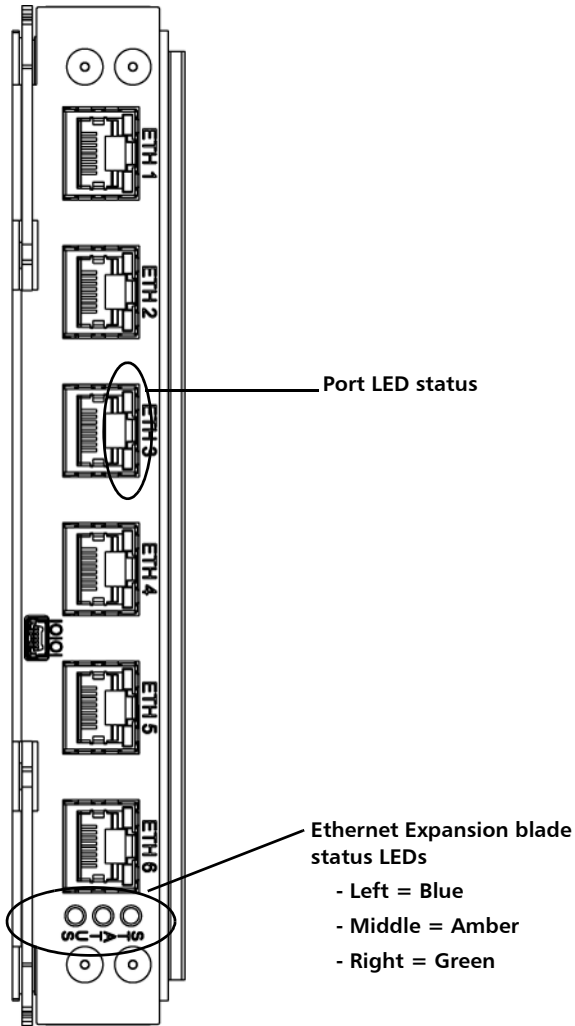
Table 11   Ethernet Expansion
Blade Status LED Descriptions

LED Color	Represents	Blade Status
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. • Blinks once per second (1 Hz) — Normal.
Amber	Health status	• Solid OFF — Normal. • Solid ON — Failure or blade is autoleveling. In conjunction with the blue LED blinking once very 10 seconds, this is a normal condition. Autoleveling takes about three minutes per blade, and blades autolevel in series. 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 not operational. • Blinks once every second (1 Hz) — Powered off. Ready to remove. • Blinks once per 10 seconds (flash) — Normal. Blade is powered on.

Table 2 Explanation of Ethernet Expansion blade Ethernet Port LED States

LED Color	Blade Status
Green	• Solid ON — Link is up; data can be sent or received through the Ethernet port. • Solid OFF — Link is down; 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.

Preparing the Library for Moving or Shipping

Before you move or ship your library, follow these steps:

> **Caution:** **When moving the library:** Manufacturer-supplied packaging, whether original or purchased, is required for complete or partial de-installations. You must install the orange robot restraint assembly to protect the robot against damage. Use the original shipping carton and packaging materials to further protect your library equipment during transport.Not using the required packaging will potentially void the support contract. Any damage to equipment will require re-certification, or for Quantum to repair any damage to the equipment, or both. Quantum offers de-installation services. Please contact your Quantum Authorized Reseller or local Quantum Representative for further details.
>
> **Caution:** **When shipping the library:** Use the shipping carton, packaging materials, and the orange robot restraint assembly that originally came with the library. This will help protect your library against damage.

1 Save the library configuration (see Saving the Library Configuration on page 489).

2 Shut down the library using the local operator panel (**Operations > System Shutdown**). This lowers the robot to the "shipping" position on the floor of the library.

3 Follow instructions on the operator panel screen.

4 Turn off library power by pressing the power button on the front panel.

5 Turn off the power to each power supply on the back of the library.

6 Install the orange robot restraint assembly that secures the robot to the floor of the library. The robot restraint assembly was part of the packaging that originally came with the library.

7 Remove all cords and cables from the rear of the library.

8 Remove all tape cartridges from the library.

9 Remove the tape drives from the library to decrease the weight when lifting the modules.

> **Warning:** Without tape drives, tape cartridges, or power supplies, a control module weighs approximately 60 lbs (27.2 kg). An expansion module, without tape drives, tape cartridges, or power supplies, exceeds 65 lbs (29.5 kg).
>
> To avoid serious injury, at least two people are required to safely lift the modules.

10 If rack-mounted, remove one module at a time from the rack. Retain the rack-mounting hardware and shelves for use in the new location.

11 Place the module in the bottom of the shipping carton.

12 Reinstall the tape drives in the module.

13 Complete the packing. For further details, see the *Unpacking Instructions*.

Troubleshooting

The Scalar i500 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 covers:

- [About RAS Tickets](#)
- [Capturing Snapshots of Library Information](#)
- [Saving and E-mailing the Library Configuration Record](#)
- [Saving and Restoring the Library Configuration](#)
- [Troubleshooting "Library Not Ready" Messages](#)
- [Duplicate Devices Discovered](#)
- [Duplicate Media Changer Devices Discovered](#)
- [Identifying Tape Drives](#)
- [Retrieving Tape Drive Logs](#)
- [Retrieving Tape Drive Sled Logs](#)
- [Identifying FC I/O Blades](#)
- [Permanently Removing FC I/O Blades](#)
- [Resetting FC I/O Blade Ports](#)

- [Viewing and E-Mailing the Command History Logs](#)

- [Interpreting LEDs](#)

- [Using the Installation Verification Test](#)

- [Configuring the Internal Network](#)

- [Library Diagnostics](#)

  - [Drive DiagnosticsDrive TestsMedia TestsEthernet Expansion Blade Control](#)

- [Robotics Diagnostics](#)

Quantum's Knowledge Base

Quantum keeps a dynamic listing of frequently asked questions, troubleshooting tips, and service bulletins for all of its products. To access the knowledge base, go to the Quantum Support Web site and click on **Knowledge Base**:

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

About RAS Tickets

The Scalar i500 library uses advanced problem detection, reporting, and notification technology to alert you of problems as soon as they occur. The library performs numerous self-tests to monitor the library's temperature, voltage and currents, and standard library operations. It performs these self-tests each time the library is powered on and during normal operation when the library is idle.

If the self-test detects a problem, the library generates a Reliability, Availability, and Serviceability (RAS) ticket that identifies the component that is likely causing the problem. The library's light emitting diodes (LEDs) may also turn on or off and flash to indicate an abnormal state. If

the problem is not severe, the library continues to provide full functionality to all unaffected partitions.

RAS tickets have three priority levels:

- Low — Informational message. Indicates that an abnormal condition exists within the library that warrants investigation and correction but the nature of the condition may have little or no effect on operations.

- High — Warning message. Indicates that a condition exists within the library that impacts system performance, redundancy, or a specific host application. Typical library operations can continue without immediate corrective action, although an application may have failed and may need to be restarted. A user should investigate the condition and correct the problem soon.

- Urgent — Critical issue. Indicates that a failure has occurred or a serious condition exists within the library 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 required for backup or restore operations are either not possible or are highly unreliable.

When possible, the RAS ticket provides instructions for resolving problems. You can view RAS tickets on both the operator panel and the Web client. Access the library's online Help system if you have questions about the instructions provided. To access the online Help system, click the **Help** icon at the top right of the Web client or operator panel user interface.

You can frequently resolve a simple problem yourself, but if the problem is complex or involves a field replaceable unit (FRU), you will be directed to contact service. Only qualified service technicians can service FRUs.

| **Caution:** | Do not work with RAS tickets while the library is performing an inventory. Doing so may result in inventory discrepancies, such as missing tape cartridges. |

Viewing RAS Tickets

Selecting **All RAS Tickets** from the **Tools** menu on both the operator panel and the Web client opens the **All RAS Tickets** screen, which lists RAS tickets in order of last occurrence of each event, beginning with the most recent.

> **Note:** **Last Occurrence** indicates the last time a ticket event occurred. This information updates any time the event recurs. **Last Occurrence** does NOT update if you open, close, or resolve the RAS Ticket.

Included in the list is a brief description of the error condition captured by the RAS ticket. The **All RAS Tickets** screen allows you to view RAS ticket details and navigate to ticket resolution information. If you want to request technical support, the **Ticket Details** and **Ticket Resolve** windows provide a link to the online service request Website.

The initial status of all RAS tickets is Unopened. Once the administrator selects the **Resolve** button on the **All RAS Tickets** screen for a ticket, its status changes to Opened. When the user closes the ticket, its status changes to Closed. You can view Opened and Unopened tickets on both the operator panel and the Web client, but you can view Closed tickets only on the Web client.

> **Caution:** Be careful when pressing the **Close All Tickets** button. This closes all RAS tickets even if they are not resolved. It is recommended that each RAS ticket be viewed, analyzed, and closed individually.

The paths to open the appropriate screens are:

- From the Web client, select **Tools > All RAS Tickets**.
- From the operator panel, select **Tools > All RAS Tickets**.

Resolving and Closing RAS Tickets

Administrators can resolve some RAS tickets. Others must be resolved by Service personnel. Only one person at a time can resolve a ticket. Multiple users can, however, view ticket details simultaneously. If your Web client session goes down while resolving a RAS ticket, you must wait 3 minutes before you can continue resolving the RAS ticket from either the Web client or the operator panel.

1 Log in to the Web client.

2 From the **Tools** menu, select **All RAS Tickets**.

The **Tools - All RAS Tickets** screen appears.

3 Identify the RAS ticket you want to resolve.

> **Note:**   You can use the **Go to RAS Ticket** text box at the bottom of the screen to locate a specific RAS ticket number. In addition, if there is more than one page of RAS tickets, use the **Page 1 of x** arrows to view the additional tickets.

4 Click **Resolve**.

The **Ticket Resolution** window appears. This window contains information on how to resolve the ticket.

5 Review the description.

6 Do one of the following:

  a To close the ticket now, click **Close**.

  The **Tools - All RAS Tickets** window displays, with the RAS ticket no longer in the list. The task is complete and the RAS ticket is resolved.

  b To leave the ticket open for future troubleshooting, click **Exit**. Then you can perform the diagnostic steps you need to resolve a related RAS ticket.

If you want to request technical support, the ticket **Resolve** window provides a link to the online service request Website.

> **Note:**   To display all closed tickets, select the **Include Closed Tickets** check box at the bottom of the screen. The **Tools - All RAS Tickets** screen refreshes, with the **Resolve** button unavailable for all closed RAS tickets.

> **Caution:**   Be careful when pressing the **Close All Tickets** button. This closes all RAS tickets even if they are not resolved. It is recommended that each RAS ticket be viewed, analyzed, and closed individually.

The path to open the appropriate screen is:

* From the Web client, select **Tools > All RAS Tickets**.

**Closing RAS Tickets
Automatically**

The library will close all currently open RAS tickets when you reboot the library. If any errors occur during the reboot, the library issues new tickets.

Automatic ticket closure will only occur when you intentionally initiate a reboot, by either restarting the library, shutting down the library, or upgrading library firmware. Automatic ticket closure will not occur if the library shuts down unexpectedly or if the power cord is unplugged.

You can always view closed tickets on the Web client by selecting **Tools > All RAS Tickets** and clicking the **Include Closed Tickets** check box. Tickets that were auto-closed are designated as "Canceled."

Automatic ticket closure is enabled by default. You can enable or disable this feature from the operator panel.

The path to open the appropriate screen is:

• From the operator panel, select **Tools > System Settings**.

Capturing Snapshots of Library Information

Technical support personnel may ask you to perform the Capture Snapshot operation, so they can better diagnose issues. The **Capture Snapshot** operation captures detailed information about the entire library in a single ASCII file that can be e-mailed to technical support personnel.

The logged information consists of configuration data, status information, and trace logs for library components. Trace logs collect problem data and provide support personnel with vital library information for troubleshooting and solving problems.

You can e-mail the snapshot file from both the operator panel and the Web client. On the Web client, you can also download the Capture Snapshot file to a computer. You cannot download Capture Snapshot files from the library's operator panel, and you cannot print Capture Snapshot files from either the Web client or the operator panel.

Depending on the library configuration and your connection speed, saving the Capture Snapshot file takes approximately 30 minutes. The resulting file size can be large. Your firewall file-size limitations could prohibit you from e-mailing the file.

On the Web client, ensure that the library e-mail account is appropriately configured before you attempt to e-mail the snapshot from the library. If the library e-mail account address is not configured, an error appears. For information on setting up the e-mail account, see Configuring the Library E-mail Account on page 92.

You can configure the library to automatically attach a library snapshot to certain RAS ticket e-mail notifications (see Configuring the Library E-mail Account on page 92). If the library is in the process of capturing an automatic snapshot, you will not be able to manually capture a snapshot via the Web client until the automatic snapshot is complete. If this happens, an error message will display. Wait about 10 minutes and try again.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Tools > Capture Snapshot.**

- From the operator panel, select **Tools > Capture Snapshot**.

Saving and E-mailing the Library Configuration Record

The library configuration record is a text file that contains details about the library's configuration. The configuration record can be saved or e-mailed to a specified e-mail address.Information in the library. The configuration record includes:

- Product information—vendor, model, product ID, product version (library firmware version), and serial number.

- Capacity on Demand (COD) license information—licensed slots and expiration date.

- Module information—vendor, module type, module serial number, and module location coordinates.

- Tape drive information:

  - SCSI tape drives—partition name, number of tape drives in partition, drive location, SCSI element address, online status, active status, ready state, vendor, model, serial number, tape drive firmware version, drive type, logical serial number, interface type, SCSI ID, and LUN.

- Fibre Channel (FC) tape drives—partition name, number of tape drives in partition, drive location, SCSI element address, online status, active status, ready state, vendor, model, serial number, tape drive firmware version, drive type, logical serial number, interface type, World Wide Node Name (WWNN) loop ID, topology, speed, and actual speed.

> **Note:** If the FC tape drive is attached to an FC I/O blade, the WWNN indicates the WWNN of the I/O blade, not the tape drive.

- Serial Attached SCSI (SAS) tape drives—partition name, number of tape drives in partition, drive location, SCSI element address, interface type, drive type, ready state, online status, barcode, media type, element address, vendor, model, physical serial number, logical serial number, SCSI ID, firmware level, control path status.

- I/O blade information—blade number, blade ID, location coordinates, serial number, WWNN, firmware version, and control LUN.

- Partition information—number of partitions, number of cleaning slots, number of unassigned slots, number of import/export (I/E) slots, I/E manual assignment setting, partition name, number of slots, number of tape drives, and number of cartridges.

E-mailing the Configuration Record

Administrators can use the **Tools - E-mail Configuration Record** screen on the Web client to e-mail the library configuration record.

Do not enter more than one e-mail address in the **E-mail Address** text box on the **Tools - E-mail Configuration Record** screen. If you need to send the configuration record to multiple e-mail addresses, repeat the procedure for each e-mail address.

Before you can e-mail the configuration record, the library e-mail account must be configured. For information on setting up the e-mail account, see <u>Configuring the Library E-mail Account</u> on page 92.

You cannot e-mail the library configuration record from the operator panel. The path to open the appropriate screen is as follows:

- From the Web client, select **Tools > E-mail Configuration Record**.

Saving the Configuration Record

Administrators can use the **Tools - Save Configuration Record** screen on the Web client to e-mail the library configuration record.

You cannot save the library configuration record from the operator panel. The path to open the appropriate screen is as follows:

- From the Web client, select **Tools > Save Configuration Record**.

Saving and Restoring the Library Configuration

The library has many configurable items, such as tape drive IDs, partitions, user accounts, Import/Export (I/E) stations, and cleaning slots. In the event of a hardware failure or firmware upgrade, the save and restore operations can be used to restore the library's firmware and configurable items to a previous state.

Note:	You cannot restore a saved configuration after removing or replacing a control module or expansion module. After removing and/or replacing the module, save the library configuration for future use.

Note:	The Saving and Restoring operations should not be performed concurrently by multiple administrators logged in from different locations. You can access the screens, but you cannot apply changes while another administrator is performing the same operation.

Saving the Library Configuration

Caution: Always save the library configuration after modifying a configurable item and before upgrading firmware. This allows you to restore the most current settings if necessary.

This operation saves your current library configuration and library firmware. Save your library configuration when it is in a known working state. In the event of a hardware failure, the saved configuration can be used to restore the configuration after hardware repairs are made. Before initiating a firmware upgrade, you should save the library configuration. You then have the option to restore the configuration after either a successful or an unsuccessful upgrade.

The Save/Restore Configuration operation is available only on the Web client. The path to open the appropriate screen is:

- From the Web client, select **Tools > Save/Restore Configuration**.

Restoring the Library Configuration and Library Firmware

You can restore the library's configurable items to a previous state using a saved configuration file. If you updated the library firmware since last saving the configuration, the library automatically restores the library firmware to the version that was saved with the configuration.

You can also downgrade library firmware to an earlier version using the **Tools > Update Library Firmware** command. Note that you will lose all your current library configuration information except for network settings, date and time, and license keys. You can restore the other configurable items using a configuration file that was saved when the earlier version of library firmware was installed on the library, or you can reconfigure your library's settings.

Note: The configuration file must be at the same or an earlier version of firmware than that which is currently installed on the library. You cannot restore a configuration file created with a later version of firmware.

> **Note:** If your library is running firmware version 600G or later, you can only restore a saved configuration that was created with firmware version 410G or later. If you need to restore a configuration created with firmware that is earlier than 410G, contact Quantum Support for assistance.

The Configuration operation is available only on the Web client. The path to open the appropriate screen is:

• From the Web client, select **Tools > Save/Restore Configuration**.

Troubleshooting "Library Not Ready" Messages

The operator panel and Web client each include a header that contains the company logo, product name, and the three main navigation buttons **Home**, **Help**, and **Logout**. In addition, a message in the header alerts you when the library is not ready. (No message displays in the header when the library is in a ready state.)

On the operator panel, **LIBRARY NOT READY** flashes at regular intervals whenever the library robotics are not yet ready to perform library functions. To view more information about the library's condition, select **Tools > About Library**. The **State** field on the **About Library** screen will display **Not ready**, followed, when applicable, by a brief explanation. For example, if the library door is open, the **State** field will display: **Not ready, door is open**.

The header in the Web client also alerts you when the library is not ready. For instance, if the library door is open, the header will display the following message: **Library's door is open**.

"Library Not Ready" messages appear in the header in the operator panel and the Web client under the following circumstances:

• The robot is in the process of calibrating. When the robot has finished calibrating, the "Library Not Ready" message no longer appears.

• The robot cannot calibrate. For example, a fiducial label is missing, preventing the robot from calibrating.

- The robot requires manual intervention. For example, the picker contains a tape cartridge that it cannot unload.

- The library door is open. The robot will not operate if the door is open.

- If none of the above situations apply, but the library is still not ready to operate, the header will display a "Library Not Ready" message without additional detail. The library generates a RAS ticket whenever the library enters a "not ready" state. The RAS ticket may provide information that can help you troubleshoot the problem. See <u>Viewing RAS Tickets</u> on page 482 for more information.

"Library Not Ready" messages continue to display in the header as well as on the **About Library** screen until the issue has been resolved, and the robot has completed its calibration.

Note: You may not see the "Library Not Ready" message in the Web client until the browser refreshes. Similarly, even if the problem has been resolved, the "Library Not Ready" message will not disappear from the Web client until the browser refreshes.

Duplicate Devices Discovered

If both target ports (ports 1 and 2) on an FC I/O blade are connected to the same host, or if more than one host is connected to a target port, you may see duplicates of all the devices connected to the initiator ports (ports 3 – 6) of that FC I/O blade. To prevent this from happening, you can do either (or both) of the following:

- If only one host is connected to a target port, you can use channel zoning to tell the target port which devices to see (see <u>Configuring FC I/O Blade Channel Zoning</u> on page 111).

- If more than one host is connected to a target port, you can use host mapping to tell each host which devices to see (see <u>Configuring Host Mapping</u> on page 118).

Duplicate Media Changer Devices Discovered

You may see one or more media changer devices (partitions) being discovered multiple times. For information on why this happens, see FC I/O Blade Internal Virtual Port for Media Changers on page 111.

To prevent this, do the following:

- Ensure that host mapping is enabled (see Enabling/Disabling FC Host Mapping on page 113).

- Assign each media changer a unique LUN and map each one to the appropriate host (see Configuring Host Mapping on page 118).

Identifying Tape Drives

You can use the operator panel and the Web client user interfaces to view information about all tape drives installed in the library. In addition, you can identify tape drives, including the control path tape drive, in selected partitions. The Web client also allows you to identify tape drives that are not assigned to specific partitions. On the Web client, you can only identify tape drives that are in a ready state.

The operator panel **Drive Information** screen lists the following information for each tape drive:

- Control path tape drive status — yes/no

- Vendor

- Model

- Type

- Serial number

- Tape drive firmware version

- Sled boot version

- Sled application version

- Mode status — online/offline, ready/not ready

- Loaded status — unloaded/loaded

- SCSI ID for SCSI tape drives

- World Wide Node Name (WWNN) for Fibre Channel (FC) tape drives

- SAS address for SAS tape drives

The Web client **Identify Drives** screen lists the following information for each tape drive:

- Location coordinates

- Mode status — online/offline

- State — ready/not ready

- Drive type

- Protocol

- Control path tape drive status — yes/no

- Vendor

- Physical serial number (P-SN)

- Logical serial number (L-SN)

- Tape drive firmware version

Note:	Bold column headings in the table can be sorted. For example, selecting the **Location** column heading will sort by location coordinates.

On the operator panel **Drive Information** screen, you can identify the tape drives assigned to the selected partition as well as the control path tape drive for the partition by flashing the green light-emitting diodes (LEDs) on the back of the tape drives.

- Use the **Identify All** button to flash the green LEDs on the back of the tape drives assigned to the partition. The LEDs blink 10 times per second for one minute.

- Use the **Identify Ctrl Path** button to flash the green LED on the back of the control path tape drive for the partition. The control path tape drive is used to connect each partition to the host application. Use

this button when you are cabling the library or troubleshooting the library control paths of tape drives. The green LED blinks 10 times per second for one minute.

On the Web client **Identify Drives** screen, you can identify the tape drives assigned to a particular partition, all unassigned tape drives, and the control path tape drive for each partition by flashing the green LEDs on the back of tape drives that are in a ready state:

- Use the **Identify All** button to flash the LEDs on the back of the selected tape drives. Only tape drives in a ready state will flash. If you have selected a specific partition or have only one partition configured, all the green LEDs on the tape drives within the partition will blink. If you have selected **Unassigned**, all the green LEDs on the unassigned tape drives will blink. If you have selected **All**, the green LEDs on all tape drives installed in the library will blink.

- Click **Identify Control Path** to flash the green LEDs on the back of the one or more control path tape drives. Only tape drives in a ready state will flash. The control path tape drive is used to connect each partition to the host application. Use this button when you are cabling the library or troubleshooting the library control paths of tape drives. If you have selected a partition, the green LED on the partition's control path tape drive will blink. If you have selected **All**, the green LEDs on all the ready control path tape drives will blink.

> **Note:** There is no control path tape drive for a partition that uses FC I/O blades to connect tape drives to a host application.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Tools > Identify Drives**.

- From the operator panel, select **Tools > Drive Info**.

Retrieving Tape Drive Logs

Administrators can use the Web client to retrieve tape drive logs. Tape drive log information can be used to help troubleshoot library and tape drive issues. You can use the **Retrieve Drive Log** screen to select the appropriate tape drive.

> **Note:** Bold column headings in the table can be sorted. For example, selecting the **Location** column heading will sort by location coordinates.

Details on retrieving tape drive log files include:

- Since the log retrieval process can take up to 30 minutes, the tape drive and associated partition are automatically taken offline during the operation and brought back online when the operation completes. You will be asked to confirm that you want to take the tape drive and partition offline.

  > **Note:** If the operation does not complete successfully, the partition remains offline until you turn it back online manually or restart the library (see <u>Taking a Partition Online or Offline</u> on page 76).

- Tape drive logs adhere to the following naming convention: **UDS_ID_SN.dmp**, where **ID** identifies the tape drive coordinate location within the library and **SN** identifies the tape drive serial number.
- You can select the interface type (SCSI, SAS, or FC) of the tape drive from which you want to retrieve logs.

For more detailed, step-by-step instructions, see your library's online Help. To access the online Help system, click the **Help** icon at the top right of the Web client or operator panel user interface.

You cannot retrieve tape drive logs from the operator panel. The path to open the appropriate screen is as follows:

- From the Web client, select **Tools > Drive Operations**.

Retrieving Tape Drive Sled Logs

Administrators can retrieve tape drive sled logs. Tape drive sled log information can be used to help troubleshoot library, tape drive sled, and tape drive issues. You can use the **Retrieve Drive Sled Log** screen to select the appropriate tape drive sled.

> **Note:** Bold column headings in the table can be sorted. For example, selecting the **Location** column heading will sort by location coordinates.

Details on retrieving tape drive sled log files include:

- Tape drive sled logs adhere to the following naming convention: **UDS_ID_SN.LOG**, where **ID** identifies the tape drive sled coordinate location within the library and **SN** identifies the tape drive sled serial number.

- You can select the interface type (SCSI, SAS, or FC) of the tape drive sled from which you want to retrieve logs.

- A **Save** dialog allows you to specify where you want to save the tape drive sled log files file.

For detailed, step-by-step instructions, see your library's online Help. To access the online Help system, click the **Help** icon at the top right of the Web client or operator panel user interface.

You cannot retrieve tape drive sled logs from the operator panel. The path to open the appropriate screen is as follows:

- From the Web client, select **Tools > Drive Operations**.

Identifying FC I/O Blades

Administrators can flash the green LED on a selected FC I/O blade to identify the physical location of the I/O blade in the library. After performing this blade operation, go to the back of the library and identify

the I/O blade with the rapidly blinking LED at the bottom of the FC I/O blade. The LED will blink for one minute.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Setup > I/O Blades > Blade Control**.

- From the operator panel, select **Setup > I/O Blades > Blade Control > Identify Blade**.

Permanently Removing FC I/O Blades

Library firmware monitors all FC I/O blades after they are installed in the library. Once an FC I/O blade is installed, the library expects the blade to be in the same installed location after every power cycle.

If an FC I/O blade is relocated or is permanently removed from the library, the library firmware must be configured to stop monitoring the blade. Administrators can perform this operation by selecting the FC I/O blade and performing the remove blade operation on the **Setup - FC I/O Blade Control** screen. If this is not done and the library continues to monitor a removed FC I/O blade, RAS tickets could be generated.

You do not need to configure the library to stop monitoring an FC I/O blade if the failed blade is replaced with a new blade. For instructions on how to remove and replace an FC I/O Blade, see <u>Adding, Removing, and Replacing FC I/O Blades</u> on page 443.

Performing the remove blade operation will cause a temporary loss of communication with connected hosts. The screen will display a warning message about the communication loss and ask you to confirm that you want to proceed.

Note: Before permanently removing the FC I/O blade, verify the location of the FC I/O blade. See <u>Identifying FC I/O Blades</u> on page 496.

> **Note:** This operation should not be performed concurrently by multiple administrators logged in from different locations. You can access the appropriate screens, but you cannot apply changes while another administrator is performing the same operation.

The paths to open the appropriate screens are as follows:

• From the Web client, select **Setup > FC I/O Blades > FC I/O Blade Control**.

• From the operator panel, select **Setup > FC I/O Blades > FC I/O Blade Control > Remove Blade**.

Resetting FC I/O Blade Ports

Administrators can reset individual ports on FC I/O blades. Resetting these ports can help troubleshoot FC I/O blade issues. The **Setup - Blade Control** screen allows you to perform the Reset Port operation on a selected FC I/O blade port.

Resetting an FC I/O blade port will cause a temporary loss of communication with connected hosts. The screen will display a warning message about the communication loss and ask you to confirm that you want to proceed.

> **Note:** This operation should not be performed concurrently by multiple administrators logged in from different locations. You can access the appropriate screens, but you cannot apply changes while another administrator is performing the same operation.

> **Note:** Before resetting FC I/O blade ports, verify the location of the FC I/O blade. See <u>Identifying FC I/O Blades</u> on page 496.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Setup > FC I/O Blades > FC I/O Blade Control**.

- From the operator panel, select **Setup > FC I/O Blades > FC I/O Blade Control > Reset Port**.

Viewing and E-Mailing the Command History Logs

When FC I/O blades are installed, administrators can use the **Command History Log** screens to view the most recent command and response activity that has occurred with externally addressable library devices, controller LUNs, partitions, and tape drives. This information can help you isolate the source of an issue, such as a library device or host application.

You can select any configured FC I/O blade in the library and display a list of associated library devices. For each device, you can view the command history log. You can also choose to e-mail the command history to a specific e-mail address. The log is sent as a text file attached to an e-mail message.

Before you can e-mail the command history log, the library e-mail account must be configured. For information on setting up the e-mail account, see <u>Configuring the Library E-mail Account</u> on page 92 in <u>Configuring Your Library</u>.

You cannot view command history logs from the Web client. The path to open the appropriate screen is as follows:

- From the operator panel, select **Tools > Command History Log**.

Interpreting LEDs

LEDs provide a visual indication about the status of certain library components. LEDs can sometimes communicate that a problem exists when RAS tickets cannot. For example, an LED can indicate a firmware problem that prohibits the library from generating RAS tickets.

The following components of the library have LEDs:

- Library control blade (LCB)
- FC I/O blade
- FC I/O fan blade
- Ethernet Expansion blade
- Tape drives
- Power supplies

Some of these components may also include a fibre port link LED.

Blade Status LEDs

This section covers status LEDs for:

- Library control blade (LCB)
- FC I/O blade
- FC I/O fan blade
- Ethernet Expansion blade

Figure 70 shows the location of the blade LEDs. Use Table 12 to interpret the current status of the LEDs.

Figure 70 Location of Blade
LEDs

Library Control Blade

Fibre-channel I/O Blade and Fan Blade

Ethernet Expansion Blade
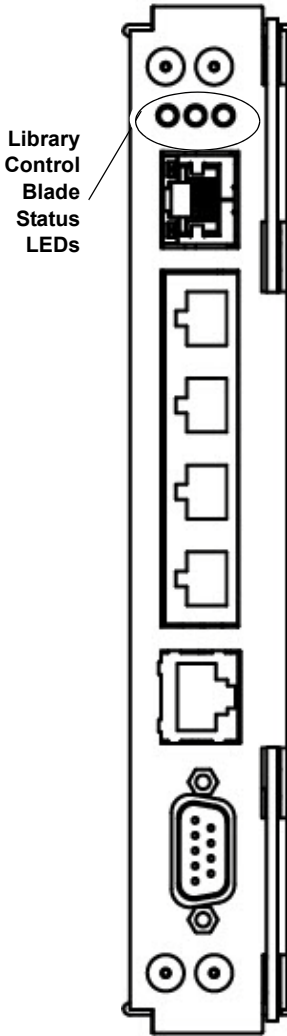
Library
Control
Blade
Status
LEDs
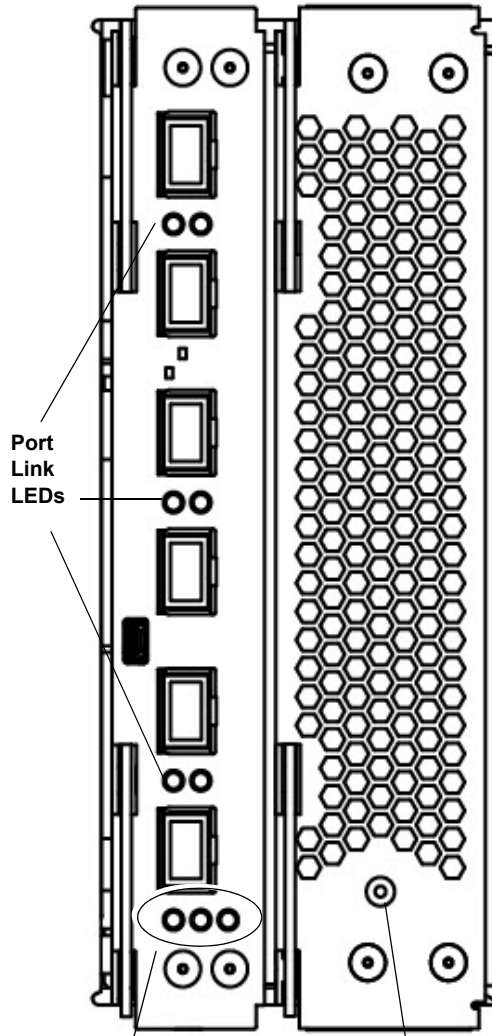
Port
Link
LEDs

Ethernet
Port LEDs

FC I/O Blade
Status LEDs

FC I/O Fan
Blade LED
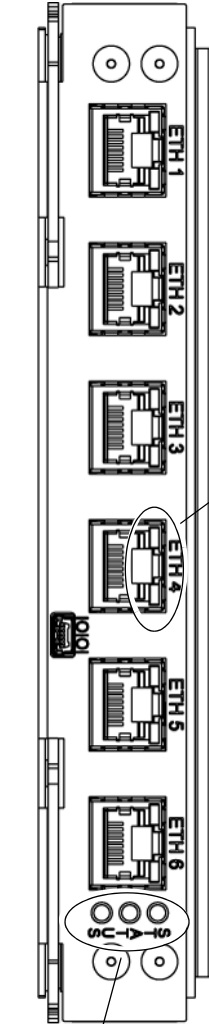
Ethernet Expansion Blade
Status LEDs

Table 12   Blade Status LEDs

LED Color	Represents	Blade Status
Green	Library application code/Blade processor status	• Blinks once per second — Normal operation. • Solid ON — Not operational. • Solid OFF — Not operational (or blade is booting). • Solid ON for 3 seconds, then blinks twice (FC I/O blade only) — Blade firmware is downloading. • Blinks 10 times per second (FC I/O blade only) — Identify mode (per user request, to distinguish it from other blades; see <u>Identifying FC I/O Blades</u> on page 496).
Amber	Health status	• Solid OFF — Normal operation. • Blinks once per second (LCB only) — Library application code is not operating or firmware upgrade/downgrade is in progress on existing compact flash. • Solid ON — • LCB — Failure OR blade is booting up or initial firmware update on new compact flash. If solid ON for more than 10 minutes, the LCB may need to be replaced. • FC I/O Blade — Failure OR blade is booting up or blade firmware is autoleveling. • FC I/O Fan Blade — There may be one or more problems, including: fan speed is too high or too low; temperature is too high; there is a faulty fan speed sensor; or there is a power control problem. • Ethernet Expansion blade — Failure OR blade is booting up. **Note:** In most cases solid ON means a failure; however, in conjunction with the blue LED blinking once every 10 seconds, an amber LED solid ON can be a normal condition for a short period of time. Autoleveling takes about three minutes per blade, and blades autolevel in series. Never remove a blade when the amber LED is solid ON unless it has been on continuously for at least 10 minutes. Never remove an LCB while the library is powered on.

LED Color	Represents	Blade Status
Blue	Power Control status	• Blinks once every 10 seconds — Normal. Blade is powered on. • Solid ON — • LCB — Error condition. Power off library before removing or replacing the LCB. • FC I/O blade — Swap mode: Blade is ready to be removed or replaced. • Ethernet Expansion blade — Blade is not operational. • Solid OFF — Blade is not receiving power. • Blinks once per second (Ethernet Expansion blade) — Powered off. Ready to remove.

Blade Port LEDs

This section describes blade port LEDs.

LCB Ethernet Hub Port LED

The LED for an Ethernet hub port is located above the port. Use Table 13 to interpret Ethernet hub link activity on an LCB.

Table 13   LCB Ethernet Hub Link Activity

LED Color	Represents	Fibre Port Link Status
Amber	Link and activity	• Solid ON — The link is up. • Blinks — The link is up and currently transmitting commands.

Fibre Port Link LED on FC I/O Blades

A fibre port link LED on a FC I/O blade shows the current state of an FC link and indicates whether or not the link is ready to transmit commands.

The link LED for an FC I/O blade fibre port is located either below or above the port. For each link LED pair on the FC I/O blade, the LED on the left belongs to the fibre port below. The LED on the right belongs to the fibre port above. Black lines on the FC I/O blade faceplate may indicate which LED belongs to which port.

Use Table 14 to interpret Fibre Channel link activity on an FC I/O blade.

Table 14   Fibre Port Link LED on FC I/O Blade

LED Color	Represents	Fibre Port Link Status
Green	Link and activity	• Blinking – Link with activity. • OFF – No link or link with constant activity*. • Solid ON – Blade is initializing.

* LED flashing increases as the activity increases and can actually appear off if the activity is high enough. Also, when the blade boots up, the link LEDs are all on until firmware initializes the ports, at which time they turn off until the port transmitter is enabled and link is acquired.

Ethernet Expansion Blade Ethernet Port LEDs

Table 15   Ethernet Expansion Blade Ethernet Port Link LED States

LED Color	Blade Status
Green	Solid ON — Link is up; data can be sent or received through the Ethernet port. Solid OFF — Link is down; data cannot be sent or received through the Ethernet port.
Amber	Blinks at irregular intervals — Data activity is occurring through the Ethernet port. Solid OFF — No data activity is occurring through the Ethernet port.

Servicing the LCB Based on LED Status

1 Observe the blinking patterns of the LEDs for at least 30 seconds.

2 Capture a snapshot of the library, and send it to Quantum Technical Support for analysis.

Tape Drive LEDs

RAS tickets typically report all problems related to tape drives, including error codes and TapeAlerts. By observing the blinking pattern of LEDs on tape drives, however, you can discern which operation the tape drive is currently performing.

Figure 71 shows where the tape drive LEDs and the fibre port link LED are located.

Figure 71 Location of Tape Drive LEDs
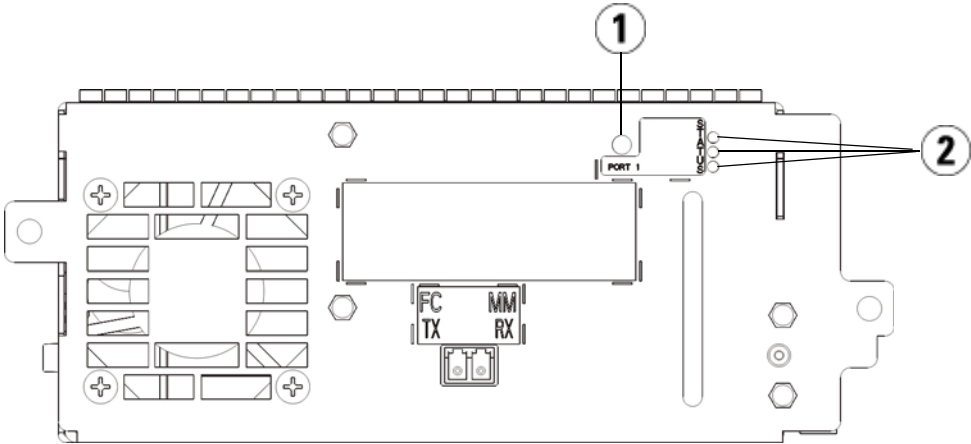
| 1 | Fibre Port LED |
| 2 | Tape Drive LEDs |

Use Table 16 to interpret tape drive activity:

Table 16 Tape Drive LEDs

LED Color	Represents	Tape Drive Status
Green	Processor activity	• Blinks once per second — Normal operation. • Solid ON/ Solid OFF — Tape drive's main processor is not operating. • 10 blinks per second — Identify mode (see <u>Identifying Tape Drives</u> on page 492). • Blinks 3 times in 3 seconds, then pauses (solid off), and then repeats — Tape drive is initializing. • Solid on for 3 seconds, then blinks twice — Tape drive firmware is downloading. • 2 quick blinks within 1.25 seconds; then on solid for 1.25 seconds; repeat — Drive sled firmware is downloading.
Amber	Health of the tape drive	• Solid OFF — Normal operation. • Solid ON — Drive has failed.
Blue	Power control status	• Blinks once every 10 seconds — Normal operation. • Solid ON — Offline. Ready to be removed or replaced. • Solid OFF — Tape drive is not receiving power.

**Tape Drive Fibre Port
Link LED**

The fibre port link LED shows the current state of the FC link and indicates whether or not the link is ready to transmit commands. The fibre port link LED on a tape drive is located on the rear of the tape drive, beside the fibre port.

Use Table 17 to interpret FC link activity:

Table 17   Fibre Port Link
Status

LED Color	Represents	Fibre Port Link Status
Green	Loop initialization protocol (LIP) and activity	• Solid ON — Loop initialization protocol (LIP) has occurred. • Blinks at regular intervals — Host command/data activity is occurring.
Amber	Online and light detected	• Solid ON — The library has enabled the tape drive data bus, and it can detect light through a fibre optic cable.
No color	No activity or no light detected	• Solid OFF — Either the tape drive is off or the tape drive cannot detect light through a fibre optic cable (which is equivalent to a missing fibre cable). If the tape drive is offline, the tape drive's blue status LED will be solidly lit.

Power Supply LEDs

RAS tickets typically report all problems related to power supplies. You can also observe the blinking pattern of LEDs on power supplies to see if the they are functioning appropriately.

Power supply LEDs indicate status by the rate at which they blink. The color of the LED identifies the area of the component being reported.

Use Table 18 to interpret power supply activity.

Table 18   Power Supply Status

LED Color and Location	Represents	Power Supply Status
Green (top)	AC OK	• Solid ON — The power supply's AC input is above the minimum requirements to operate. • Solid OFF — The power supply's AC input is below the minimum requirements to operate.
Green (middle)	DC OK	• Solid ON — The power supply's output voltage is within regulation. • Solid OFF — The power supply's output voltage is not within regulation.
Blue (bottom)	Standby	• Solid OFF — Normal. • Solid ON — Swap mode: Ready to be removed or replaced.

In the RAS tickets associated with the defective power supply, record both the number of the module and the number of the power supply connected to that module.

The expansion modules are numbered according to their position in relation to the control module. The control module is assigned the number 0. All expansion modules stacked beneath the control module are assigned a negative number, while expansion modules stacked above the control module are assigned a positive number. For example, expansion module -2 is the second expansion module beneath the control module, while expansion module +2 is the second expansion module above the control module.

Each module can have up to two power supplies. The power supply on the left is #1, while the power supply on the right is #2.

Using the Installation Verification Test

Administrators can run the Installation Verification Test (IVT) following a library service action to determine if the library is ready for production use. Examples of such library service actions include installing a new library or replacing a FRU or CRU.

Note:	IVT is optimized for library firmware versions 520G and above and libraries built after July 1, 2008 (serial numbers with last four digits 8602 and above). • If your library was built on or before July 1, 2008, and you are running firmware version 520G or above, you will not be able to run the IVT test, even though the selection is available. • If your library was built on or before July 1, 2008, and you are running firmware version 500G or below, you can run the test, but it is not recommended because it may produce erroneous results.

A new IVT Log is created each time you run IVT. The log reports detailed information about library readiness and indicates where specific marginal conditions and failures are located in the library subsystems if there are any.

The full IVT is divided into five subtests. You may choose to run only certain subtests depending on the amount of time available and your area of interest. The full IVT may take up to five and one-half hours to complete for a maximum configured library that includes five modules, five I/E stations and 18 drives.

- The **Robot** test evaluates the basic functionality of the library robotics assembly, including the picker assembly and the Y-carriage assembly, the barcode scanner and the calibration sensors. Time required to complete the Robot test is five minutes.

- The **Frame** test assesses the control and expansion module configuration and alignment.Time required to complete the Frame test is three minutes per module.

- The **I/E Station** test assesses the configuration and functionality of each I/E station. Time required to compete the I/E Station test is three minutes per I/E station.

- **Drives** performs functional tests on the library drives. Time required to complete the Drives test is 15 minutes per drive.

- **Tour** moves a scratch data cartridge through all storage slots in the extreme library locations. It also scans the top and bottom-most slots in the library. Time required to complete the Tour is five minutes per module.

Details on running the IVT subtests include:

- All IVT subtests are preselected by default. Clear the check box next to a subtest name to exclude that test from this IVT run. Select **Apply** when you are ready to run the IVT.

- The Robot, Drives and Tour subtests each require that you to provide a scratch data cartridge before the test can begin. If you select one of these subtests, you will be prompted to place a scratch data cartridge into the top I/E station slot. When you close the I/E station, the **Assign I/E** screen appears if the **Manual Cartridge Assignment** setting is enabled on the operator panel **System Settings** screen (**Tools > System Settings**). Assign the new scratch data cartridge to the **System** partition, and then select **Apply**.

- The Drives subtest only tests those tape drives that have the same media type as the scratch data cartridge. For example, if the scratch data cartridge is LTO-3, then all tape drives that are not LTO-3 will be skipped in the Drives test. If the tape drives in the library have different media types, you must run the Drives test multiple times with a different scratch data cartridge for each tape drive media type.

- If a subtest is missing required resources (for example, scratch data cartridges) the subtest will fail.

- The IVT starts by performing an inventory of the library. The inventory is recorded in the IVT log along with the test results.

- Select **Details** on the **Library Test Progress** screen to see the IVT results. If the IVT is still running, you will only see results for tests that have completed.

- Select **Stop** on the **Library Test Progress** screen to cancel the current IVT run between subtests. The last issued commands will complete before library control is returned.

- Once the selected tests are complete, select **Next**. You can choose to view the detailed IVT log or e-mail the detailed IVT log. Make your choice and select **Next**.

The IVT test cannot be performed from the Web client. The path to open the appropriate screen is as follows:

- From the operator panel, select **Tools > Library Tests > Installation & Verification Tests**.

Viewing the IVT Logs

A new IVT log is created each time you run IVT. The log reports detailed information about library readiness and indicates where specific marginal conditions and failures are located in the library subsystems if there are any. You can view a summary or detailed version of a log following an IVT run.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Reports > Log Viewer > Installation Verification Test Summary Log**.

- From the Web client, select **Reports > Log Viewer > Installation Verification Test Detailed Log**.

- From the operator panel, select **Tools > Library Tests > View Last Summary Log**.

- From the operator panel, select **Tools > Library Tests > View Last Detailed Log**.

Saving and E-mailing the IVT Logs

You can save and e-mail the summary and detailed IVT logs as a text file using the Web client. From the operator panel, you can e-mail the detailed IVT log as a text file.

The path to open the appropriate screens are as follows:

- From the Web client, select **Reports > Log Viewer > Installation Verification Test Summary Log**.

- From the Web client, select **Reports > Log Viewer > Installation Verification Test Detailed Log**.

- From the operator panel, select **Tools > Library Tests > E-mail Last Detailed Log**.

Running Library Demo

Administrators can run Library Demo, a simple way to test robotics functionality following a FRU or CRU replacement. It shows the library's ability to correctly move a scratch data cartridge from an I/E station to randomly selected open storage slots until the demonstration is stopped.

Details on running Library Demo include:

- Media in the storage magazines are not affected by the demonstration. The scratch data cartridge is returned to the I/E station following each cycle of 20 moves or when the demonstration is stopped.

- Before running Library Demo, ensure that no host applications are accessing the library.

- After you select **Library Demo** on the **Tools > Library Tests** screen, you will be prompted to place a scratch data cartridge into the top I/E station slot. The library robot will use this cartridge to perform its moves during the demonstration.

- When you close the I/E station, the **Assign I/E** screen appears if the **Manual Cartridge Assignment** setting is enabled on the operator panel **System Settings** screen (**Tools > System Settings**). Assign the new scratch data cartridge to the **System** partition, and then select **Apply**.

- Before the demonstration starts, the library may perform an inventory. If the screen shows the flashing "Library Not Ready" message, which indicates that an inventory is occurring, wait until the library is ready before you select **Apply** to begin Library Demo.

- The operator panel will show that the demonstration is in progress. There is an intentional delay of two seconds between move media commands to prevent unnecessary wear on the robotics

- To stop the demonstration, select **Stop** on the **Library Demo** screen. The last issued commands will complete before the demonstration is stopped and library control is returned. The operator panel will display a "Demo Being Stopped" message.

Library Demo cannot be performed from the Web client. The path to open the appropriate screen is as follows:

- From the operator panel, select **Tools > Library Tests > Library Demo**.

Configuring the Internal Network

When installing your library, you need to make sure that the external network setting is different than the internal network setting on the library. If the external and internal network settings are the same, the Web client cannot connect to the library. If DHCP is enabled or you do not know what your external network setting is, check with your network administrator.

From the operator panel, you can change the setting of your internal network using the **Internal Network Configuration** screen. Select the new internal IP address from the list on the screen.

The screen is only accessible from the operator panel. The path to open the appropriate screen is:

• From the operator panel, select **Tools > Internal Network**.

Library Diagnostics

The Diagnostics menu contains a number of tests you can run to determine if tape drives, robotics, and Q-EKM path (if Q-EKM is licensed) are working as they should. The following sections describe the Diagnostics tests:

• <u>Drive Diagnostics</u> on page 514

• <u>Robotics Diagnostics</u> on page 517

• <u>Using EKM Path Diagnostics</u> on page 183 (only available if EKM is licensed on the library)

Notes about Diagnostics include:

• Only users with Admin level privileges can access Diagnostics.

• Only one user can be logged into Diagnostics at a time. Entering Diagnostics disconnects all other library users with the same or lower privileges, on both the operator panel and the Web client. When one Admin-level user is logged into Diagnostics, all other users with

Admin level privileges and below will be unable to log in to the library and will get an error message stating that Diagnostics is in progress.

- Entering Diagnostics takes all your library partitions offline. Be sure any crucial operations have stopped before you enter Diagnostics. When you exit Diagnostics, your partitions return to the online/offline status they were in previously.

Diagnostics cannot be performed from the operator panel (the only exception is the Drive Reset operation; see <u>Drive Reset</u> on page 514). The path to open the appropriate screen is as follows:

- From the Web client, select **Tools > Diagnostics**.

Drive Diagnostics

Drive diagnostics are separated into the following categories:

- <u>Drive Tests</u> — Tests any tape drive and does not require you to use a scratch tape.
- <u>Media Tests</u> — Tests only IBM tape drives and requires you to insert a scratch tape in the top I/E station slot to perform the test.
- <u>Ethernet Expansion Blade Control</u> — Allows you to power cycle an Ethernet Expansion blade and remove an Ethernet Expansion blade from the library's configuration.

Drive Tests

The Drive Tests currently include only one test, the Drive Reset operation.

Drive Reset

The Drive Reset operation power cycles the tape drive while the tape drive remains in the drive sled in the library. You may want to perform a reset if a tape drive does not come ready or it is not behaving properly (for example, if a tape is stuck in the drive and will not unload).

After the reset operation completes, the tape drive is rebooted and reconfigured. This takes about 60 seconds. Wait 60 seconds before performing further drive operations.

> **Note:** This operation should not be performed concurrently by multiple administrators. You can access the screen, but you cannot apply changes while another administrator is performing the same operation.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Tools > Diagnostics**, then select **Drives > Drive Tests > Drive Reset**.

- From the operator panel, select **Tools > Drive Mgmt > Reset drives**.

Media Tests

The Media Tests are drive tests that require you to insert a scratch or suspect tape into the library's top (uppermost) I/E station slot. You can only run these tests on IBM tape drives. The following tests are available:

- **Drive Self Test —** Performs the drive's Power On Self Test (POST) to make sure that drive hardware is working properly.

- **Read/Write Test —** Reads and writes 96 wraps worth of data in each of the scratch tape's four data sections. During the test, the drive overwrites the data on the scratch tape.

- **Fast Read/Write Test —** Reads and writes two wraps worth of data in each of the scratch tape's four data sections. During the test, the drive overwrites the data on the scratch tape.

- **Media Test —** Run this test if you suspect media damage in a tape cartridge. Since media damage usually comes from the tape edges, this test reads and writes two wraps worth of data on each of the two outside data bands on both edges of the tape for the entire length of the tape. For this test, insert the suspect cartridge in the top I/E station slot. The data will be overwritten on the suspect cartridge.

Media tests cannot be performed from the operator panel. The path to open the appropriate screen is as follows:

- From the Web client, select **Tools > Diagnostics > Drives > Media Tests**.

Ethernet Expansion Blade Control

The Ethernet Expansion Blade Control menu allows you to perform the following functions:

- Power Cycling the Ethernet Expansion Blade

- Removing an Ethernet Expansion Blade from the Library's Configuration

Power Cycling the Ethernet Expansion Blade

Administrators can power cycle individual Ethernet Expansion blades in the library. You might want to power cycle an individual Ethernet Expansion blade when troubleshooting, such as when resolving a Reliability, Availability, and Serviceability (RAS) ticket.

From the **EE Blade Control** screen, click the **Cycle** button corresponding to the Ethernet Expansion blade you want to power cycle.

> **Note:** Power cycling an Ethernet Expansion blade may cause key exchange failures if FIPS is enabled.

It takes approximately 1 minute to power cycle an Ethernet Expansion blade. The status displays as "Booting" during the power cycle.

You can only power cycle the Ethernet Expansion blade from the Web client. The path to open the appropriate screen is as follows:

- From the Web client, select **Tools > Diagnostics > Drives > EE Blade Control**.

Removing an Ethernet Expansion Blade from the Library's Configuration

This feature is described in detail in Permanently Removing or Relocating an Ethernet Expansion Blade on page 472.

Robotics Diagnostics

The Robotics diagnostics currently include only one test, the Get/Put Test.

Get/Put Test

The Get/Put Test requires the robot to remove one tape cartridge from the top I/E station slot, and then put the tape cartridge back into the same slot. To run this test, you must insert a tape into the library's top (uppermost) I/E station slot.

Robotics tests cannot be performed from the operator panel. The path to open the appropriate screen is as follows:

• From the Web client, select **Tools > Diagnostics > Robotics > Robotics Get/Put Test**.

Working With Cartridges and Barcodes

This chapter describes how to work with cartridges and barcodes. When working with tape cartridges, certain considerations should be taken into account. For example, all tape cartridges in the library must have a barcode label. In addition, when loading your library, you should be aware of whether or not your cartridges are write-protected.

This chapter discusses these types of items in general terms. See Library Specifications on page 524 for information on what type of tape cartridges are supported for each drive type.

This chapter covers:

- Handling Cartridges Properly
- Write-Protecting Cartridges
- Barcode Label Requirements
- Supported Barcode Formats
- Installing Barcode Labels

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 on 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.

• Store cartridges in a location that is as free from dust as possible. Dust can damage or degrade performance of tape media.

• For external long-term vaulted storage, store cartridges in a vertical orientation.

• If cartridges must be stacked horizontally for moving and handling, do not stack cartridges more than five high.

• The operating temperature range for Linear Tape Open (LTO) cartridges is 50°F to 113°F (10°C to 45°C). The operating relative humidity range is 10% to 80% (non-condensing). The storage temperature range is 60.8°F to 89.6°F (16° to 32°C). Temperatures above 125.6°F (52°C) can cause permanent damage.

• 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 barcode 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 tape drives.

- Do not touch the tape or tape leader.

> **Caution:**   Do not degauss cartridges that you intend to reuse.

Write-Protecting Cartridges

All cartridges have a write-protect (write-inhibit) switch to prevent accidental erasure or overwriting of data. Before loading a cartridge into the library, make sure that the write-protect switch is positioned correctly (either on or off).

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.

Barcode Label Requirements

Cartridges must have an external barcode label that is machine readable. Quantum-supplied barcode labels provide the best results. Barcode labels from other sources can be used, but they must meet the following requirements:

> **Note:**   Checksum characters are not supported on barcode labels.

- ANSI MH10.8M-1983 Standard.

- Font: Code 39 (3 of 9).

- Allowable characters: Uppercase letters A to Z and numeric values 0 to 9.

- Number of characters: 5 to 16 (default for LTO is 6+2).

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

- Background reflection: Greater than 25 percent.

- Print contrast: Greater than 75 percent.

- Ratio: Greater than 2.2.

- Module: Minimum .254 mm (10 mil).

- Print tolerance: ± 57 mm.

- Length of the rest zones: 5.25 mm ± 0.25 mm.

- No black marks may be present in the intermediate spaces or rest
  zones.

- No white areas may be present on the bars.

Supported Barcode Formats

Quantum supplies industry standard LTO barcode labels with a length of
6 + 2 corresponding to the Standard Six and Plus Six formats listed below.
For advanced uses, your Quantum library supports label lengths of up to
16 characters allowing you to create custom labels. Refer to Barcode Label
Requirements on page 520 for label details.

The library supports the following tape cartridge barcode formats:

- **Standard —** Five to 16 characters total, including a barcode number
  and optional two-character media ID. If a media ID is included, the
  label must have a five to 14 character barcode number followed by a
  media ID; for example, "XXXXXXXXXXXXXL4". If a media ID is not
  included, the label must have a five to 16 character barcode number;
  for example, "XXXXX" or "XXXXXXXXXXXXXXXX". Only the
  barcode number is reported to the host.

- **Standard Six** — Six character barcode number with or without a two-character media ID; for example, "XXXXXXL4" or "XXXXXX". Only the six character barcode number is reported to the host.

- **Plus Six** — Six character barcode number followed by a two-character media ID; for example, "XXXXXXL4". The six character barcode and media ID are reported to the host.

- **Extended** — Five to 16 characters total, including a barcode number and optional two-character media ID. All characters are reported to the host, regardless of the barcode label having a media ID or not. If a media ID is included, the label must have a five to 14 character barcode followed by a media ID; for example, "XXXXXXXXXXXXL4". If a media ID is not included, the label must have a five to 16 character barcode number; for example, "XXXXX" or "XXXXXXXXXXXXXXXX".

- **Media ID Last** — Five to 14 character barcode number followed by a two-character media ID, for example, "XXXXXXXXXXXXL4". The media ID is reported to the host last, as in "XXXXXXXXXXXXL4".

- **Media ID First** — Five to 14 character barcode number followed by a two-character media ID, for example, "XXXXXXXXXXXXL4". The media ID is reported to the host first, as in "L4XXXXXXXXXXXXX".

Installing Barcode Labels

Each cartridge in the library must have an external label that is machine readable to identify the barcode. Most manufacturers offer cartridges with the labels already applied or with the labels included that you can attach.

All barcode labels must be applied to the front of a cartridge. Peel off the label and place it on the cartridge. The label must be placed entirely within the recessed area on the cartridge. Verify that the label is oriented so that the numbers appear above the barcode (see on page 523).

Place the barcode label as level as possible in the provided space for the label. If the label is not placed horizontally level, barcode label scan/read operations may encounter difficulties reading the label.

The cartridge cannot have any stickers or labels attached to the top or bottom because if the labels come loose, they can get caught in the tape drives or become unreadable by the scanner.

Caution: Do not place a barcode label or any labels on the top or bottom of a cartridge. Doing so can cause the tape cartridge and tape drive operations to fail.

Figure 72 Barcode Label Orientation
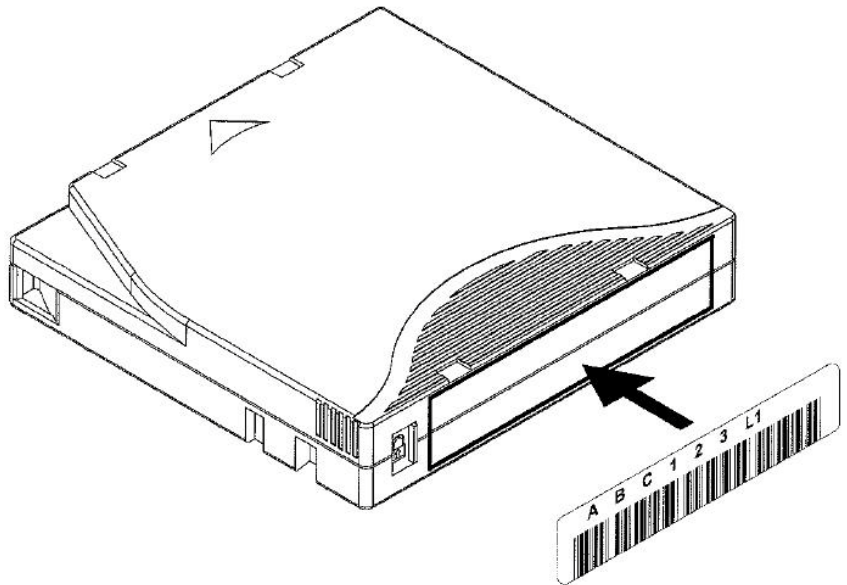
Library Specifications

Scalar i500 libraries follow the specifications described in this chapter.

Supported Components

The Scalar i500 library supports the following components.

Supported Cartridges	• LTO-1 (read-only in LTO-3 drives)
	• LTO-2 (read/write in LTO-2 and LTO-3 drives; read-only in LTO-4 drives)
	• LTO-3 (read/write in LTO-3 and LTO-4 drives; read-only in LTO-5 drives; supports write-once, read-many (WORM) functionality)
	• LTO-4 (read/write in LTO-4 and LTO-5 drives; supports WORM functionality)
	• LTO-5 (read/write in LTO-6 drives; supports WORM functionality)
	• LTO-6 (read/write in LTO-6 drives; supports WORM functionality)

Supported Tape Drive Types	• IBM LTO-2 (SCSI and Fibre Channel)
	• RoHS-compliant IBM LTO-3 (SCSI and Fibre Channel)
	• RoHS-compliant HP LTO-4 (Fibre Channel and SAS)
	• RoHS-compliant IBM LTO-4 (SCSI, Fibre Channel, and SAS)
	• HP LTO-5 Dual Port Fibre Channel Tape Drive
	• HP LTO-5 Single Port SAS Tape Drive
	• IBM LTO-5 Single Port Fibre Channel Tape Drive
	• LTO-5 Dual Port SAS Tape Drive
	• LTO-6 Single Port Fibre Channel Tape Drive
	• LTO-6 Dual Port SAS Tape Drive
Supported SAS Cable	SFF-8088
Library Robot Control	Logical Unit Number (LUN)
Connectivity	Native drive interface
Power	350W with optional redundant power supply and line cord
Library Management	• Operator panel touch screen
	• Web client
	• SNMP protocol
	• SMI-S protocol

Library Capacity

Library capacity is as follows.

> **Note:** Slot counts in this user's guide do not include five inaccessible slots in the bottom row of any library configuration. For more information about these slots, see <u>Unused Slots</u> on page 247.

	5U	**14U**	**23U**	**32U**	**41U**
Maximum Available Storage Slots (Including I/E Station Slots)	41	133	225	317	409
I/E Station Slots Available	0, 6	0, 6, 12, 18	0, 6, 12, 18, 24, 30	0, 6, 12, 18, 24, 30, 36, 42	0, 6, 12, 18, 24, 30, 36, 42, 48, 54
Maximum Drive Capacity	2	6	10	14	18
Maximum Power Supplies	2	4	6	8	10
Maximum Partitions	2	6	10	14	18
Maximum FC I/O Blades	0	2	4	4	4

Environmental Requirements

The environmental requirements for the library are listed below.

> **Note:**   Temperature ranges apply to product inlet temperatures, not necessarily to ambient room temperatures. Airflow restrictions or other heat-generating equipment within the rack enclosure may cause a rise over ambient room temperatures.

	Operating	**Non-Operating**	**Storage**
Altitude	Up to 10,000 ft. (3,048 m)	Up to 10,000 ft. (3,048 m)	Up to 10,000 ft. (3,048 m)
Temperature	50º to 104º F (10º to 40º C)	50º to 113º F (10º to 45º C)	–40º to 150º F (–40º to 65º C)
Relative Humidity	20 to 80%, non-condensing	10 to 90%, non-condensing	0 to 95%, non-condensing

Electrical Requirements

Electrical requirements for the library are: 100–240 VAC, 50–60 Hz

Dimensions

Library Configuration	Rack Height	H x W x D
5U control module	5U	8.6 in. x 17.4 in. x 31.4 in (21.9 cm x 44.2 cm x 79.8 cm)
9U expansion module	9U	15.8 in. x 17.4 in. x 31.4 in (40 cm x 44.2 cm x 79.8 cm)
5U control module + (1) 9U expansion module	14U	24.4 in. x 17.4 in. x 31.4 in (61.9 cm x 44.2 cm x 79.8 cm)
5U control module + (2) 9U expansion modules	23U	40.1 in. x 17.4 in. x 31.4 in (101.9 cm x 44.2 cm x 79.8 cm)
5U control module + (3) 9U expansion modules	32U	55.9 in. x 17.4 in. x 31.4 in (141.9 cm x 44.2 cm x 79.8 cm)
5U control module + (4) 9U expansion modules	41U	71.6 in. x 17.4 in. x 31.4 in (181.9 cm x 44.2 cm x 79.8 cm)

Component Weights

Component	Weight
Drive Sled	10 lbs (4.6 kg)
Power Supply	5 lbs (2.3 kg)
5U Chassis (empty)	60 lbs (27.2 kg)

Component	Weight
9U Chassis (empty)	65 lbs (29.5 kg)
5U Packaging Kit	20 lbs (9 kg)
9U Packaging Kit	24 lbs (10.9 kg)
14U Packaging Kit	40 lbs (18 kg)

Library Power Consumption and Heat Output

The typical library power consumption (Watts/hour) and heat output (BTU/hour) is listed below.

> **Note:** "Typical" values for tape drives assumes tape drives are writing.

Library Configuration	Typical Power Consumption (kW/Hour)	Typical Heat Output (BTU/Hour)
Subassembly Power Consumption:		
Scalar I500 Library with Robot and LCB (no tape drives installed; robot moving; LCB installed)	0.079	269.0
UDS3 IBM LTO-2 Drive Sled Module (SCSI)	0.029	99.0
UDS3 IBM LTO-2 Drive Sled Module (Fibre Channel)	0.032	109.2
UDS3 IBM LTO-3 Drive Sled Module (SCSI)	0.027	92.1
UDS3 IBM LTO-3 Drive Sled Module (Fibre Channel)	0.029	99.0
UDS3 IBM LTO-4 Drive Sled Module (SCSI)	0.038	129.7
UDS3 IBM LTO-4 Drive Sled Module (Fibre Channel)	0.040	136.5

Library Configuration	Typical Power Consumption (kW/Hour)	Typical Heat Output (BTU/Hour)
UDS3 IBM LTO-4 Drive Sled Module (SAS)	0.038	129.7
UDS3 HP LTO-4 Drive Sled Module (Fibre Channel)	0.037	126.2
UDS3 HP LTO-4 Drive Sled Module (SAS)	0.035	119.4
UDS3 IBM LTO-5 Drive Sled Module (Fibre Channel)	0.048	163.8
UDS3 HP LTO-5 Drive Sled Module (Fibre Channel)	0.030	102.4
UDS3 HP LTO-5 Drive Sled Module (SAS)	0.028	95.5
UDS3 IBM LTO-6 Drive Sled Module (Fibre Channel)	0.034	116.0
UDS3 IBM LTO-6 Drive Sled Module (SAS)	0.032	109.2
UDS3 HP LTO-6 Drive Sled Module (Fibre Channel)	0.030	102.4
UDS3 HP LTO-6 Drive Sled Module (SAS)	0.028	95.5
Fibre Channel I/O Blade	0.080	272.8
Ethernet Expansion Blade	0.010	34.1
Control Module:		
Minimum (no drives installed; robot not moving)	0.047	160.0
Maximum (2 drives writing; robot moving)	0.166	565.0
Expansion Module:		
Minimum (no drives installed; robot not moving)	0.012	41.0
Maximum (4 drives writing; 2 Fibre-Channel I/O blades installed; robot moving)	0.256	879.0

TapeAlert Flag Descriptions

TapeAlert is an open industry standard that flags errors and provides possible solutions for storage devices and their media. This section provides information about TapeAlert flags issued by tape drives, including the identifying number, severity, recommended message, and probable cause. Table 19 explains the severity codes, and Table 20 lists all the existing TapeAlert flags and their descriptions.

Support for specific TapeAlert flags may vary based on tape drive type and firmware revision. Not all tape drives support every TapeAlert. Consult your tape drive SCSI manual for more information.

For more information on TapeAlert, see http://www.t10.org/index.html for INCITS *SCSI Stream Commands - 3 (SSC-3)*.

Table 19   TapeAlert Flag Severity Codes

I	Informational.
W	Warning — The system may not be operating optimally. Continued operation without corrective action may cause a failure or raise critical TapeAlert flags.
C	Critical — Either a failure has already occurred or a failure is imminent. Corrective action is required.

Table 20   Tape Drive
TapeAlert Flag Descriptions

No.	Flag	Severity	Recommended Application Client Message	Probable Cause
1	Read warning	W	The tape drive is having problems reading data. No data has been lost, but there has been a reduction in the performance of the tape.	The drive is having severe trouble reading.
2	Write warning	W	The tape drive is having problems writing data. No data has been lost, but there has been a reduction in the capacity of the tape.	The drive is having severe trouble writing.
3	Hard error	W	The operation has stopped because an error has occurred while reading or writing data which the drive cannot correct.	The drive had a hard read or write error.
4	Media	C	Your data is at risk: **1** Copy any data you require from this tape. **2** Do not use this tape again. **3** Restart the operation with a different tape.	Media can no longer be written/read, or performance is severely degraded.
5	Read failure	C	The tape is damaged or the drive is faulty. Call the tape drive supplier help line.	The drive can no longer read data from the tape.
6	Write failure	C	The tape is from a faulty batch or the tape drive is faulty: **1** Use a good tape to test the drive. **2** If the problem persists, call the tape drive supplier help line.	The drive can no longer write data to the tape.

No.	Flag	Severity	Recommended Application Client Message	Probable Cause
7	Media life	W	The tape cartridge has reached the end of its calculated useful life: **1** Copy any data you need to another tape. **2** Discard the old tape.	The media has exceeded its specified life.
8	Not data grade	W	The tape cartridge is not data-grade. Any data you write to the tape is at risk. Replace the cartridge with a data-grade tape.	The drive has not been able to read the MRS* stripes.
9	Write protect	C	You are trying to write to a write-protected cartridge. Remove the write-protection or use another tape.	Write command is attempted to a write-protected tape.
10	Media removal prevented	I	You cannot eject the cartridge because the tape drive is in use. Wait until the operation is complete before ejecting the cartridge.	Manual or software unload attempted when prevent media removal on.
11	Cleaning media	I	The tape in the drive is a cleaning cartridge.	Cleaning tape loaded into drive.
12	Unsupported format	I	You have tried to load a cartridge of a type which is not supported by this drive.	Attempted load of unsupported tape format.
13	Recoverable mechanical cartridge failure	C	The operation has failed because the tape in the drive has experienced a mechanical failure: **1** Discard the old tape. **2** Restart the operation with a different tape.	Tape snapped/cut or other cartridge mechanical failure in the drive where medium can be demounted.

No.	Flag	Severity	Recommended Application Client Message	Probable Cause
14	Unrecoverable mechanical cartridge failure	C	The operation has failed because the tape in the drive has experienced a mechanical failure: **1** Do not attempt to extract the tape cartridge. **2** Call the tape drive supplier help line.	Tape snapped/cut or other cartridge mechanical failure in the drive where medium cannot be demounted.
15	Memory chip in cartridge failure	W	The memory in the tape cartridge has failed, which reduces performance. Do not use the cartridge for further write operations.	Memory chip failed in cartridge.
16	Forced eject	C	The operation has failed because the tape cartridge was manually demounted while the tape drive was actively writing or reading.	Manual or forced eject while drive actively writing or reading.
17	Read-only format	W	You have loaded a cartridge of a type that is read-only in this drive. The cartridge will appear as write protected.	Media loaded that is read-only format.
18	Tape directory corrupted on load	W	The directory on the tape cartridge has been corrupted. File search performance will be degraded. The tape directory can be rebuilt by reading all the data on the cartridge.	Tape drive powered down with tape loaded, or permanent error prevented the tape directory being updated.
19	Nearing media life	I	The tape cartridge is nearing the end of its calculated life. It is recommended that you: **1** Use another tape cartridge for your next backup. **2** Store this tape cartridge in a safe place in case you need to restore data from it.	Media may have exceeded its specified number of passes.

No.	Flag	Severity	Recommended Application Client Message	Probable Cause
20	Cleaning required	C	The tape drive needs cleaning: **1** If the operation has stopped, eject the tape and clean the drive. **2** If the operation has not stopped, wait for it to finish and then clean the drive. Check the tape drive user's manual for device-specific cleaning instructions.	The drive thinks it has a head clog or needs cleaning.
21	Cleaning requested	W	The tape drive is due for routine cleaning: **1** Wait for the current operation to finish. **2** Then use a cleaning cartridge. Check the tape drive user's manual for device-specific cleaning instructions.	The drive is ready for a periodic cleaning.
22	Expired cleaning media	C	The last cleaning cartridge used in the tape drive has worn out: **1** Discard the worn-out cleaning cartridge. **2** Wait for the current operation to finish. **3** Then use a new cleaning cartridge.	The cleaning tape has expired.
23	Invalid cleaning tape	C	The last cleaning cartridge used in the tape drive was an invalid type: **1** Do not use this cleaning cartridge in this drive. **2** Wait for the current operation to finish. **3** Then use a valid cleaning cartridge.	Invalid cleaning tape type used.

No.	Flag	Severity	Recommended Application Client Message	Probable Cause
24	Retension requested	W	The tape drive has requested a retension operation.	The drive is having severe trouble reading or writing, which will be resolved by a retension cycle.
25	Multi-port interface error on a primary port	W	A redundant interface port on the tape drive has failed.	Failure of one interface port in a dual-port configuration (for example, Fibre Channel).
26	Cooling fan failure	W	A tape drive cooling fan has failed.	Fan failure inside tape drive mechanism or tape drive enclosure.
27	Power supply failure	W	A redundant power supply has failed inside the tape drive enclosure. Check the enclosure user's manual for instructions on replacing the failed power supply.	Redundant power supply unit failure inside the tape drive enclosure or rack subsystem.
28	Power consumption	W	The tape drive power consumption is outside the specified range.	Power consumption of the tape drive is outside specified range.
29	Drive preventive maintenance required	W	Preventive maintenance of the tape drive is required. Check the tape drive user's manual for device-specific preventive maintenance tasks or call the tape drive supplier help line.	The drive requires preventative maintenance (not cleaning).
30	Hardware A	C	The tape drive has a hardware fault: **1** Eject the tape or magazine. **2** Reset the drive. **3** Restart the operation.	The drive has a hardware fault that requires reset to recover.

No.	Flag	Severity	Recommended Application Client Message	Probable Cause
31	Hardware B	C	The tape drive has a hardware fault: 1 Turn the tape drive off and then on again. 2 Restart the operation. 3 If the problem persists, call the tape drive supplier help line.	The drive has a hardware fault that is not read/write related or requires a power cycle to recover.
32	Primary interface	W	The tape drive has a problem with the host interface: 1 Check the cables and cable connections. 2 Restart the operation.	The drive has identified an interface fault.
33	Eject media	C	The operation has failed: 1 Eject the tape or magazine. 2 Insert the tape or magazine again. 3 Restart the operation.	Error recovery action.
34	Microcode update fail	W	The microcode update has failed because you have tried to use the incorrect microcode for this tape drive. Obtain the correct microcode and try again.	Microcode update failed.
35	Drive humidity	W	Environmental conditions inside the tape drive are outside the specified humidity range.	Drive humidity limits exceeded.
36	Drive temperature	W	Environmental conditions inside the tape drive are outside the specified temperature range.	Cooling problem.
37	Drive voltage	W	The voltage supply to the tape drive is outside the specified range.	Drive voltage limits exceeded.
38	Predictive failure	C	A hardware failure of the tape drive is predicted. Call the tape drive supplier help line.	Predictive failure of drive hardware.

No.	Flag	Severity	Recommended Application Client Message	Probable Cause
39	Diagnostics required	W	The tape drive may have a hardware fault. Run extended diagnostics to verify and diagnose the problem. Check the tape drive user's manual for device-specific instructions on running extended diagnostic tests.	The drive may have a hardware fault that may be identified by extended diagnostics (i.e., SEND DIAGNOSTIC command).
40 – 46	Obsolete			
47 – 49	Reserved			
50	Lost statistics	W	Media statistics have been lost at some time in the past.	Drive or library powered down with tape loaded.
51	Tape directory invalid at unload	W	The tape directory on the tape cartridge just unloaded has been corrupted. File search performance will be degraded. The tape directory can be rebuilt by reading all the data.	Error prevented the tape directory being updated on unload.
52	Tape system area write failure	C	The tape just unloaded could not write its system area successfully: **1** Copy data to another tape cartridge. **2** Discard the old cartridge.	Write errors while writing the system area on unload.
53	Tape system area read failure	C	The tape system area could not be read successfully at load time: **1** Copy data to another tape cartridge.	Read errors while reading the system area on load.
54	No start of data	C	The start of data could not be found on the tape: **1** Check that you are using the correct format tape. **2** Discard the tape or return the tape to your supplier.	Tape damaged, bulk erased, or incorrect format.

No.	Flag	Severity	Recommended Application Client Message	Probable Cause
55	Loading or threading failure	C	The operation has failed because the media cannot be loaded and threaded: **1** Remove the cartridge, inspect it as specified in the product manual, and retry the operation. **2** If the problem persists, call the tape drive supplier help line.	The drive is unable to load the media and thread the tape.
56	Unrecoverable unload failure	C	The operation has failed because the medium cannot be unloaded: **1** Do not attempt to extract the tape cartridge. **2** Call the tape driver supplier help line.	The drive is unable to unload the medium.
57	Automation interface failure	C	The tape drive has a problem with the automation interface: **1** Check the power to the automation system. **2** Check the cables and cable connections. **3** Call the supplier help line if problem persists.	The drive has identified an interface fault.
58	Microcode failure	W	The tape drive has reset itself due to a detected microcode fault. If problem persists, call the supplier help line.	Microcode bug.
59	WORM medium — integrity check failed	W	The tape drive has detected an inconsistency during the WORM medium integrity checks. Someone may have tampered with the cartridge.	Someone has tampered with the WORM medium.

No.	Flag	Severity	Recommended Application Client Message	Probable Cause
60	WORM medium — overwrite attempted	W	An attempt had been made to overwrite user data on a WORM medium: **1** If a WORM medium was used inadvertently, replace it with a normal data medium. **2** If a WORM medium was used intentionally: **a)** Check that the software application is compatible with the WORM medium format you are using. **b)** Check that the medium is bar-coded correctly for WORM.	The application software does not recognize the medium as WORM.
61 – 64	Reserved			

* Media Recognition System (MRS) is a method where pre-defined stripes are placed at the beginning of the media to identify the media. The MRS stripes are read to determine if the media is of data-grade. Data-grade media should be used in SCSI streaming devices since it is of the required quality and consistency to be used to store data (i.e., audio/video grade media should not be used).

Glossary

1U, 2U, 3U, etc. Racks manufactured for mounting computer hardware often define vertical space as "units." The components that are mounted in the racks are defined by how many units of rack space they require. For example, the height of a unit in a rack is 1.75 inches. If a component is 5.25 inches in thickness, the component is said to be a 3U component.

A

Arbitrated loop A Fibre Channel configuration that attaches multiple communicating ports in a loop. Two or more ports can interconnect, but only two ports can communicate simultaneously.

Arbitration The submission of a request to gain access to an arbitrated loop by a device, so that it can transmit data in the loop.

Availability A RAS attribute that refers to the accessibility of a system resource in a timely manner; for example, the measurement of a system's uptime.

B

Barcode A printed array of varied rectangular bars and spaces that can be scanned and read for object identification.

Bus A transmission channel through which electrical signals are carried from one device to another device.

C

CAN (Controller Area Network)   A serial bus network of microcontrollers that connects devices, sensors and actuators in a system or sub-system for real-time control applications. There is no addressing scheme used in controller area networks, as in the sense of conventional addressing in networks (such as Ethernet). Rather, messages are broadcast to all the nodes in the network using an identifier unique to the network.

Cartridge   A container that is a protective housing for storage media, such as cartridges for tapes or optical disks.

Channel zoning   A method of subdividing a storage area network into disjoint zones on a per-channel basis in order to enhance security and qualify access.

Cleaning tape / cleaning cartridge   A tape used to clean recording heads and reading heads on a tape drive.

Cleaning slot   The physical home where a cleaning tape or cartridge resides.

CLI (Command Line Interface)   A method of interfacing with a file system in which the user types commands, using a specific command syntax, from a command line.

COD (Capacity on Demand)   A library feature that allows users to have a large physical library, but only be licensed to use a subset of its total capacity. Users pay only for what they are currently using. License upgrades enable more capacity without causing a system interruption.

Compact flash   A card on the LCB that stores information about a library's contents and configuration.

Connectivity   The method by which hardware devices or software communicate with other hardware or software.

Control module   The first module of the library. It consists of an operator panel touch screen, library control blade (LCB), storage, tape drives, power supplies, I/E station.

Control path   The connection between a partition and host application. The control path connection is made through a designated tape drive. Only one tape drive can be selected as the control path per partition.

Controller   The PCB or system that translates computer data and commands into a form suitable for use by the storage disks.

CRU (Customer Replaceable Unit)   The smallest hardware component that can be replaced at a customer installation by a customer.

D

Default   A value or setting that is selected by the hardware or software unless specified otherwise by the user.

DHCP (Dynamic Host Configuration Protocol)   A protocol for assigning dynamic IP addresses to devices on a network. DHCP supports a mix of static and dynamic IP addresses.

Directory   A file that contains a list of other files. *Directory* is short for *directory file*.

Drivers   Software programs that enable a computer to communicate with hard drives, CD ROM drives, printers, and other peripherals. Drivers are stored on a hard disk and loaded into memory at boot up.

E

Element ID - Logical   An address used by a library to locate and track library component. The address is specified in programming logic rather than on the physical location of a component within a library. When a logical library is used, the logical element ID masks the physical element ID.

Element ID - Physical   An address used by a library to locate and track library component. The address is based on the physical location of a component within a library. Applications expect to see resources at specific IDs.

Ethernet   A type of local area network designed to transport data at rates up to 10 million bits per second. Other software, such as TCP/IP runs on top of Ethernet to provide high-level networking services to applications.

Event   A condition that matches a numbered, predefined set of circumstances.

Event log   A list of all predefined events logged by library and software management tools.

Expansion Module   An optional module of the library. It provides additional storage, tape drive capacity, power, and optional I/E stations. The module lacks an operator panel touch screen and LCB.

F

F_Port Fabric Port. A port on a fabric switch to which N_Ports may be directly connected. The F_Port is not capable of communicating with FC-AL protocol.

FC (Fibre Channel) A high speed data transfer architecture. Using optical fibre to connect devices, Fibre Channel communications are serial communications that occur at full duplex and achieve data transfer rates of 200 MBps.

FC-AL (Fibre Channel Arbitrated Loop) A form of Fibre Channel network in which up to 126 nodes are connected in a loop topology. See also *Arbitrated loop*.

FC-AL Device A device that employs Fibre Channel-Arbitrated Loop and consists of one or more NL_Ports.

Fiber A thin filament of glass. An optical waveguide consisting of a core and a cladding which is capable of carrying information in the form of light. Fiber is also a general term used to cover all physical media types supported by Fibre Channel, such as optical fiber, twisted pair, and coaxial cable.

Fiducial In a library storage context, fiducials may be "fiducial labels" or "fiducial tabs," allowing reliable identification of cartridge magazines and drive sleds, including both location and media domain information. In the Scalar i500 tape library, a "fiducial tab" refers to the plastic locator tabs which are installed on the media storage columns. The robot determines the location of these tabs to identify media storage locations. A "fiducial label" refers to the barcode label on cartridge magazines or drive sleds which identify magazine or drive sled type.

Firewall A set of security tools designed to separate an internal network from the public Internet in order to keep unauthorized users out of a restricted network. Firewalls are the primary line of security defense for businesses.

FL_Port Fabric Loop Port. An F_Port that is capable of supporting an attached Fibre Channel Arbitrated Loop. An FL_Port on a loop will have the AL_PA hex'00' giving the fabric the highest priority access to the loop. N_Ports or NL_Ports can attach to it in an Arbitrated Loop topology and are capable of communicating with FC-AL protocol.

FMR (Field Microcode Replacment) tape See *FUP (Firmware Upgrade) tape*.

FRU (Field Replaceable Unit)   The smallest hardware component that can be replaced at a customer installation by a certified field service representative.

G

Gb E or GigE (Gigabit Ethernet)   A transport protocol used for transmitting data across traditional LANs. GigE is an enhanced version of the Ethernet protocol that has been used for many years as the underlying transport technology in IP networks.

GUI (Graphical User Interface)   A computer environment that provides a visual view of a system by incorporating windows, icons, menus, and a pointing device. Also referred to as a Windows, Icons, Mouse, and Pointers (WIMP) interface.

H

HAT (Host Access Table)   The HP FC Storage Networking drive saves current and previously logged-in host information in a Host Access Table (HAT). An entry is a combination of a host's WWPN and the drive's FC port to which it is connected. Host information is stored and maintained in the HAT until filled up, in which case the oldest unused entry is freed to allow a new host to get registered in the HAT.

HDD (High Density Drive)   A drive that contains increased storage capacity of bits and/or tracks per square inch.

Home position   Accessor axes positioned at 0 vertical and 0 horizontal, that serve as the point of reference for the position of other library components. Home position is used as a basis for calibration.

Host   In general, a host is a computer or program that contains data and provides services to other computers or devices. In Fibre Channel terms, a host is a computer that initiates contact with storage devices.

Hot swappable   The ability to replace a defective component while the system continues to function normally.

HTTP (Hypertext Transfer Protocol)   The communication rules by which a Web browser (client) and a server delivering Web pages exchange information.

I

I/E (Import/Export or Insert/Eject)   The movement of data or hardware in and out of processing and storage systems.

I/E slot A bin that contains a single piece of media in the I/E station.

I/E station A door on the front of the library that contains tape magazines, into which cartridges to be imported are placed manually or cartridges to be exported are placed by the picker.

Interoperability The capability of two or more hardware devices or two or more software routines to work together.

IP (Internet Protocol) A protocol that specifies the formats of packets and addresses. Addresses are formulated as four groups of 2 or 3 digit numbers separated by periods, such as 255.255.255.255.

K

Kernel The heart of the UNIX operating system. The kernel is the part of the operating system that allocates resources and controls processes. The design strategy has been to keep the kernel as small as possible and to put the rest of the UNIX functionality into separately compiled and executed programs.

L

L_Port Loop Port. It only has the capability to communicate over FC-AL hubs and through FL_Ports.

LED (Light Emitting Diode) The mode of data transmission for multimode cables with short wave optical transceivers. Single-mode cables, by comparison, use high powered, long wave lasers.

Library A large-scale tape device with robotics that can house multiple tape drives and a significant amount of tape cartridges.

Library Control Module See *Control module*.

License key An absolute value that can only increase a licensed feature. For example, a license key can be applied to the library to enable unlicensed slots.

Logical library See *Partition*.

Loop With this Fibre Channel option, the port operates with attached loop-capable devices. If a point-to-point device is attached, the appliance is not able to communicate with it.

Loop ID A unique 7-bit value from 0 to 126 that represents the 127 valid AL_PAs (physical addresses) on a loop.

LTO (Linear Tape Open) A family of magnetic tape media that are "open" in the sense of not being owned by a single proprietor. LTO comes in two formats, Accelis and Ultrium. Accelis is the fast

access implementation, while Ultrium is the high capacity implementation.

LUN (Logical Unit Number)   A unique identifier used on a SCSI bus to distinguish between devices that share the same bus. A LUN can be an end user, a file, or an application. In storage technology, a single large storage device might be divided into smaller pieces, either to make the vast storage space more manageable or because the storage space is dedicated to different servers, drives, or applications. When the storage space is divided into smaller parts, each part is configured with its own SCSI unique identifier, or LUN.

M

Magazine   A container for removable media storage used in tape libraries.

Media   A material that stores data, such as tapes in cartridges or optical disks.

Media changer device   A SCSI term referring to a tape library or a partition, including the robot that services it.

Media ID   A barcode number attached to a specific piece of media.

Media type   A format/size of media, for example, LTO.

Medium   See *Media*.

Mixed media   The ability of a library to simultaneously support multiple types of storage media.

N

N_Port   Node Port. It only has the capability to communicate through an F-Port. It is a port on a computer, disk drive, and so on, through which the device does its Fibre Channel communication as a direct fabric-attached port for use with the point-to-point or fabric topology. It is identified by a World Wide Name.

NL_Port   Node Loop Port. It has the capability to communicate over both FC-AL hubs and through F_Ports.

O

Online   A status for a component that indicates it is active and available for use.

Operator Intervention Message   See *RAS ticket*.

OS (Operating System)   A control program for a computer that allocates computer resources, schedules tasks, and provides the user with a way to access the resources.

Partition   An abstraction of an underlying physical library that may present a different personality, capacity, or both to a host. It is a representation of real physical elements, combined to create a grouping that is different from the physical library. Also 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 application.

Pathname   A list of directories separated by slashes (/) and ending with the name of a directory or nondirectory file. A pathname is used to trace a path through the file structure to locate or identify a file.

Picker   The robotic hand that handles cartridges.

Point to Point   A Fibre Channel topology that consists of a dedicated connection between two devices: a sending device and a receiving device.

Rackmount   An industry standard communication and computer equipment rack cabinet.

RAS (Reliability, Availability, and Serviceability)   Three key attributes of computing system quality design. See *Reliability*, *Availability*, and *Serviceability*. An infrastructure to support serviceability in order to identify, diagnose, and fix problems within the system. This approach is designed to address the ability of service personnel and customers to diagnose and resolve problems identified within the system. Additionally, configuration is addressed to support detection of hardware configuration compatibility issues and persistence across FRUs.

RAS ticket   A ticket that alerts service personnel and customers of an issue with the library. RAS tickets identify which library components are most likely causing the issue. When possible, a RAS ticket provides instructions for resolving the issue.

Reliability   A RAS attribute that is designed to prevent failure of a storage solution. See also *RAS*.

S

SAM (SCSI Architecture Model) An ANSI standard that defines the generic requirements and overall framework in which other SCSI standards are defined. New generations of this standard are identified by a numeric suffix; for example, the second generation standard is SAM2.

SAN (Storage Area Network) A dedicated network that connects storage devices and servers in a pool, providing consolidated storage and storage management. Storage interconnects between many initiators and target devices. The SAN allows for sharing resources (target devices) among multiple servers (initiators).

SCSI (Small Computer System Interface) A set of standards for a high-speed, parallel interface that connects processing devices to peripheral devices, such as storage subsystems. The acronym is pronounced "scuzzy."

SCSI ID (Small Computer Systems Interface Address) An address on a SCSI BUS. Typically there are 16 addresses on a single channel SCSI BUS.

Server A powerful, centralized computer (or program) designed to provide information to clients (smaller computers or programs) upon request.

Serviceability A RAS attribute that refers to a component that is designed to accurately diagnose and report failures, as well as minimize downtime in a storage solution. See also *RAS*.

Setup wizard A tool for initially configuring the library. It appears the first time the user starts the library. However, it can be used to modify configurable items anytime after the initial configuration.

Sled See *UDS*.

SMI-S (Storage Management Initiative Specification) An industry standard SMI-S application programming interface (API) developed by SNIA that facilitates the management of multi-vendor devices in a storage area networks (SANs) environment.

Snapshot A rapid, point-in-time image of a volume created initially on the same disk as the original by duplicating metadata rather than copying the full data set. Snapshots are often used to protect against data corruption (viruses, etc.) or to create test or pre-production environments. Snapshots are also often used as a first step for creating non-disruptive point-in-time backups, and for copying datasets to a second disk to create a full duplicate copy of the volume. Snapshots are created on disk, and in the same

format as the original data. Snapshots are also referred to as point-in-time copies and as shadow copies.

SNMP (Simple Network Management Protocol) The protocol governing network management and the monitoring of network devices and their functions. Similar in function to SAM, except SNMP governs LAN, whereas SAM governs SAN.

SSL (Secure Sockets Layer) A protocol that provides encrypted communications on the Internet. SSL is layered beneath application protocols such as HTTP, SMTP, Telnet, FTP, Gopher, and NNTP and is layered above the connection protocol TCP/IP.

Storage device An appliance containing data that can be accessed, added to, changed, or deleted by the user. The storage media types include tapes and optical disks. A storage device can be a single disk drive, or constitute thousands of tapes in a large tape library.

Storage slot The physical home where a data cartridge resides.

Subsystem status A feature that provides predictive alerts, warning of any loss of connectivity or device failure using local or remote alerts. Subsystem status allows administrators to correct faults before they affect backup or other data transfer operations.

T

Tape drive A device that spins disks and tapes while it reads and writes data in storage.

TCP/IP (Transmission Control Protocol/Internet Protocol) The communications protocol used by the Internet. It runs on top of Ethernet to provide high-level networking services to applications.

Topology The logical and/or physical arrangement of stations on a network.

Trap An SNMP alert that is sent when predefined conditions are met. For example, an error trap tests for an error condition and provides a recovery routine.

U

UDS (Universal Drive Sled) The hardware that houses Fibre Channel and SCSI tape drives in a module.

User ID An alphanumeric value that the password database associates with a login name. Also, UID.

UTC (Coordinated Universal Time)   The world-wide standard for time, commonly considered to be the equivalent of "Greenwich Mean Time" and "Zulu time." For all of these time standards, zero (0) hours is midnight in Greenwich England, which lies on the zero longitudinal meridian. The sequence of the letters in the acronym is a compromise between the English and French terms (*Temps Universel Coordonné*).

W

WORM (Write Once, Read Many)   A common type of data storage medium, in which data can be read and reread, but not altered, after it has been recorded.

WWNN (World Wide Node Name)   A unique number assigned by a recognized naming authority. The World Wide name is integral to Fibre Channel operations.

WWPN (World Wide Port Name)   The WWPN is a 64-bit, hard-coded address for each port on an FC-connected device. It is used to identify available SAN devices at end points.

X

X-axis, X-position   The horizontal position of the library's robotic arm.

Y

Y-axis, Y-position   The vertical position of the library's robotic arm.