Quantum

Quantum Scalar i500 Tape Library

Scalar i500

Scalar i500 User's Guide, 6-01210-04**,** Ver. A**,** October 2008, 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

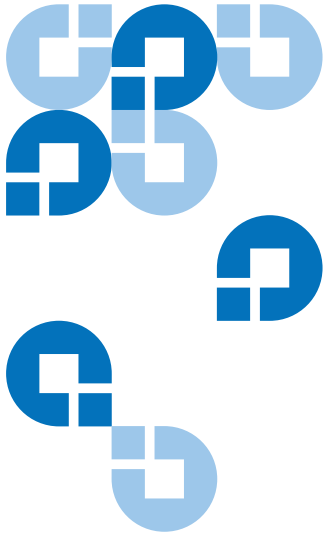**Chapter 2**   **Understanding the User Interface**   **33**

Chapter 3   **Configuring Your Library**   **47**

Chapter 4   **Running Your Library**   **122**

Chapter 8   Troubleshooting   323

Glossary 382

Tables

Figures

Preface

> **Warning:** Before operating this product, read all instructions and warnings in this document and in the *System, Safety, and Regulatory Guide*.

⚠ 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
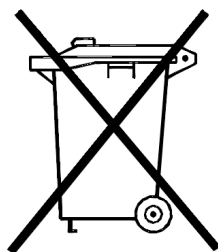
This symbol on the product or on its packaging indicates that this product should not be disposed of with your other waste. Instead, it should be handed over to a designated collection point for the recycling of electrical and electronic equipment. The separate collection and recycling of your waste 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, discusses the 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, Running Your Library, explains how to perform library, tape drive, and media operations.

- Chapter 5, Getting Information, explains how to use the library's built-in reports to get information you need.

- Chapter 6, Updating Library and Tape Drive Firmware, explains how to update library and tape drive firmware.

- Chapter 7, 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 8, Troubleshooting, describes the library's diagnostic reporting system (RAS tickets) and how to use it. Also describes a number of diagnostic tests you can run to troubleshoot problems.

- Chapter 9, 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:** Notes emphasize important information related to the main topic.

> **Caution:** Cautions indicate potential hazards to equipment and are included to prevent damage to equipment.

> **Warning:** Warnings indicate potential hazards to personal safety and are included to prevent injury.

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. The documents can be found in the box, on the product CD, or at http://www.quantum.com/ServiceandSupport/SoftwareandDocumentationDownloads/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 Intelligent Libraries Reference Guide for the Scalar i500 and Scalar i2000	Provides an interface standard that can be used in a SAN environment.
6-01370-xx	Scalar i500 SNMP Reference Guide	Describes information you can obtain from the Scalar i500 library SNMP.
6-00676-xx	SNC Firmware 4 and 5 User's 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 (14U)	Unpacking instructions.

Document No.	Document Title	Document Description
6-01525-xx	Scalar i500 Unpacking Instructions (23U)	Unpacking instructions.
6-01378-xx	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

To order documentation on the Scalar i500 or other products contact:

Quantum Corporation
P.O. Box 57100
Irvine, CA 92619-7100
(949) 856-7800
(800) 284-5101

Technical Publications

To comment on existing documentation send e-mail to:

doc-comments@quantum.com

Quantum Home Page

Visit the Quantum home page at:

http://www.quantum.com

Getting More Information or Help

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

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

Global Call Handling	1-800-284-5101
For additional contact information:	www.quantum.com/support
To open a Service Request:	www.quantum.com/osr
Quantum Corporation	www.quantum.com
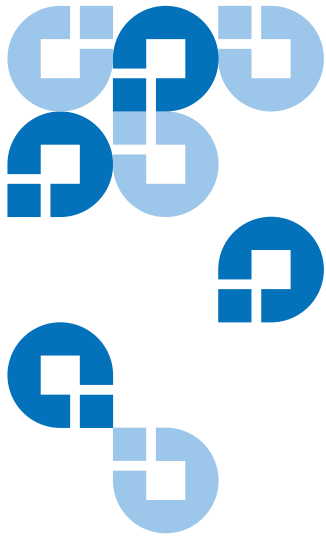
The Scalar i500 tape library automates the retrieval, storage, and management of tape cartridges. Tape cartridges are stored in the library and mounted and dismounted from tape drives using firmware running on the library or software running on the host systems.

The Scalar i500 tape library is different from other tape libraries because it is an intelligent library (see Intelligent Storage on page 13). 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").

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. Figure 1 shows the front view of a 5U library.

- A 14U library, consisting of one 5U control module and one 9U expansion module. Figure 2 on page 11 shows the front view of a 14U library.

- A 23U library, consisting of one 5U control module and two 9U expansion modules. Figure 3 on page 12 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)
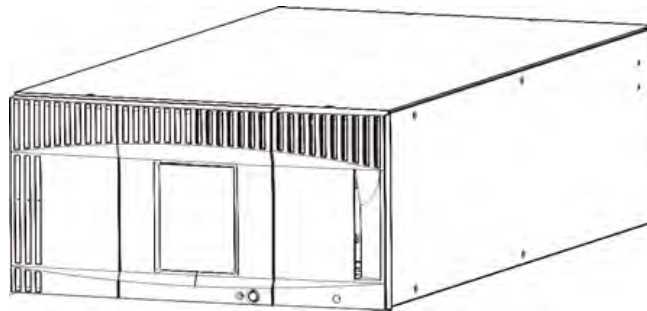
Figure 2 14U Library
Configuration (5U Control
Module Plus One 9U
Expansion Module)
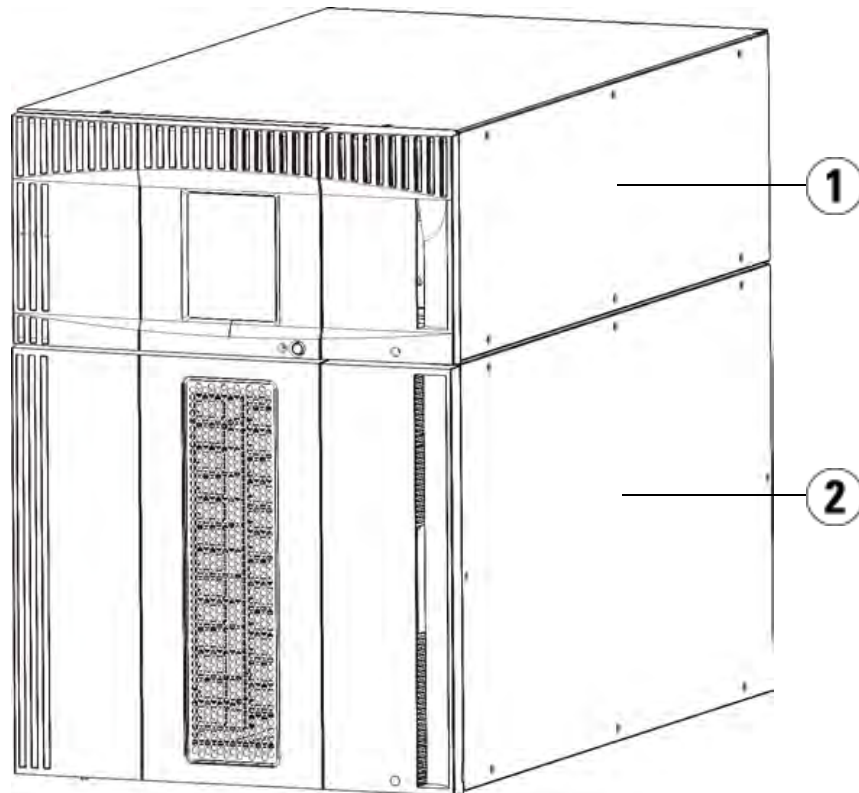
| 1 | Control module |
| 2 | Expansion module |

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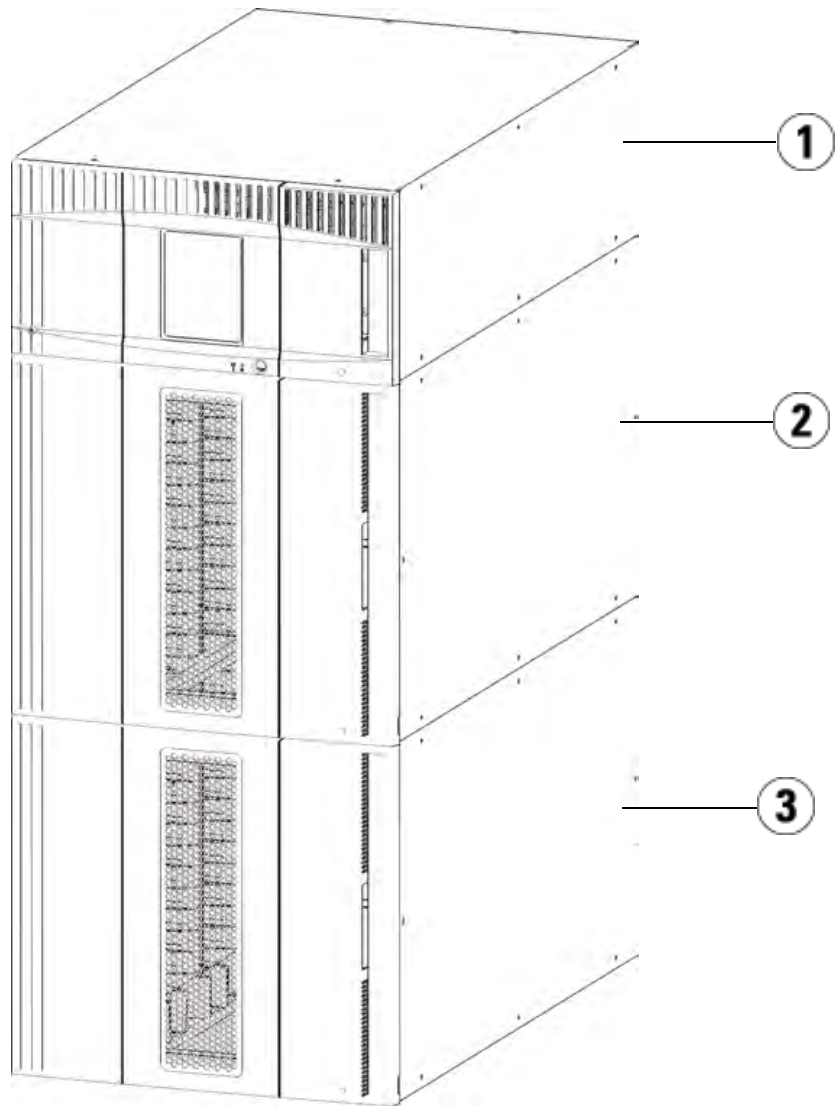
1	5U control module
2	9U expansion module
3	9U expansion module

> **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.

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.

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 15 for an illustration of library scalability. For information on installing, removing, and replacing modules, see Installing, Removing, and Replacing on page 170.

Each module has a specific number of fixed storage slots, I/E station slots, and tape drive slots available. See Library Capacity on page 365 for the number of slots available for each library configurations.

> **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 Unused Slots on page 131.

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
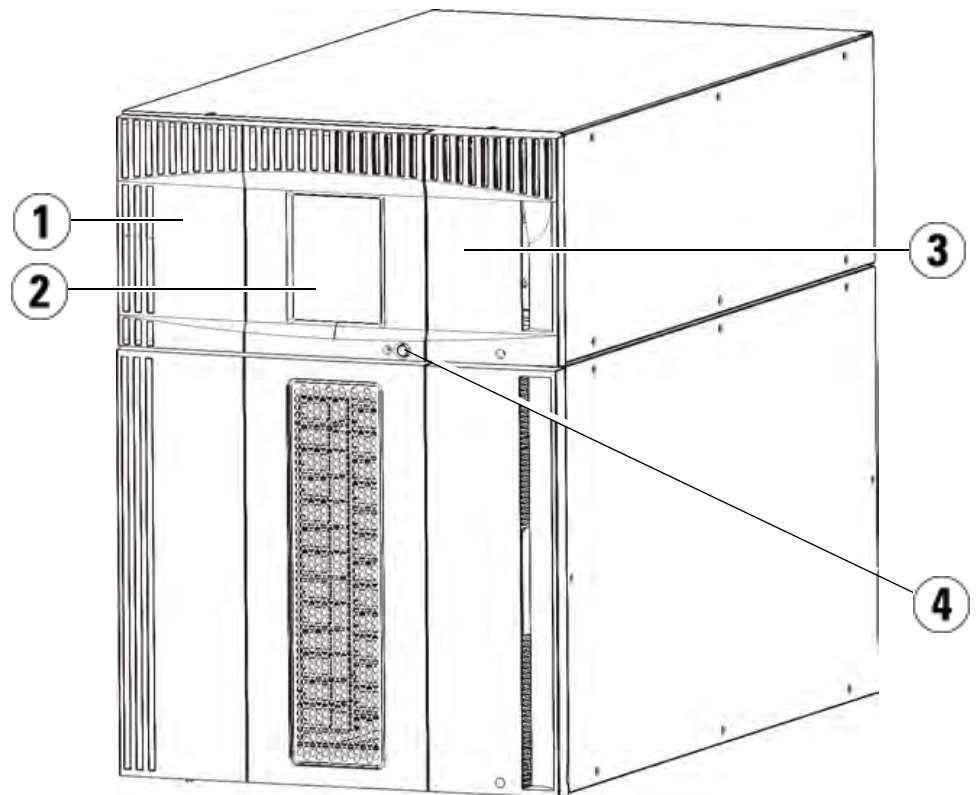
1	Access door
2	Operator panel
3	I/E station
4	Front power switch

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 bulkload 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 Locking and Unlocking the I/E Stations on page 143.

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 that 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 Chapter 2, Understanding the User Interface.

Front Power Switch

Turning off the front power switch turns off the robot and operator panel, but power still runs to the power supplies. Use the front power switch to manually shut down the library. See Shutting Down or Restarting the Library on page 145 for instructions on how to shut down or restart the library safely.

Back Panel Components

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

Figure 6 Back Panel
Components
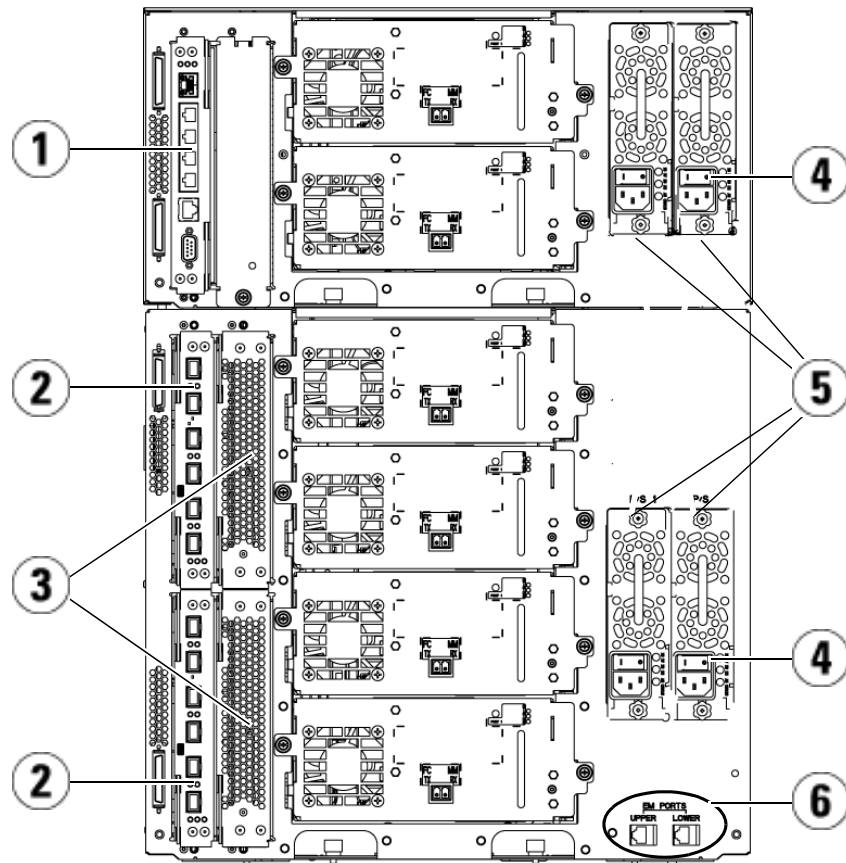
1	Library control blade (LCB)
2	FC I/O blade (optional)
3	FC I/O fan blades (required with FC I/O blades)
4	Rear power switch
5	Power supplies
6	Upper and lower Ethernet ports on expansion module

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 or Restarting the Library on page 145 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).

> **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 346.

Figure 7 Power Supply LEDs
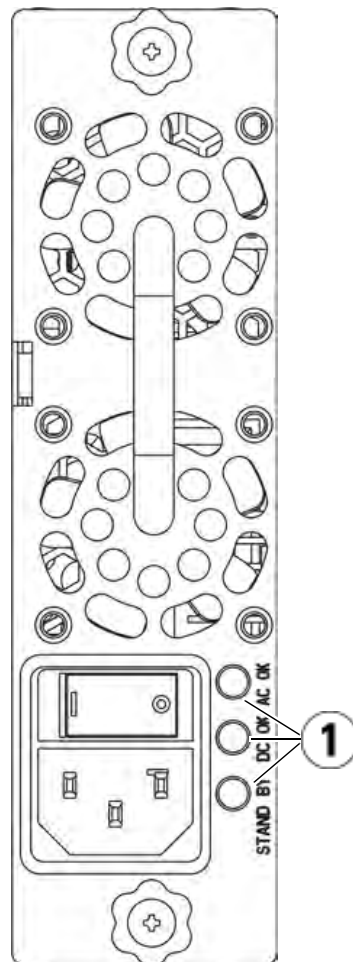
1	LEDs

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 LCB and FC I/O Blade LEDs on page 340.

Figure 8 Library Control Blade
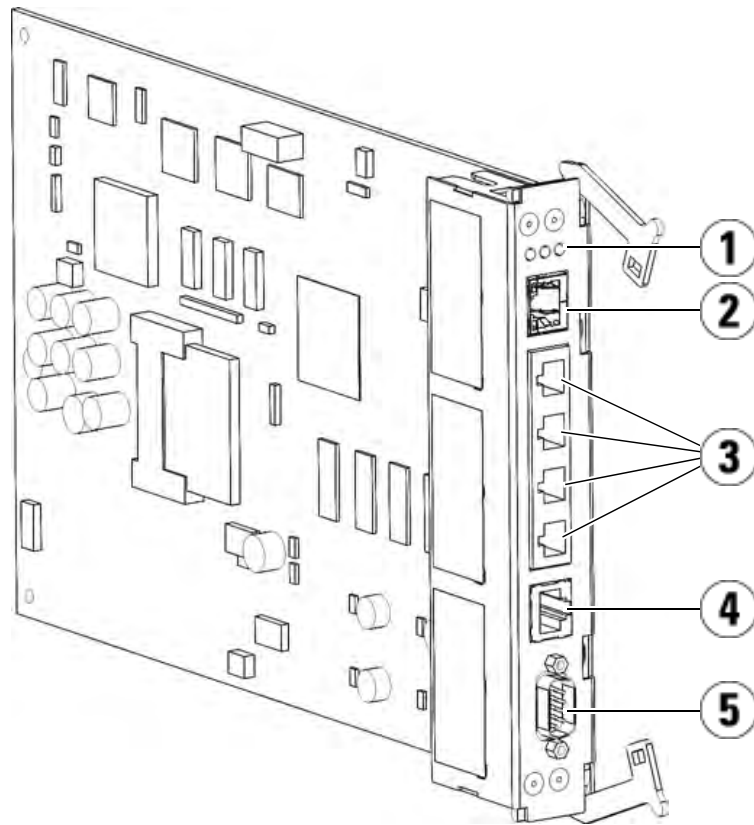
1	LEDs (blue, amber, green)
2	Gigabit Ethernet (external network) port
3	Ethernet I/O blade control ports (inactive if FC I/O blades are not installed)
4	Service Ethernet port
5	Service serial port

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. Any FC tape drive in the library, including drives in the control module, can be connected to an FC I/O blade in an expansion module. 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 LCB and FC I/O Blade LEDs on page 340.

For information on configuring I/O blades, see Working With FC I/O Blades on page 102.

For information on installing and cabling FC I/O blades and FC tape drives, see Chapter 7, Installing, Removing, and Replacing.

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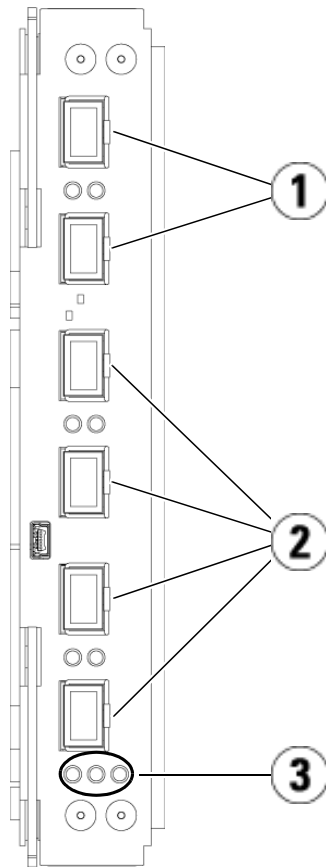
1	FC ports to host(s)
2	FC ports to drive(s)
3	LEDs (blue, amber, green)

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 I/O Fan Blade on page 317.

Figure 10 shows the I/O fan blade, including the LED. The single amber LED represents health status. For more information on the behavior of the I/O fan blade LED, see FC I/O Fan Blade LED on page 343.

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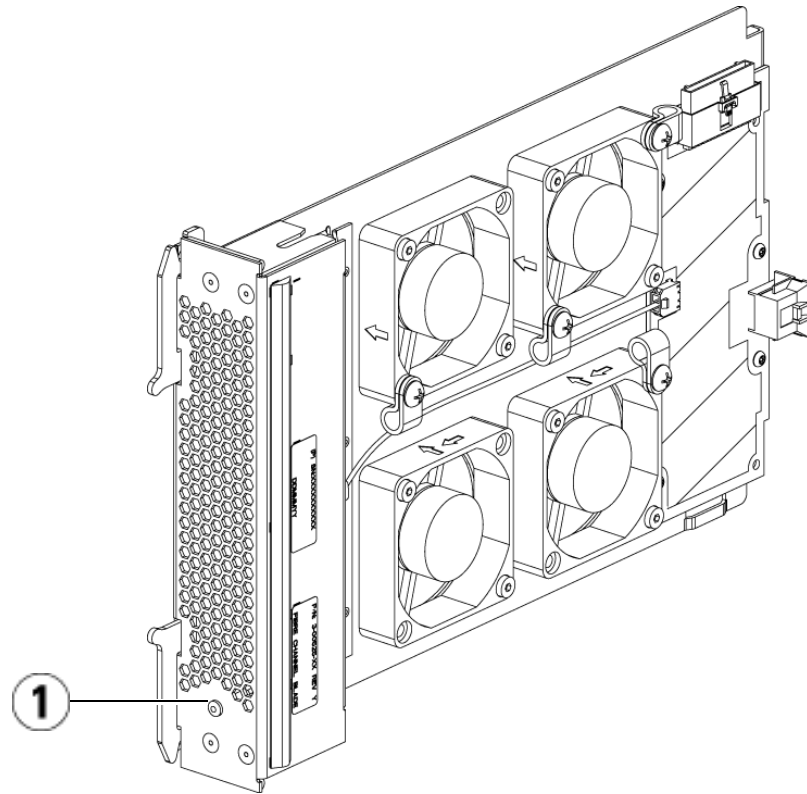
1	LED (amber)

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 9, 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 363 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 61.

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 102.

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 303.

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. If one of the resources is not available due to a failure or other cause, the other partitions and their assigned components are still available. Partitions can also 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 61.

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. By default, the first tape drive assigned to a partition is designated the control path. In the event that the control path connection to the host application fails, you can select a new control path for the partition.

> **Note:** Control paths are not used in partitions that contain FC tape drives connected to host applications through FC I/O blades. For more information, see Working With Control Paths on page 78.

Support for WORM

Scalar i500 tape libraries support WORM (write once, read many) technology in LTO-3 and LTO-4 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:

- Capacity on Demand (COD)
- Quantum Encryption Key Manager (Q-EKM)
- Advanced Reporting

If you purchase these features with your library, they 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 Adding or Upgrading Licensable Features on page 80.

Capacity on Demand (COD)

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.

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 1 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 1   Available Slots and
COD Upgrades Per
Configuration

	5U	**14U**	**23U**	**32U**	**41U**
Minimum, Maximum Available Slots (including I/O 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

Quantum Encryption Key Manager (Q-EKM)

Quantum Encryption Key Manager (Q-EKM) is a Java software program that generates, protects, stores, and manages encryption keys. These keys are used by the IBM LTO-4 tape drive to encrypt information being written to, and decrypt information being read from, tape media. Q-EKM is installed on a server or servers. The library is configured to communicate with these server(s). The encryption keys pass through the library-to-drive interface, so that encryption is "transparent" to the applications.

If you purchase Q-EKM after you purchased your library, you must install the license key on your library to enable the Q-EKM functionality.

When you purchase Q-EKM, Quantum's Service department will schedule an appointment to install the application onto your server(s). Once the application is installed, you must configure Q-EKM settings on the library. These settings are not visible until after the license key is installed. For instructions on configuring your library to use Q-EKM, see Configuring Quantum Encryption Key Manager (Q-EKM) on page 84.

The Q-EKM license corresponds to the size of your library. If you purchase Q-EKM for a particular size library and later expand the library, you must purchase an additional Q-EKM license at that time. Your new license key contains the entire license corresponding to your expanded library size. The new license key replaces your current license key.

Table 2 describes the licenses available for the different library configurations.

Table 2   Q-EKM License Configurations

	5U	14U	23U	32U	41U
Default Licensed	0	0	0	0	0
License Capacity	5U license	14U license	23U license	23U license plus one 9U license	23U license plus two 9U licenses
Maximum Number of Drives licensed for Q-EKM	2	6	10	14	18

Advanced Reporting

Advanced Reporting provides the following reports that you can configure for viewing and analysis:

- **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.

For information on how to use the advanced reporting capabilities, see Using Advanced Reporting on page 154.

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.
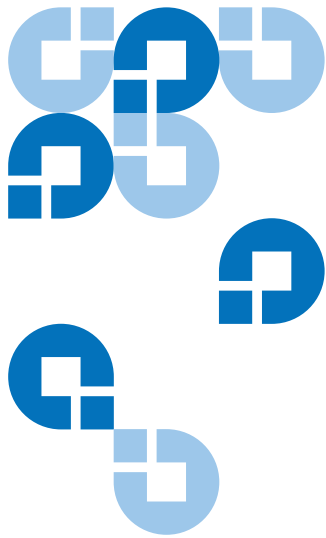
Chapter 2
Understanding the User Interface

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.

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.

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 36 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 330 for more information on "Library Not Ready" messages displayed in the header.

Figure 11 and Figure 12 show the operator panel and the web client interfaces.

Figure 11 Operator Panel User Interface
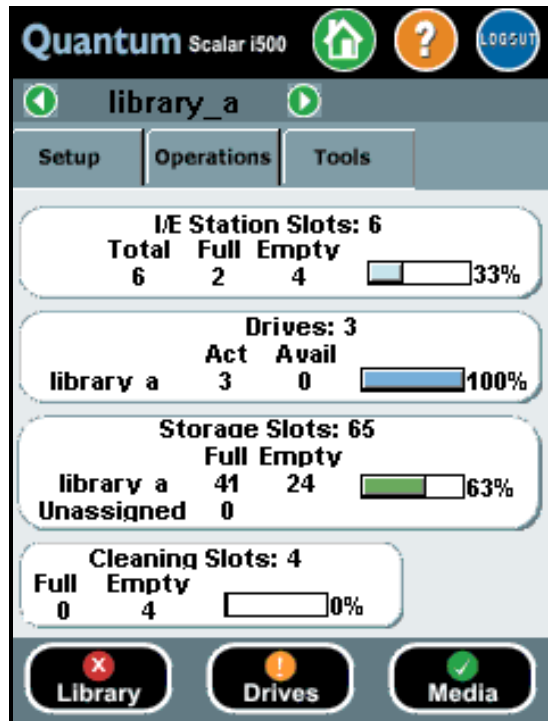
Figure 12 Web Client User Interface
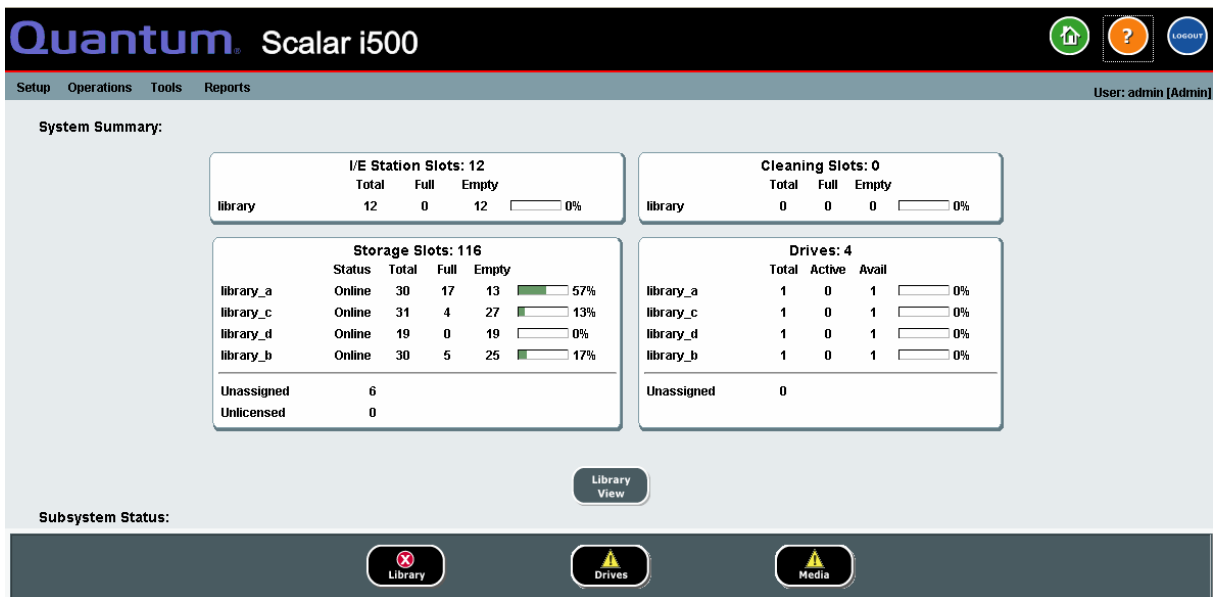
System Summary and Subsystem Status

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 button has three states indicated by color. The three states are:

- **Green —** No RAS tickets exist or, if any tickets do exist, they have all been closed.

- **Yellow —** The library contains open and unopened, low or high priority RAS tickets.

- **Red —** The library contains open and unopened urgent RAS tickets.

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** checkbox.

You can also open the **All RAS Tickets** screen by selecting **Tools > All RAS Tickets**. See About RAS Tickets on page 323 for more information about RAS tickets.

Home Page

The home page is common to both the operator panel and the web client. The web client home page provides two modes of navigation to access the user interface screens: tabs on the **Capacity View** and categorized function links on the **Library View**. The home page on the operator panel displays only the library **Capacity View**.

Capacity View

The Capacity View screen is the default view of the library and provides tabular data on the capacity of the library's partitions, slots, and drives. You can use the Capacity View 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 in the Capacity View.

Details about Capacity View 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 44 and.

On the web client, users can toggle between the **Capacity View** and the **Library View**.

Library View

Selecting the **Library View** button on the web client displays the Library View. The Library View provides a graphical representation of the library as well as another mode of navigation. Use the Library View to navigate through the library. The control module is labeled with "hot" areas that can be selected to access the functions for each area of the library. The Library View represents the actual configuration of the user's library,

including the order in which the modules are stacked. You will find the same navigation buttons on the Library View as on the Capacity View.

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 118.

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.

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 System Requirements on page 364 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 Configuring Library Security Settings on page 117 for information on setting the network configuration settings for remote use.

Menu Trees

The following menus organize operations and commands into logical groupings:

- The **Setup** menu consists of commands that users with administrative privileges 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. Administrative users 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. Administrative users have access to all menu commands, but users' privileges are more limited.

Table 3 lists the web client menus. Some menu commands are available only to users with administrative privileges. I/O blade menu items are available for libraries that contain I/O blades.

Table 3   Web Client Menus

Setup Menu[a]	Operations Menu	Tools Menu[a]	Reports Menu
Setup Wizard	Media >Move >Import >Export	All RAS Tickets	System Information
Partitions	Cleaning Media >Import >Export	Capture Snapshot	Library Configuration
Cleaning Slots	Partitions >Change Mode	Save/Restore Configuration	Network Settings
I/E Station Slots	Drive >Load >Unload >Change Mode	Email Configuration Record	Logged in Users[a]
Drive Settings	I/E Station Lock/Unlock[a]	Save Configuration Record	All Slots
Control Path	System Shutdown[a]	Identify Drives	Log Viewer
License	Log Out	Drive Operations	Advanced Reporting >Drive Resource Utilization >Media Integrity Analysis
Notification >Setup >E-mail Account >Contact Information		Download SNMP MIB	About[a] >Scalar i500 >Open Source Licenses

Setup Menu[a]	Operations Menu	Tools Menu[a]	Reports Menu
Network Management >Network >SNMP >SNMP Trap Registrations		IO Blade Info[b]	
User Management >User Accounts >Remote Authentication		IO Blade Port Info[b]	
IO Blades[b] >Port Configuration >Channel Zoning >Host Mapping >Host Management >Host Port Failover >Data Path Conditioning >Blade Control		Update Library Firmware	
Encryption >System Configuration >Partition Configuration		Diagnostics	
Date & Time			
Register Library			

[a]Administrative users only. [b]Available only when the library contains I/O blades.

Table 4 lists the operator panel menus. Some menu commands are available only to users with administrative privileges. I/O blade menu items are available for libraries that contain I/O blades.

Table 4   Operator Panel Menus

Setup Menu[a]	Operations Menu	Tools Menu
Partition Mgmt >Create Partition >Delete Partition >Configure I/E Station Slots >Configure Cleaning Slots	Move Media	All RAS Tickets[a]
User Mgmt >Create User >Modify User	Import Media	Capture Snapshot[a]
Drive Settings >Fibre >SCSI > SAS	Export Media	Drive Mgmt[a] >Clean drive > Reset drives
Notification >Email Alerts >Email Account >Customer Contact	Import Cleaning Media	Drive Info
Licenses	Export Cleaning Media	About Library >Network Info >View Drive Info >Partition Info
Date and Time	Change Partition Mode	

Setup Menu[a]	Operations Menu	Tools Menu
Network Mgmt If IPv6 is configured: >IP version 4 >IP version 6	Load Drive	Internal Network[a]
Control Path	Unload Drive	System Settings >User session timeout (minutes)[a] >Touch screen audio >Unload assist[a] >Logical SN Addressing[a] >Manual Cartridge Assignment[a] >Disable Remote Service User[a] >Enable SSL >Enable SNMP V1/V2 >Enable IPv6 >Enable SMI-S
IO Blades[b] >Port Configuration >Channel Zoning >Host Mapping[c] >Host Management[c] >Host Port Failover >Data Path Conditioning >Blade Control	Change Drive Mode	Security[a] >Network Interface >SSH Services >ICMP >Remote UI >SNMP >SMI-S

Setup Menu[a]	Operations Menu	Tools Menu
	Lock/Unlock I/E Station[a]	Display Settings
		>Brightness
		>Contrast
		>Defaults
	Shutdown[a]	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]Administrative users 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 92 for more information on setting user privilege levels.

Three types of users are defined in Scalar i500 libraries:

- **Administrative users** have access to the entire physical library and all of its partitions. The library ships with a default administrative user account. The user name for the default administrative user account is

admin and the password is **password**. You cannot modify or delete the user name for the default administrative account, but you can modify the password. If you misplace the password for the default administrative account, contact Quantum Technical Support. For contact information, 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 perform operations that affect the physical library (such as creating or deleting partitions).

- **Service users** have 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 user account.

Details on user privileges include:

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

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

- The same user can be logged in from multiple 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 administrative user out.

- All users are logged out automatically after a configurable period of inactivity. The default timeout period is 30 minutes, but users with administrative privileges can change this to a value from 15 minutes to 480 minutes (eight hours). See Configuring System Settings on page 118.

- 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 administrative user can disable any access to the library from the web client. For more information, see Configuring System Settings on page 118.

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

- For security purposes, an administrative user 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 118.

User Access

See Table 3 on page 40 for the web client menu tree and privilege level information. See Table 4 on page 42 for the operator panel menu tree and privilege level information.
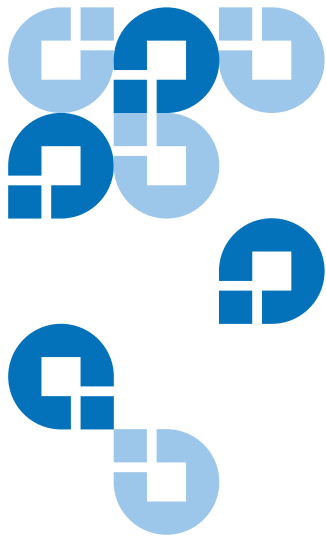
Configuring Your Library

Once you have installed the hardware as described in the *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 329.

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, administrative users can always use the Setup Wizard on the web client or use commands on the **Setup** and **Operations** menus to modify all library settings, including network settings. See <u>Completing the Library Configuration With Menu Commands</u> on page 48.

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 Default Configuration Settings on page 51.

For additional information, see Using the Setup Wizard on page 49.

Using the Default Administrative User 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 administrative user 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 administrative account. For information on changing passwords, see Modifying Local User Accounts on page 94.

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

Note:	If you misplace the password for the default administrative account, contact Quantum Technical Support. For contact information, see Getting More Information or Help 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, administrative users 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 Menu Trees on page 39.

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 Setup Wizard Tasks on page 51).

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** checkbox. Click **Next**. Configure the network settings.

- **If you are using IPv6:** On the **Setup Wizard: Enable IPv6** screen, select the **Enable IPv6** checkbox 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 administrative 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 Viewing the Library Configuration on page 149 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 administrative user 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 Default Configuration Settings on page 51).

- 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 administrative users 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 51 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 64.

See also About the Setup Wizard on page 47.

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.

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

- Managing the Network (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**.

- Applying a License Key (operator panel and web client) — Allows you to enter keys for licensed features. For more information, see Adding or Upgrading Licensable Features on page 80.

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

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

- Working With Partitions (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 issues, 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 Saving and Restoring the Library Configuration on page 329.

Note:	Setup Wizard operations cannot be performed concurrently by multiple administrative users logged in from different locations. You can access the screens, but you cannot apply changes while another administrative user 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.

Logging On to 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

Administrative users can configure the following:

- Network settings that allow remote access to the library. For more information, see Modifying Network Settings on page 54.

- 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 Enabling SSL on page 56.

- 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 Configuring SNMP Settings on the Library on page 57.

> **Caution:** Security settings must be enabled to allow SNMP, SMI-S, and IP address access to the library network. After applying any of the settings on the Network Management screens, verify the settings on the Security Settings screen. See Configuring Library Security Settings on page 117.

Modifying Network Settings

The operator panel Setup Wizard allows administrative users 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.

> **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

Administrative users 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 *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 *Basic SNMP Reference Guide(6-01370-xx)*. For information on integrating MIBs with an SNMP management application, contact your network management application vendor.

Administrative users 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 .

- Enable or disable support for SNMP v1 and v2c. SNMP v3 is enabled by default and cannot be disabled. For more information, see .

- Modify the default Read 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 Read SNMP Community String on page 60.

- 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 60.

- 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 61.

Registering External Management Applications

Administrative users 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 54.

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

Note:	This operation should not be performed concurrently by multiple administrative users logged in from different locations. You can access the appropriate screens, but you cannot apply changes while another administrative user 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

Administrative users 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 *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**.

Modifying the Read SNMP Community String

Administrative users can modify the Read SNMP community string. The Read 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 Read SNMP community string used by the library must match the string used by the external management application.

The default Read 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 *Basic SNMP Reference Guide (6-01370-xx)* for further configuration and access details.

You cannot modify the read 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

Administrative users 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 *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. Administrative users 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 *Basic SNMP Reference Guide (6-01370-xx)* or contact Quantum Technical Support. For contact information, 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 administrative users to select the number of new library partitions to create.

At any time after the initial configuration of the library, administrative users 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 (FC, SCSI, or SAS) and tape drive vendor. 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 administrative user can create partitions one at a time. Creating partitions manually gives you more control over resource allocation. You can, for example, assign different tape drive types to the same partition. You can create partitions manually only on the web client. When you manually create partitions, you add to the number of existing partitions.

The maximum number of partitions that can be created is equal to the number of drives in the library. Table 5 shows the possible number of partitions that can be created for each of the available library configurations.

Table 5   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:

- Administrative users 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 67 and Removing the Expansion Module on page 236.

Automatically Creating Partitions

At any time after the initial configuration of the library, administrative users 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) and tape drive vendor.

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 66 and Deleting Partitions on page 67.

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

The default number of partitions created is the number of distinct tape drive interface/vendor combinations of the tape drives that are not currently assigned to a partition. For example:

• If your library contained two tape drives, a FC IBM LTO-3 and a FC IBM LTO-4, one partition would be created since they are the same interface type and vendor.

• If your library contained two tape drives, a SCSI IBM LTO-2 and a SCSI HP LTO-2, two partitions would be created because the tape drive vendors are different.

If you choose to create fewer partitions than the default, but more than one partition, some resources will not be assigned to a partition. However, if you choose to create one single partition, all available resources will be assigned to the one partition. When the library automatically creates partitions, it creates control paths. See Working With Control Paths on page 78 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 66.

Note:	This operation cannot be performed concurrently by multiple administrative users logged in from different locations. You can access the screen, but you cannot apply changes while another administrative user 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, administrative users 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.

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 <u>Modifying Partitions</u> on page 66 and <u>Deleting Partitions</u> on page 67.

When you manually create partitions, the library creates control paths. See <u>Working With Control Paths</u> on page 78 for a description of the default control paths and how to change them.

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

- **Emulation Type** — the type of library that the partition is emulating:
  - ADIC Scalar i500 (default)
  - Quantum Scalar i500
  - Quantum Scalar i2000
  - ADIC Scalar i2000
  - ADIC Scalar 100
  - ADIC Scalar 24
- **Partition Name** — limited to a maximum of 12 lower-case alphanumeric characters and underscores (_)
- **Media Barcode Format** — defaults to Standard. The available options are as follows:
  - **Standard Six** — Six character barcode number with or without a one or two-character media ID, for example, "XXXXXXL4" or "XXXXXX". Only the six character barcode is reported to the host.
  - **Plus Six** — Six character barcode number followed by a media ID, for example, "XXXXXXL3". Six character barcode and media ID are reported to the host.
  - **Extended** — Five to 16 characters total, including a barcode number and optional media ID. All characters are reported to the host, regardless of 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, "XXXXXXXXXXXXXXL2". If a media ID is not included, the label must have a five to 16 character barcode, for example, "XXXXXXXXXXXXXXXX".
  - **Media ID Last** — Five to 14 character barcode number followed by media ID, for example, "XXXXXXXXXXXXXXLT". The media ID is reported to the host last.

- **Media ID First** — Five to 14 character barcode number followed by media ID, for example, "XXXXXXXXXXXXXXL4". The media ID is reported to the host first.

- **Standard** — (default) Five to 16 characters total, including a barcode number and optional media ID. The media ID is not reported to the host. If a media ID is included, the label must have a five to 14 character barcode followed by a media ID, for example, "XXXXXXXXXXXXXXL3". If a media ID is not included, the label must have a five to 16 character barcode, for example, "XXXXXXXXXXXXXXXX".

- **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 135.

Note:	Creating Partitions operations cannot be performed concurrently by multiple administrative users logged in from different locations. You can access the screen, but you cannot apply changes while another administrative user 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**.

Modifying Partitions

Using the web client, administrative users 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 <u>Working With Control Paths</u> on page 78.

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

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

- **Emulation Type** — the type of library that the partition is emulating. See [Manually Creating Partitions](#) on page 64 for descriptions of available options.

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

- **Media Barcode Format** — defaults to **Standard**. See [Manually Creating Partitions](#) on page 64 for descriptions of available options.

- 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 modifying partitions, verify that all tape drives are unloaded and that all cartridges are in their appropriate storage slot location. For information on unloading tape drives, see [Unloading Tape Drives](#) on page 135.

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. Administrative users 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 [Unloading Tape Drives](#) on page 135 and [Exporting Media](#) on page 132.

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 69.

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

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

Deleting Partitions Before Removing or Replacing Modules

You should delete partitions before:

- Removing the control module and replacing it with a new control module

- Removing an expansion module and replacing it with a new expansion module

- Permanently removing an expansion module from the library

Because partitions 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 partitions and modifying shared resources such as cleaning slots and I/E slots.

See Installing, Removing, and Replacing on page 170 for detailed instructions on preparing your library for the permanent removal or replacement of a control module or an expansion module. The following is a high-level summary of the preparation process:

- You may find it helpful to review your library's current configuration before removing the module. See Viewing the Library Configuration on page 149.

- Using your I/E station, export all the tape cartridges from your library. See Exporting Media on page 132.

- Reduce the number of cleaning slots in the library to 0. You can designate new cleaning slots after the module has been removed or replaced. See Configuring Cleaning Slots on page 71.

- Delete all partitions in the library. You can create new partitions after the module has been removed or replaced. See Working With Partitions on page 61.

- Set the number of I/E stations slots to 6. You can reconfigure I/E stations slots after the module has been removed or replaced. See Configuring I/E Station Slots on page 73.

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 administrative user 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 administrative user.

- **Privilege Level** — Determines the user's access privileges. See User Privileges on page 44 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**.

Changing Partition Modes

This topic focuses on using the library user interface, not the host application, to change partition mode. Changing a partition mode using the library user interface may affect your host application. See your host application documentation for more information.

There are two partition modes: online and offline.

- **Online** — Normal operating condition for the partition. In this mode, all host application commands are processed.

- **Offline** — Move commands are not processed. If the partition is taken offline, the physical library and other partitions are not affected.

When you are changing the partition mode, be aware of the following:

- 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 states.

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

- If a tape drive within a partition is Active, that partition cannot be taken offline until the tape drive is Idle. The number of active tape drives within a partition is indicated in the Active column of the partition table.

> **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

Administrative users can disable or enable manual cartridge assignment. When manual cartridge assignment is enabled (the default setting), the **Assign IE** screen automatically appears on the operator panel once cartridges are placed into the I/E station. The **Assign IE** 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.

When manual cartridge assignment is disabled, the **Assign IE** screen does not appear on the operator panel, and the cartridges in the I/E station are visible to all partitions, as well as the system partition, and can be used by any partition.

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, Configuring System Settings on page 118.

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.

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.**

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.

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 73.

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.

Administrative users 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 [Modifying Partitions](#) on page 66 and [Deleting Partitions](#) on page 67.

Administrative users can also clean tape drives manually. For information, see [Manually Cleaning Tape Drives](#) on page 141.

> **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 administrative users logged in from different locations. You can access the screen, but you cannot apply changes while another administrative user 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. Administrative users 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 <u>Configuring Zero I/E Station Slots</u> on page 75.

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 6 lists the number of I/E station slots available per library for all base library configurations.

Table 6   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 143.

- 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 on page 149.

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 bulkload and unload tape cartridges, disrupting library operations. See Bulkloading on page 129.

- 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 122.

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 administrative users logged in from different locations. You can access the screen, but you cannot apply changes while another administrative user 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

Administrative users can view and modify certain tape drive parameters. You can set the SCSI ID for a SCSI-attached tape drive and 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.

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, a SCSI ID can be set 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:

- 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.

- 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)

- The requested interface speed can be set to Auto (default), 1 Gb/s, 2 Gb/s, and 4 Gb/s. When you set the speed to 4 Gb/s using the web client, a caution message appears informing you that the 4 Gb/s speed selection may not be applicable to all FC tape drives installed in the library. Acknowledge the message by clicking **OK**.

- 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 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. describes how these control paths are assigned and how to change them.

Table 7   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.
One or more FC I/O blades	At least one FC tape drive	The FC I/O blade	It is recommended that you allow the FC I/O blade to be the control path for the partition. (You can select a tape drive as control path if the tape drive is not connected to an FC I/O blade; however, your host will end up seeing multiple medium changers. In addition, using the FC I/O blade as the control path allows you to utilize the LUN mapping and host port failover features.)
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.

Control paths should not be selected for partitions that contain FC tape drives connected to a host applications through FC I/O blades, unless the control path tape drive is NOT connected to an FC I/O blade.

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 111.

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**.

Adding or Upgrading Licensable Features

Several features can be added to the standard library configuration either with your initial purchase or afterward. These are called licensable features and they include:

- Capacity on Demand (COD)
- Quantum Encryption Key Manager (Q-EKM)
- Advanced Reporting

For more information about these features, see Licensable Features on page 29.

If you purchase these features with your library, they 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.

Viewing Licenses and License Keys

To see the licenses you have purchased and obtained, go to the following Web sites:

Feature	Web Site URL
COD	http://www.quantum.com/Scalari500/Upgrades/COD
Q-EKM	http://www.quantum.com/Scalari500/Upgrades/EKM
Advanced Reporting	http://www.quantum.com/Scalari500/Upgrades/AdvancedReporting

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**.

About License Keys

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.

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. For contact information, 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 web site for the feature you want:

Feature	URL
COD	http://www.quantum.com/Scalari500/Upgrades/COD
Q-EKM	http://www.quantum.com/Scalari500/Upgrades/EKM
Advanced Reporting	http://www.quantum.com/Scalari500/Upgrades/AdvancedReporting

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

6 Click **Submit**.

If you have entered a valid serial number, the website 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 Contacts 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 website 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 Applying a License Key.

Applying a License Key

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

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

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

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.

The paths to open the appropriate screens are as follows:

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

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

Configuring Quantum Encryption Key Manager (Q-EKM)

Quantum Encryption Key Manager (Q-EKM) is a centralized key manager application that manages the encryption keys used as part of the LTO-4 drive-based data encryption process. Library-managed encryption is an optional, licensed feature that must be enabled from the Scalar i500 library in order to begin encrypting data using the LTO-4 tape drive encryption capabilities.

For more information about Q-EKM and its license, see Quantum Encryption Key Manager (Q-EKM) on page 31.

Step 1: Upgrade Firmware

Upgrade your library and tape drive firmware to the latest released versions.

Step 2: Install the License Key on the Library

If your license key is not already installed on the library, install it now (see Applying a License Key on page 83).

Step 3: Install Q-EKM on a Server or Servers

You must supply a server or servers on which to install Q-EKM. Quantum Field Services will schedule an appointment to install the software and configure your servers.

> **Note:** Since the Scalar i500 library needs to communicate with the Q-EKM server in real time when reading from or writing to an encryption-enabled drive, it is strongly recommended that you use both a primary and secondary Q-EKM server. This way, if the primary server is unavailable at the time the library needs encryption information, the secondary server can handle the request. The Scalar i500 library allows you to configure up to two Q-EKM servers for redundancy/failover purposes.

Step 4: Configure Q-EKM Server TCP/IP Addresses

Make sure you complete Steps 1 through 3 above before proceeding.

1 From the web client, select **Setup > Encryption > System Configuration**.

2 If you want to enable Secure Sockets Layer (SSL) for communication between the library and the Q-EKM servers, select the **SSL for Q-EKM Servers** "Enable" checkbox. The default is Disabled. If you enable SSL, you must make sure that the primary and secondary Q-EKM Port Numbers (see 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 server to a tape drive, whether SSL is enabled or not. Enabling SSL provides additional security.

3 In the **Primary Q-EKM IP Address or Host** text box, enter either:

- The IP address of the primary Q-EKM server (if DNS is not enabled), or

- The host name of the primary Q-EKM server (if DNS is enabled).

4 Enter the port number for the primary Q-EKM server into the **Primary Q-EKM port number** text box. 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 port number for the Q-EKM server from the default setting on the library, you must also change the port number on the Q-EKM server to match or Q-EKM will not work properly. See the *Quantum Encryption Key Manager User's Guide* for information on setting the port number on the Q-EKM server.

5 Optionally, enter the IP address or host name of the secondary Q-EKM server into the **Secondary Q-EKM IP Address or Host** text box.

> **Note:** If you do not plan to use a secondary Q-EKM server, you may type a zero IP address, 0.0.0.0, into the **Secondary Q-EKM IP Address or Host** text box, or you may leave this text box blank.

6 If you configured a secondary Q-EKM server (previous step), enter the port number for the secondary Q-EKM server into the **Secondary Q-EKM port number** text box. The default port number is 3801, unless SSL is enabled. If SSL is enabled, the default port number is 443.

> **Note:** If you are using a secondary Q-EKM server, then the port numbers for both the primary and secondary Q-EKM servers must be set to the same value. If they are not, synchronization and failover will not occur.

7 Click **Apply**.

Step 5: Configure Partition 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.

If you encrypt a partition, all Q-EKM-supported tape drives in that partition are enabled for encryption. Any non-Q-EKM-supported tape drives in that partition are not enabled for encryption, and data written to non-supported media is not encrypted.

Data written to encryption-supported media in Q-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).

Configure the partition(s) as follows:

1 From the web client, select **Setup > Encryption > Partition Configuration**.

A list of all your partitions displays, along with a drop-down menu displaying the encryption method for each partition.

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

3 Select an encryption method from the drop-down menu for each partition. (For tape drives that support encryption, the default is **Allow Application Managed.**) The Encryption Method applies to all encryption-capable tape drives and media in that partition.

Encryption Method	Description
Enable Library Managed	**For use with Q-EKM.** Enables encryption support via a connected Q-EKM server for all encryption-capable tape drives and media assigned to the partition.
Allow Application Managed	**Not for use with Q-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 Q-EKM 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 Q-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.

4 Click **Apply**.

5 Save the library configuration (see <u>Saving the Library Configuration</u> on page 329).

Setting Customer Contact Information

Administrative users 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 <u>techsup@quantum.com</u> 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 <u>Creating E-mail Notifications</u> on page 91.

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 > Notification > 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 > Notification > E-mail Account** 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 most e-mail notifications. This feature is turned off by default. Library snapshot files can also be sent to specified e-mail addresses using the capture snapshot operation. The capture snapshot operation allows you to create the snapshot in ASCII format. See Capturing Snapshots of Library Information on page 326.

- **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 Saving and Restoring the Library Configuration on page 329.

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

The paths to open the appropriate screens are as follows:

- From the web client, select **Setup > Notification > E-mail Account**.

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

Working With 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 Configuring the Library E-mail Account on page 88 for information on how to configure the e-mail account.

See Creating E-mail Notifications on page 91 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:** 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 levels:

- **Low Filter** — Notifies e-mail recipients of all library issues, including minor, medium-level, and the most critical issues.

- **Medium Filter** — Notifies e-mail recipients of medium-level and the most critical issues.

- **High Filter** — Notifies e-mail recipients of only the most critical issues.

Administrative users 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 > Notification > Setup**.

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

Creating E-mail Notifications

Administrative users 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 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 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 > Notification > Setup**.

Modifying E-mail Notifications

Administrative users 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 Working With E-mail Notifications on page 90.

> **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 > Notification > Setup**.

Deleting E-mail Notifications

Administrative users 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 > Notification > Setup**.

Working With User Accounts

Administrative users 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. To use LDAP authentication, a user must enter a directory service user name and password and specify an LDAP domain.

About Local User Accounts

Administrative users can create and modify two types of local user accounts: user and administrative user. 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.

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

The library ships with a default administrative user 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 administrative user account is used to perform the initial configuration of the library. If you misplace the password for the default administrative account, contact Quantum Technical Support. For contact information, see Getting More Information or Help on page 8.

See User Privileges on page 44 for more information on library permission levels. For information on changing passwords, see Modifying Local User Accounts on page 94.

Creating Local User Accounts

During or after the initial configuration, you can use the default administrative user account to create up to eighteen additional local user accounts, including other accounts with administrative privileges. These administrative users can themselves create other local administrative user and user accounts. Users without administrative privileges cannot create user accounts. The library can contain eighteen user accounts, including the default administrative user 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 6–12 lower-case alphanumeric characters and can include also include underscores (_), periods (.), hyphens (-), asterisks (*), and ampersands (@). For example: **pass_19**.

- **Privilege —** is set to either **User** or **Admin**. See <u>User Privileges</u> on page 44 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, administrative users 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 6–12 lower-case alphanumeric characters and can include also include underscores (_), periods (.), hyphens (-), asterisks (*), and ampersands (@). For example: **pass_19**.

- **Privilege —** set to either **User** or **Admin**. See <u>User Privileges</u> on page 44 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

Administrative users can delete other local administrative user and user accounts when they are no longer needed.

> **Note:**   The default administrative user 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

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

Administrative users 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 About Local User Accounts on page 93.

Using Microsoft Active Directory

The library supports the Microsoft® Active Directory® LDAP server. If you use Microsoft Active Directory, you must use either:

- Windows® Services for Unix® 2.5

- Kerberos

If you use Kerberos, you don't need to use Windows Services for Unix 2.5. For specific instructions on configuring Kerberos, see Configuring Kerberos on page 97.

If you use Windows Services for Unix 2.5:

- When setting up a user account in Microsoft Active Directory, make sure to populate the UNIX attributes with information. This requires all Active Directory users to be part of an NIS Domain, or have NIS Domain information entered. After entering NIS Domain information for a user, you will need to reset the user's password.

- The library supports user account information in the schema defined by RFC 2307. User password schemes must be encrypted using UNIX crypt. In addition, user names (uid) and passwords (userPassword) must be created using lowercase characters to be compatible with the library.

LDAP Server Guidelines

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 correspond to the library partition names. Users with user privileges must be assigned to these groups on the LDAP server to have access to the corresponding partitions on the library. LDAP users with administrative privileges have access to all partitions and administrative functions and do not need to be assigned to partition-related groups on the LDAP server.

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

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:

- **Repository 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.

- **Group DN** — the distinguished name that contains the groups.

- **User DN** — the distinguished name that contains the users.

- **Default domain** — the domain in which the user accounts reside (user names and groups, including library user group and admin group below).

- **Principle authorization** — an LDAP user login ID with permissions to search the LDAP directory. The library logs into LDAP using this ID.

- **Credential authorization** — the password for the principal authorization login ID.

- **Library user group** — the name of the group you want to associate with the library. This group is equivalent to the local user privilege level. Any member of this group can manage this library. See User Privileges on page 44 for more information on user privilege levels.

- **Admin group** — the name of the group associated with the library administrator, equivalent to the local administrative user privilege level. Any member of this group has administrative privileges. See User Privileges on page 44 for more information on user privilege levels.

The **Test LDAP** button tests communication between the library and the LDAP server. If you change the LDAP settings, click **Apply** before using this button. While the test is in progress, the Progress Window appears. If the test is successful, **Operation Successful** appears in the Progress Window. If the test is unsuccessful, Operation Failed appears in the Progress Window. Follow the instructions listed in the Progress Window to resolve any issues that occur during the operation.

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 web client. You cannot use the operator panel.

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 to use Microsoft Active Directory without Windows Services for Unix 2.5.

Make sure that both the library and the Kerberos 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 101.

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.

- **KDC (AD Server)** — The server on which Kerberos is installed.

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

- **Service Keytab** — Click the **Browse** button to select the service keytab file. The service keytab file is a file you generate on your Kerberos (AD) server. To generate the file, follow these instructions:

Generating the Service Keytab file

1 Set up an Active Directory domain on the Windows 2003 server.

2 At the command prompt, enter **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 checkboxes 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

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

The path to open the appropriate screen is as follows:

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

Setting the Date, Time, and Time Zone

Administrative users 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 administrative users logged in from different locations. You can access the appropriate screens, but you cannot apply changes while another administrative user 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.

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. Administrative users 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:

- At least one NTP server must be configured and available.

- 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 100.

- 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 54 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, and LTO-4 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 105.

- **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 106.

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

- [Fibre-Channel Input/Output Blades](#) on page 23
- [Controlling FC I/O Blade Power](#) on page 144
- [Viewing FC I/O Blade Information](#) on page 161
- [Viewing FC I/O Blade Port Information](#) on page 162
- [Connecting Library FC Cables to FC I/O Blades](#) on page 180
- [Recommended Library Cabling for FC I/O Blades](#) on page 187
- [Identifying FC I/O Blades](#) on page 336
- [Resetting FC I/O Blade Ports](#) on page 338

> **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, administrative users 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 [Viewing FC I/O Blade Port Information](#) on page 162.

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 [Saving and Restoring the Library Configuration](#) on page 329.

The paths to open the appropriate screens are as follows:

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

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

FC I/O Blade Internal Virtual Port for Medium Changers

FC I/O blades use an internal virtual port to access the medium changer devices (every defined partition has a medium changer device). Each FC I/O blade can access all medium 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 medium 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 medium changers 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 medium changers visible on ports 1 and 2 of both FC I/O blades, for a total of 16). To minimize unnecessary discovery of medium changers, you need to configure host mapping. See [Managing FC Hosts and Host Mapping](#) on page 106.

Configuring FC I/O Blade Channel Zoning

When FC I/O blades are installed in the library, administrative users can configure channel zoning for selected 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 I/O blade. Channel zoning does not affect medium changer LUNs (partitions). If you want to map hosts to medium 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 106.

Note:	If both channel zoning and host mapping are enabled, the channel zoning settings supersede any host LUN mapping on the 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 113.

- The **Setup - 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 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 I/O blade. If both channel zoning and host mapping are enabled, the channel zoning settings supersede any host LUN mapping on the 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 329.

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

The paths to open the appropriate screens are as follows:

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

- From the operator panel, select **Setup > 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, administrative users 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 Enabling/Disabling FC Host Mapping on page 107.

> **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

Administrative users 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 administrative users logged in from different locations. You can access the appropriate screens, but you cannot apply changes while another administrative user 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**.

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 > I/O Blades > Host Management**.

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

Creating, Modifying, and Deleting an FC Host Connection

Administrative users 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 shutting down the library. You can add up to 32 FC host connections per 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 Saving and Restoring the Library Configuration on page 329.

> **Note:** These operations should not be performed concurrently by multiple administrative users logged in from different locations. You can access the appropriate screens, but you cannot apply changes while another administrative user 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

Administrative users 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 <u>Controlling FC I/O Blade Power</u> on page 144.

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 <u>FC I/O Blade Internal Virtual Port for Medium Changers</u> on page 104). 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 I/O blade may discover tape drives attached to ports 3–6, each of which report themselves at LUN 0. The 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 medium changer 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 medium changer, 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 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 medium changer devices found on the 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 > I/O Blades > Host Mapping**) are not available unless FC host mapping is enabled. See <u>Enabling/Disabling FC Host Mapping</u> on page 107.

Configuring Host Mapping

To configure host mapping, you need to select the partition, tape drive, or medium changer 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 107.

- The **Setup - 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 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, medium 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 <u>Saving and Restoring the Library Configuration</u> on page 329.

> **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 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 <u>Modifying an FC Host Connection</u> on page 109.

> **Note:** If both channel zoning and host mapping are enabled, the channel zoning settings supersede any host LUN mapping on the I/O blade. For information on channel zoning, see <u>Configuring FC I/O Blade Channel Zoning</u> on page 105.

The paths to open the appropriate screens are as follows:

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

- From the web client, select **Setup > I/O Blades > Host Mapping**.

Configuring FC Host Port Failover

When I/O blades are installed in the library, administrative users 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 I/O blade as point-to-point connections (**Setup > I/O Blades > Port Configuration**). 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 > 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:	When both target ports on the I/O blade are attached to the same SAN fabric, you may see duplicate medium changers 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 111.

For information on configuring I/O blade ports and channel zoning, see Configuring FC I/O Blade Ports on page 103 and Configuring FC I/O Blade Channel Zoning on page 105.

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 114.

Details on configuring host port failover 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 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 checkbox to enable FC Host Port Failover. Clearing the checkbox 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 329.

Note:	This operation should not be performed concurrently by multiple administrative users logged in from different locations. You can access the appropriate screens, but you cannot apply changes while another administrative user 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 323.

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 Saving and Restoring the Library Configuration on page 329.

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

For information on how to configure the repaired port as the standby or active target port, see Configuring FC Host Port Failover on page 113.

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, administrative users 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 administrative users logged in from different locations. You can access the appropriate screens, but you cannot apply changes while another administrative user 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

Administrative users can use the operator panel **Security Settings** screen to change the following security features:

- **Network Interface** — enables or disables all external access to the library. This setting is enabled by default to allow external access.

- **SSH Services** — enables or disables Secure Shell (SSH) services, such as SSH (port 22), from accessing the library. This setting is enabled by default.

- **ICMP** — enables or disables 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** — enables or disables remote access to the library via the web client (port 80). This setting is enabled by default.

- **SNMP** — enables or disables SNMP traffic to the library (port 161). This setting is enabled by default.

- **SMI-S** — enables or disables SMI-S traffic to the library (port 5988). This setting is enabled by default.

> **Note:** This setting differs from enabling/disabling SMI-S in the **Tools > System Settings** menu (see <u>Configuring System Settings</u> on page 118).

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.

From the operator panel, administrative users 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

You can use the operator panel **System Settings** screen to configure the following system-wide settings:

- **User session timeout (minutes)** — The library automatically logs out a user or administrative user 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.

- **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.

- **Logical SN addressing** — The library uses the actual tape drive serial numbers by default. Selecting the **Logical SN addressing** check box enables the library to assign logical serial numbers to all tape drives in the library. Specifically, the library assigns a logical serial number to a tape drive in a specific location, not the serial number of the particular tape drive. If the tape drive is then replaced by another tape drive in the same library location, the logical serial number remains the same. From the host application's perspective, the replacement tape drive is the same as the original.

> **Caution:** If you change the logical serial number addressing setting, you must power cycle the library (perform a shutdown and press the power button) or remove power from each tape drive for the change to take effect.

- **Manual Cartridge Assignment** — Administrative users can disable or enable manual cartridge assignment. When manual cartridge assignment is enabled (the default setting), the **Assign IE** screen automatically appears on the operator panel once cartridges are placed into the I/E station. The **Assign IE** 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

- **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.

- **Enable SSL —** Allows you to enable Secure Socket Layer (SSL) for secure data transmission between the library and remote clients. This option is disabled by default.

- **Enable SNMP V1/V2 —** Allows you to enable or disable support for Simple Network Management Protocol (SNMP) V1 and V2c. This option is disabled by default.

> **Note:** SNMP v3 is always enabled. For more information on SNMP, see Configuring SNMP Settings on the Library on page 57.

- **Enable IPv6 —** Allows you to enable or disable support for IPv6 addresses. This option is disabled by default.

- **Enable SMI-S —** Allows you to enable or disable SMI-S running on the library. This setting is disabled by default.

> **Note:** This setting differs from enabling/disabling the SMI-S port in the **Tools > Security** menu (see Configuring Library Security Settings on page 117).

Details on the system settings include:

- Users can configure only the **Touch screen audio** setting.

- Administrative users can configure all the settings on the **System Settings** screen.

You cannot configure the system settings from the web client.The path to open the appropriate screen is as follows:

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

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**.
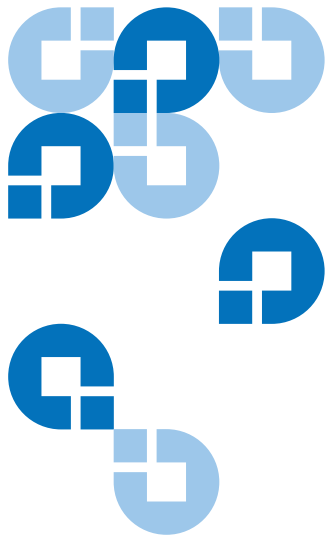
Registering the Library

Registering the library activates the warranty. After completing the initial setup of the library, choose **Setup > Register Library** on the web client to access the online product registration form.

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**.

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.

Logging In

All users, service users, and administrative users 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 administrative user account. Passwords are limited to 6–12 lower-case alphanumeric characters and can also include underscores (_), periods (.), hyphens (-), asterisks (*), and ampersands (**@**). For example: **pass_1**. For

information on changing passwords, see <u>Modifying Local User Accounts</u> on page 94.

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

Logging In When LDAP or Kerberos is Enabled

When LDAP or Kerberos is enabled, the **Login** screen displays the following items in addition to the User Name and Password text boxes:

- **Use Local Authentication** — Select this option to log in using a local user name and password.

- **Use LDAP Authentication** — Select this option to select or enter a domain and log in using a directory service user name and password.

For more information on LDAP, see <u>Configuring LDAP</u> on page 95.

For more information on Kerberos, see <u>Configuring Kerberos</u> on page 97.

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**.

Understanding the Location Coordinates

This section describes the numbering system used to identify components of the library. The library location coordinates contain the following digits: [Module],[Column],[Slot]. Figure 13 shows how a library with a control module and an expansion modules numbered.

Figure 13 Library Location
Coordinates
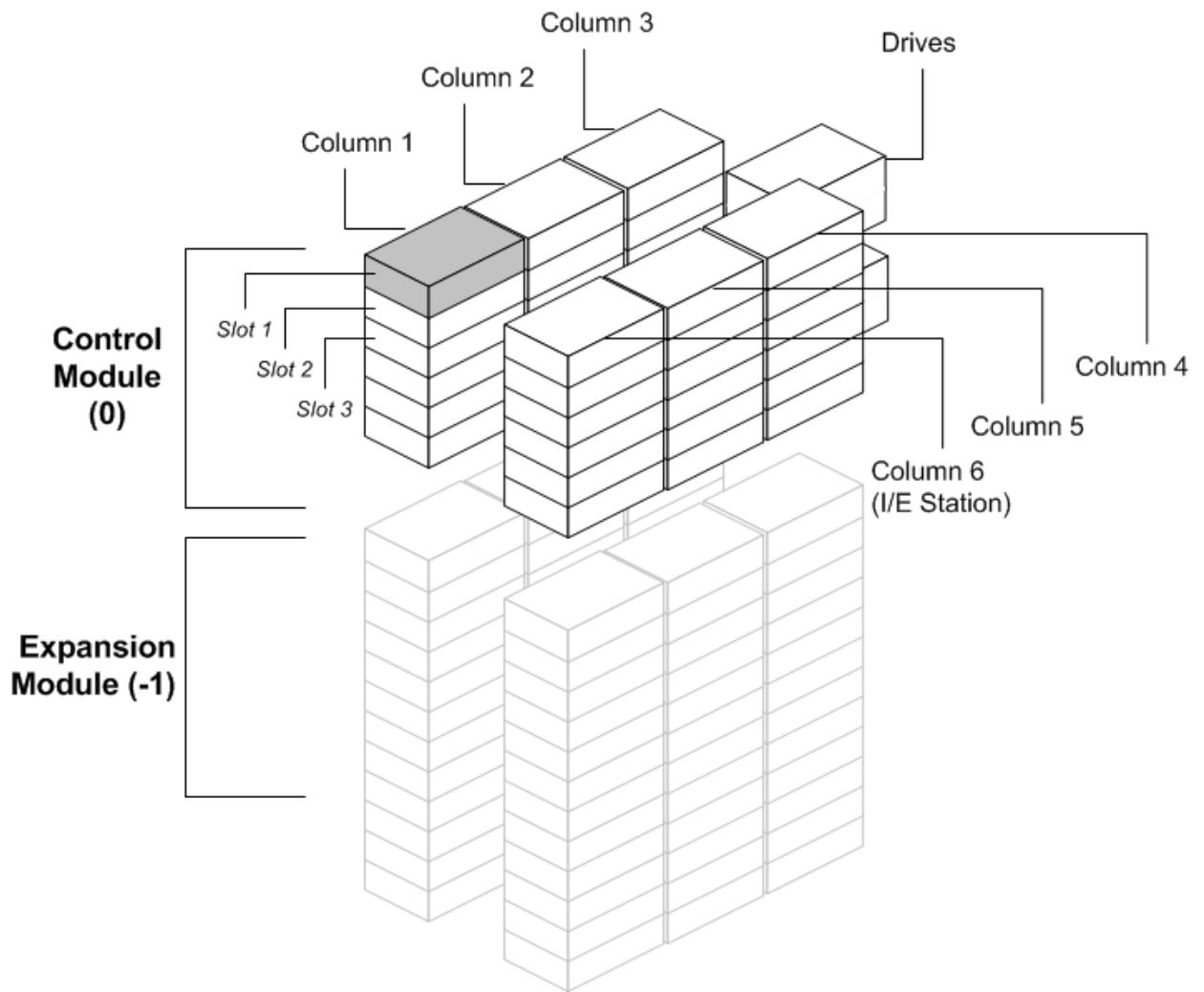
Modules

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 , 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].

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.

Performing Media Operations

Administrative users 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, administrative users 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 73.

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.

When manual cartridge assignment is enabled (the default setting), you cannot import cartridges until you have assigned them to a partition. After you have loaded the cartridges into the I/E station and closed the I/E station door, the **Assign IE** screen automatically appears on the operator panel. The **Assign IE** 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.

Administrative users can disable manual cartridge assignment. In this case, the **Assign IE** 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. For more information, see Disabling/Enabling Manual Cartridge Assignment on page 70.

Before importing cartridges, verify that all tape drives are unloaded and that all cartridges are in their appropriate storage slot locations. Doing this will avoid over-loading the library with cartridges.

If you have AutoClean enabled, you can also import cleaning cartridges into the library. For information, see Importing Cleaning Media on page 138. In addition, you can bulkload cartridges into the library rather than use the I/E station to import media. For information, see Bulkloading on page 129.

You must have access to the library's I/E station and the operator panel to import cartridges.

> **Note:** 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.

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 IE** 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 IE** screen appears, do the following:

a Assign the cartridges to the appropriate partition by selecting a partition listed on the **Assign IE** screen. The screen lists only the partitions to which you have been given access.

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 IE** screen will appear again.

b Select **Apply**.

c 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.

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 follo**ws:**

- **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.

Bulkloading

Bulkloading is another way to load media into the library. If zero I/E station slots are configured, you will always need to bulkload cartridges into the library. If I/E station slots have been configured, you may want to perform an initial bulkload when you first start using your library. The library will perform an inventory after the bulkload is complete.

Before bulkoading, 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 Viewing the Library Configuration on page 149.

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 bulkload tape cartridges into the library without first unlocking the I/E station door. If possible, bulkload 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 143. For information on configuring I/E station slots, see Configuring I/E Station Slots on page 73.

To perform an initial bulkload, 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 131.

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 323.

After the initial bulkload, 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 127.

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 bulkloading 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 Configuring I/E Station Slots on page 73.

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.

- 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 Configuring I/E Station Slots on page 73.

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 Exporting Cleaning Media on page 140.

> **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.

- 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.

- 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.

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.

Changing the Tape Drive Mode

You can take the tape drive online or offline. When the tape drive mode is online, the tape drive is available for use. When the tape drive mode is offline, the tape drive is offline to the host application and is not available for use.

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.

> **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 Working With Control Paths on page 78.

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 Administrative users 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 71. For information on importing and exporting cleaning media, see [Importing Cleaning Media](#) on page 138 and [Exporting Cleaning Media on page 140](#).

> **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. Administrative users can clean tape drives manually at any time, using commands on the operator panel or web client. For more information, see <u>Manually Cleaning Tape Drives</u> on page 141.

Enabling AutoClean

To enable AutoClean, an administrative user must configure at least one cleaning slot in the library. For information on configuring cleaning slots, see <u>Configuring Cleaning Slots</u> on page 71. For a description of AutoClean, see <u>About Cleaning Tape Drives</u> on page 137.

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 <u>Configuring Cleaning Slots</u> on page 71. For a description of AutoClean, see <u>About Cleaning Tape Drives</u> on page 137.

When manual cartridge assignment is enabled (the default setting), you cannot import cartridges 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 <u>Importing Media</u> on page 127 and <u>Disabling/Enabling Manual Cartridge Assignment</u> on page 70.

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 73.

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 IE** 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 IE** screen appears, do the following:

a On the **Assign IE** 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 71. For a description of AutoClean, see About Cleaning Tape Drives on page 137.

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.

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.

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 administrative users 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 71), 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 your library has zero I/E station slots, you will not be able to manually clean tape drives. See <u>Configuring I/E Station Slots</u> on page 73.

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 166.

- 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 335.

- Retrieve tape drive sled logs. Tape drive sled logs can be retrieved from any sled installed in the library. For more information, see Retrieving Tape Drive Sled Logs on page 336.

- Clean tape drives. Tape drive can be cleaned manually at any time. For more information, see About Cleaning Tape Drives on page 137.

- Upload/remove tape drive firmware for autoleveling. Available only for FC tape drives connected to an FC I/O blade. For more information, see Autoleveling Tape Drive Firmware on page 168.

- 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 Drive Reset on page 355.

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.

Administrative users 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

Administrative users 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 administrative users logged in from different locations. You can access the appropriate screens, but you cannot apply changes while another administrative user 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**.

Shutting Down or Restarting the Library

Administrative users can use the **System Shutdown** screen to shut down or restart the library. Some maintenance activities require that the library be shut down or restarted.

The **Shutdown** command shuts down the library's operating system and firmware. When performing a shutdown, the library finishes all active commands received from the host application and does not process any new commands. It shuts down all partitions and lowers the robot to the "shipping" position on the floor of the library. To finish the shutdown, press the power switch on the front of the control module.

Always perform a shutdown before completely removing power from the library. To completely remove power from the library, you must turn off the power switch on each power supply. Power is completely removed from the library when the blue LED on each power supply turns off.

To turn the library back on, turn on the power switch on each power supply, press the front power switch again, and then follow the login procedure.

> **Caution:** If you do not perform a shutdown before you physically power off the library, loss of library configuration data could occur.
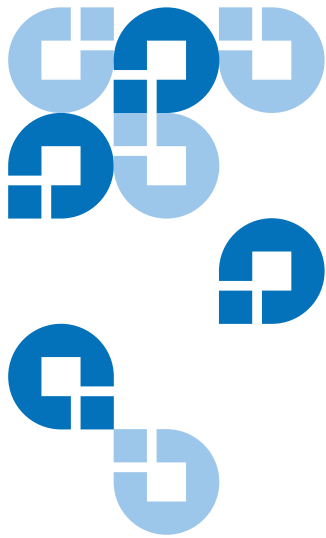
Restart shuts down and restarts the library's operating system and firmware. When performing a restart, the library finishes all active commands received from the host application and does not process any new commands. The library shuts down all partitions and restarts them during the reboot. In addition, the library performs an inventory of cartridges, tape drives, and slots during a reboot. Restarting takes approximately 5 minutes for the control module and longer for the 14U and 23U 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 Viewing RAS Tickets on page 324.

> **Note:** The Restart operation should not be performed concurrently by multiple administrative users. You can access the screen, but you cannot apply changes while another administrative user is performing the same operation.

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**.

Getting Information

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 administrative privileges can view only certain reports. See <u>User Privileges</u> on page 44 for information about user privileges.

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 System Information

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, and the date the BSP was last updated.

- **Library Partitions**— name, serial number, control path, status, encryption method, number of slots, number of media, and number of tape drives.

- **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.

- **I/O blades** — if the library contains FC I/O blades, this table lists the location coordinates, worldwide node name (WWN), firmware level, and ready status.

The path to open the report from the web client is **Reports > System Information**.

Viewing the Library Configuration

The **Library Configuration** report is a dynamic representation of the physical locations of various library resources, including tape drives, slots, partitions, and modules. Use the report to view 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, online status, assigned partition name, location coordinates, 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, SCSI ID, SAS address, tape drive firmware level, control path status, and encryption method of each tape drive.

- **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, put retries, and cleaning status (cleaning slot only) of each slot. For more details about slot data, see

- **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 Network Settings

The **Network Settings** 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.

- **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 **User Login** 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 administrative user, **User** for non-administrative, 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 Slot Information

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.

- **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. Currently, only IBM LTO-4 Fibre Channel and SAS tape drives are encryption capable. 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 [Using the Installation Verification Test](#) on page 348.

- **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 [Using the Installation Verification Test](#) on page 348.

- **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.

The path to open the report from the web client is **Reports > Log Viewer**.

Using Advanced Reporting

Advanced Reporting provides the following reports that you can configure for viewing and analysis:

- **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.

> **Note:** To use Advanced Reporting:
> - You must have Advanced Reporting licensed on your library. For details, see Adding or Upgrading Licensable Features on page 80.
> - Your library firmware must be at version 520G or higher.

Details about using Advanced Reporting include:

- The data for these 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 report contains 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 only contains the last seven days of data, even if you select a range longer than seven days. (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 Advanced Reporting Data on page 160.

- 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.

> **Note:** To view this report you must have Advanced Reporting licensed on your library. For details, see Adding or Upgrading Licensable Features on page 80.

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:

- 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.

  - Mount Count — the number of tape cartridge mounts.

  - Media Mount Time — the total amount of time a tape cartridge spent in the selected drive(s).

  - Media Motion Time — the total amount of time the 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 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 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 count 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.

The Media Integrity Analysis report collects the following information for each TapeAlert:

- Cartridge barcode

- Tape drive physical serial number

- Tape alert value

- Occurrence count of each TapeAlert

- Time and date (UTC) of TapeAlert occurrences

To configure the report, specify the following:

- 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)

- Attributes—Specifies which values are included in the report, and how they are combined. Select in any combination, including all (default) and none. If you select no attributes, the chart displays the TapeAlert count for the selected Grouping.

  - Cartridge Barcode — All relevant tape cartridges.

  - Drive Physical SN — All relevant tape drives.

  - TapeAlert — The TapeAlert flags that were issued. For a description of all TapeAlert flags, see Appendix B, TapeAlert Flag Descriptions.

- Chart — How the data is displayed in the chart. Choose Area, Bar (default), Line, or Pie.

- Type — 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 range.

  - Selected Drive by Physical SN — An individual tape drive. Only tape drives which issued a TapeAlert during the specified 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 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 14).

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 Saving and E-mailing Advanced Reporting Data).

Figure 14 Report Data Buttons

Saving and E-mailing Advanced Reporting Data

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**.

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 15 Saving and E-mailing the Report Data

Viewing FC I/O Blade Information

Administrative users 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

Administrative users 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, or 4 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 Configuring FC I/O Blade Ports on page 103.

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 Technical Support. You can also regularly monitor the Quantum Service & Support website at www.quantum.com/support for firmware upgrades, but you need to make sure that the firmware you download is compatible with your library and tape drives.

> **Note:** Verify with Quantum Technical Support or the current release notes that you are selecting the correct firmware version to download.

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.

Library firmware is available at the Quantum Service & Support website www.quantum.com/support. Navigate to the appropriate firmware version and 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 Technical Support that you are updating the library with the correct version of firmware. For technical support contact information, 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.

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 329.

It is also a good idea to capture a snapshot of current logged 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 326.

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 329 and Restoring the Library Configuration and Library Firmware on page 330.

> **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:** This operation should not be performed concurrently by multiple administrative users. You can access the screen, but you cannot apply changes while another administrative user 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 in the library firmware upgrade package you download from the Quantum Support 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**.

Updating Tape Drive Firmware

You can use the web client to upgrade one or more tape drives in your library with an image file downloaded from the Quantum Service & Support website.

Using an Image File to Upgrade Tape Drive Firmware

The web client allows you to upgrade tape drive firmware using a firmware image file. Note that updating tape drive firmware using an image file is a lengthy process, taking up to 90 minutes for each tape drive.

Tape drive firmware is available at the Quantum Service & Support website http://www.quantum.com/support. Navigate to the appropriate firmware version and download the file to your computer hard drive. Tape drive firmware comes bundled with library firmware, firmware upgrade instructions, and release notes. Verify with the release notes or Quantum Technical Support that you are updating the tape drives with the correct version of firmware. For contact information, see Getting More Information or Help on page 8.

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.

You can find detailed instructions on updating library firmware in the firmware upgrade package you download from the Quantum Service & Support 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.

> **Caution:** Before you upgrade tape drive firmware, make sure that cartridges are not loaded in any tape drives. If cartridges are loaded in tape drives during the upgrade process, the library loses knowledge of the cartridges' storage slot location, resulting in library and host application inventory issues.

> **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 administrative users. You can access the appropriate screens, but you cannot apply changes while another administrative user 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

When FC I/O blades are installed, the autoleveling feature enables you to automatically upgrade firmware on all FC tape drives that are connected to the FC I/O blades. This allows you to keep all FC tape drives of the same type (for example, LTO-3) 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 rebooted, 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 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-3, and LTO-4), 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 Technical Support that you are uploading the correct version of firmware. For technical support contact information,

You must have access to a tape drive firmware image file to enable autoleveling. Tape drive firmware is available at the Quantum Service & Support website. Navigate to the appropriate firmware version and download the file to your computer hard drive.

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**.

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-2 tape drives with LTO-3 tape drives, you no longer need the LTO-2 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**.

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 58 lbs. An expansion module, without tape drives, tape cartridges, or power supplies, exceeds 65 lbs.
>
> To avoid serious injury, at least two people are required to safely lift the modules into position.

Taking the Library Online/Offline

Taking a library online makes it accessible to host applications via the Storage Area Network (SAN). Taking a library offline makes it inaccessible to host applications via the SAN.

> **Warning:** Without tape drives, tape cartridges, or power supplies, a control module weighs approximately 58 lbs. An expansion module, without tape drives, tape cartridges, or power supplies, exceeds 65 lbs.
>
> To avoid serious injury, at least two people are required to safely lift the modules into position.

Taking a Library 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

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 cabling procedure appropriate for your drive type.

Connecting Library SCSI Cables to Hosts

Use this procedure, along with Figure 16 and Figure 17, 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 16 Stand-Alone 5U
Control Module SCSI Cabling
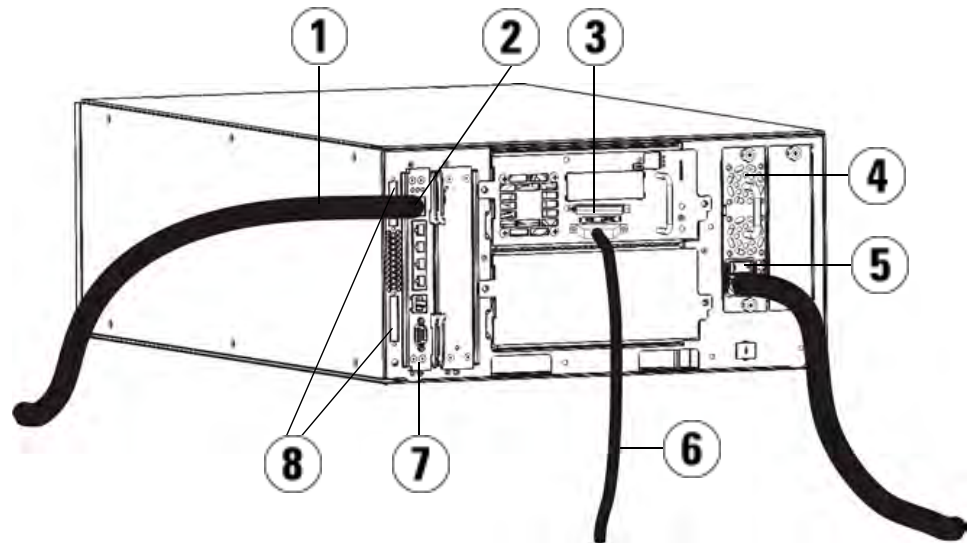
1	Ethernet cable to customer network
2	GB Ethernet port
3	SCSI terminator
4	Power supply
5	Rear power switch
6	SCSI cable to host
7	Library control blade
8	Module terminators

Figure 17 Multi-Module SCSI
Cabling
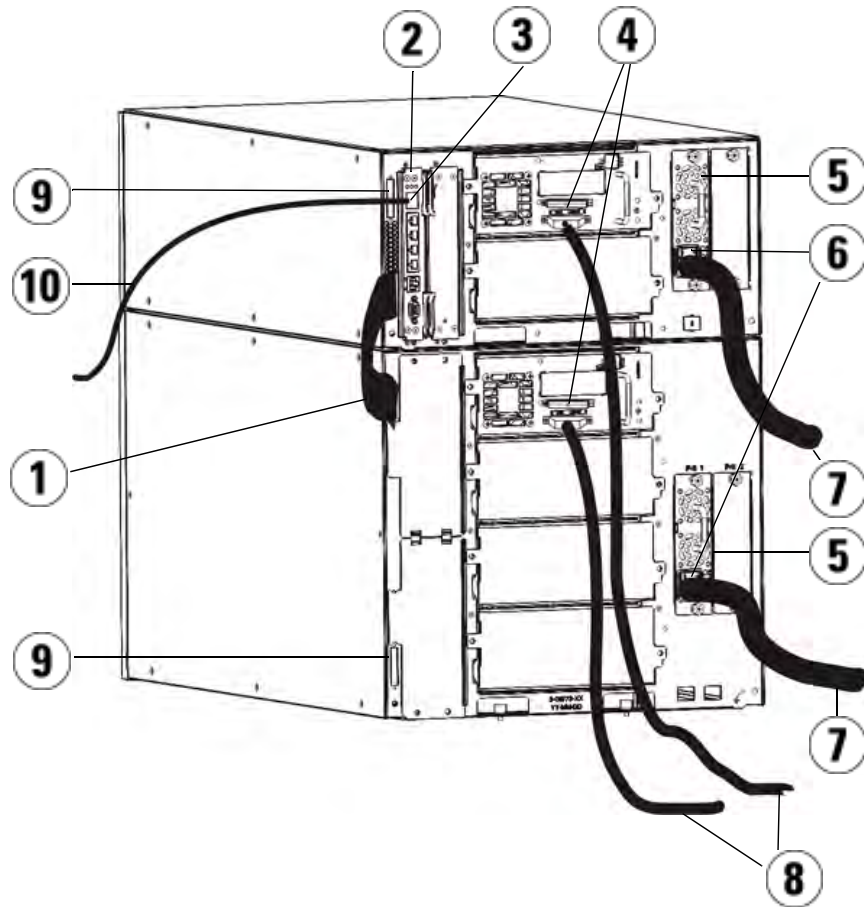
1	Module-to-module cable
2	Library control blade
3	GB Ethernet port
4	SCSI terminator
5	Power supply
6	Rear power switch
7	Power cords
8	SCSI cables to host
9	Module terminators
10	Ethernet cable to customer network

1 If your library is 14U or larger, install it in a rack. See <u>Installing the Library in a Rack</u> on page 284 for instructions. The instructions include procedures for removing and replacing tape drives.

2 Connect the SCSI cables to the tape drives.

    a Terminate the SCSI tape drive with an appropriate SCSI terminator.

    b Connect the SCSI tape drive to the 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 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 switch.

    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 47.

Connecting Library FC Cables Directly to Host

Use this procedure, along with <u>Figure 18</u> and <u>Figure 19</u>, if you are installing a library that includes FC tape drives that are connected directly to a host.

Figure 18 Stand-Alone Control
Module Fibre Channel Cabling
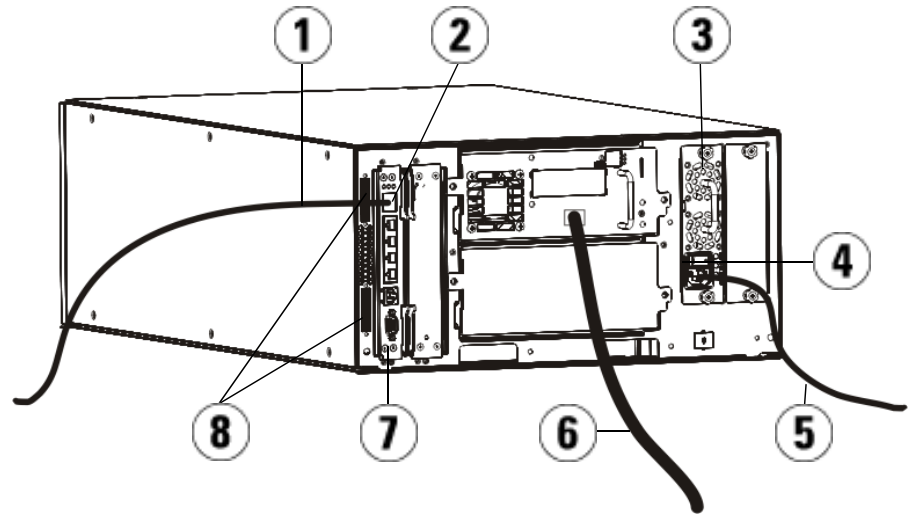
1	Ethernet cable to customer network
2	GB Ethernet port
3	Power supply
4	Rear power switch
5	Power cord
6	Fibre cable to host
7	Library control blade (LCB)
8	Module terminators

Figure 19 Multi-Module Fibre
Channel Cabling
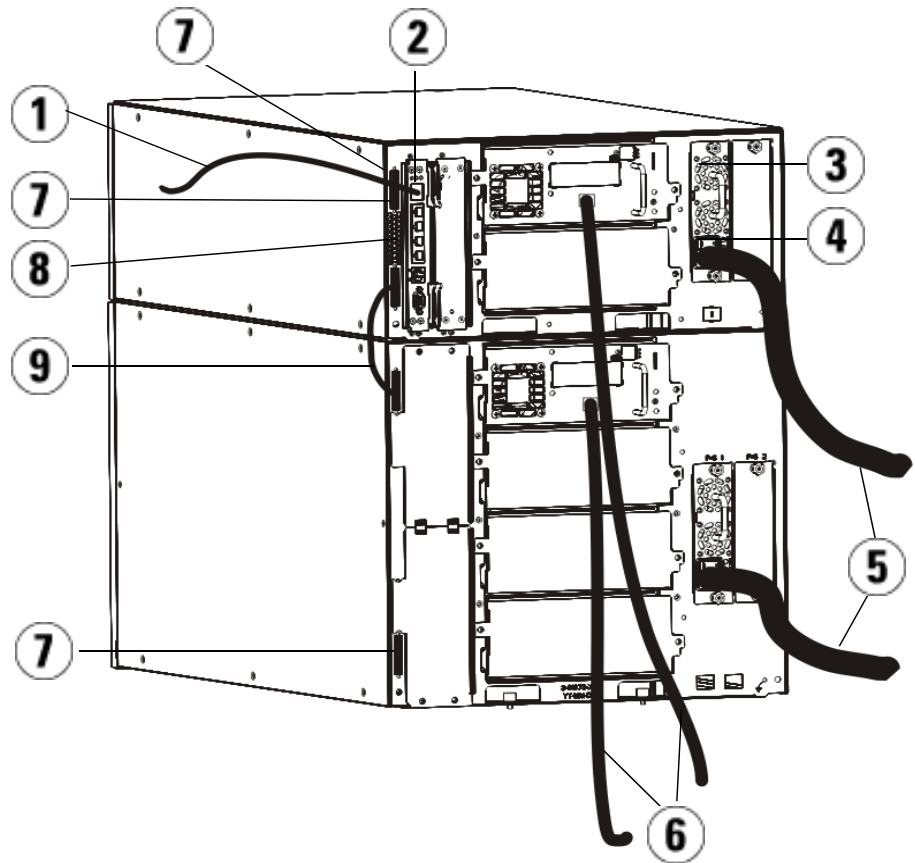
1	Ethernet cable to network
2	GB Ethernet port
3	Power supply
4	Rear power switch
5	Power cords
6	Fibre cables to host
7	Module terminators
8	Library control blade (LCB)
9	Module-to-module cable

> **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 14U or larger, install it in a rack.

See 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 47.

Connecting Library FC Cables to FC 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, and LTO-4 drives. For information on installing FC I/O blades, see <u>Adding, Removing, and Replacing FC I/O Blades</u> on page 306.

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 defined zone. For information on partitioning, configuring FC I/O blade ports, channel zoning, and host mapping, see Configuring Your Library on page 47.

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 20.

- SAN-ready tape drives that are shipped with FC I/O blades include 24-inch, orange fibre optic cables to connect drives to initiator ports on an I/O blade.

- 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 193 for best-practice guidelines for cabling a library.

Figure 20 FC I/O Blade

---
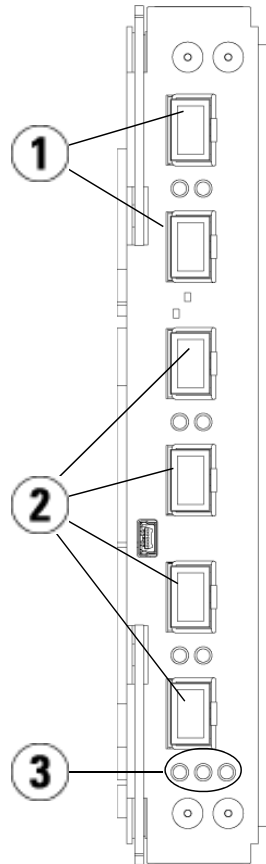
1   Target ports 1 and 2 to host(s)

2   Initiator ports 3 – 6 to drives

3   LEDs (blue, amber, green)

Use the following procedure, along with Figure 21, if you are installing a library that includes FC tape drives that are connected to FC I/O blades.

Figure 21 FC With I/O Blade
Cabling
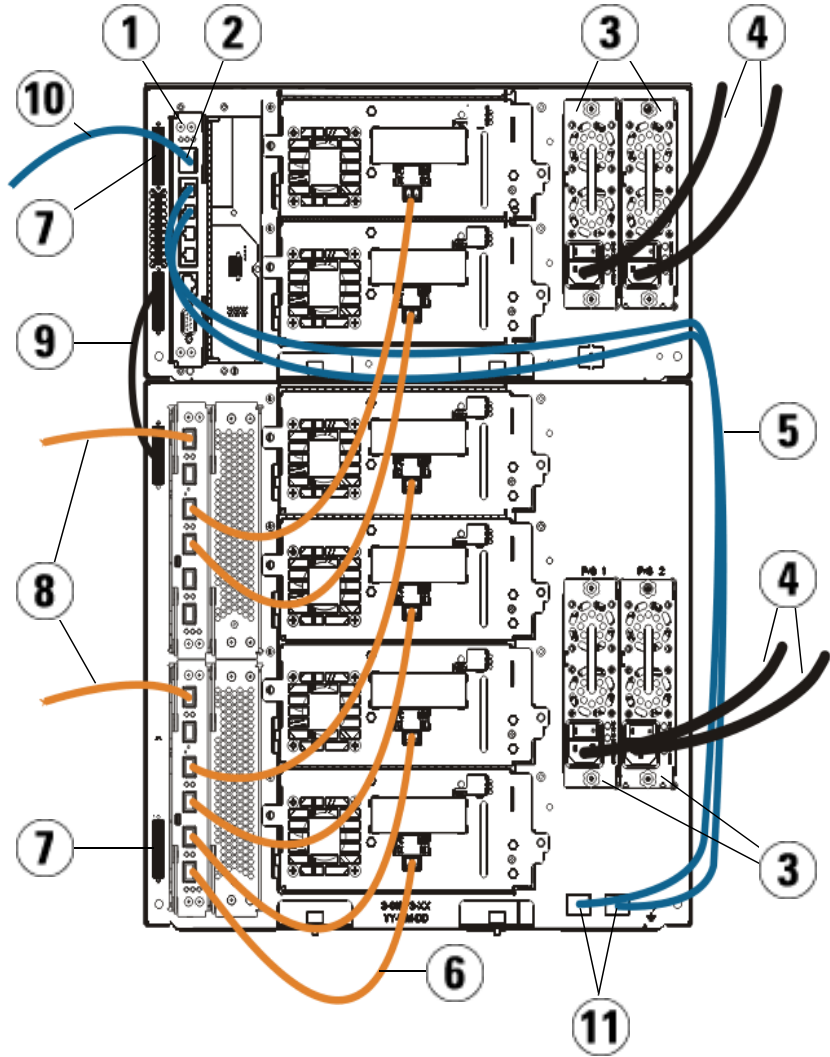
1	Library control blade (LCB)
2	GB Ethernet port
3	Power supplies
4	Power cords
5	Ethernet cables from LCB to expansion module
6	FC cable from FC I/O blade to tape drive
7	Module terminator
8	FC cable to host
9	Module-to-module cable
10	Ethernet cable to network
11	UPPER and LOWER Ethernet ports

Required tools: None

1 If your library is 14U or larger, install it in a rack.See 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 Cable Management Guidelines on page 193 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 193 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 switch.

    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 <u>Configuring Your Library</u> on page 47.

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.
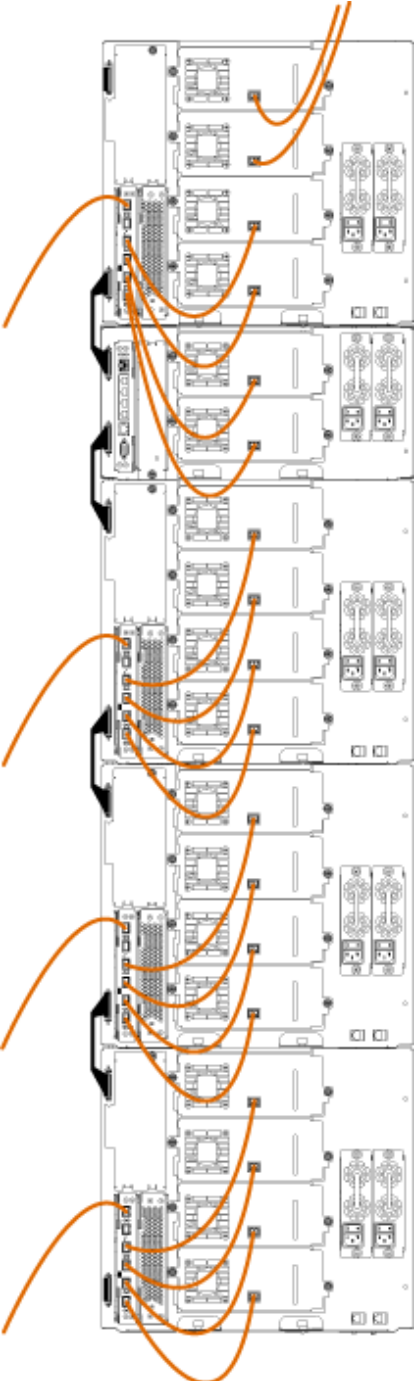
> **Note:** This section applies to libraries containing Fibre Channel tape drives, which are connected to a host or a Fibre Channel switch using an FC I/O blade. For tape drives that are directly attached to a host or a SAN switch, follow standard fibre optic cable handling best practices.

SAN-ready tape drives that are shipped with FC I/O blades include 24-inch fibre optic cables to connect drives to initiator ports on an FC I/O blade. The short length of these fibre cables is intentional. 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.

The 24-inch fibre cables are orange in color. 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 I/O Blades In Maximum Capacity Library	Tape Drive	I/O Blade	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

**Connecting Library SAS
Cables Directly to Host**

Use this procedure, along with [Figure 22](#) and [Figure 23](#), 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 22 Stand-Alone Control
Module SAS Cabling
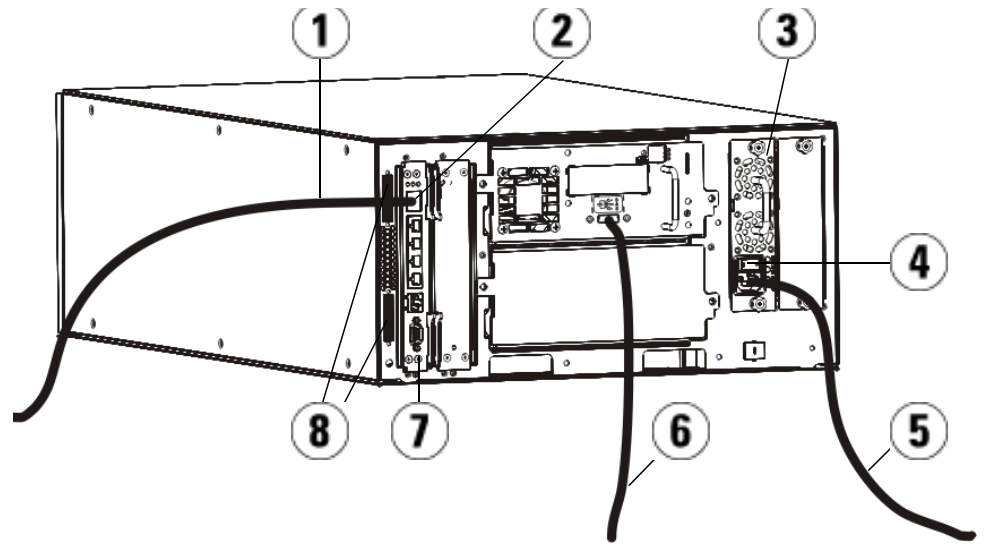
1	Ethernet cable to network
2	GB Ethernet port
3	Power supply
4	Rear power switch
5	Power cord
6	SAS cable to host
7	Library control blade
8	Module terminators

Figure 23 Multi-Module SAS
Cabling
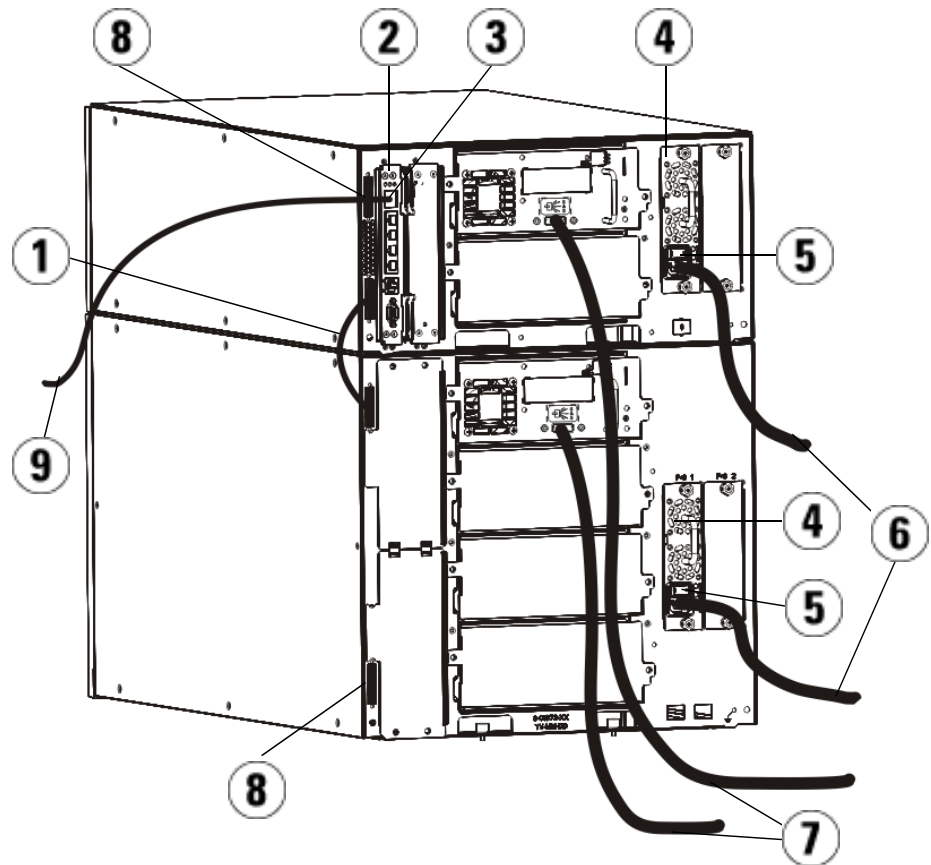
1	Module-to-module cable
2	Library control blade
3	GB Ethernet port
4	Power supply
5	Rear power switch
6	Power cords
7	SAS cables to host
8	Module terminators
9	Ethernet cable to network

1 If your library is 14U or larger, install it in a rack. See <u>Installing the Library in a Rack</u> on page 284 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 switch.

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 47.

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 <u>Cable Management Kit</u> section below. For recommended cabling of tape drives, see <u>Recommended Library Cabling for FC I/O Blades</u> on page 187.
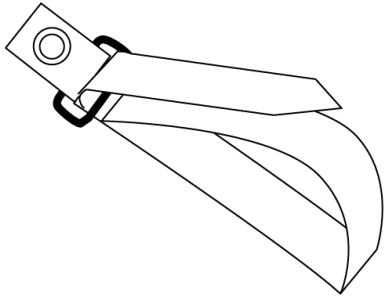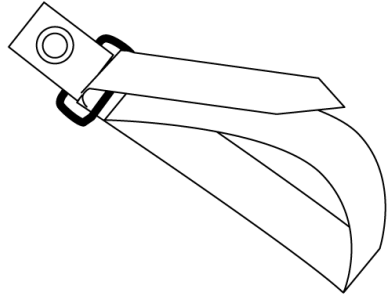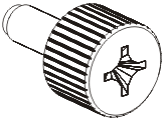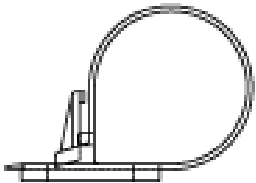
Cable Management Kit

If you purchase a Fibre Channel I/O 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 <u>http://shop.quantum.com</u>. 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
	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

Component	Description	Quantity
	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 24 Power Cord
Management
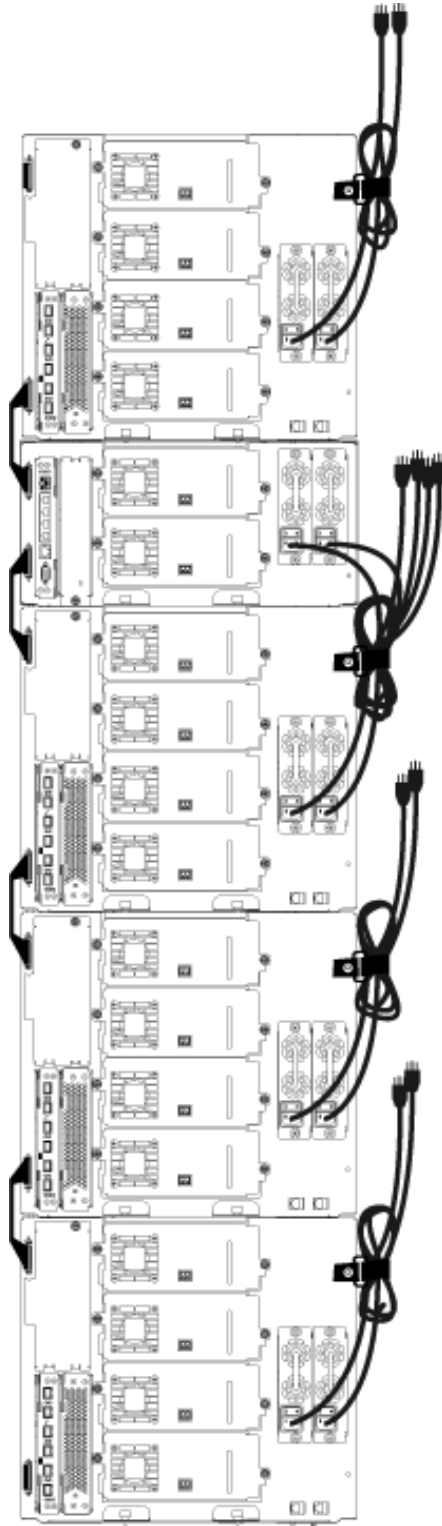
**Managing Ethernet
Cables**

A Scalar i500 library with FC I/O 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 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 FC I/O 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 up to four FC I/O 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 I/O 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 Figure 25 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 Figure 25.

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 Figure 25 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 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 25 Ethernet Cable
Management
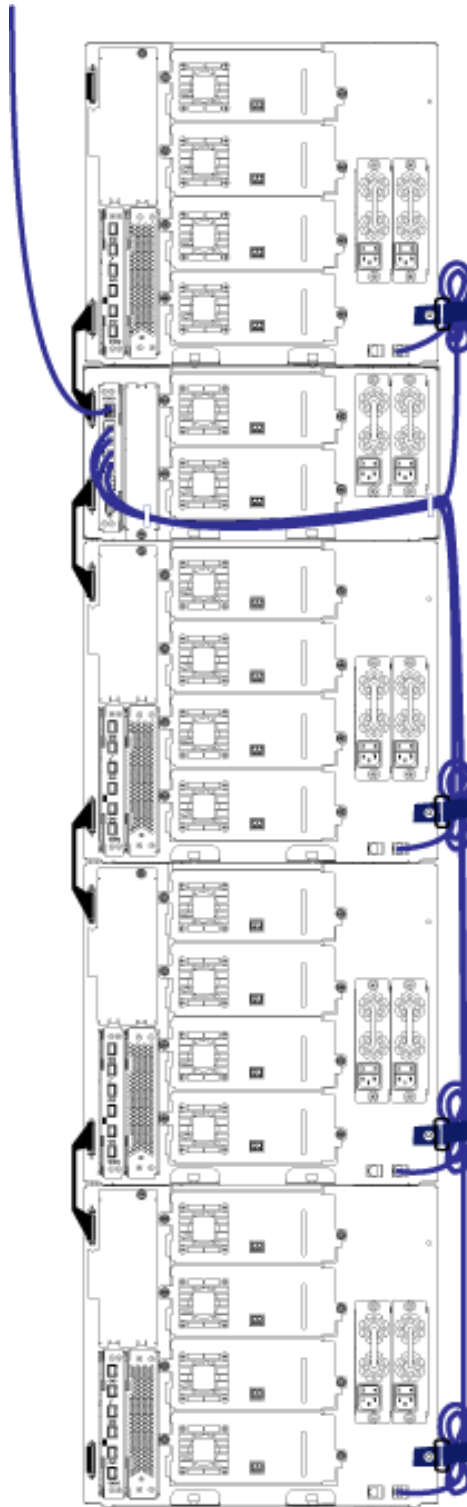
Figure 26 shows how a 41U library would appear with power, Ethernet, and fibre cables installed and managed according to these guidelines.

Figure 26 Cable Management, All Cables
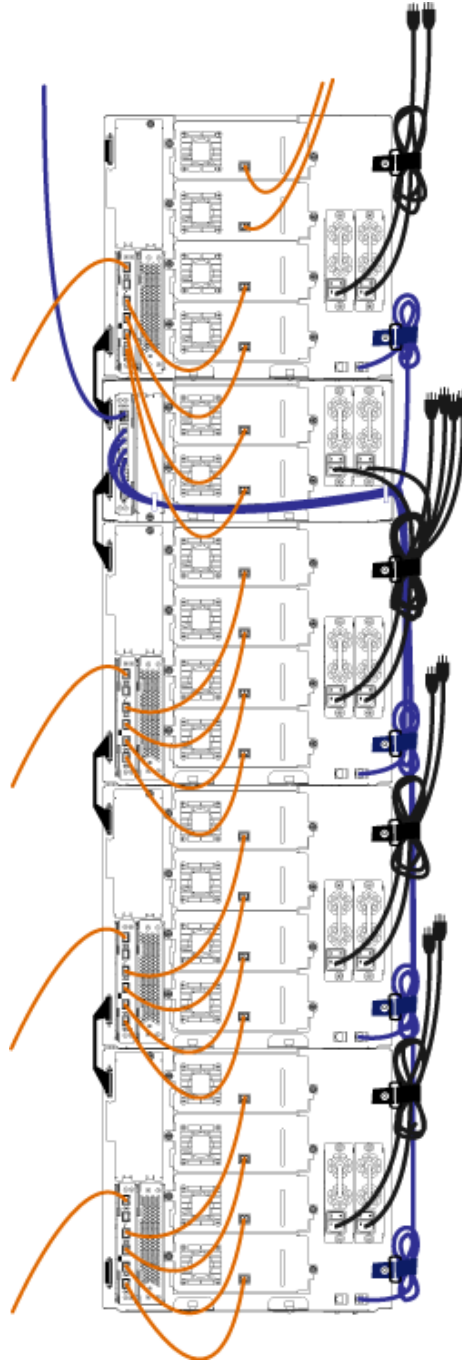
Installing a Stand-Alone 5UControl Module

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 284 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 303 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 281 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 293.

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 276 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 281 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 172.

11 Install module terminators in the top and bottom module terminator connectors. See <u>Cabling the Library</u> on page 172 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.
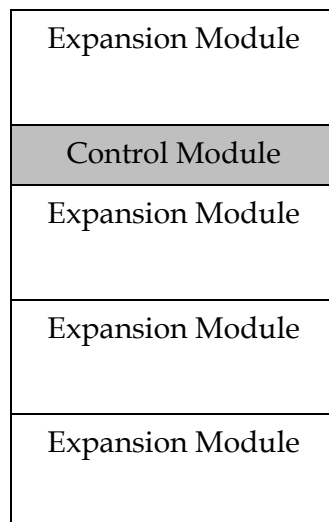
Expansion Module
Control Module
Expansion Module
Expansion Module
Expansion Module

> **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 <u>Installing the Library in a Rack</u> on page 284 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 <u>Adding, Removing, and Replacing Tape Drives</u> on page 303 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 <u>Adding, Removing, and Replacing Power Supplies</u> on page 281 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.

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.

> **Caution:** Before removing the control module's bottom cover plate, the robot assembly must be parked as described in <u>Step 4</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 27 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.
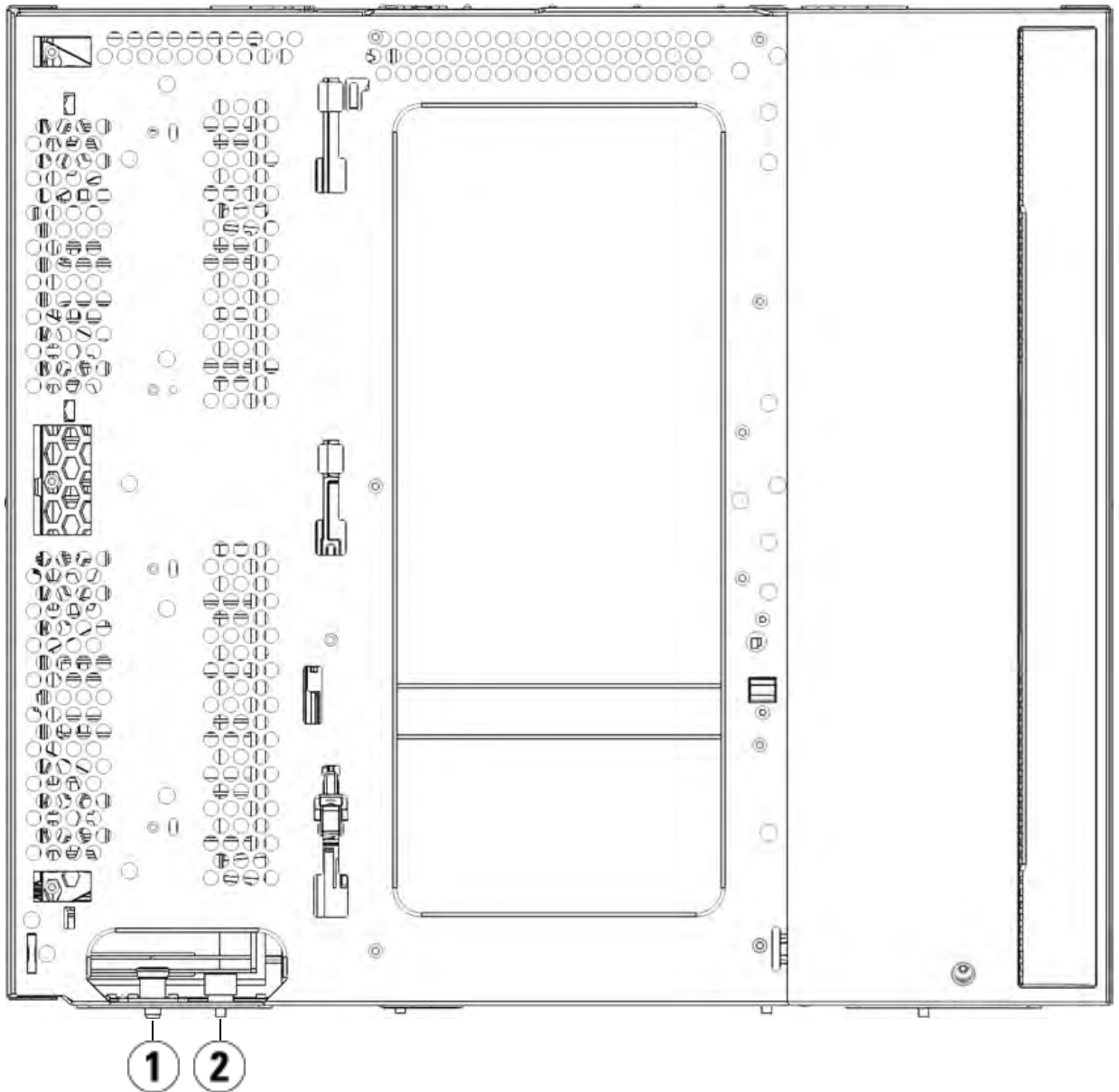
1	Guide pin
2	Thumbscrew

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 <u>Installing the Library in a Rack</u> on page 284 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 28 Y-Rail in Unlocked, Functional Position
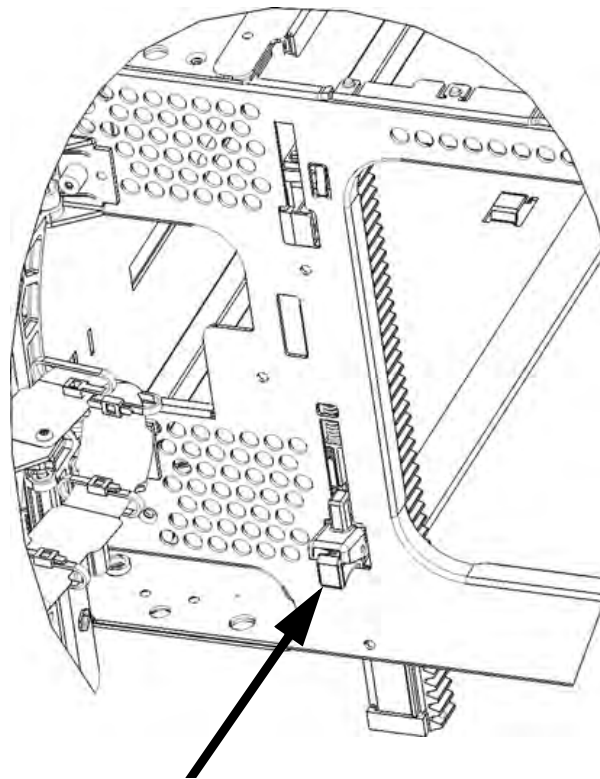
7 Repeat these steps for each expansion module you are installing.

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 276 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.

   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.
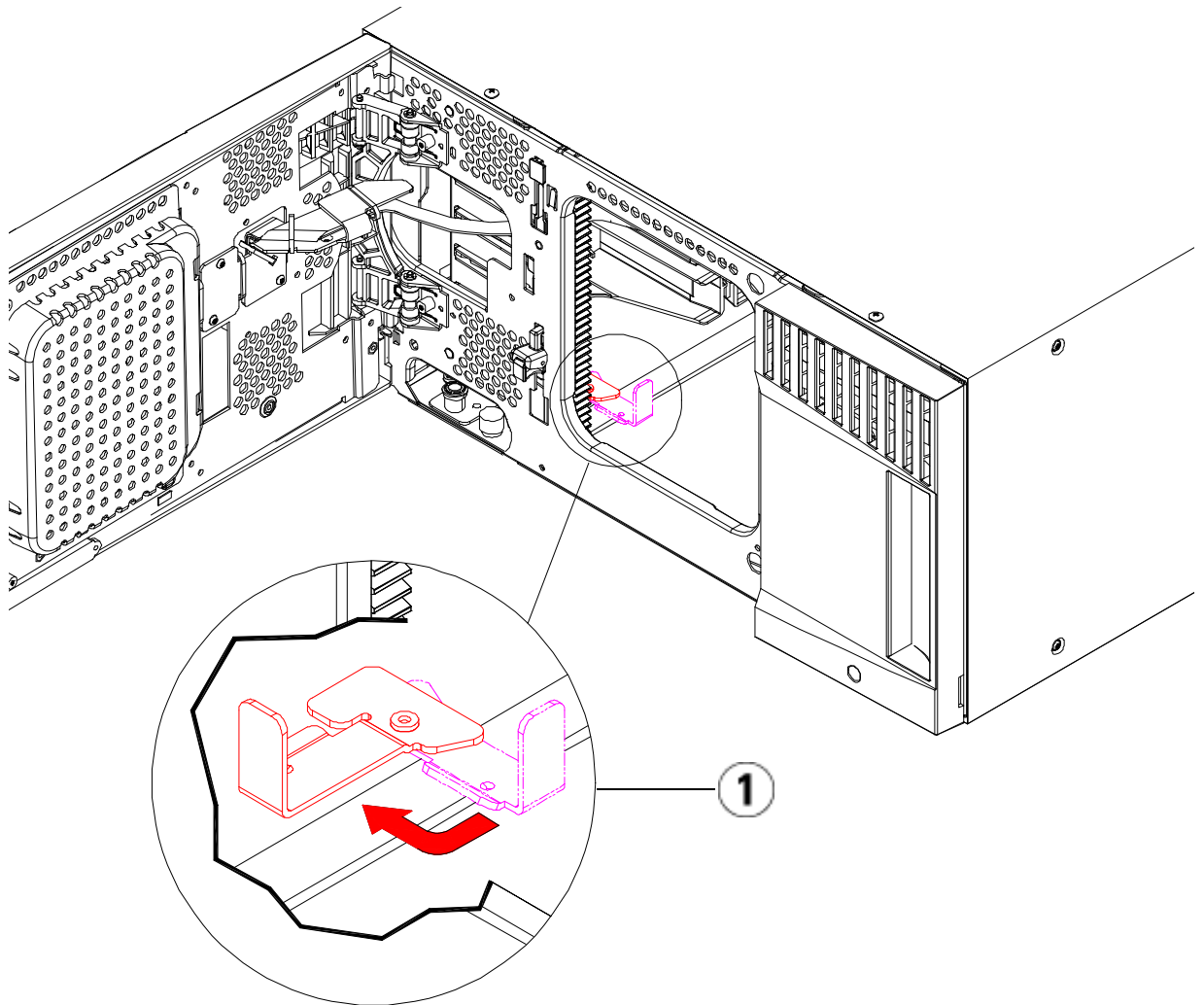
| 1 | Parking tab in "unparked" position |

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 303.

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 I/O Fan Blade on page 317.

5 Add the power supplies. For details, see <u>Adding, Removing, and Replacing Power Supplies</u> on page 281.

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 172.

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 163 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 58 lbs. A 9U expansion module, without tape drives, tape cartridges, or power supplies, exceeds 65 lbs.
>
> To avoid serious injury, at least two people are required to safely lift the modules into position.

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 58 lbs. A 9U expansion module, without tape drives, tape cartridges, or power supplies, exceeds 65 lbs.
>
> To avoid serious injury, at least two people are required to safely lift the modules into position.

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 <u>Updating Library and Tape Drive Firmware</u> on page 163 for information on upgrading firmware.

2 Remove all tape cartridges from the library using the import and export commands of the operator panel or web client.

3 Power off the library.

4 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.

5 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.

    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 |

6 Remove all power supplies from each module.

7 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.
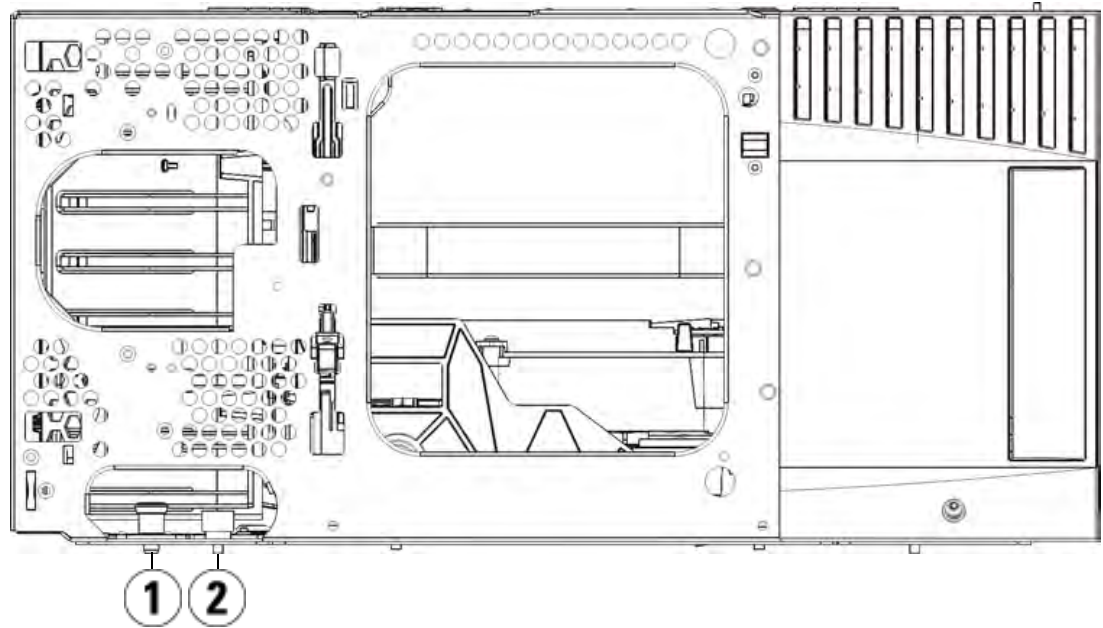
1	Guide pin
2	Thumbscrew

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 284 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 29 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.
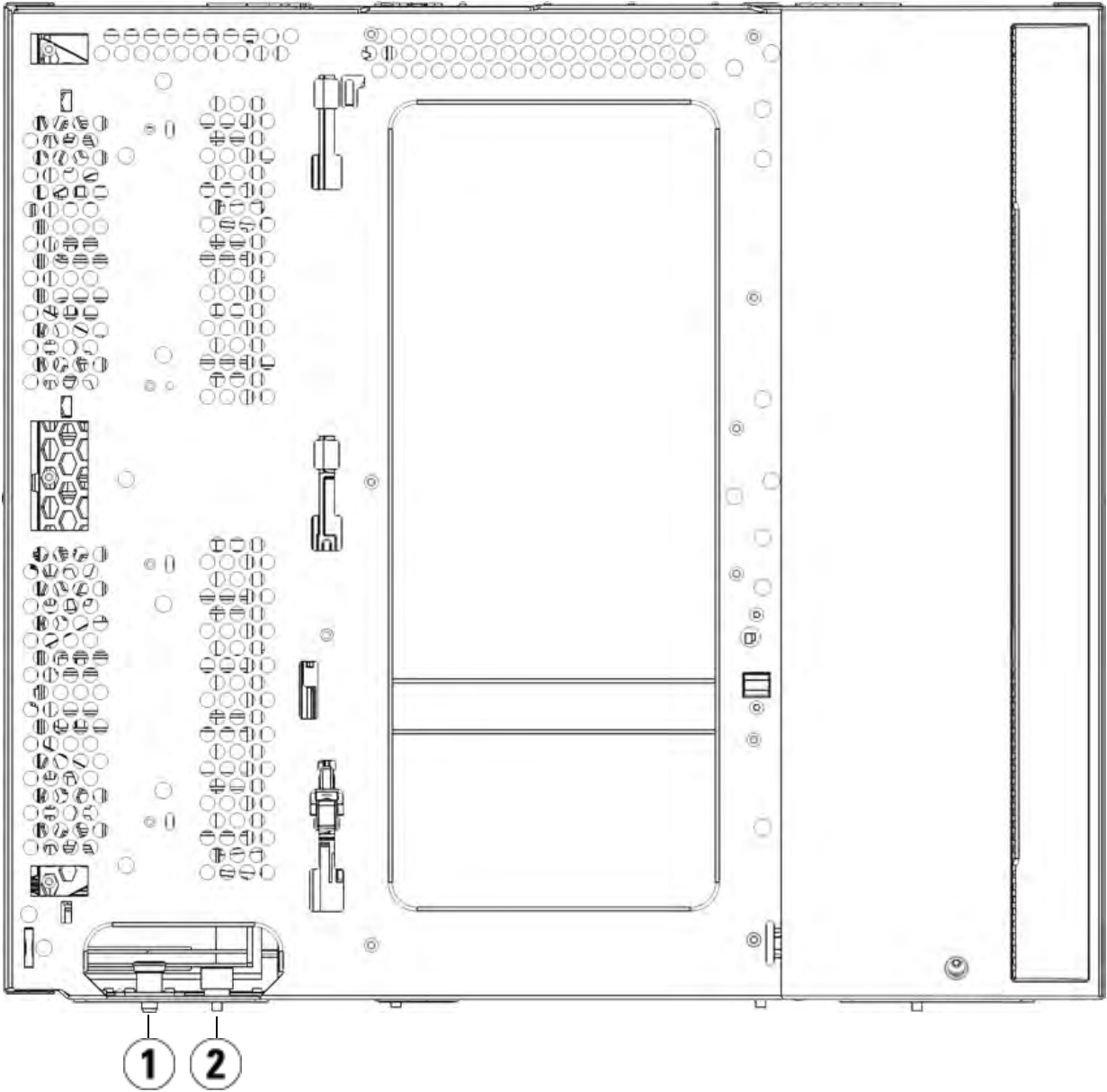
| 1 | Guide pin |
| 2 | Thumbscrew |

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.
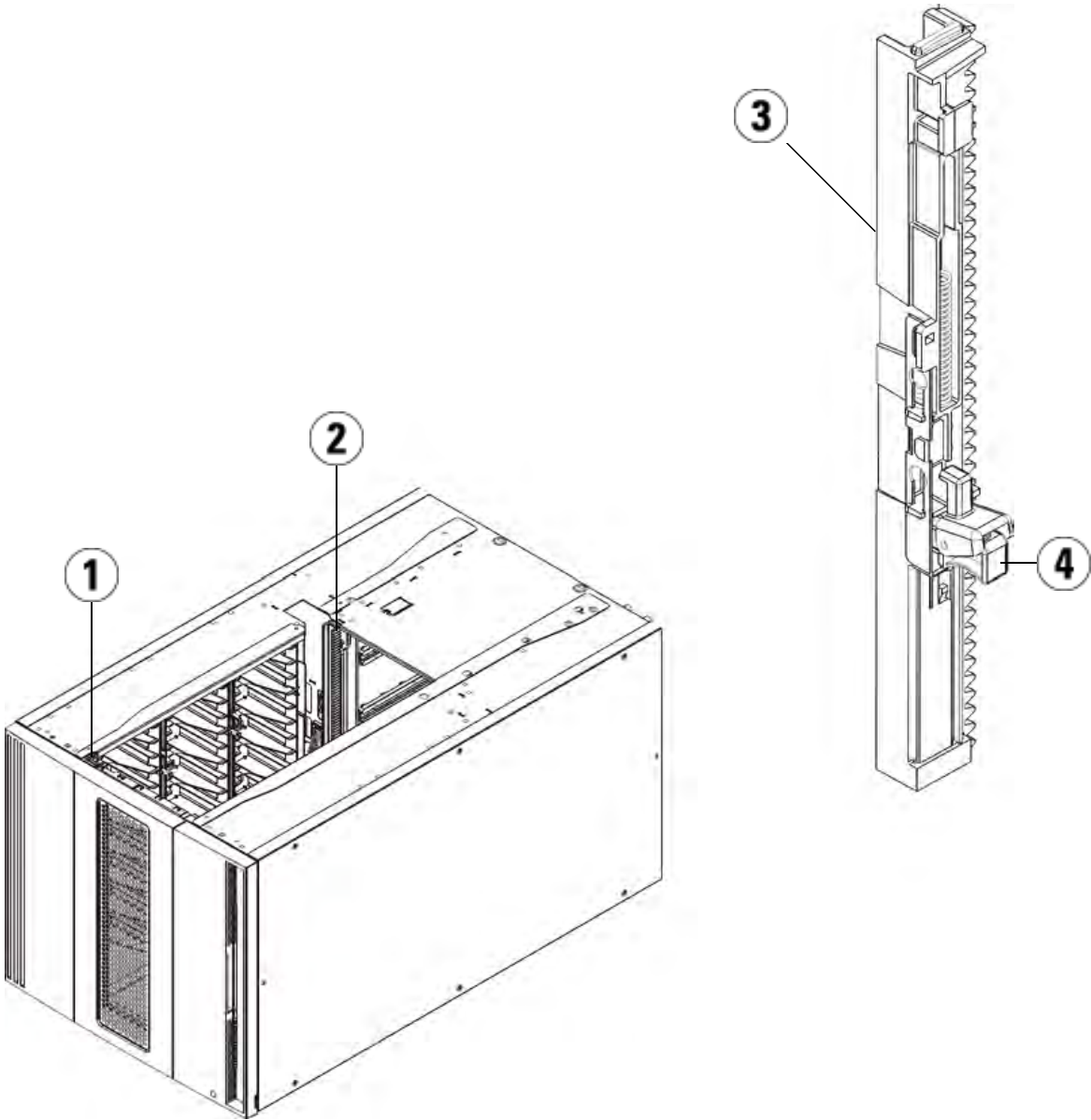
1	Front Y-rail
2	Rear Y-rail
3	Y-rail (this end up)
4	Squeeze here to release

   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.
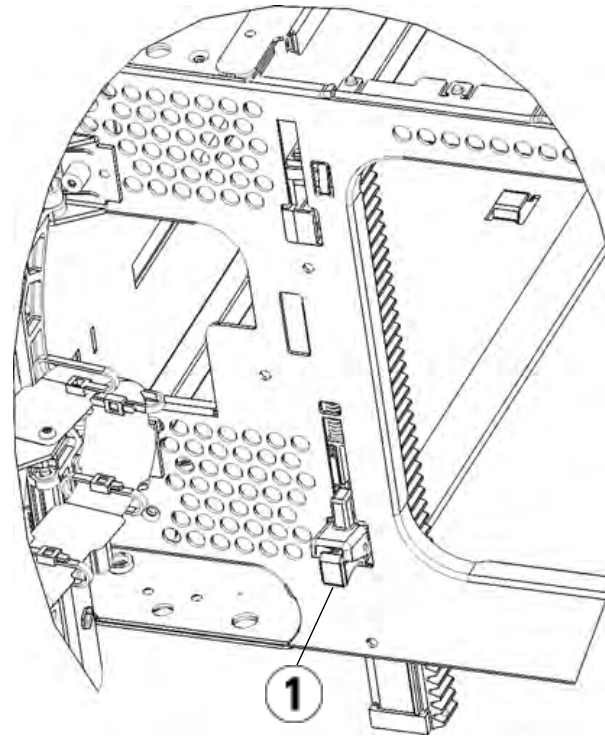
1	Y-rail in unlocked, functional position

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 Adding, Removing, and Replacing Tape Drives on page 303.

2 Add the power supplies. For details, see Adding, Removing, and Replacing Power Supplies on page 281.

3 Add the LCB to the control module. For details, see Removing and Replacing the Library Control Blade and LCB Compact Flash Card on page 276.

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 306 and <u>Adding, Removing, and Replacing the I/O Fan Blade</u> on page 317.

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.

    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.
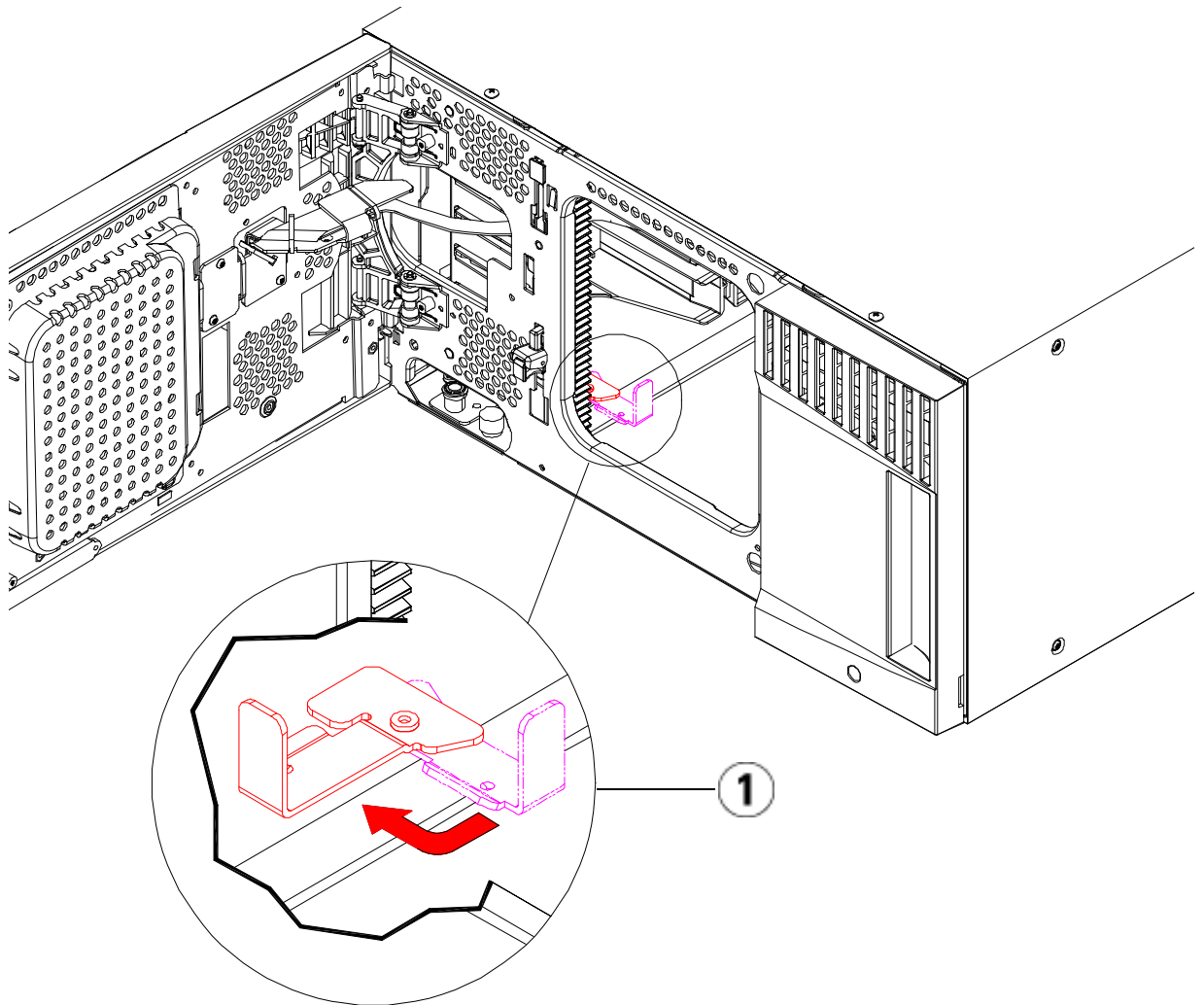
1	Parking tab in "unparked" position

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 <u>Cabling the Library</u> on page 172.

7 Power on the library.

8 Reconfigure the library, including applying the new COD license key, using the operator panel or web client.

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.

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.

The best practice before removing an expansion module is to:

- Using your I/E station, export all the tape cartridges from your library.

- Delete all partitions.

- Delete all cleaning slots.

- Set the number of I/E station slots to six.

> **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 58 lbs. A 9U expansion module, without tape drives, tape cartridges, or power supplies, exceeds 65 lbs.
>
> To avoid serious injury, at least two people are required to safely lift the modules into position.

Preparing to Permanently Remove the 9U Expansion Module

Follow these instructions to prepare to permanently remove the expansion 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

1 Remove all tape cartridges from the library using the import and export commands of the operator panel or web client.

2 Reconfigure the library with the following settings:

- Partitions: 0
- Cleaning slots: 0
- I/E station slots: 6

3 Power off the library.

4 Disconnect all power cords, network data cables, and module-to-module cables from each module you will be removing.

5 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.

    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

6 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 281.

7 Remove all tape drives from each module that you intend to remove. For details, see <u>Adding, Removing, and Replacing Tape Drives</u> on page 303.

Removing the Expansion Module

To remove the expansion module:

1 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 Permanently Remove the 9U Expansion Module</u> on page 233.

---

2 Disengage the Y-rails so the modules can be unstacked safely.
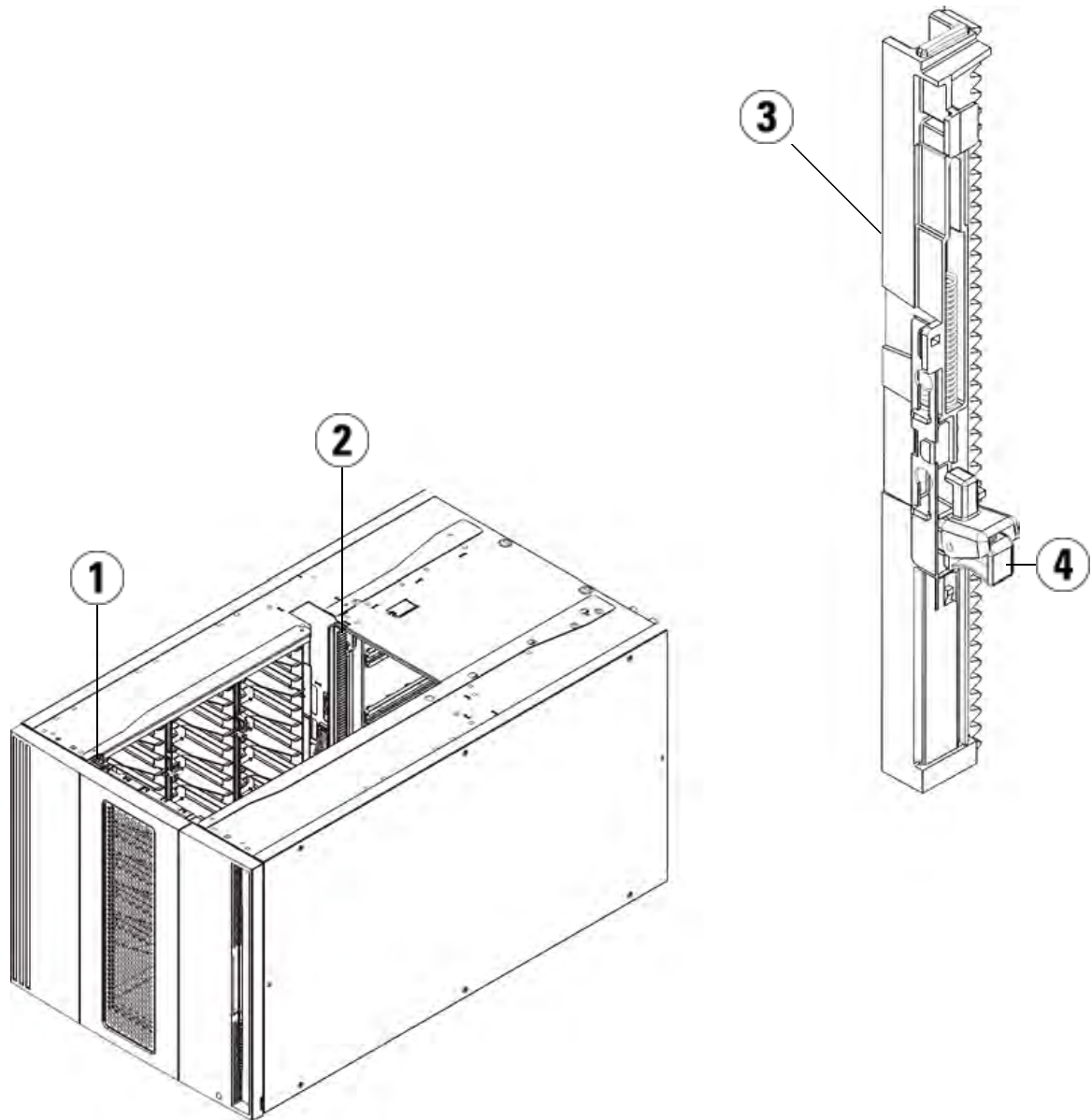
1	Front Y-rail
2	Rear Y-rail
3	Y-rail (this end up)
4	Squeeze here to release

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.
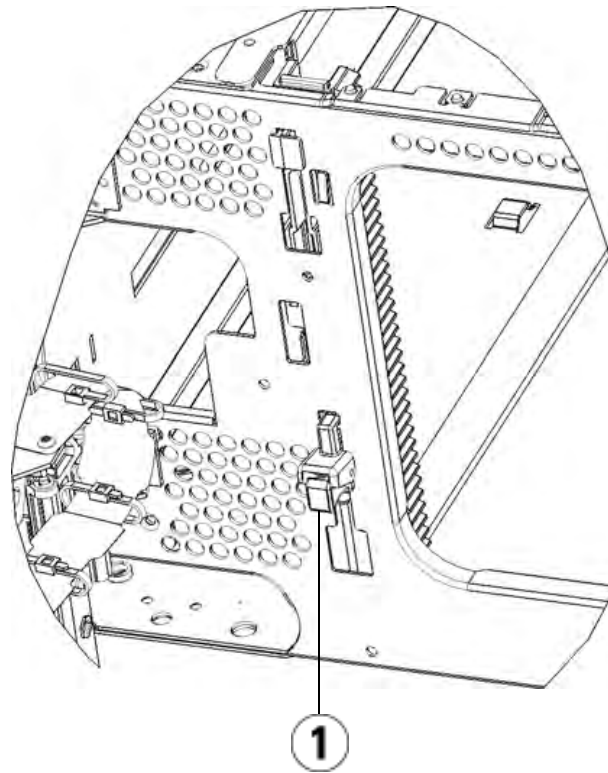
1	Y-rail in locked, non-functional position

3 Remove the rack ears that fasten the module to the rack. See for detailed instructions on using the rack ears.

4 Loosen the thumbscrews located at the base of the front of the module.

| 1 | Thumbscrews (behind doors) |

5 Loosen the two thumbscrews located at the base of the back of the module.

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.

7 From the front of the library, slide the entire module toward you and lift it off of the module below it.

8 Repeat these procedures for each module that you intend to remove.

9 Remove and replace the cover plates, if appropriate (see Figure 30).

> **Caution:** Before removing the control module's bottom cover plate, the robot assembly must be parked as described in Preparing to Permanently Remove the 9U Expansion Module 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 30 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 303.

3 Add the power supplies. For details, see Adding, Removing, and Replacing Power Supplies on page 281.

4 Add the LCB to the control module. For details, see Removing and Replacing the Library Control Blade and LCB Compact Flash Card on page 276.

5 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 306 and Adding, Removing, and Replacing the I/O Fan Blade on page 317.

6 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.

   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.
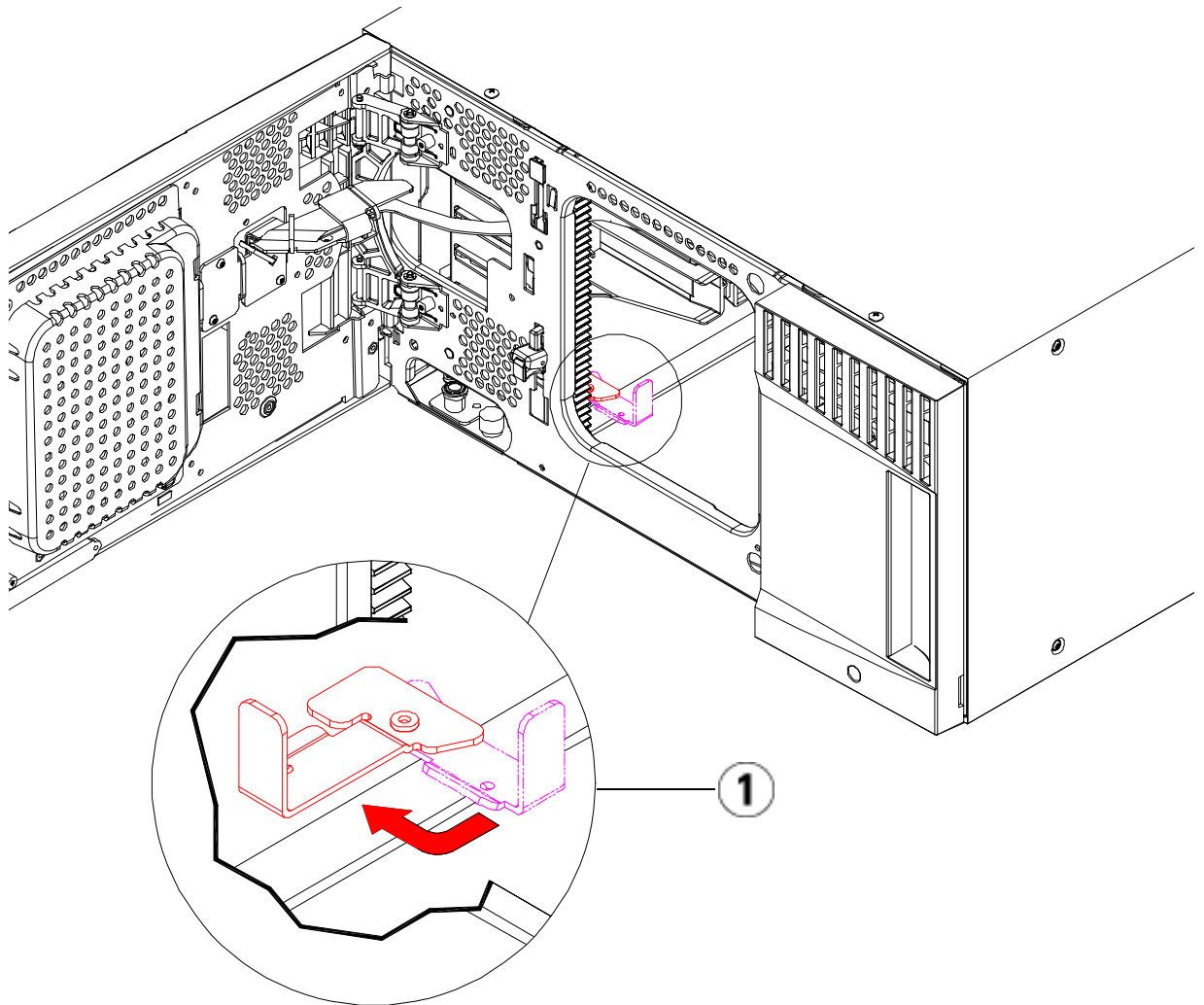
1	Parking tab in "unparked" position

7 Close the library's I/E station and access doors.

8 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 172.

9 Power on the library.

10 Add the tape cartridges to the library's modules using the I/E station commands from the operator panel or web client.

11 Reconfigure the library settings using the operator panel or web client.

12 Open the host application and reinventory in order to synchronize its logical inventory with the physical inventory of the library.

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 Adding or Upgrading Licensable Features on page 80.

- A partition with all resources in the removed module will be present with no slots or drives. This partition can only be deleted.

The best practice before removing the control module is to:

- Using your I/E station, export all the tape cartridges from your library.

- Delete all partitions.

- Delete all cleaning slots.

- Set the number of I/E station slots to six.

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.

Before removing the control module, you must first remove all expansion modules (if any) positioned above the control module.

> **Warning:** Without tape drives, tape cartridges, or power supplies, a control module weighs approximately 58 lbs. An expansion module, without tape drives, tape cartridges, or power supplies, exceeds 65 lbs.
>
> To avoid serious injury, at least two people are required to safely lift the modules into position.

> **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 284 for more information.

Preparing to Remove the Control 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

1 Power off the library.

2 Disconnect all power cords, network data cables, and module-to-module cables from each expansion module located above the control module, and from the control module itself.

> **Note:** You should label all cables before you remove them so you can later reconnect them to their proper locations.

3 Remove all power supplies from each module that you intend to remove. For details, see Adding, Removing, and Replacing Power Supplies on page 281.

4 Remove all tape drives from each module that you intend to remove. For details, see Adding, Removing, and Replacing Tape Drives on page 303.

5 Remove the tape cartridges from each module that you intend to remove.

> **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 they were removed from. Since the library assigns slots to a partition, you must create a map to locate each tape cartridge or create a map of cartridge slots that belong to each partition. You can do this by going to the **Reports > Library Configuration** screen on the web client and clicking the **Show BarCodes** button.

> **Note:** If you are unsure about which cartridge's barcode belongs in which partition, export the tape cartridges via the I/E station while keeping track of which partition they came from. Reconfigure the library and then re-import the cartridges via the I/E station into the appropriate partitions.

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.

> **Note:** 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.

   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.
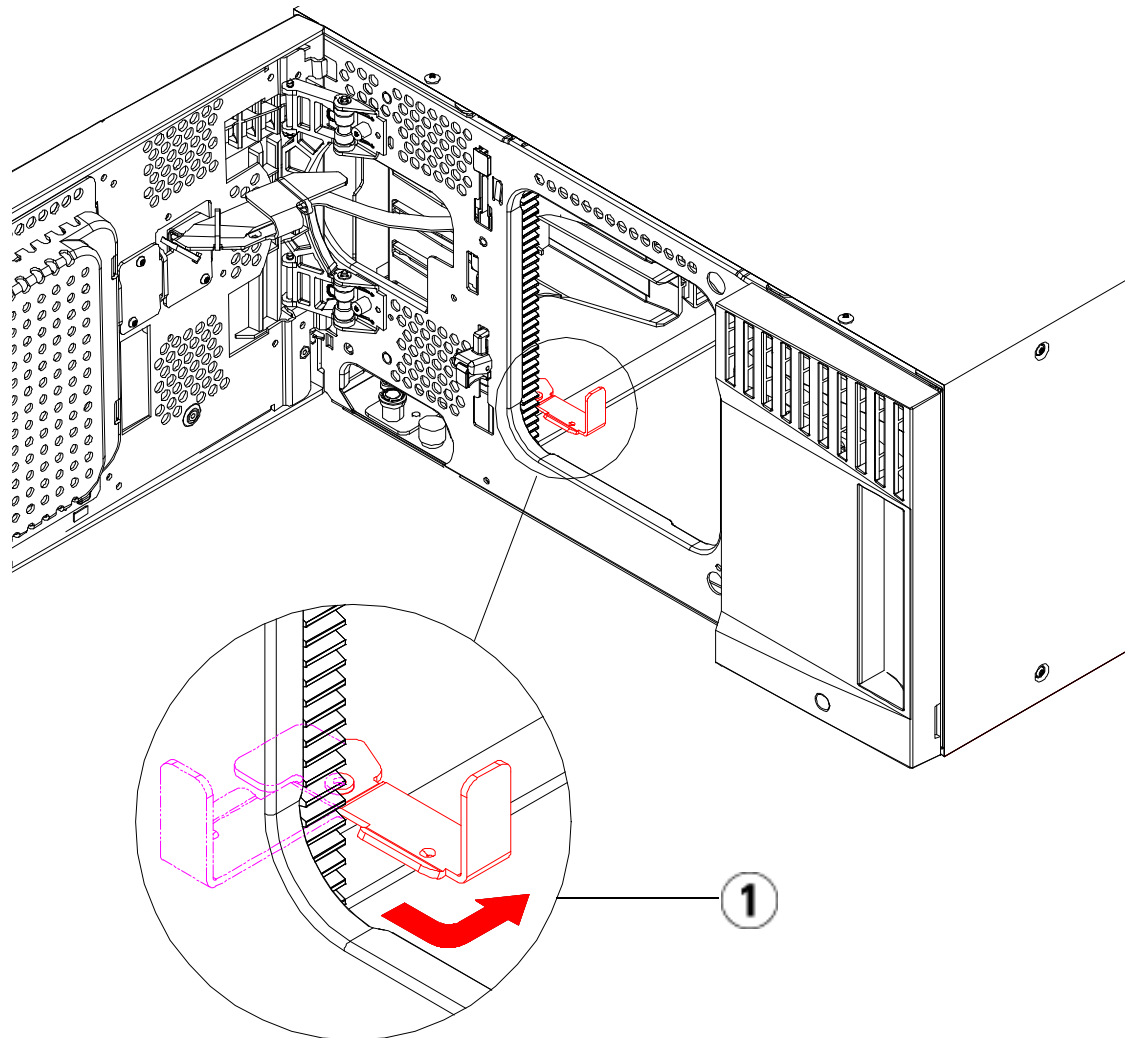
| 1 | Parking tab in "parked" position |

7 If there are expansion modules stacked above the control module, remove them now.

Removing the Control Module

1 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 the Control Module](#) above.

2 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	Control module (front)
2	Thumbscrews
3	Control module (rear)

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.
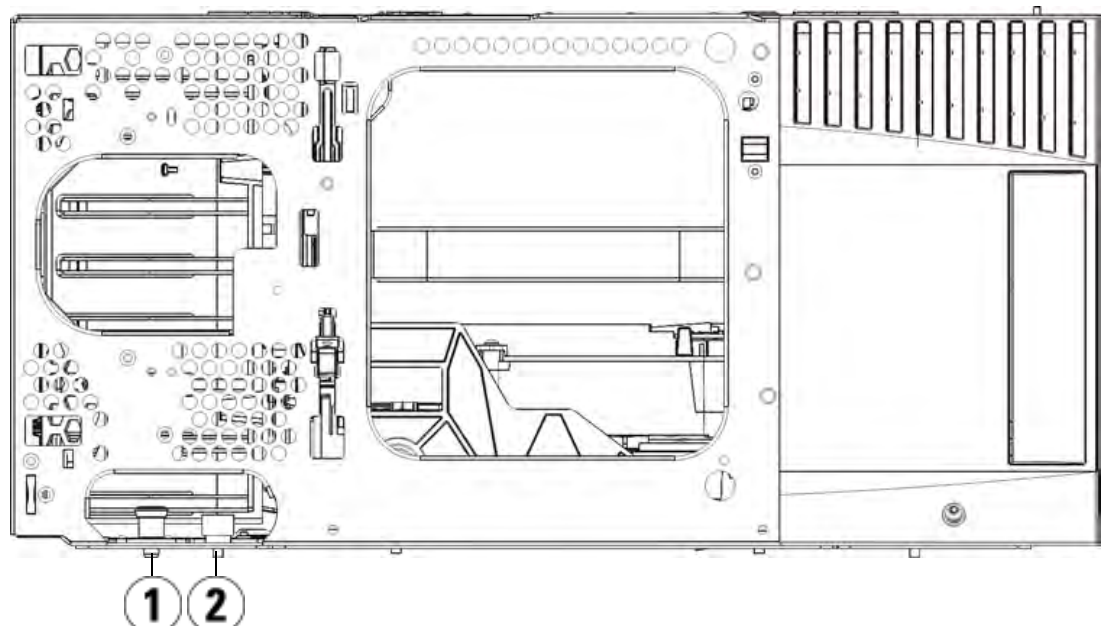
1	Guide pin
2	Thumbscrew

6 Slide the entire module toward you and lift it off of the module below it.

Replacing the Control Module

1 Remove the tape drives from the new control module.

2 Remove the power supplies from the new control module.

3 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 Preparing to Remove the Control Module above.

  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.

4 Remove the LCB from the 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 Removing and Replacing the Library Control Blade and LCB Compact Flash Card on page 276.

> **Note:**   If you plan to stack the control module on top of a 9U expansion module, be sure to park the picker in the control module first.

5 If the library configuration includes expansion modules below the control module, install them in the library now.

6 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.

7 Use rack ears to fasten the control module on top of a 9U expansion module.

8 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.

9 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.

10 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
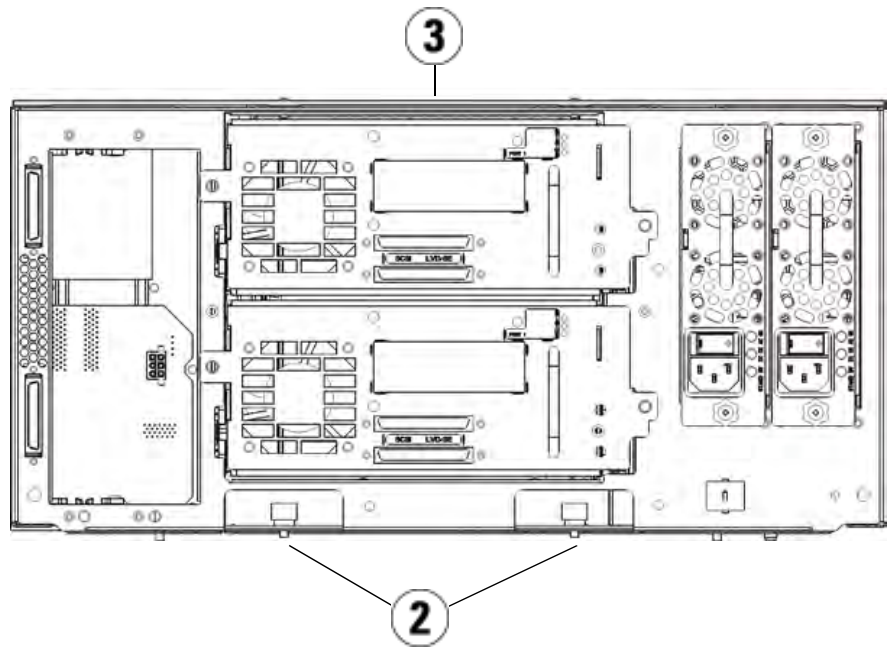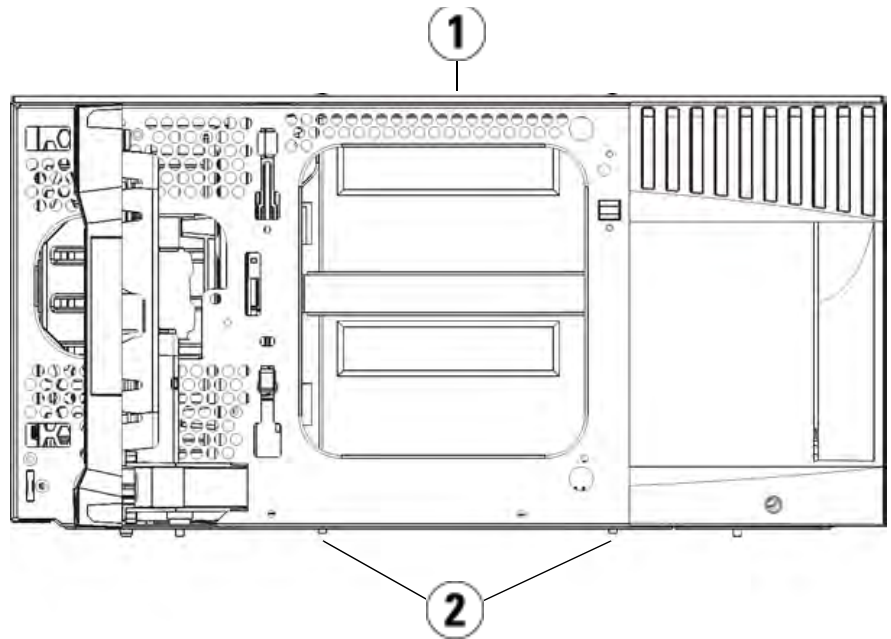module. Squeeze the handle of the Y-rail release mechanism, lift
it out of its locked position, and slide it downward as far as it will
go.

11 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.

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.
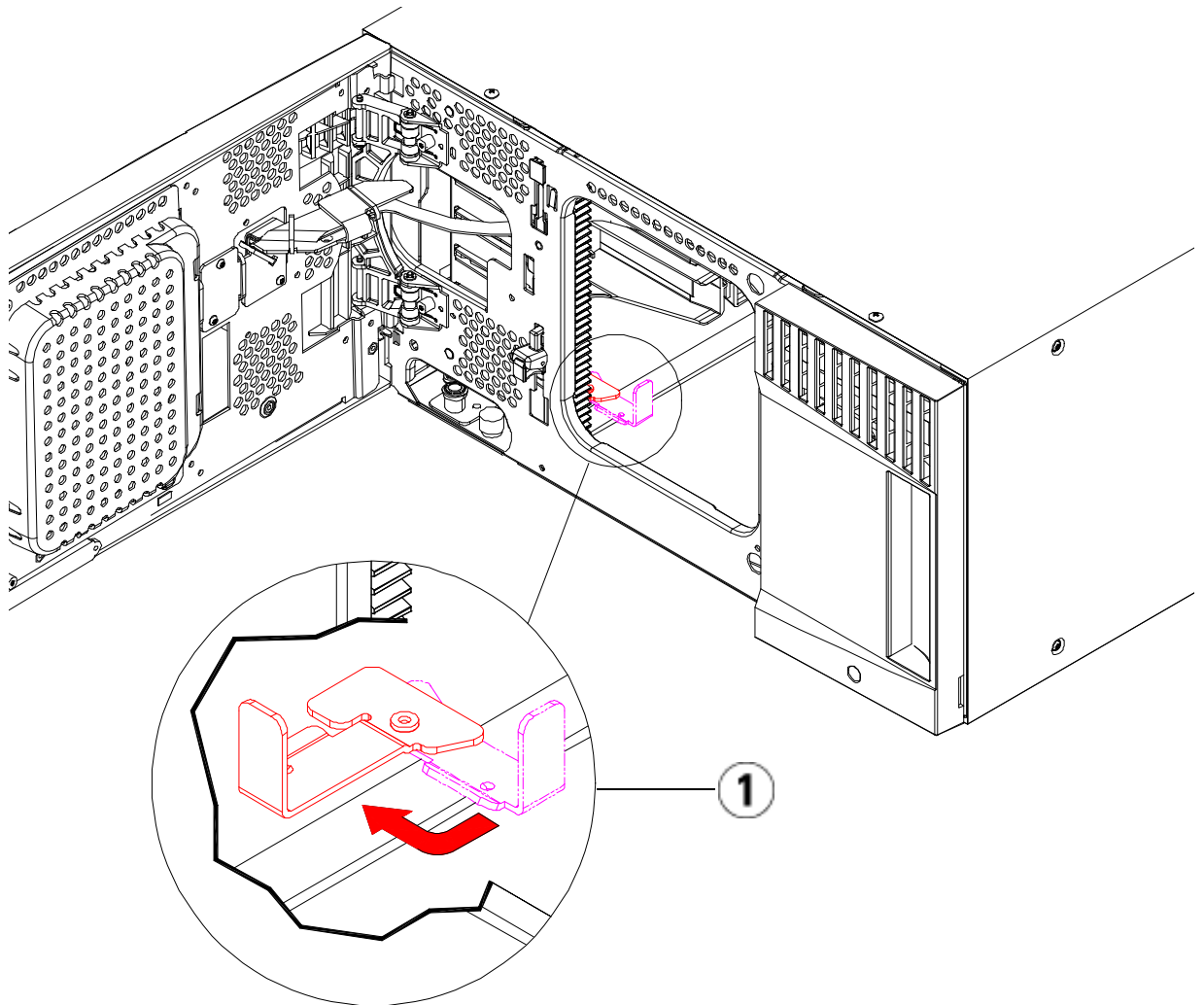
1	Parking tab in "unparked" position

**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 [Adding, Removing, and Replacing Tape Drives](#) on page 303.

3 Add the power supplies. For details, see [Adding, Removing, and Replacing Power Supplies](#) on page 281.

4 Add the LCB to the control module. For details, see [Removing and Replacing the Library Control Blade and LCB Compact Flash Card](#) on page 276.

5 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 306 and [Adding, Removing, and Replacing the I/O Fan Blade](#) on page 317.

6 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 [Cabling the Library](#) on page 172.

7 Power on the library.

8 Add the tape cartridges to the library's modules using the I/E station commands from the operator panel or web client.

9 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.

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.

The best practice before removing and replacing an expansion module is to:

- Using your I/E station, export all the tape cartridges from your library.

- Delete all partitions.

- Delete all cleaning slots.

- Set the number of I/E station slots to six.

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 163 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 58 lbs. An expansion module, without tape drives, tape cartridges, or power supplies, exceeds 65 lbs.
>
> To avoid serious injury, at least two people are required to safely lift the modules into position.

Preparing to Remove the Expansion 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

1 Power off the library.

2 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.

3 Remove all power supplies from each module that you intend to remove. For details, see Adding, Removing, and Replacing Power Supplies on page 281.

4 Remove all tape drives from each module that you intend to remove. For details, see Adding, Removing, and Replacing Tape Drives on page 303.

5 If your library 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 306 and Adding, Removing, and Replacing the I/O Fan Blade on page 317.

6 Remove the tape cartridges from each module that you intend to remove.

> **Caution:** The library will not be able to locate tapes that are removed from one partition and returned to a different partition. The tapes must be returned to the same partition they were removed from. Since the library assigns slots to a partition, you must create a map to locate each tape or create a map of tape slots that belong to each partition. You can do this by going to the **Reports > Library Configuration** screen on the web client and clicking the **Show BarCodes** button.

> **Note:** If you are unsure about which cartridge's barcode belongs in which partition, export the tape cartridges via the I/E station while keeping track of which partition they came from. Reconfigure the library and then re-import the cartridges via the I/E station into the appropriate partitions.

7 If you are removing a expansion module located below the control module, continue with the next step and substeps. If not, skip to the next section.

8 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.

   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 |

**Removing the 9U
Expansion Module**

1 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 the Expansion Module</u> above. |

2 Disengage the Y-rails so the modules can be unstacked safely.
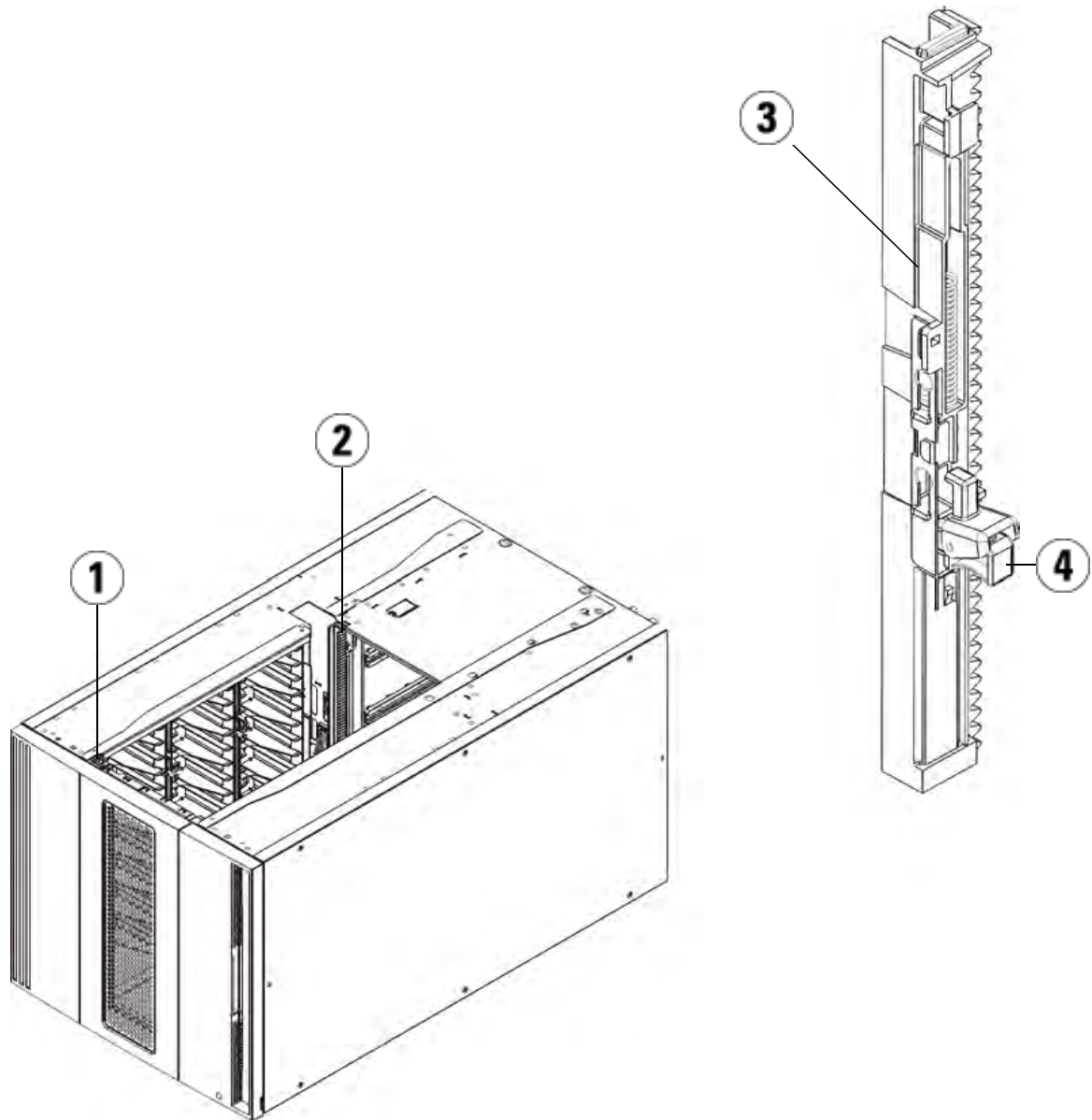
1	Front Y-rail
2	Rear Y-rail
3	Y-rail (this end up)
4	Squeeze here to release

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.
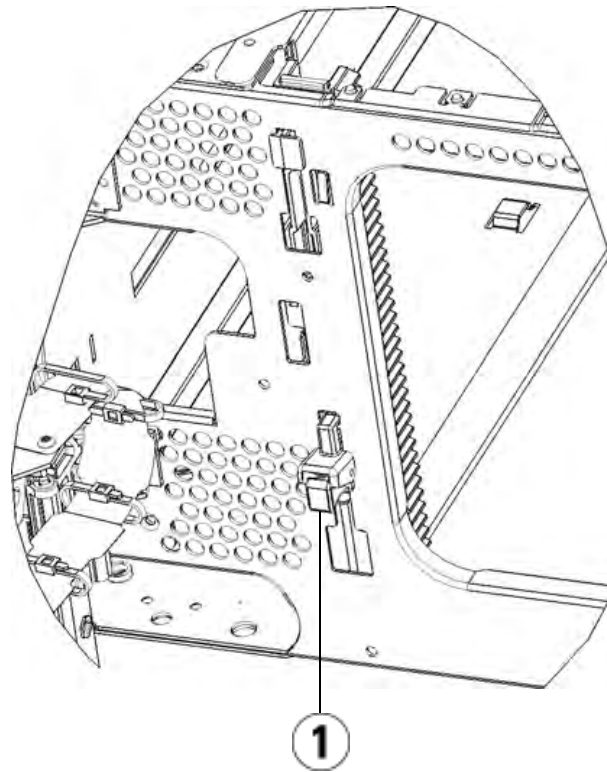
1	Y-rail in locked, non-functional position

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.

3 Remove the rack ears that fasten the module to the rack. See Installing the Library in a Rack on page 284 for detailed instructions on using the rack ears.

4 Loosen the thumbscrews located at the base of the front of the module.

| 1 | Thumbscrews (behind doors) |

5 Loosen the two thumbscrews located at the base of the back of the module.

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.

7 From the front of the library, slide the entire module toward you and lift it off of the module below it.

8 Repeat these procedures for each module that you need to remove.

9 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 Preparing to Remove the Expansion Module.

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 Adding, Removing, and Replacing Tape Drives on page 303 for instructions on removing tape drives.

2 Remove the power supplies from the expansion module that you are adding. See Adding, Removing, and Replacing Power Supplies on page 281 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.
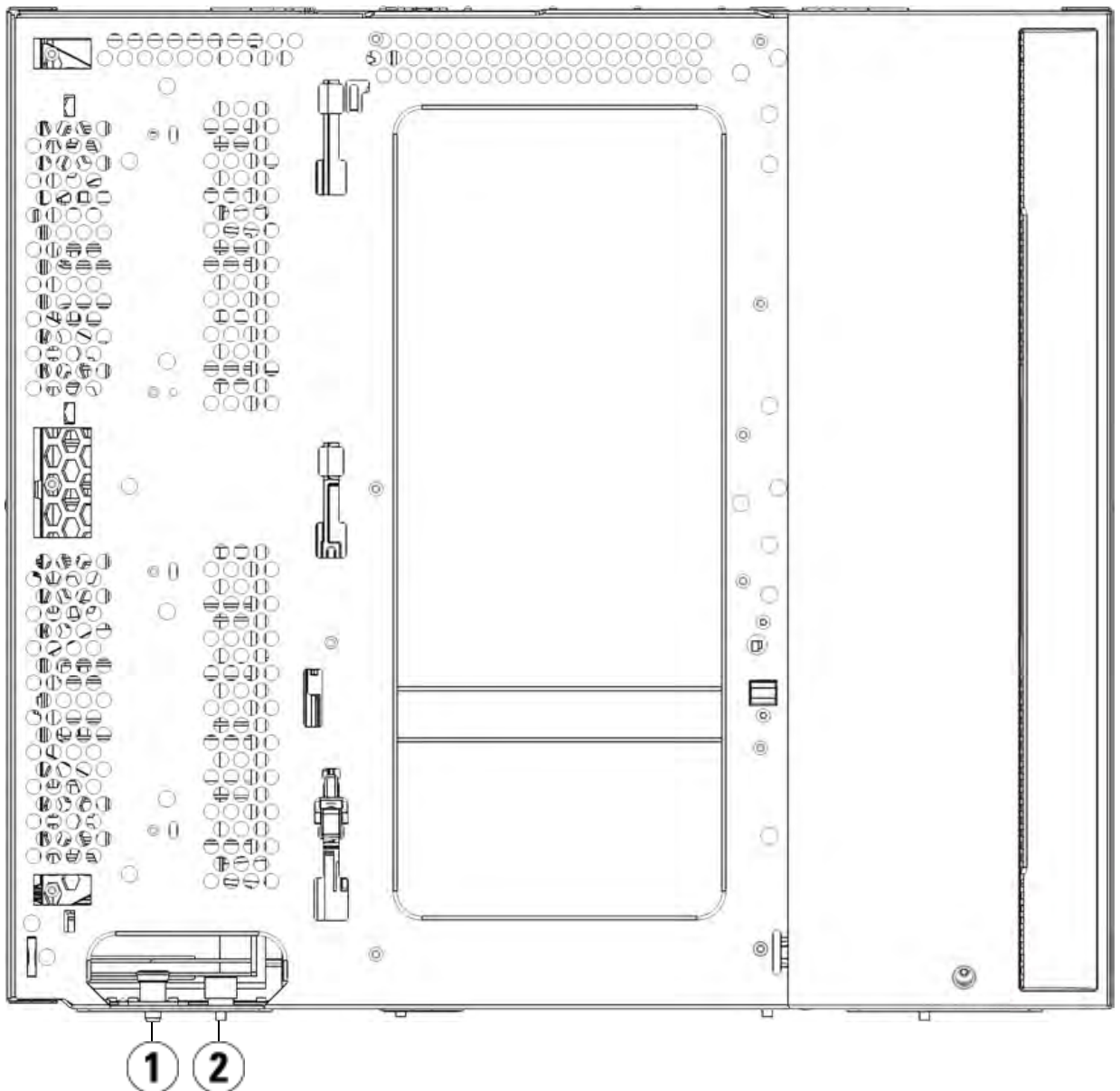
1	Guide pin
2	Thumbscrew

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.

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.
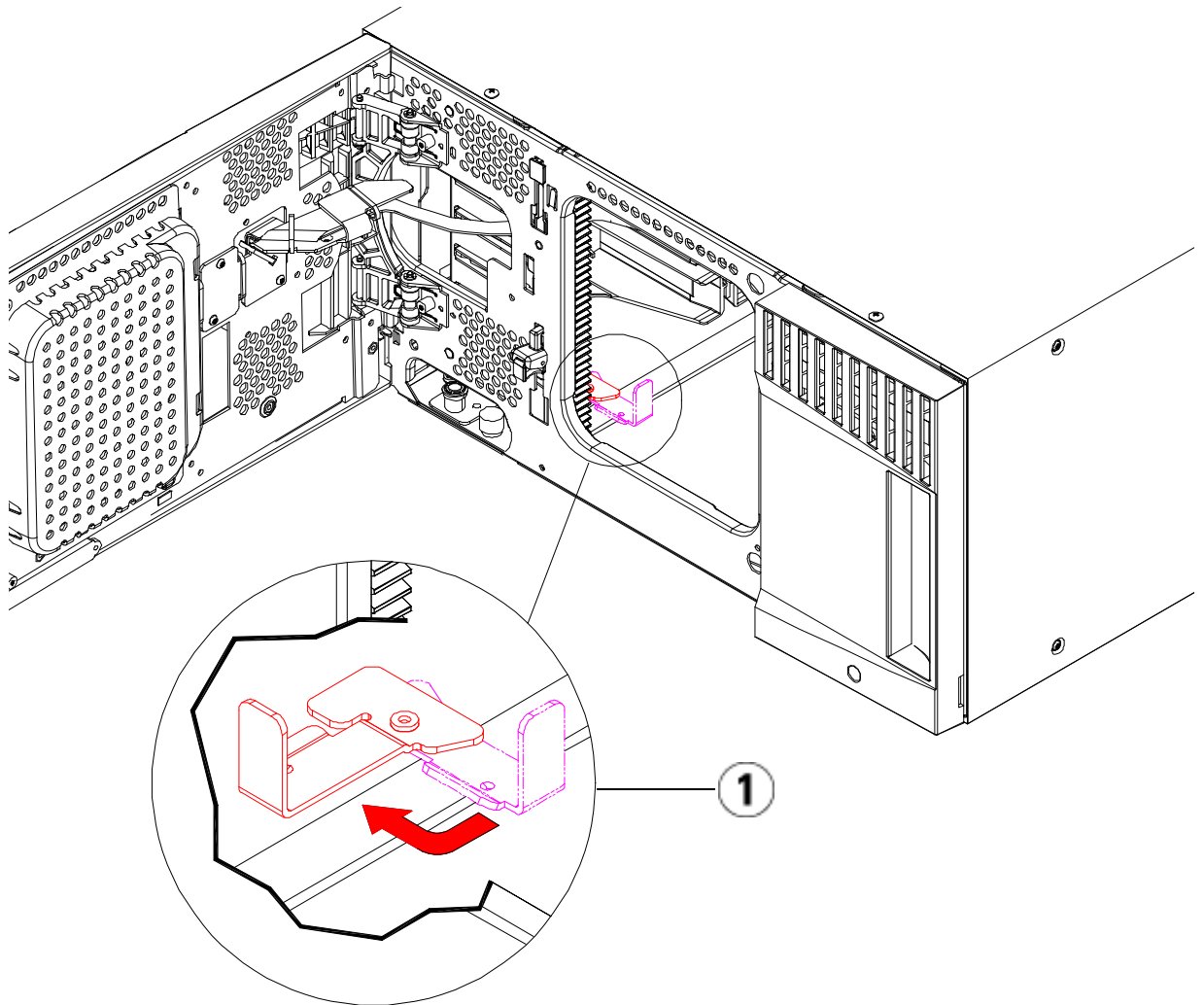
1	Parking tab in "unparked" position

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 Adding, Removing, and Replacing Tape Drives on page 303.

3 Add the power supplies. For details, see Adding, Removing, and Replacing Power Supplies on page 281.

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 306 and <u>Adding, Removing, and Replacing the I/O Fan Blade</u> on page 317.

5 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 276.

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 172.

7 Power on the library.

8 Once the console appears, use the operator panel or web client to delete and recreate all partitions.

9 Add the tape cartridges to the library's modules using the I/E station commands from the operator panel or web client.

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 picker assembly, and is responsible for running system tests to ensure that the library is functioning properly.

These instructions explain how to remove a library control blade (LCB) and replace it with a new one. 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.

Replacing the LCB and LCB Compact Flash Card

These instructions explain how to remove the existing LCB and existing LCB compact flash card and replace them with a new LCB and a new 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.
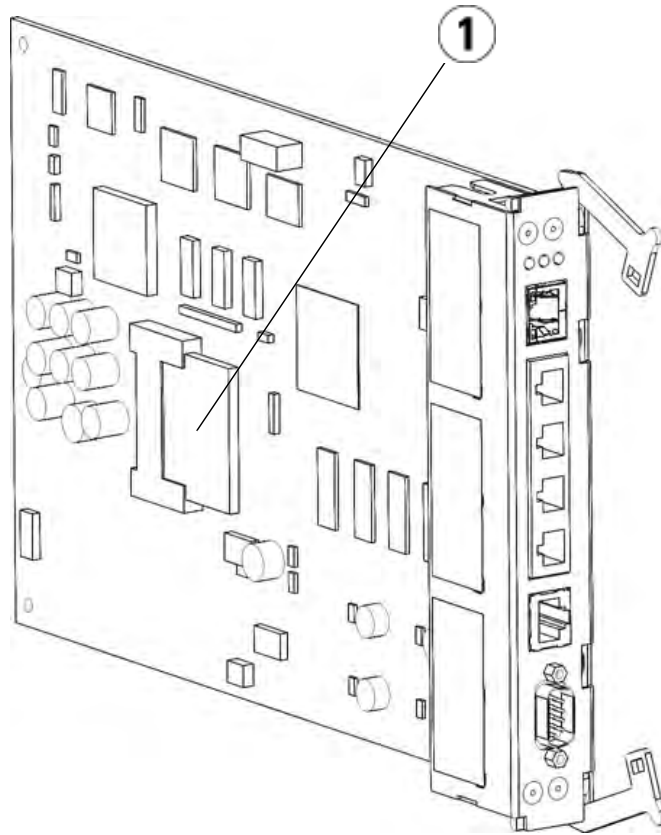
1	LCB compact flash card

6 Insert the new LCB compact flash card into the new LCB.

7 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.

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.

12 On the library's operator panel, a screen appears with instructions on how to proceed. Read the instructions and click **OK** to close the instruction screen.

13 When the login screen appears, login with user name **admin** and password **password**.

14 Complete the next few screens to configure the host name and IP address(es) for your library. You are prompted to choose whether to enable IPv6. When you are finished configuring, click **Apply**. A progress window indicates the system is processing. When the progress window indicates "success," close the progress window.

> **Note:** The system defaults to DHCP. For IPv4 only, you can deselect the DHCP option and assign a static IP address (press the filled circle to the right of "**Use DHCP:**" to deselect). You cannot assign a static IP address for IPv6.

15 The next screen lists one or more IP addresses assigned to the library. Take note of the addresses, then click **Close**. The system logs you out of the operator panel and you return to the login screen.

16 Via an Internet browser, connect to your library using one of the IP addresses assigned to the library in the previous step.

A screen appears on the web client with instructions on how to upgrade library firmware.

17 Follow the onscreen instructions to upgrade library firmware to the most recent version.

Firmware downloads are available at www.quantum.com/support.

18 Restore the library configuration (see <u>Saving and Restoring the Library Configuration</u> on page 329). If you did not save a recent configuration, you may need to manually restore your settings.

> **Note:** If your last saved configuration contained down-rev library firmware, the library will restore the down-rev firmware, overwriting the firmware you installed in <u>Step 17</u>.

Replacing the LCB While Retaining the Old Compact Flash Card

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.
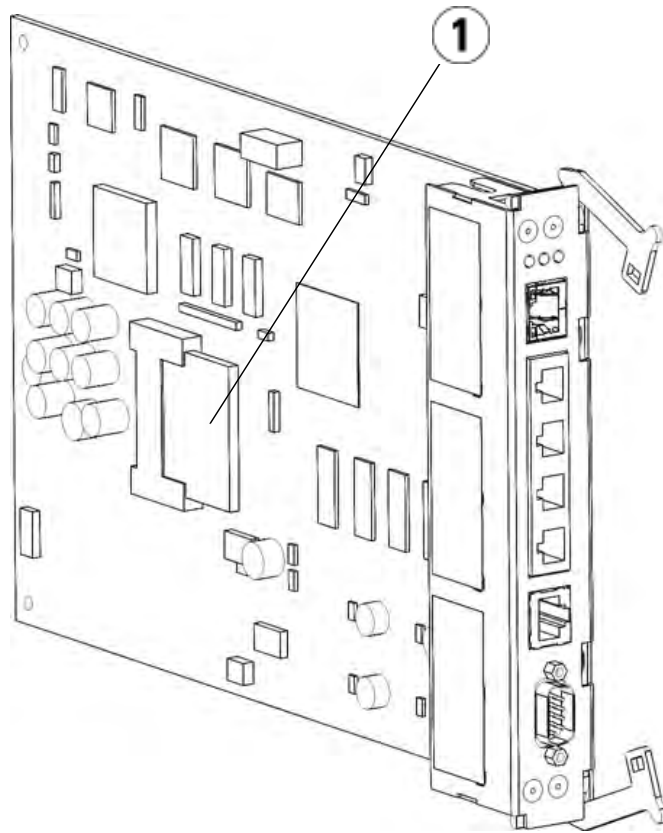
1	LCB compact flash card

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.

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 329).

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 329).

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 Saving the Library Configuration on page 329).

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:	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 58 lbs. An expansion module, without tape drives, tape cartridges, or power supplies, exceeds 65 lbs.
	To avoid serious injury, at least two people are required to safely lift the modules into position.
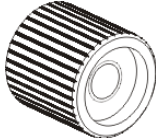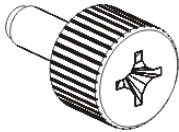
Note:	The rackmount kit cannot be used with every type of rack. Racks with threaded rails or unique hole spacing, for example, may not support the rackmount kit.
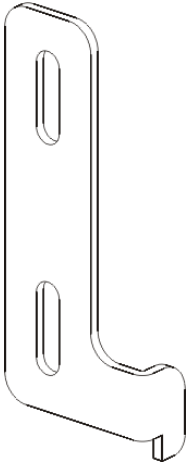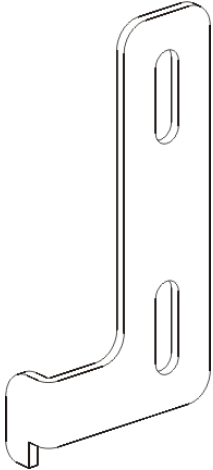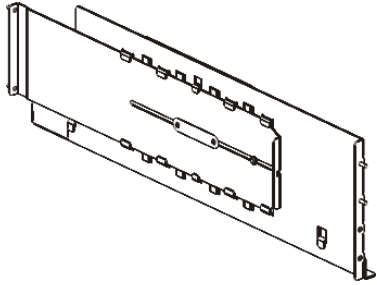
Preparing for Installation

Required tools: None

1 Before beginning installation, verify the contents of the rackmount kit (see Table 8) and the rack ear kit (see Table 9).

- 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 8   Rackmount Kit Contents

Component	Description	Quantity
	Small ferrule — Used in racks with round holes	10 (8 required; 2 spares)
	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

Component	Description	Quantity
	Rack ear, left — Holds the modules in the rack	1
	Rack ear, right — Holds the modules in the rack	1
	Rack shelf, left — Secures the modules in the rack	1
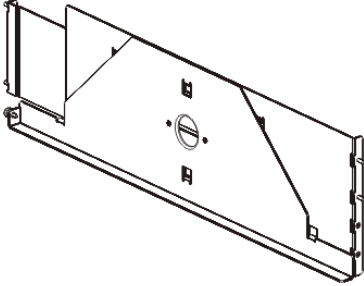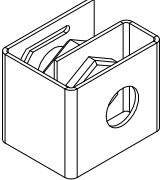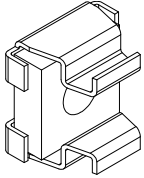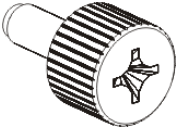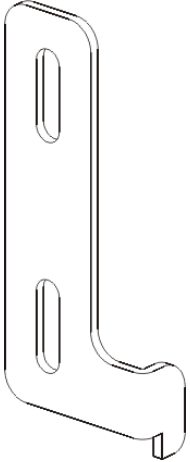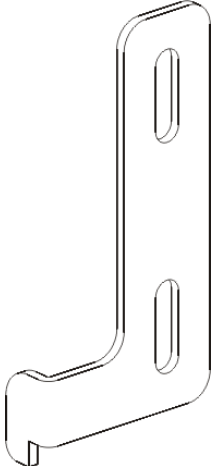
Component	Description	Quantity
	Rack shelf, right—Secures the modules in the rack	1

Table 9   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

Component	Description	Quantity Required
	Rack ear, left — Holds the modules in the rack	1
	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 Installing a New Multi-Module Library Configuration on page 203.

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 Preparing for Installation on page 285.
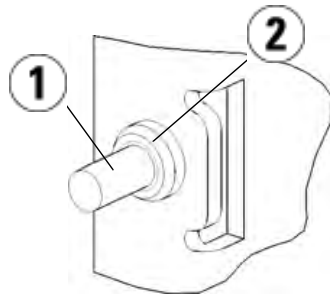
1	Stud
2	Ferrule

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.
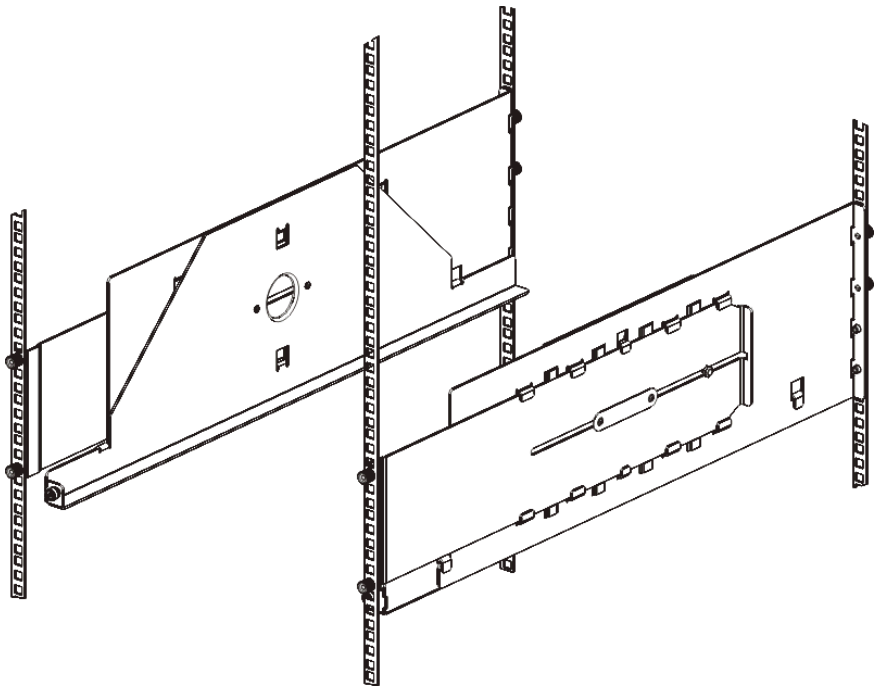
    b Position the shelf to the appropriate side of the rack (right or left) and align the shelf at the desired height.

    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.
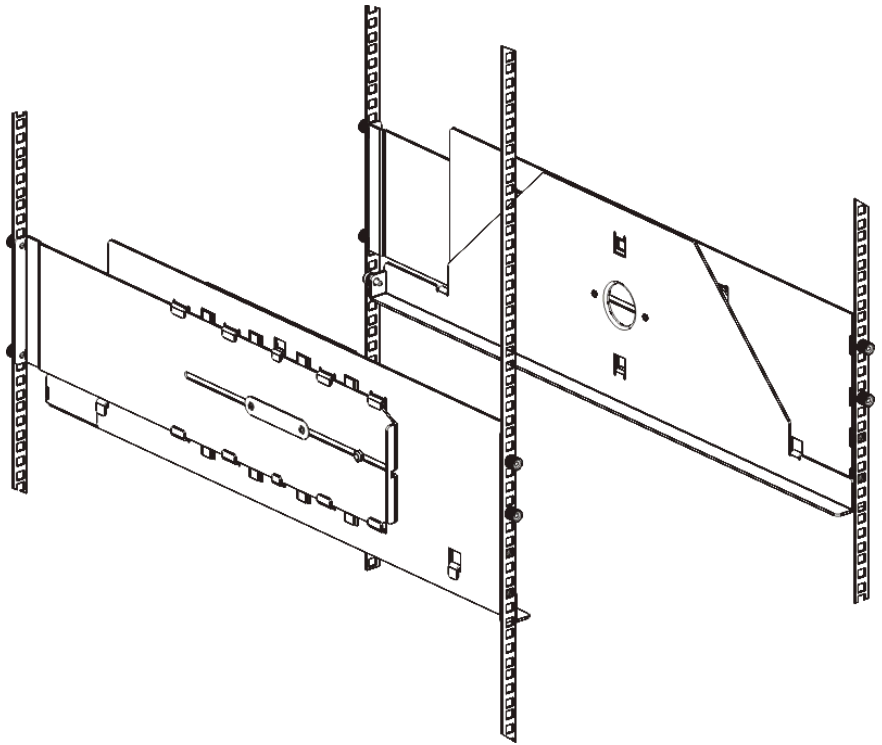
f If the studs do not reach the mounting holes, pull the front of the shelf toward you to extend it to the necessary length. Hold the base of the shelf with one hand, and pull the extensible part of the shelf with your other hand.

> **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 Your Library 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 drives 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 58 lbs. An expansion module, without tape drives, tape cartridges, or power supplies, exceeds 65 lbs.
>
> To avoid serious injury, at least two people are required to safely lift the modules into position.

3 Follow the instructions in the related sections in this chapter that explain how to install modules and libraries. These related sections contain important information on how to prepare the module safely and correctly for installing in a rack, including parking the robot in the control module and removing top and bottom covers. The appropriate sections are:

- Installing a Stand-Alone 5UControl Module on page 202
- Installing a New Multi-Module Library Configuration on page 203
- Adding Expansion Modules to an Existing Library on page 214
- Replacing the Control Module on page 247
- Replacing an Expansion Module on page 259

**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.
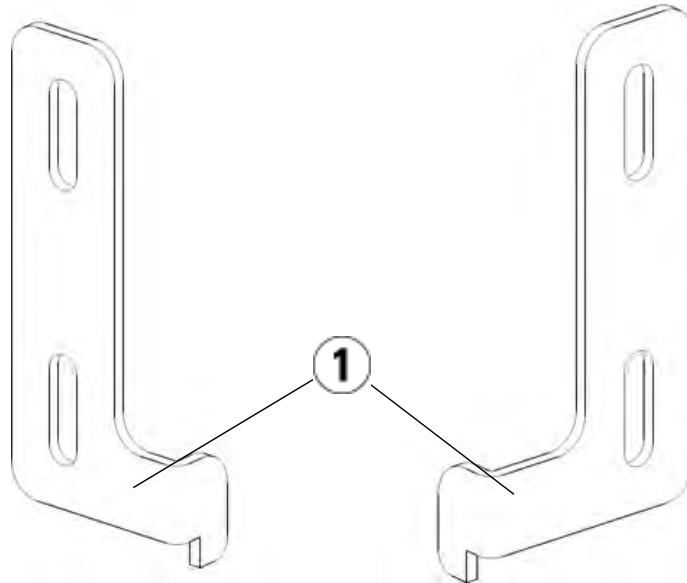
1	Hinge of rack ears

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.
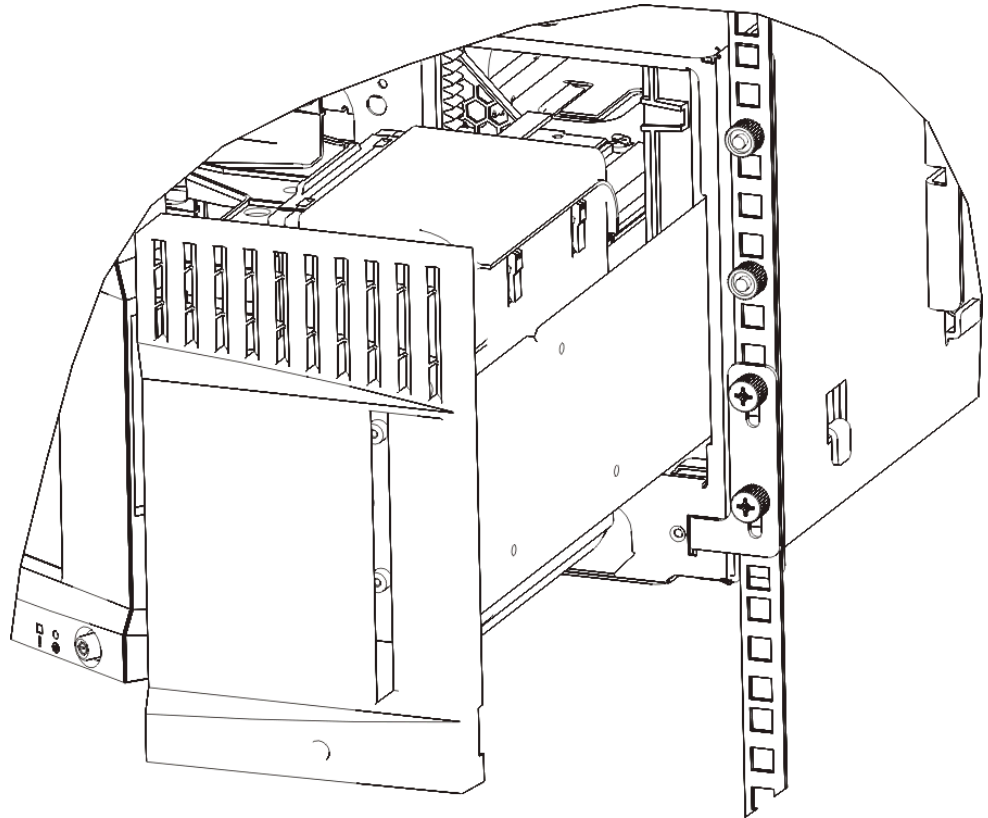
4 Install the left rack ear.

    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.
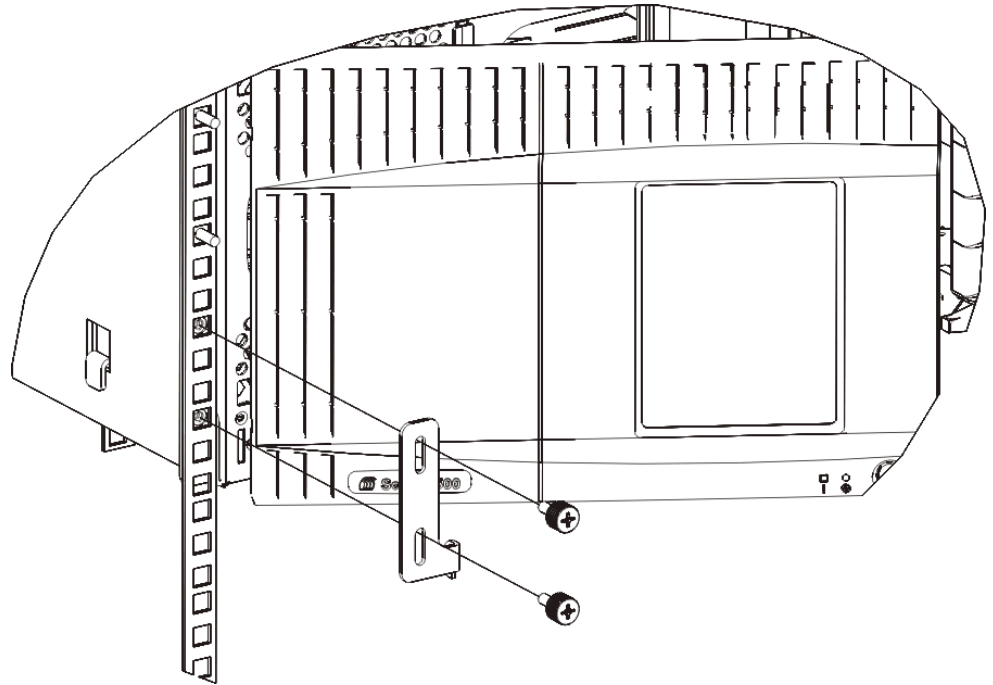
5 Close the module's doors.

6 Install the remaining modules of your library (if any), following the instructions in <u>Installing Additional Modules Into the Rack</u> on page 295.

7 Reinstall the tape drives in the library.

8 Cable your library as necessary, following the instructions provided in <u>Cabling the Library</u> on page 172.

9 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 222.

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.
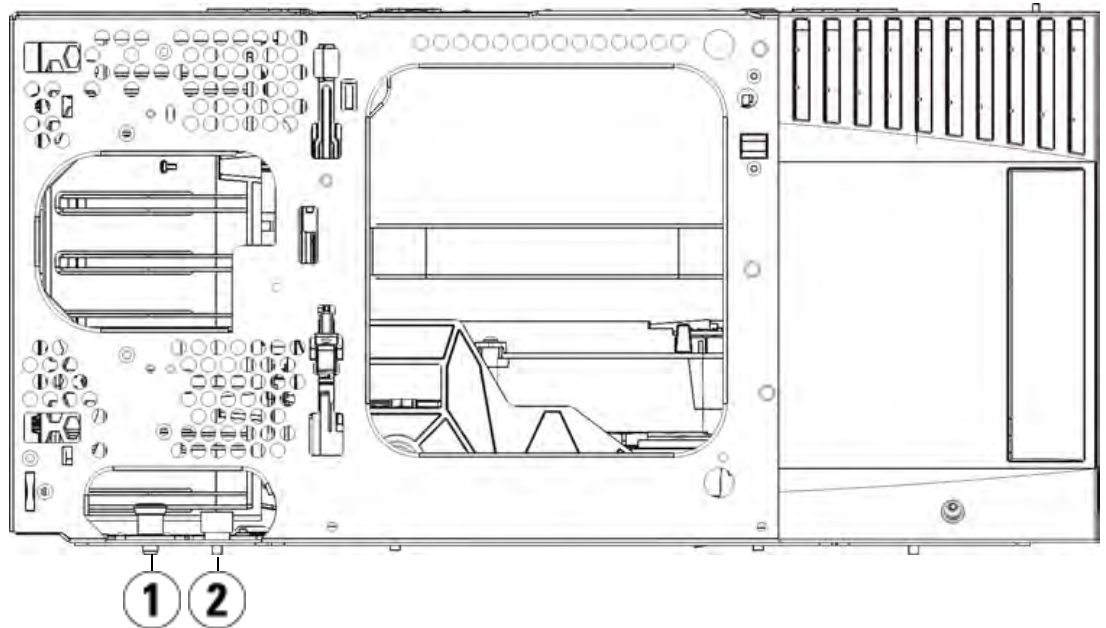
1	Guide pin
2	Thumbscrew

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.
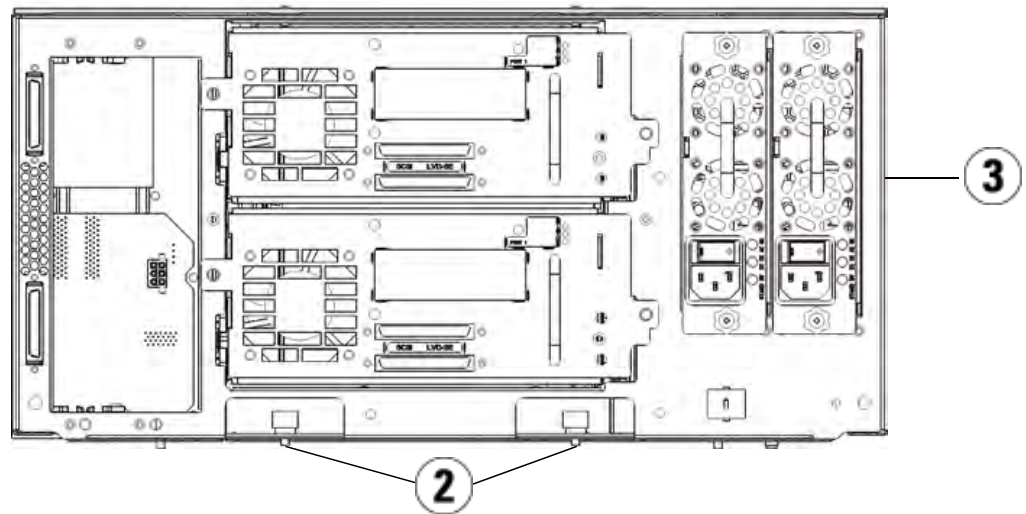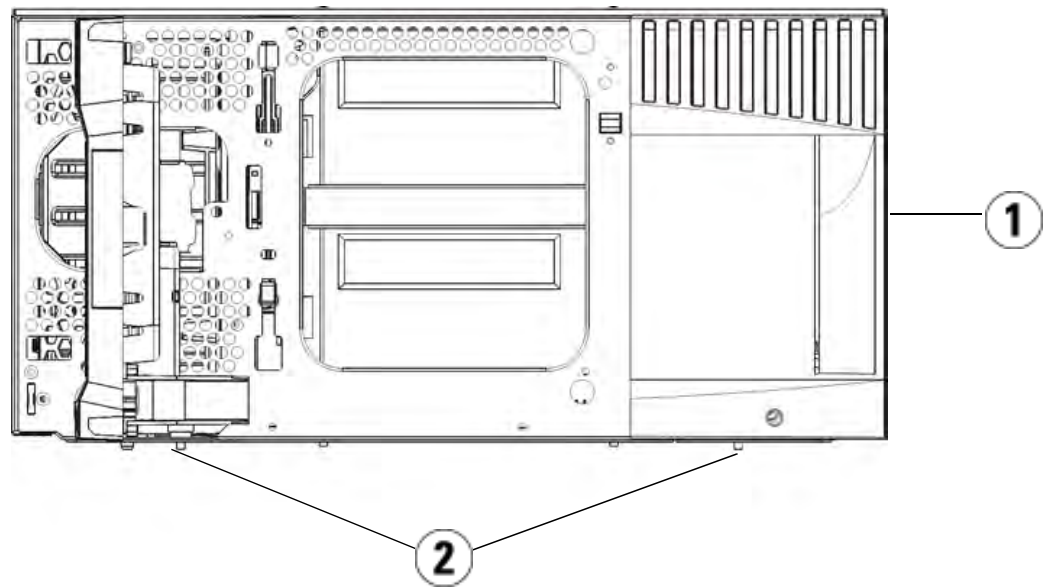
1	Control module (front)
2	Thumbscrews
3	Control module (rear)

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.
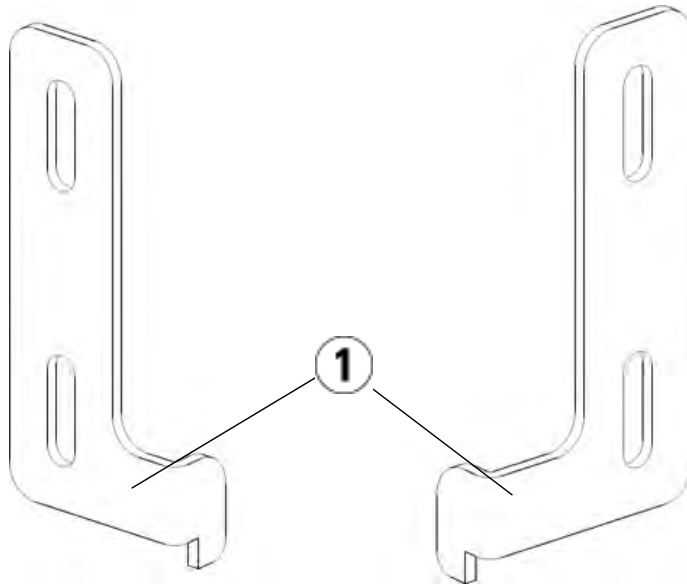
1	Hinge of rack ears

    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.
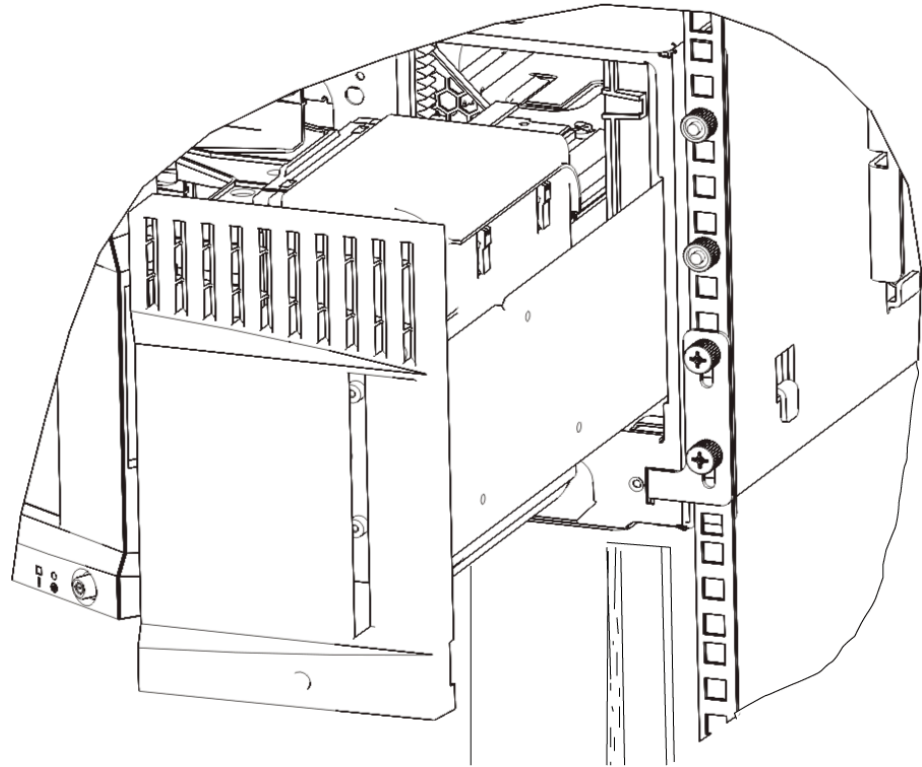
9 Install the left rack ear.

    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.
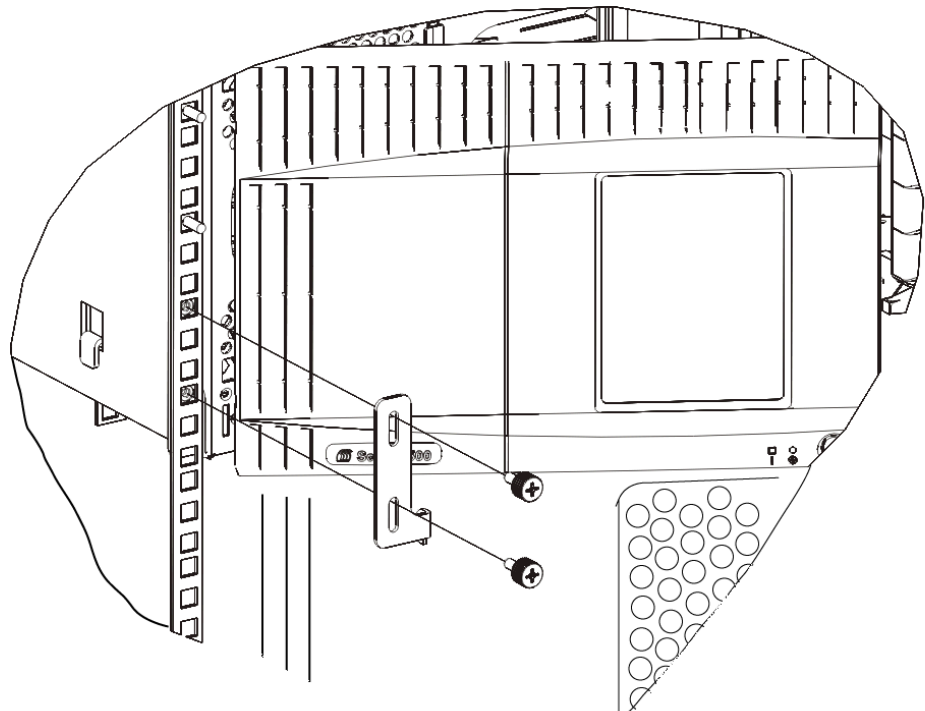
10 Close the module's doors.

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 172.

13 Power on the library.

Adding, Removing, and Replacing Tape Drives

The tape drive enables you to connect the library to servers within your storage area network (SAN).

Note:	Newly added tape drives need to be installed and verified one at a time. Alternatively, all of the tape drives can be added to the drive bays at one time with no wait time between adding tape drives.

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 <u>Saving the Library Configuration</u> on page 329).

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.

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 Check the tape drive's LEDs to make sure that the drive functions correctly.

When the UDS firmware is downloading, the green LED is solidly lit for three seconds and then blinks twice. If the blue and amber LEDs never become lit, reinstall the tape drive.

8 Connect the host interface cables to the tape drive.

9 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**.

10 If necessary, update drive firmware by following the instructions provided in <u>Updating Library and Tape Drive Firmware</u> on page 163. The library can use the drive immediately after the tape drive firmware is downloaded.

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 eject it.

4 Using the web client, delete the partitions 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 drive slot.

If you cannot find a cover plate, 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.

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.

Required tools: None

1 Prepare host applications for tape drive removal.

2 Save the library configuration.

3 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**.

4 If there is a cartridge in the tape drive, use the web client to eject it.

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 it's not powered on already).

11 Check the tape drive's LEDs to ensure that it functions correctly.

When the tape drive is downloading firmware, the green LED is solidly lit for three seconds and then blinks twice. Firmware begins to download as soon as the library detects a new tape drive. Firmware downloads may take more than 15 minutes.

If the blue and amber LEDs never become lit, reinstall the tape drive.

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 If necessary, update drive firmware by following the instructions provided in the <u>Updating Library and Tape Drive Firmware</u> on page 163. The library can use the tape drive immediately after the drive firmware is downloaded.

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, and LTO-4 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 <u>Working With Control Paths</u> on page 78. If you do not configure control paths correctly, you will experience communication problems with tape drives, partitions, and the medium changer (robot).

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 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 31</u> shows the FC I/O blade and I/O blade fan installed in the expansion module. For instructions on installing the I/O blade fan, see <u>Adding, Removing, and Replacing the I/O Fan Blade</u> on page 317.

- 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 31 FC I/O Blade and
Fan Blade Bays in Expansion
Module
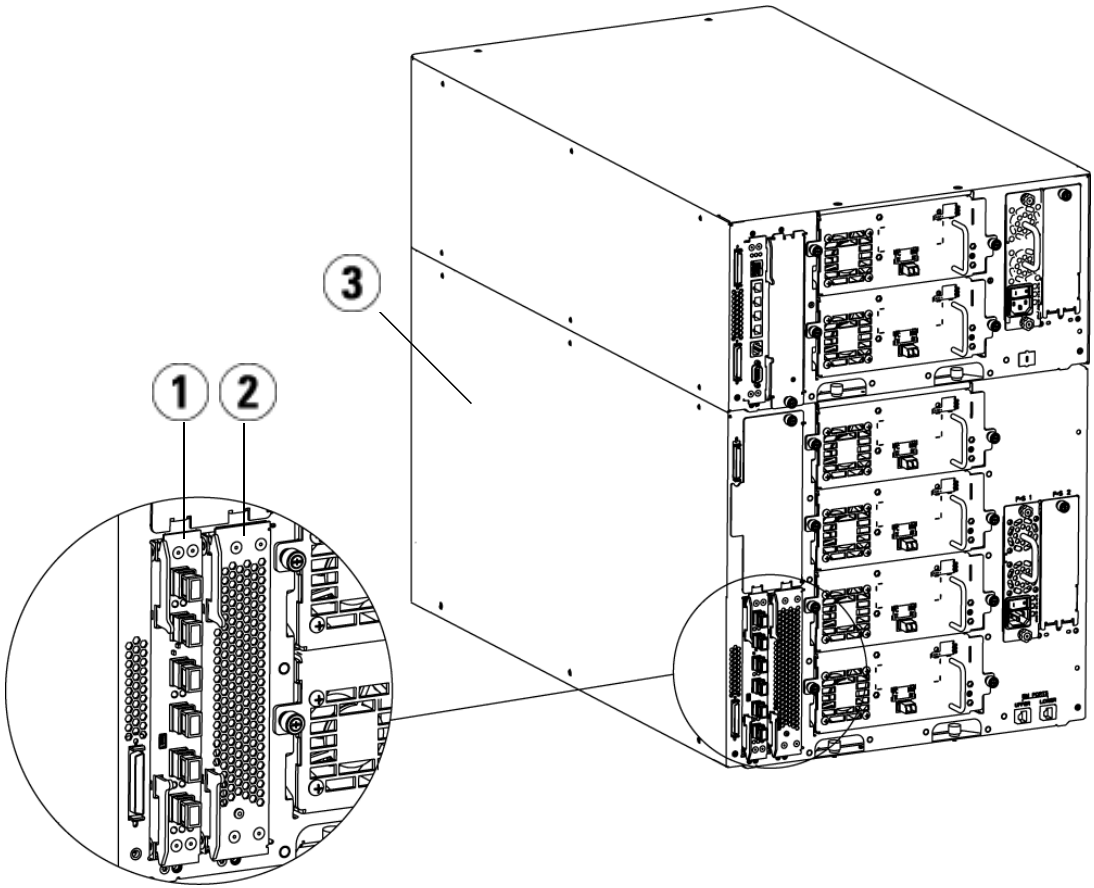
1	FC I/O blade
2	Fan blade
3	Expansion module

**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 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 78. If you do not configure control paths correctly, you will experience communication problems with tape drives, partitions, and the medium changer (robot).

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 329).

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 21 on page 183).

> **Note:** 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 Adding, Removing, and Replacing the I/O Fan Blade on page 317. 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 appropriate instructions in this sheet. 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 Figure 21 on page 183). See also Recommended Library Cabling for FC I/O Blades on page 187.

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 Working With Control Paths on page 78 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 109 and Configuring Host Mapping on page 111. To configure host mapping:

a From the operator panel or web client, select **Setup > I/O Blades > Blade Control** and enable host mapping.

b From the operator panel or web client, select **Setup > I/O Blades > Host Mapping**.

12 Configure host port failover on the FC I/O blade (optional). From the web client, select **Setup > I/O Blades > Host Port Failover**. To enable host port failover, you must configure target ports 1 and 2 on the I/O blade as point-to-point connections (**Setup > I/O Blades > Port Configuration**). For more information, see Configuring FC Host Port Failover on page 113.

13 Save the library configuration (see Saving the Library Configuration on page 329).

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 FC I/O blade bay.

3 Press up and out to open the latch hooks on each side of the FC I/O blade.
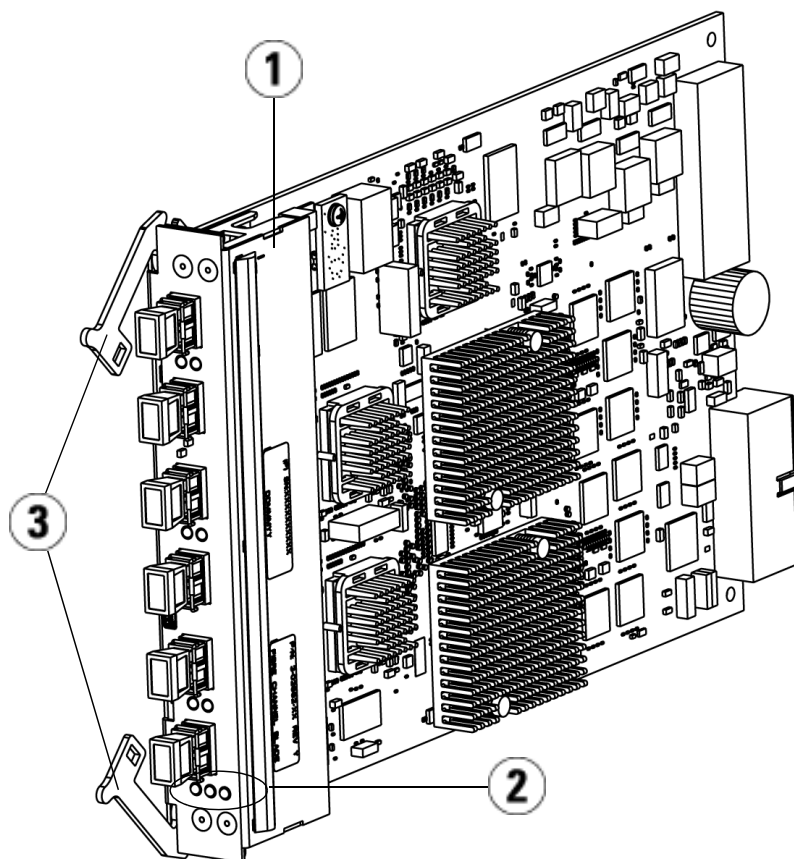
1	FC I/O blade
2	LEDs
3	Latch hooks, open

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 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 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.
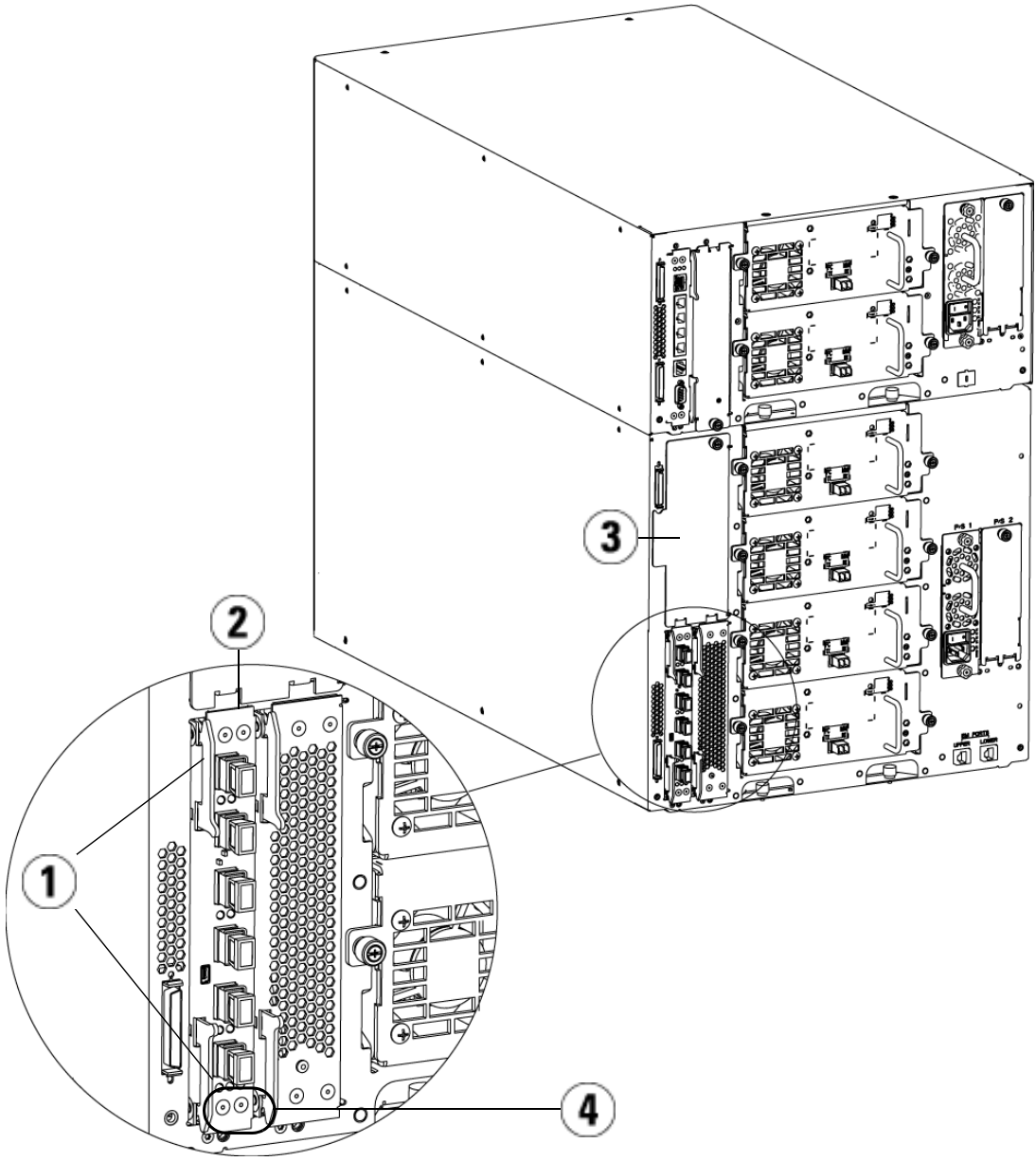
1	Latch hooks, locked
2	FC I/O blade
3	Cover plate on empty bay
4	FC I/O blade LEDs

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 Connecting Library FC Cables to FC I/O Blades on page 180.

9 Save the library configuration (see Saving the Library Configuration on page 329).

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 Controlling FC I/O Blade Power on page 144.

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 337).

8 Save the library configuration (see Saving the Library Configuration on page 329).

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 144.

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 315.

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 Saving the Library Configuration
on page 329).

> **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
> LCB and FC I/O Blade LEDs on page 340.

Adding, Removing, and Replacing the 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 31 on page 308 shows the FC I/O blade and I/O fan blade installed side-by-side in the expansion module.

Adding an I/O Fan Blade

These instructions explain how to add an I/O fan blade to your library. You can add an 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 I/O fan blade. The LED must be at the bottom of the blade.
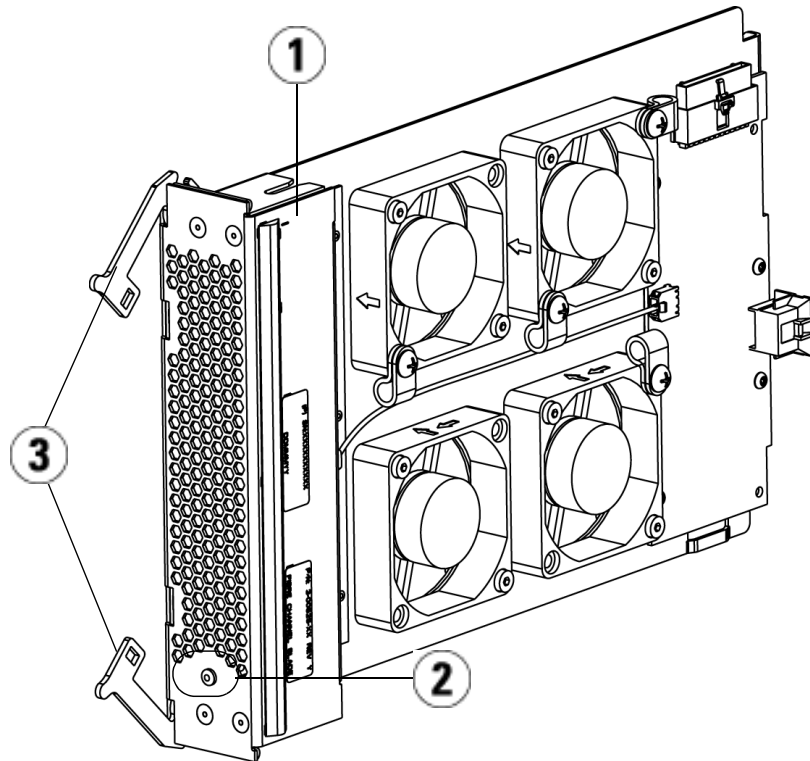
1	I/O Fan blade
2	LED
3	Latch hooks, open

> **Caution:**   Forcing the blade into the bay can cause the pins to bend.

4 Evenly apply pressure to both sides of the 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 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 Saving the Library Configuration on page 329).

Removing an I/O Fan Blade

These instructions explain how to remove an I/O fan blade from your library. You can remove an I/O fan blade while the library is powered on.

Required tools: None

1 Access the back of the expansion module containing the I/O fan blade.

2 Lift the latch hooks out of the locked position and push them up. You will feel the 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 I/O fan blade out of the expansion module.

5 If you are permanently removing the 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 329).

Replacing an FC I/O Fan Blade

These instructions explain how to replace an I/O fan blade in your library. You can remove and replace an 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 I/O Fan Blade</u> on page 319.

3 Press up and out to open the latch hooks on each side of the replacement I/O fan blade.

4 Carefully align the 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 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 329).

Preparing the Library for Moving or Shipping

Before you move or ship your library, follow these steps:

> **Caution:** When moving the library: You must install the orange robot restraint assembly to protect the robot against damage. It is recommended that you use the original shipping carton and packaging materials to further protect your library.
>
> **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.c

1 Save the library configuration (see <u>Saving the Library Configuration</u> on page 329).

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 58 lbs. An expansion module, without tape drives, tape cartridges, or power supplies, exceeds 65 lbs.
>
> To avoid serious injury, at least two people are required to safely lift the modules into position.

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*.
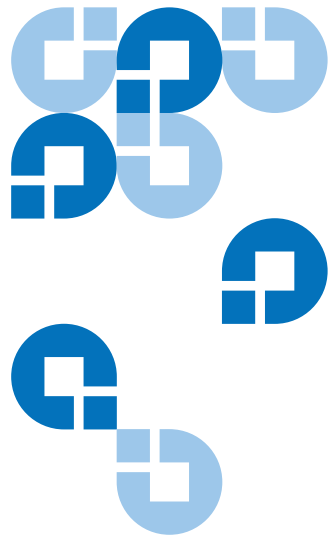
Troubleshooting

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.

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.

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.

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 web site.

The initial status of all RAS tickets is Unopened. Once the administrative user 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 RAS Tickets

Administrative users 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 web site.

> **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**.

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 Capture 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 perform the Capture Snapshot operation, so that the library can send Capture Snapshot files to the recipient. 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 88.

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 name (WWN) loop ID, topology, speed, and actual speed.

> **Note:** If the FC tape drive is attached to an FC I/O blade, the WWN indicates the WWN of the I/O blade, not the tape drive.

- 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, WWN, 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

Administrative users can use the **Tools - Email 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 - Email 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

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 > Email Configuration Record**.

Saving the Configuration Record

Administrative users 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 configurable items to a previous state.

Note:	The Saving and Restoring operations should not be performed concurrently by multiple administrative users logged in from different locations. You can access the screens, but you cannot apply changes while another administrative user 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.

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 [Viewing RAS Tickets](#) on page 324 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 Configuring FC I/O Blade Channel Zoning on page 105).

- 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 Configuring Host Mapping on page 111).

Duplicate Medium Changers Discovered

You may see one or more medium changers being discovered multiple times. For information on why this happens, see FC I/O Blade Internal Virtual Port for Medium Changers on page 104.

To prevent this, do the following:

- Ensure that host mapping is enabled (see Enabling/Disabling FC Host Mapping on page 107).

- Assign each medium changer a unique LUN and map each one to the appropriate host (see Configuring Host Mapping on page 111).

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

Administrative users 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.

- 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

Administrative users 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

Administrative users 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 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. Administrative users can perform this operation by selecting the FC I/O blade and performing the remove blade operation on the **Setup - 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 306.

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 336.

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

The paths to open the appropriate screens are as follows:

- From the web client, select **Setup > IO Blades > Blade Control**.

- From the operator panel, select **Setup > IO Blades > Blade Control > Remove Blade**.

Resetting FC I/O Blade Ports

Administrative users 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 administrative users logged in from different locations. You can access the appropriate screens, but you cannot apply changes while another administrative user is performing the same operation.

> **Note:**   Before resetting FC I/O blade ports, verify the location of the FC I/O blade. See Identifying FC I/O Blades on page 336.

The paths to open the appropriate screens are as follows:

- From the web client, select **Setup > IO Blades > Blade Control**.

- From the operator panel, select **Setup > IO Blades > Blade Control > Reset Port**.

Viewing and E-Mailing the Command History Logs

When FC I/O blades are installed, administrative users 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 Configuring the Library E-mail Account on page 88 in Configuring Your Library.

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

- Tape drives

- Power supplies

Some of these components may also include a fibre port link LED.

LCB and FC I/O Blade LEDs

LCB and FC I/O blade 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 10 to interpret the current status of the LCB and FC I/O blade LEDs.

Table 10   LED Color and Blade
Status

LED Color	Represents	Blade Status
Green	Library Application Code status	• Solid on/solid off — Library application code not operating. • Solid on for 3 seconds, then blinks twice — Blade firmware is downloading. • 1 blink per second — Normal: Library application code operating. • 10 blinks per second — Identify mode (per user request, to distinguish it from other blades).
Amber	Health status	• Solid on — Booting up or compact flash memory problems. • 1 blink per second — Library application code not operating. • Solid off — Normal: Blade operational.
Blue	Power Control status	• Solid on — Swap mode: Ready to be removed or replaced. • 1 blink per 10 seconds — Normal: Blade on. • Solid off — Blade not receiving power.

Amber LED on the LCB and FC I/O Blade

Under normal operating conditions, the amber LED on the blade is not lit. If you see that the amber LED on an LCB or FC I/O blade is either blinking continuously or solidly lit for at least 10 minutes, service the blade as soon as possible. The library may or may not generate RAS tickets, depending on the source of the problem.

> **Caution:**   Never remove an LCB when its amber LED is solidly lit, unless it has been solidly lit for at least 10 minutes.

Table 11 indicates the actions you can take, based on the condition of the amber LED.

Table 11   Amber LED Actions

State of Amber LED	Suggested Service Action
Solid on for 10+ minutes	Replace the LCB.
1 blink per second	Check the firmware for the LCB and make sure that you have the most current firmware available.
	Do not replace the LCB. It is unlikely that the LCB hardware is the source of the problem.

Ethernet Hub Port LEDs on the LCB

The LED for an Ethernet hub port is located above the port. Use table 12 to interpret Ethernet hub link activity on an LCB.

Table 12   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.

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.

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 to interpret Fibre Channel link activity on an FC I/O blade.

Table 13   Fibre Port Link LED on FC I/O Blade

LED Color	Represents	Fibre Port Link Status
Green	Link and activity	• Off – no link or link with constant activity* • Solid On – link or blade is booting • Flashing – link with activity

* 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.

FC I/O Fan Blade LED

RAS tickets typically report problems related to fan blades. Use to interpret fan blade activity.

Table 14   Fan Blade Status

LED Color	Represents	Fibre Port Link Status
Amber	Health of the fan blade	• Solid off — The fan blade is operating normally. • Solid on — 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.

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 32 shows where the tape drive LEDs and the fibre port link LED are located.

Figure 32 Location of Tape Drive LEDs
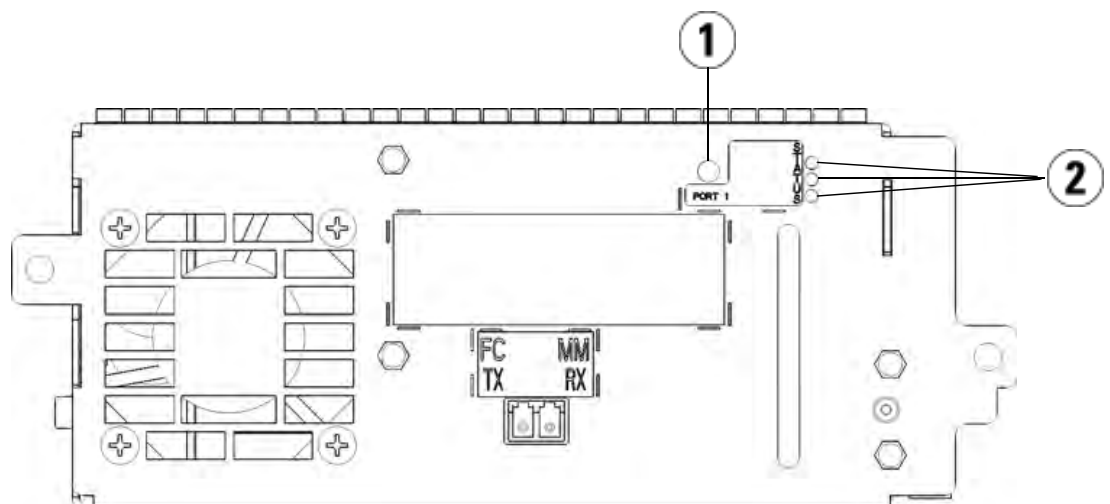
1	Fibre Port LED
2	Tape Drive LEDs

Use table 15 to interpret tape drive activity:

Table 15   Tape Drive Activity

LED Color	Represents	Tape Drive Status
Green	Processor activity	• Solid on/solid off— Tape drive's main processor is not operating. • 1 blink per second — Normal operation. • 2 quick blinks within 1.25 seconds; then on solid for 1.25 seconds; repeat — Tape drive sled firmware is downloading. • 3 quick blinks within 1.25 seconds; then off for 1.25 seconds; repeat — Tape drive is activating. • 10 blinks in 1.25 second; then off for 1.25 seconds; repeat — Tape drive firmware is downloading. • 10 blinks per second — Identify mode.
Amber	Health of the tape drive	• Solid on — Drive has failed. • Solid off — Normal.
Blue	Power control status	• Solid on — Swap mode: Ready to be removed or replaced. • 1 blink per 10 seconds — Normal: Drive operational. • Solid off — Drive is not receiving power.

Fibre Port Link LED on Tape Drives

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 16 to interpret FC link activity:

Table 16   Fibre Port Link Status

LED Color	Represents	Fibre Port Link Status
Green	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 17 to interpret power supply activity.

Table 17   Power Supply Status

LED Color	Represents	Power Supply Status
Green	AC OK (top)	• 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	DC OK (middle)	• Solid on — The power supply's output voltage is within regulation. • Solid off — The power supply's output voltage is not within regulation.
Blue	Standby (bottom)	• Solid on — Swap mode: Ready to be removed or replaced. • Solid off — Normal.

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

Administrative users may 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 IE** 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

Administrative users 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 IE** 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:

- Q-EKM Path Diagnostics on page 353
- Drives Diagnostics on page 355
- Robotics Diagnostics on page 357

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 355). The path to open the appropriate screen is as follows:

- From the web client, select **Tools > Diagnostics**.

Q-EKM Path Diagnostics

The Q-EKM Path Diagnostics consists of a series of tests between a selected tape drive and the primary and secondary Q-EKM servers. It is a good idea to test each tape drive that communicates with Q-EKM servers.

Run this test any time you change the Q-EKM server settings or library encryption settings.

The diagnostics consists of the following tests:

- **Ping —** Verifies the Ethernet communication between the library and the Q-EKM servers.

- **Drive —** Verifies the tape drive's path in the library (communication from library to tape drive sled and from tape drive sled to tape drive).

- **Path —** Verifies that Q-EKM services are running on the Q-EKM servers.

- **Config —** Verifies that the Q-EKM servers are capable of serving encryption keys to the selected tape drive.

To perform the diagnostics:

1 Access the Q-EKM Path Diagnostics screen in one of two ways:

- Enter library Diagnostics (select **Tools > Diagnostics**) and then select **Q-EKM > Q-EKM Path Diagnostics**. Note that entering Diagnostics will log off all other users of the same or lower privileges and take your partitions offline. See [Library Diagnostics] on page 352 for more information.

- Select **Setup > Encryption > System Configuration** and click the link that says "Click here to run Q-EKM Path Diagnostics."

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.

2 Select the tape drive on which you want to perform diagnostics and click **Apply**.

A dialog box appears telling you that the selected partition will be taken offline.

3 Click **OK** to start the diagnostics.

The Progress Window appears. The Progress Window contains information on the action, elapsed time, and status of the requested operation.

4 The library performs the diagnostics and reports pass/fail results on each of the tests in the Progress Window.

> **Note:** The diagnostics tests may take several minutes to complete.

5 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 Q-EKM server host is running and accessible from the network the library is on.

- **Drive Test Failure —** Look for any tape drive RAS tickets and follow the resolution instructions in the ticket.

- **Path Test Failure —** Verify that the Q-EKM server is actually running and that the port/SSL settings match the library configuration settings.

- **Config Test Failure —** Verify that the Q-EKM server is set up to accept the tape drive you are testing.

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 able to be performed. Follow the instructions listed in the Progress Window to resolve any issues that occurred during the operation.

Drives Diagnostics

Drive diagnostics are separated into two categories:

- Drive Tests — Tests any tape drive and does not require you to use a scratch tape.

- Media Tests — Tests only IBM tape drives and requires you to insert a scratch tape in the top I/E station slot to perform the test.

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 administrative users. You can access the screen, but you cannot apply changes while another administrative user 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.

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**.

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**.
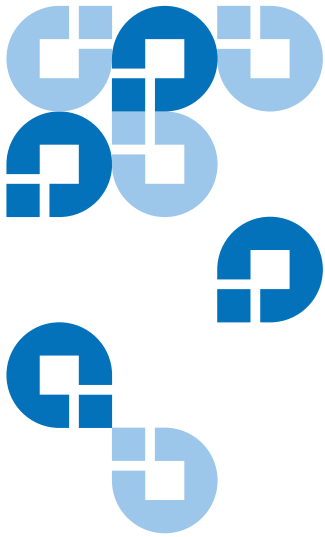
Working With Cartridges and Barcodes

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 section discusses these types of items in general terms. See Library Specifications on page 363 for information on what type of tape cartridges are supported for each drive type.

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.

- Do not stack cartridges more than five high.

- The operating temperature range for Linear Tape Open (LTO) cartridges is 10º to 45ºC. The storage temperature range is 16º to 32ºC in a dust-free environment with a relative humidity range between 20% and 80% (noncondensing).

- If cartridges have been exposed to temperatures outside the ranges specified above, stabilize the cartridges at room temperature for the same amount of time they were exposed to extreme temperatures or 24 hours, whichever is less.

- Do not place cartridges near sources of electromagnetic energy or strong magnetic fields, such as computer monitors, electric motors, speakers, or x-ray equipment. Exposure to electromagnetic energy or magnetic fields can destroy data and the embedded servo code written on the media by the cartridge manufacturer, rendering the cartridges unusable.

- Place identification labels only in the designated slots on the cartridges.

- If you ship cartridges, ship them in their original packaging or something stronger.

- Do not insert damaged cartridges into 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 Requirements

Cartridges must have an external barcode label that is machine and operator-readable. A barcode must use only uppercase letters A to Z and/or numeric values 0 to 9. The library supports Code 39 (3 of 9) type barcodes.

The supported tape cartridge barcode formats are as follows:

- Standard Six — Six character barcode number with or without a one or two-character media ID, for example, "XXXXXXL4" or "XXXXXX". Only the six character barcode is reported to the host.

- Plus Six — Six character barcode number followed by a media ID, for example, "XXXXXXL3". Six character barcode and media ID are reported to the host.

- Extended — Five to 16 characters total, including a barcode number and optional media ID. All characters are reported to the host, regardless of 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, "XXXXXXXXXXXXXXL2". If a media ID is not included, the label must have a five to 16 character barcode, for example, "XXXXXXXXXXXXXXXX".

- Media ID Last — Five to 14 character barcode number followed by media ID, for example, "XXXXXXXXXXXXXXLT". The media ID is reported to the host last.

- Media ID First — Five to 14 character barcode number followed by media ID, for example, "XXXXXXXXXXXXXXL4". The media ID is reported to the host first.

- Standard — (default) Five to 16 characters total, including a barcode number and optional media ID. The media ID is not reported to the host. If a media ID is included, the label must have a five to 14 character barcode followed by a media ID, for example, "XXXXXXXXXXXXXXL3". If a media ID is not included, the label must have a five to 16 character barcode, for example, "XXXXXXXXXXXXXXXX".

Quantum-supplied barcode labels provide the best results. Barcode labels from other sources can be used, but they must meet the following requirements:

- ANSI MH10.8M-1983 Standard

- Number of digits: 5 to 16 (default for LTO is 6+2)

- Background reflection: greater than 25 percent

- Print contrast: greater than 75 percent

- Ratio: greater than 2.2

- Module: minimum .254 mm (10 mil)

- Print tolerance: ± 57 mm

Additional Requirements:

- Length of the rest zones: 5.25 mm ± 0.25 mm

- No black marks should be present in the intermediate spaces or rest zones

- No white areas should be present on the bars

Installing Barcode Labels

Each cartridge in the library must have an external label that is machine and operator-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. Verify that the label is oriented so that the numbers appear above the barcode. 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.

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; supports write-once, read-many (WORM) functionality)
	• LTO-4 (read/write in LTO-4 drives; supports WORM functionality)
Supported Drive Types	• IBM Ultrium 2 (SCSI and Fibre Channel)
	• RoHS-compliant IBM Ultrium 3 (SCSI and Fibre Channel)
	• RoHS-compliant HP LTO-4 (Fibre Channel and SAS)
	• RoHS-compliant IBM Ultrium 4 (SCSI, Fibre Channel, and SAS)

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

System Requirements

The Scalar i500 web client interface supports the following browsers:

- Firefox, version 1.0.6 and above
- Microsoft® Internet Explorer™ version 6.0 and above

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 131.

Table 18   Library Capacity

	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 Specifications

The environmental specifications of 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**	**Shipping & Storage**
Altitude	3,048 m (10,000 ft.)	3,048 m (10,000 ft.)	3,048 m (10,000 ft.)
Temperature	50º – 100º F* (10º – 38º C)	50º – 113º F* (10º – 45º C)	-40º – 150º F* (-40º – 65º C)
Relative Humidity	20 – 80%, non-condensing	10 – 90%, non-condensing	0 – 95%, non-condensing

Dimensions

The physical dimensions of the library are listed below in inches (in).

Library Configuration	Rack Height	Maximum Physical Height (in)
5U control module	5U	8.61
5U control module + (1) 9U expansion module	14U	24.36
5U control module + (2) 9U expansion modules	23U	40.11
5U control module + (3) 9U expansion modules	32U	55.86
5U control module + (4) 9U expansion modules	41U	71.86

Component Weights

The weight of the library hardware components is listed below in pounds (lbs).

Component	Weight (lbs)
Drive Sled	9.0
Power Supply	4.0
Robot	2.5
5U Chassis (empty)	47.5
9U Chassis (empty)	65.0
5U Package Kit	approx. 20
9U Package Kit	approx. 24
14U Package Kit	approx. 40

Library Power Consumption and Heat Output

The typical library power consumption (Watts) and heat output (BTU/hr) is listed below. <u>Figure 33</u> on page 370 on page 281 shows the typical and maximum library power consumption (Watts) and heat output (BTU/hr), and <u>Figure 34</u> on page 371 shows the library typical and maximum power draw. t

> **Note:** "Typical" values for tape drives assumes tape drives are writing.

Library Configuration	Typical Power Consumption (Watts)	Typical Heat Output (BTU/Hour)
Subassembly Power Consumption:		
Scalar I500 Library with Robot and LCB (no tape drives installed; robot moving; LCB installed)	79	269
UDS3 IBM Ultrium 2 Drive Sled Module (SCSI)	29	99
UDS3 IBM Ultrium 2 Drive Sled Module (Fibre Channel)	32	109
UDS3 IBM Ultrium 3 Drive Sled Module (SCSI)	27	92
UDS3 IBM Ultrium 3 Drive Sled Module (Fibre Channel)	29	97
UDS3 IBM Ultrium 4 Drive Sled Module (SCSI)	40	135
UDS3 IBM Ultrium 4 Drive Sled Module (Fibre Channel)	42	143
UDS3 IBM Ultrium 4 Drive Sled Module (SAS)	43	148
UDS3 HP LTO-4 Drive Sled Module (Fibre Channel)	40	135
UDS3 HP LTO-4 Drive Sled Module (SAS)	37	127
Fibre-Channel I/O Blade	36	123
Control Module:		
Minimum (no drives installed; robot not moving)	47	160
Maximum (2 drives writing; robot moving)	166	565
Expansion Module:		
Minimum (no drives installed; robot not moving)	12	41
Maximum (4 drives writing; 2 Fibre-Channel I/O blades installed; robot moving)	256	879

Figure 33 Library Power
Consumption and Heat Output

Power
Consumption
(Watts)

Heat
Output
(BTU/hr)

Number of Drives

Typical Power

Maximum Power
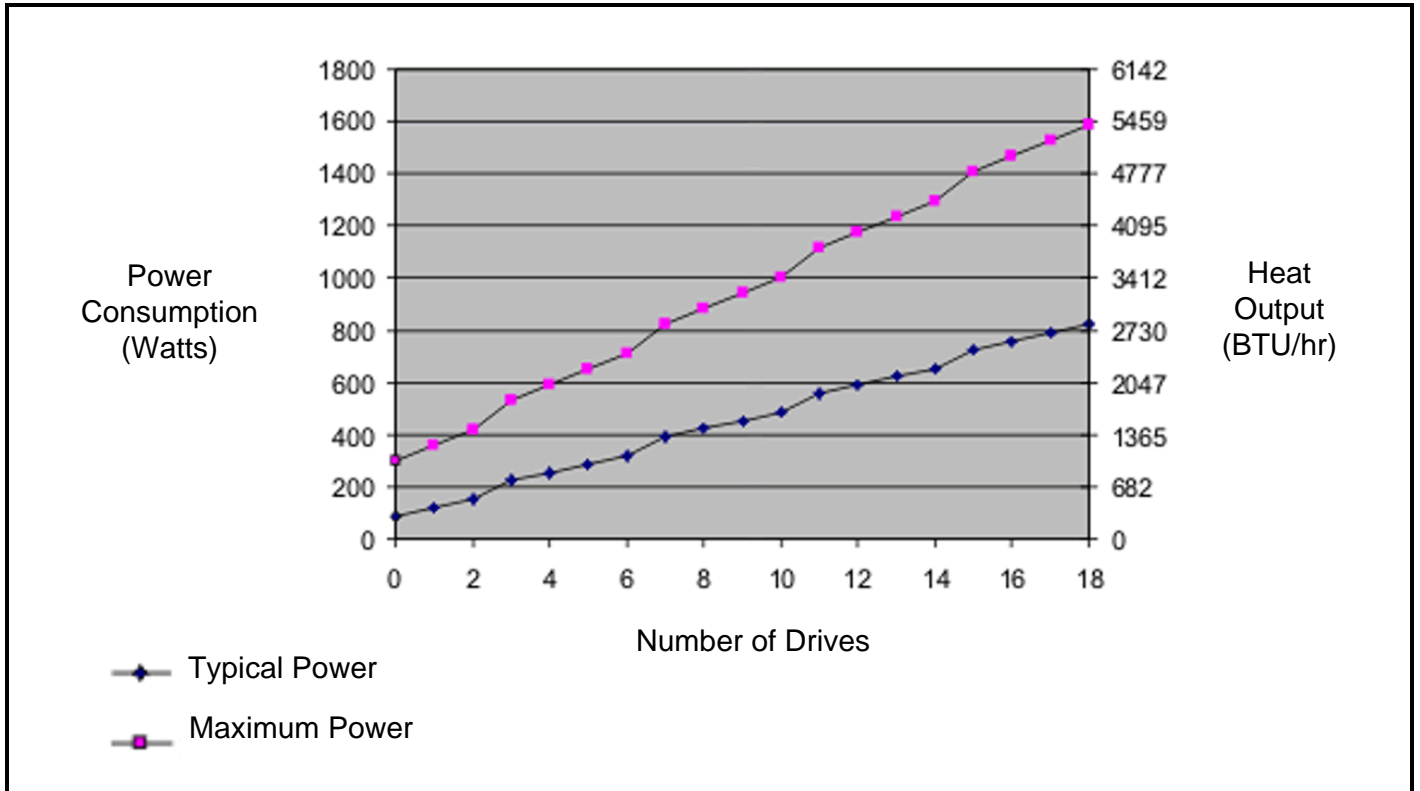
Figure 34 Library Current Draw
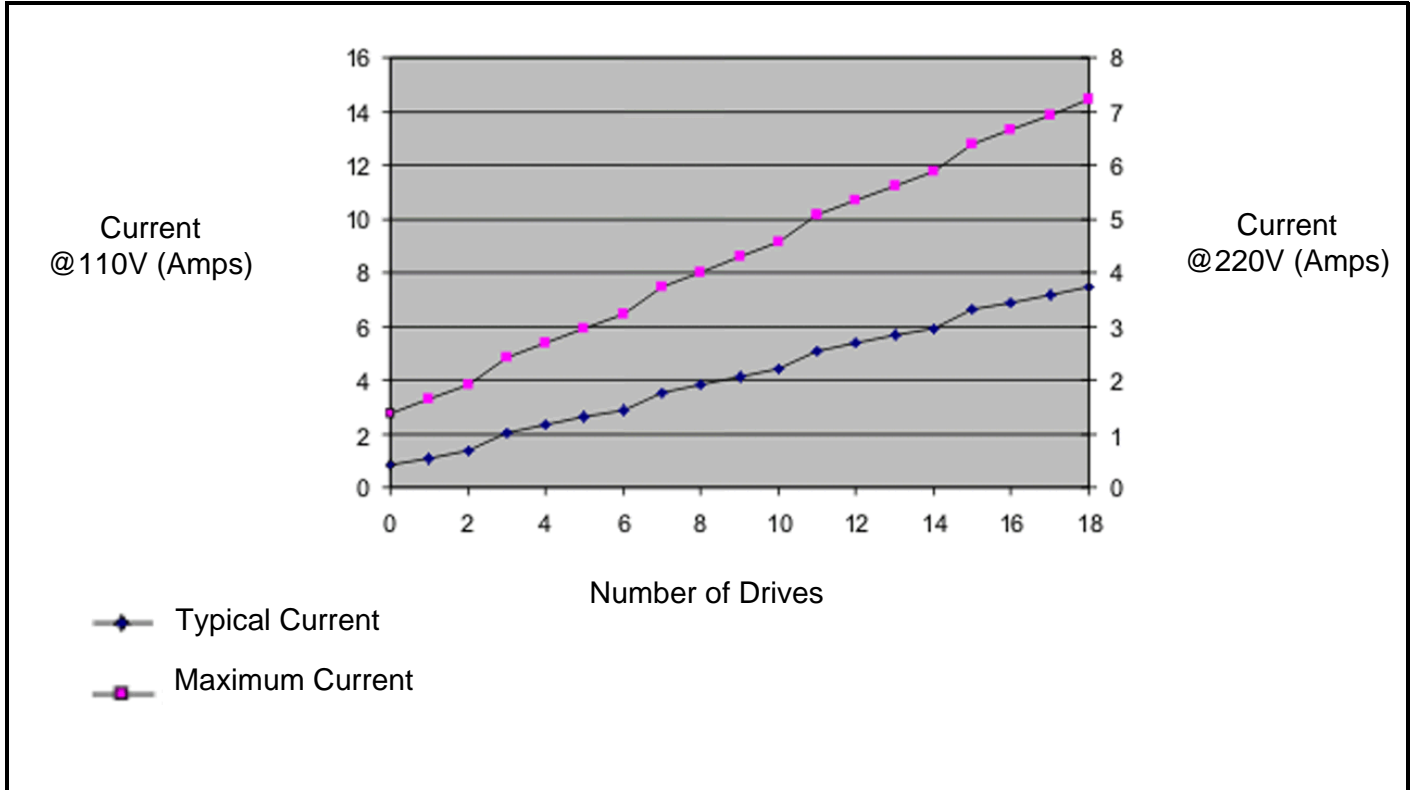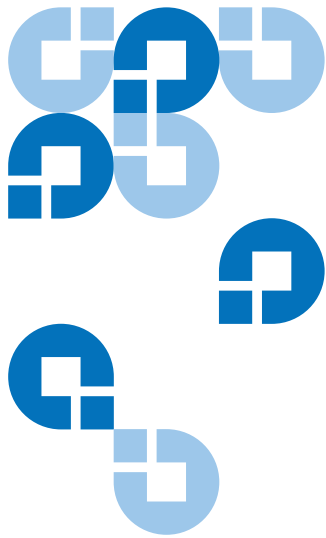
TapeAlert Flag Descriptions

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, 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 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).
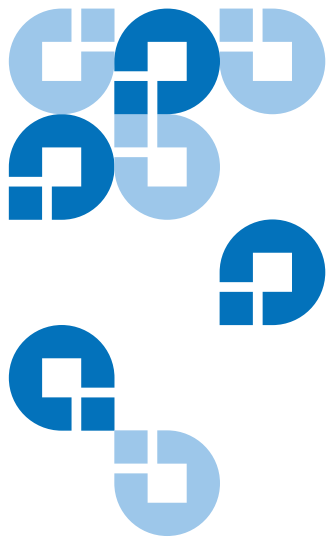
Glossary

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". If a component is 5.25" 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 subsystem 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 medium changer (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

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 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.

P

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.

R

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.