

Introduction	2
Setting Up the PowerVault ML6000 Library	6
Description	14
Understanding the User Interface	42
Configuring Your Library	56
Advanced Reporting	132
Capacity on Demand	144
Library Managed Encryption	146
Running Your Library	161
Getting Information – Logs and Reports	188
Updating Library and Tape Drive Firmware	199
Installing, Removing, and Replacing	210
Troubleshooting	377
Working With Cartridges and Barcodes	414
Library Specifications	421
TapeAlert Flag Descriptions	PO
Contacting Dell	PY



Chapter 1 Introduction

This guide contains information and instructions necessary for the normal operation and management of the PowerVault ML6000 library. This guide is intended for anyone interested in learning about or anyone that needs to know how to install, configure, and operate the PowerVault ML6000 library. Be aware that administrator level privileges are required to configure many of the features described in this guide.

Product Safety Statements

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

This unit is engineered and manufactured to meet all safety and regulatory requirements. Be aware that improper use may result in bodily injury, damage to the equipment, or interference with other equipment.

Mercury Statement



Projectors, LCD displays, and some multifunction printers may use lamp(s) that contain a small amount of mercury for energy-efficient lighting purposes. Mercury lamps in these products are labeled accordingly. Please manage the lamp according to local, state, or federal laws. For more information, contact the Electronic Industries Alliance at www.eiae.org. For lamp-specific disposal information check www.lamprecycle.org.

Explanation of Symbols and Notes

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

Note: A NOTE indicates important information that helps you make better use of your system.

Caution: A CAUTION indicates potential damage to hardware or loss of data if instructions are not followed.

Warning: A WARNING indicates a potential for property damage, personal injury, or death.

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.

Other Documents You Might Need

The following documents are also available for this product. These documents can be found on the Dell Support Web site. For the Dell Support Web site address, see [Appendix C, Contacting Dell](#).

- *Dell PowerVault ML6000 Getting Started Guide*
- *Dell PowerVault ML6000 SMI-S Reference Guide*
- *Dell PowerVault ML6000 Basic SNMP Reference Guide*
- *Dell PowerVault ML6000 SCSI Reference Guide*
- *Dell LTO Media Handbook, Version 2.0*
- *Servers and Storage Systems Safety, Environmental, and Regulatory Information*
- *Servers and Storage Systems Warranty and Support Information*
- *Dell Software License Agreement*

Note: Release Notes are also available for this product. The Release Notes describe changes to your system or firmware since the last release, provide compatibility information, and discuss any known issues and workarounds. Release Notes are included in the firmware downloads from the Dell Support Web site. See [Appendix C, Contacting Dell](#) for the Dell Support Web site address.

Supported Configurations

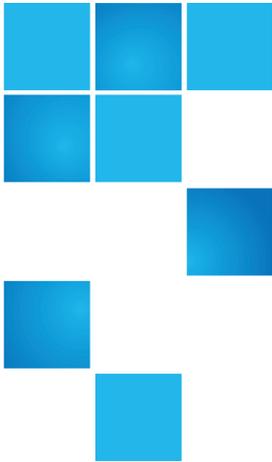
Caution: ML6030 (and higher) CM and Expansion Modules require professional installation. Professional installation may have been included with your purchase. Please call 1-800-945-3355 to schedule professional installation of your PowerVault library.

The available PowerVault ML6000 library configurations are as follows:

- The ML6010 CM is a 5U Library Control Module
- The ML6020 CM consists of one (1) ML6010 CM 5U Library Control Module and one (1) PowerVault ML6000 EM 9U Expansion Module (14U total)
- The ML6030 CM consists of one (1) ML6010 CM 5U Library Control Module and two (2) PowerVault ML6000 EM 9U Expansion Modules (23U total)

In addition, the ML6030 CM configuration can be expanded as follows:

- The ML6030 CM plus one (1) PowerVault ML6000 EM 9U Expansion Module (32U total)
- The ML6030 CM plus two (2) PowerVault ML6000 EM 9U Expansion Modules (41U total)



Setting Up the PowerVault ML6000 Library

This chapter provides an overview of the steps required to unpack, set up, and install the PowerVault ML6000 library.

For basic library setup instructions, see the *Dell PowerVault ML6000 Getting Started Guide* at <http://support.dell.com>. A copy of the *Dell PowerVault ML6000 Getting Started Guide* is also included in the product box with your library.

For complete installation instructions, see [Installing, Removing, and Replacing](#).

In addition, read the documents listed in [Other Documents You Might Need](#) on page 4. The information in these documents guides you through setting up, using, and maintaining your library.

Finding a Location

To avoid damage, the library must be positioned in a stable location. Refer to the *Servers and Storage Systems Safety, Environmental, and Regulatory Information* document listed in [Other Documents You Might Need](#) on page 4 for more information on finding an optimal location for your library.

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

Details on positioning the library include:

- Make sure a power source (only of the type marked on the product label) is available. See [Library Specifications](#) for power requirements.
- Route any cables to avoid walking on them or pinching them with items placed on or against them. Pay particular attention to the cord at the wall receptacle and the point where the cord exits from the library.
- Make sure that objects will not fall and liquids will not spill into the library's chassis through openings.

Read this Section Before Unpacking and Installing the PowerVault ML6000

This section includes important information you need to know before unpacking, installing, and powering up your PowerVault ML6000 library.

Warning: Without tape drives, tape cartridges, or power supplies, a 5U Library Control Module weighs approximately 60 lbs (27.2 kg). A 9U Expansion Module, without tape drives, tape cartridges, or power supplies, exceeds 65 lbs (29.5 kg). To avoid serious injury, two people are required to safely lift the modules.

Warning: All libraries 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.

Caution: ML6030 (and higher) CM and Expansion Modules require professional installation. Professional installation may have been included with your purchase. Please call 1-800-945-3355 to schedule professional installation of your PowerVault library.

Before installing the library:

- Remove any power supplies. The library can have a maximum of ten power supplies. Rack-mount the library before re-installing the power supplies. For complete rack-mounting instructions, see [Chapter 12, Installing, Removing, and Replacing](#).
- Remove any tape drives. The library can have a maximum of 18 drives. Rack-mount the library before re-installing the tape drives.
- Prior to loading media into the PowerVault ML6000, be sure that all tape cartridges have barcode labels.
- Prior to powering on your library, see the information on module terminator and cable installation in the *Dell PowerVault ML6000 Getting Started Guide* or in [Chapter 12, Installing, Removing, and Replacing](#).

Note: For the latest product updates, refer to <http://support.dell.com>.

Unpacking your Library

Caution: Remove all interior packaging material from the library before powering the library on or installing the library in a rack.

Note: Save all packaging material in case you need to move or ship the library in the future.

- Open the I/E station door and remove the yellow strip in the I/E station.
- Remove the orange robot restraint assembly securing the robot to the floor of the library. You can access the restraint assembly either through the library's access door or through the top of the library if you remove library's the top cover.

Installing and Rack-Mounting

Caution: ML6030 (and higher) CM and Expansion Modules require professional installation. Professional installation may have been included with your purchase. Please call 1-800-945-3355 to schedule professional installation of your PowerVault library.

To properly and safely rack-mount the PowerVault ML6000, see the rack-mount instructions in [Chapter 12, Installing, Removing, and Replacing](#).

Follow the detailed preparation and installation instructions for your library configuration.

If your library configuration is:	Then see these installation instructions:
ML6010 CM – A stand-alone 5U Library Control Module	<ul style="list-style-type: none"> • Installing a Stand-Alone 5U Library Control Module on page 245 • Installing the Library in a Rack on page 333
ML6020 CM – One 5U Library Control Module and one 9U Library Expansion Module	<ul style="list-style-type: none"> • Installing a Stand-Alone 5U Library Control Module on page 245 • Installing the Library in a Rack on page 333
ML6030 CM – One 5U Library Control Module and two 9U Library Expansion Modules	<ul style="list-style-type: none"> • Installing a Stand-Alone 5U Library Control Module on page 245 • Installing the Library in a Rack on page 333
ML6030 CM + 1 ML6000 EM – One 5U Library Control Module and three 9U Library Expansion Modules	<ul style="list-style-type: none"> • Installing a Stand-Alone 5U Library Control Module on page 245 • Installing the Library in a Rack on page 333
ML6030 CM + 2 ML6000 EMs – One 5U Library Control Module and four 9U Library Expansion Modules	<ul style="list-style-type: none"> • Installing a Stand-Alone 5U Library Control Module on page 245 • Installing the Library in a Rack on page 333

Before Running and Configuring the Library

Note: The PowerVault ML6000 can take up to 30 minutes to perform the initial boot. It is not safe to power cycle the library until the **Setup Wizard** appears in the operator panel.

Note: Initial power-on and initialization should occur prior to loading media. Excessive initialization time can occur with media loaded

Initial Administrative Login ID and Password Information

- Login ID: **admin**
- Password: **password**

Setup Wizard

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 as well as any modifications you made. See [Default Configuration Settings](#) on page 60 for more information.

Configuration Details

Note: You must use the Web client to manually create partitions. At the initial power-on, partitions can only be created automatically via the operator panel user interface.

- If your PowerVault ML6000 will be configured with zero I/E station slots, be sure to complete bulk loading of tape cartridges before configuring partitions. You may also bulk load tape cartridges while the system is powered down. For more information on bulk loading, see [Chapter 9, Running Your Library](#). For more details regarding configuring I/E station slots, see [Chapter 5, Configuring Your Library](#).
- When configuring network settings for the Default Gateway, you must enter a valid IP address. The library will not accept a blank value or 0.0.0.0.
- Before updating library firmware, be sure to save the library configuration. For instructions, see [Saving and Restoring the Library Configuration](#) on page 384.
- When drive topology changes are made, the library state may need updating before the partition can be used. To update the library state, perform one of the following actions:
 - Change the partition state to offline and change the state back to online.
 - Open the library door and close the door 10 seconds later.
 - Remove the drive from the rear of the library and insert the drive 1 minute later.
 - Reboot the library.

Caution: Please check your host backup software documentation for driver requirements. If Windows drivers are required, either the Windows default driver may be used (recommended), or the PowerVault ML6000 device-specific device driver can be found at <http://support.dell.com>. To avoid a possible performance reduction in a SAN environment, please consult Microsoft Knowledge Base article 842411 when using device-specific drivers.



Chapter 3 Description

The PowerVault ML6000 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 PowerVault ML6000 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, 9U Library Expansion Modules can be added to the library, allowing a configuration of up to a full 41 rack units (41U, where 1U = 1.75”).

- [Understanding the Location Coordinates](#)
- [Understanding Logical Element Addressing](#)

Library Configuration

The PowerVault ML6000 library is designed for ease of installation, configuration, and field upgrades. The PowerVault ML6000 library is built upon two basic building blocks: the 5U Library Control Module and 9U Library Expansion Module.

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

- The ML6010 CM is a 5U Library Control Module. [Figure 1](#) on page 15 shows the front view of the ML6010 CM.
- The ML6020 CM consists of one (1) ML6010 CM 5U Library Control Module and one (1) PowerVault ML6000 EM 9U Library Expansion Module (14U total). [Figure 2](#) on page 16 shows the front view of the ML6020 CM.
- The ML6030 CM consists of one (1) ML6010 CM 5U Library Control Module and two (2) PowerVault ML6000 EM 9U Library Expansion Modules (23U total). [Figure 3](#) on page 17 shows the front view of the ML6030 CM.

In addition, the ML6030 CM configuration can be expanded as follows:

- The ML6030 CM plus one (1) PowerVault ML6000 EM 9U Library Expansion Module (32U total)
- The ML6030 CM plus two (2) PowerVault ML6000 EM Library 9U Expansion Modules (41U total)

Figure 1 ML6010 CM Library Configuration (Standalone 5U Library Control Module)

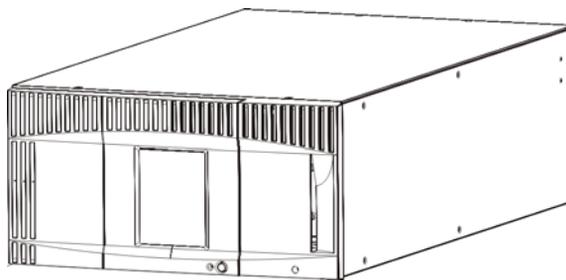
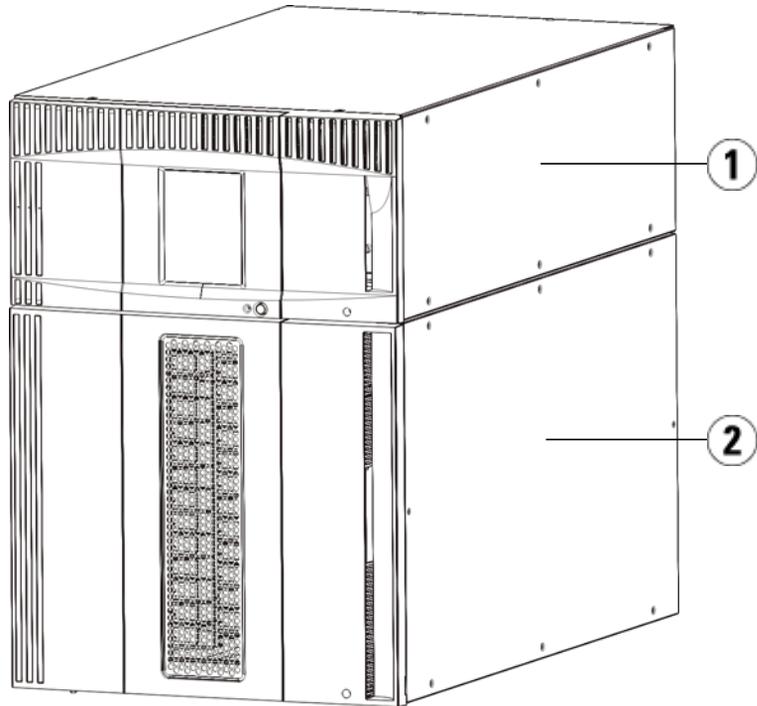
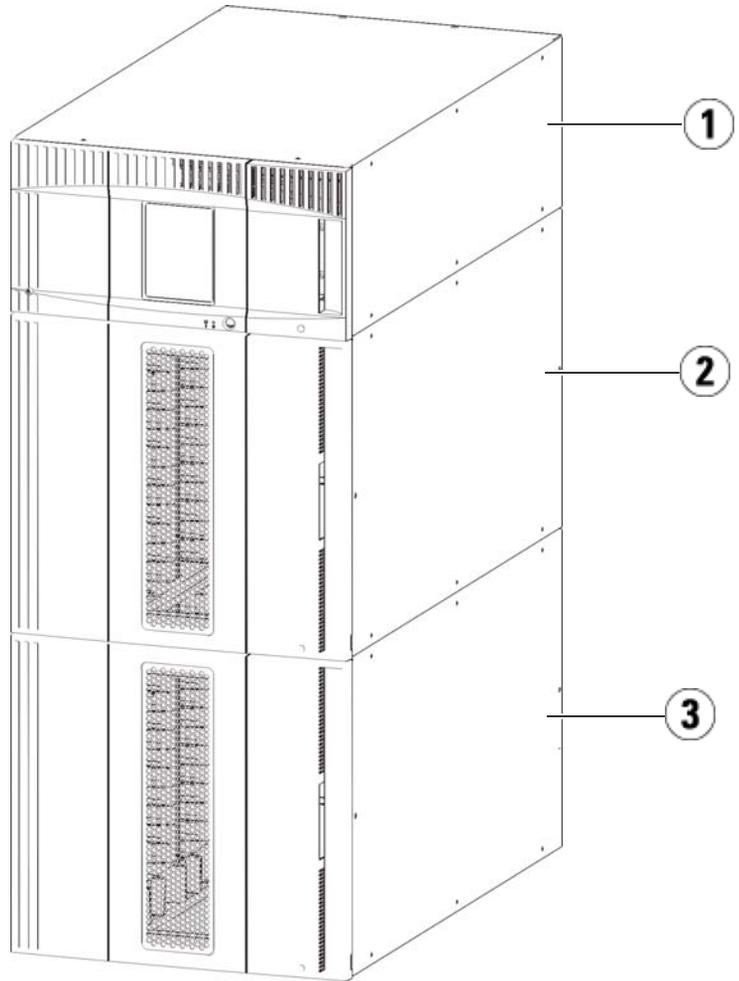


Figure 2 ML6020 CM Library Configuration (5U Library Control Module Plus One 9U Library Expansion Module)



-
- 1 5U Library Control Module
 - 2 9U Library Expansion Module
-

Figure 3 ML6030 CM Library Configuration (5U Library Control Module Plus Two 9U Library Expansion Modules)



-
- 1 5U Library Control Module
 - 2 9U Library Expansion Module
 - 3 9U Library 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.

Caution: ML6030 (and higher) CM and Expansion Modules require professional installation. Professional installation may have been included with your purchase. Please call 1-800-945-3355 to schedule professional installation of your PowerVault library.

Modules

PowerVault ML6000 libraries are modular, and you can increase the size at any time. The three base systems for the PowerVault ML6000 library are as follows:

- ML6010 CM (5U rack height)
- ML6020 CM (14U rack height)
- ML6030 CM (23U rack height)

These configurations can be scaled up by adding PowerVault ML6000 EM 9U Library Expansion Modules to a maximum rack height of 41U. 9U Library Expansion Modules provide additional capacity as your storage and tape drive requirements change. See [Figure 4](#) on page 20 for an illustration of library scalability. For information on installing, removing, and replacing modules, see [Installing, Removing, and Replacing](#) on page 210.

Each module has a specific number of fixed storage slots, I/E station slots, and tape drive slots available. See [Library capacity is as follows](#), on page 423 for the number of slots available for each library configurations.

Note: Slot counts in this document do not include five inaccessible slots in the bottom row of any library configuration. For more information about these slots, see [Unused Slots](#) on page 171.

Caution: ML6030 (and higher) CM and Expansion Modules require professional installation. Professional installation may have been included with your purchase. Please call 1-800-945-3355 to schedule professional installation of your PowerVault library.

5U Library Control Module

The 5U Library Control Module is required in any PowerVault ML6000 library configuration. The 5U Library Control Module contains the robotic controls, library control blade (LCB), and touch screen display. The 5U Library Control Module also contains an import/export (I/E) station, fixed storage slots, tape drives, and at least one power supply.

9U Library Expansion Modules

9U Library Expansion Modules are supplementary modules that can be stacked above or below the 5U Library Control Module. Each 9U Library Expansion Module contains fixed storage slots, tape drive slots, and power supply slots. The I/E stations on 9U Library Expansion Modules are included and may be configured as storage. 9U Library Expansion Modules also contain bays for optional Fibre Channel (FC) Input/Output (I/O) blades.

If a 9U Library 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 5U Library Control Module.

Stackability

The maximum rack height of the library is 41U, which consists of a 5U Library Control Module and four 9U Library Expansion Modules. [Figure 4](#) illustrates the stackability of the library.

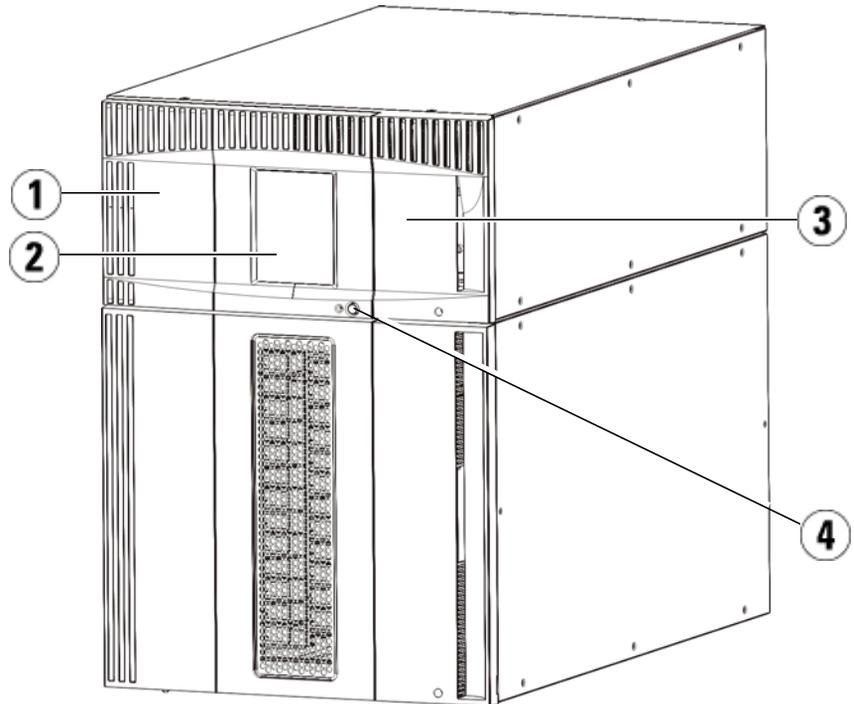
Figure 4 Base Systems Plus
9U Library Expansion Modules

ML6010 (41 slots)	ML6020 (133 slots)	ML6030 (225 slots)	ML6030 CM + 1 9U Library Expansion Module (317 slots)	ML6030 CM + 2 9U Library Expansion Modules (409 slots)
				9U Library Expansion Module
			5U Library Control Module	5U Library Control Module
		5U Library Control Module	9U Library Expansion Module	9U Library Expansion Module
	5U Library Control Module	9U Library Expansion Module	9U Library Expansion Module	9U Library Expansion Module
5U Library Control Module	9U Library Expansion Module	9U Library Expansion Module	9U Library Expansion Module	9U Library Expansion Module

Front Panel Components

[Figure 5](#) shows the front panel components of the library. The paragraphs following [Figure 5](#) describe the components in detail.

Figure 5 Front Panel Components



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

Access Door

The access door allows access to the internal components of the library. Each 5U Library Control Module and 9U Library Expansion Module has an access door. In most cases, you will not need to access the library through this door except when you want to bulk load or unload cartridges from the library.

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

You can lock and unlock the I/E station door using commands on the **Operations** menu. If necessary, you can also manually unlock the I/E station door. For more information, see [Locking and Unlocking the I/E Stations](#) on page 185.

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 5U Library Control Module and on the front of 9U Library Expansion Modules. A 5U I/E station has a capacity of six cartridges. A 9U I/E station has a capacity of 12 cartridges.

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

Operator Panel

The operator panel is the touch screen display device upon which the graphical user interface (GUI) appears. The operator panel is located on the access door of the 5U Library 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 4, Understanding the User Interface](#).

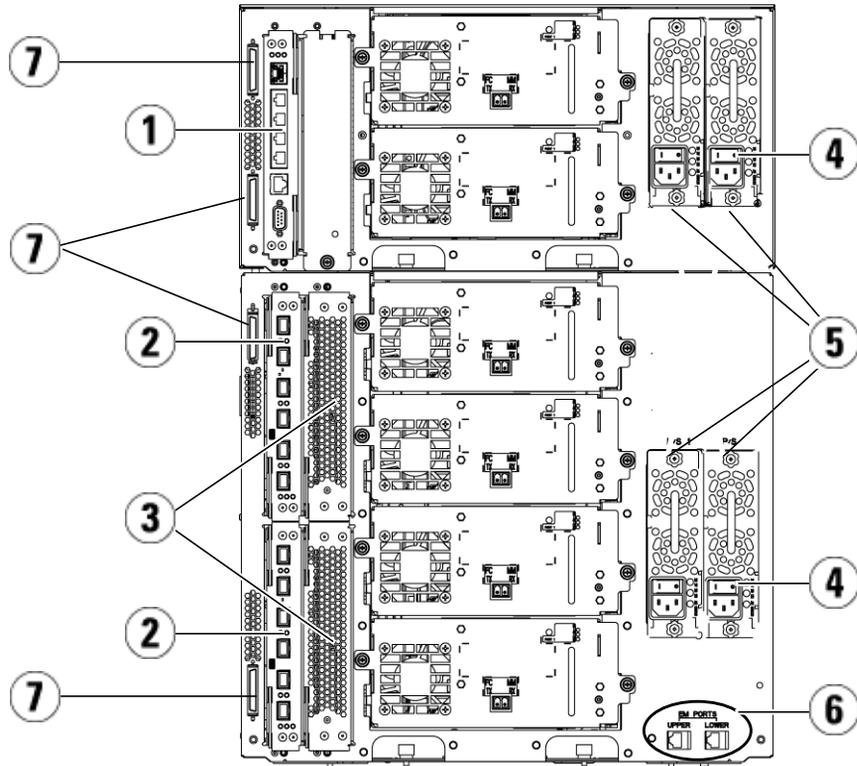
Front Power Button

Turning off the front power button turns off the robot and operator panel, but power still runs to the power supplies. Use the front power button to manually shut down the library. See [Shutting Down, Powering Off, and Completely Removing Power](#) on page 162 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 9U Library Expansion Module
 - 7 Module terminator connectors (CAN bus connectors)
-

Rear Power Switches

Rear power switches are located on each power supply. Turning off the rear power switch on a power supply removes all power from the library. The rear power switches should be used in all emergency and service situations.

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

Caution: Except in emergencies, use the shutdown procedure before switching off the rear power switch. See [Shutting Down, Powering Off, and Completely Removing Power](#) on page 162 for instructions on how to shut down the library.

Power System

The library supports single and redundant power configurations. The single power configuration has a single AC line input and single DC power supply. The redundant configuration has dual AC line input and dual DC power supplies.

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

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

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

Caution: The 9U Library Control Module and each 9U Library 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:

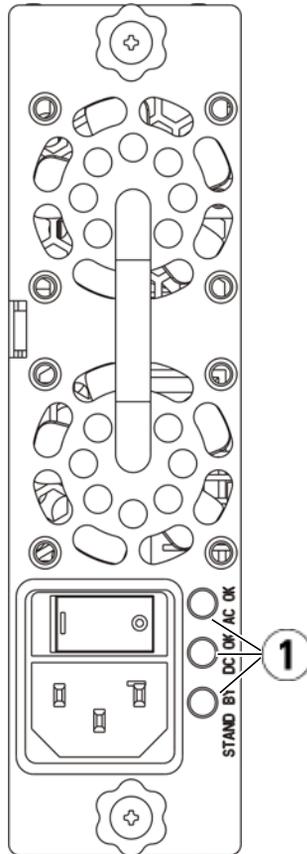
- Power supply
- AC power cord

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 404.

Figure 7 Power Supply LEDs



1 LEDs

Library Control Blade

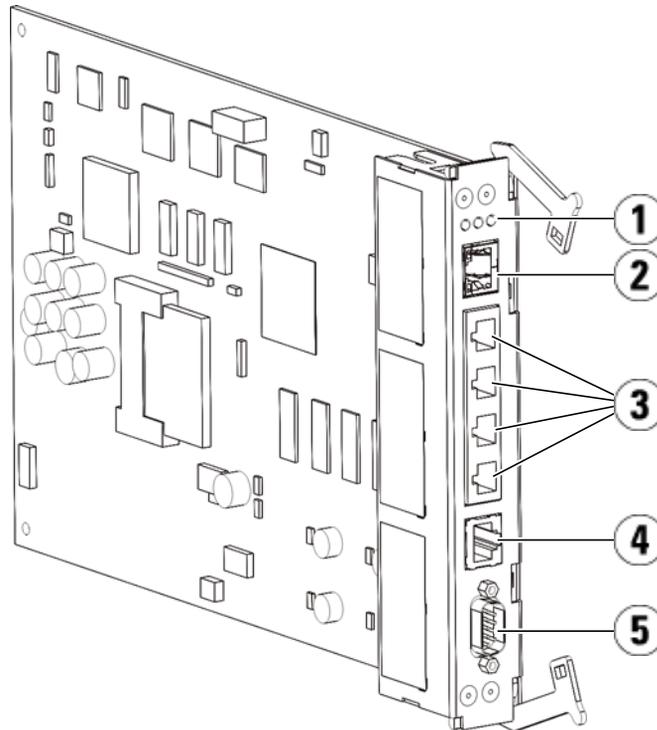
The library control blade (LCB) manages the entire library, including the operator panel and picker assembly, and is responsible for running system tests to ensure that the library is functioning properly. The LCB also provides internal communication to Fibre Channel (FC) I/O blade slots. The LCB has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

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

- **Green** represents processor status.
- **Amber** represents health status.
- **Blue** represents power-control status.

[Figure 8](#) shows the location of the LCB components, including LEDs. For more information on the behavior of the LCB LEDs, see [Blade Status LEDs](#) on page 396.

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

9U Library 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 9U Library Expansion Module. FC I/O blades and fan blades are hot-swappable.

FC I/O blades cannot be installed in the 5U Library Control Module, so your library configuration must include at least one 9U Library Expansion Module to include FC I/O blades. Each 9U Library Expansion Module can house up to two FC I/O blades. Depending on the number of installed 9U Library 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 5U Library Control Module, can be connected to an FC I/O blade in a 9U Library Expansion Module.

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

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

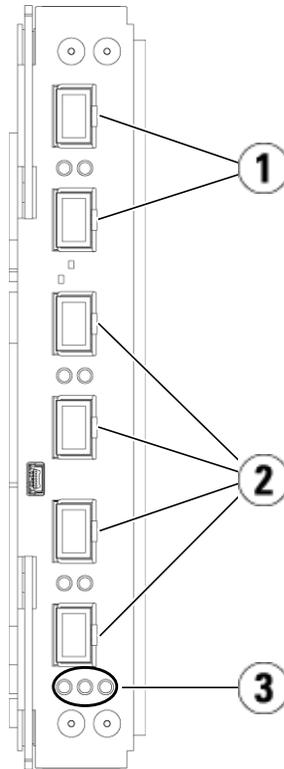
- **Green** represents processor status.
- **Amber** represents health status.
- **Blue** represents power-control status.

[Figure 9](#) shows the FC I/O Blade, including LEDs. For more information on the behavior of the FC I/O Blade LEDs, see [Blade Status LEDs](#) on page 396.

For information on configuring I/O blades, see [Working With FC I/O Blades](#) on page 109.

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

Figure 9 FC I/O Blade

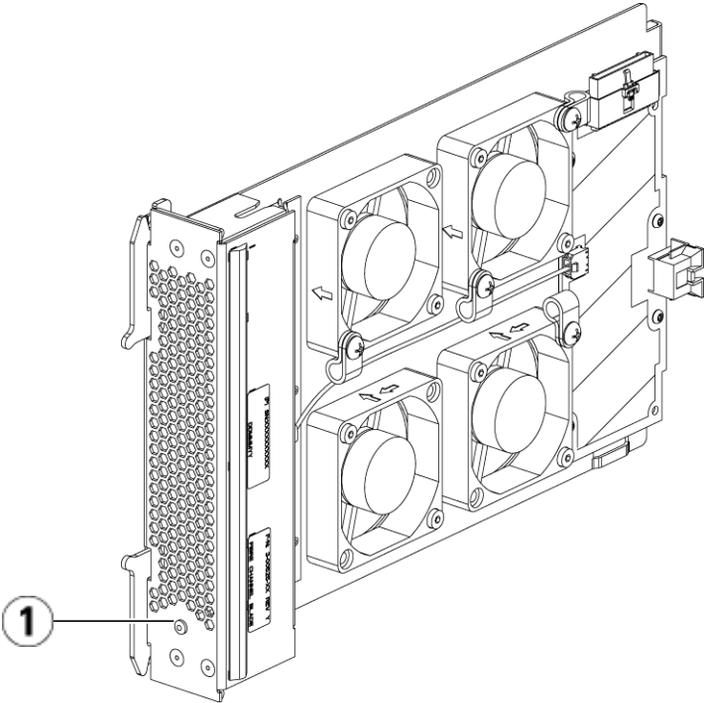


-
- 1 FC ports to host(s)
 - 2 FC ports to drive(s)
 - 3 LEDs (blue, amber, green)
-

Each FC I/O blade is cooled by a fan blade that is installed next to the FC I/O blade in the 9U Library Expansion Module. For information on installing the fan blade, see [Adding, Removing, and Replacing the FC I/O Fan Blade](#) on page 370.

[Figure 10](#) shows the FC I/O fan blade, including the LED. The single amber LED represents health status. For more information on the behavior of the FC I/O fan blade LED, see [Tape Drive LEDs](#) on page 400.

Figure 10 FC I/O Fan Blade



1 LED (amber)

Robotic System and Barcode Scanner

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

Each tape cartridge must contain a barcode that the barcode scanner reads during the inventory process. During the inventory process, the barcode scanner reads the fiducial labels to identify the types of magazines and tape drives that are installed in the library.

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

Tape Drive Support

Details about tape drive support include:

- Every library configuration must contain at least one tape drive.
- 5U Library Control Modules can hold a maximum of two tape drives.
- 9U Library Expansion Modules can hold a maximum of four tape drives.

Please see [Supported Components](#) on page 421 for a list of tape drives and media supported by the PowerVault ML6000 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 71.

SCSI and SAS tape drives are attached directly to the host. FC tape drives can be directly attached to hosts or to the Storage Area Network (SAN). FC tape drives can also be attached to FC I/O blades, which manage communication between the hosts and the drives. For more information on FC I/O blades, see [Working With FC I/O Blades](#) on page 109.

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 [Adding a Tape Drive](#) on page 354.

Library Features

This section describes several features of PowerVault ML6000 libraries.

User Interface

The operator panel is located on the front door of the 5U Library 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 [Chapter 4, Understanding the User Interface](#) for more information about the operator panel and the Web client.

Partitions

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

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

For more information on partitions, see [Working With Partitions](#) on page 71.

Control Path Modification

The control path tape drive is used to connect a partition to a host application. Only one tape drive can be selected as the control path at one time. For more information, see [Working With Control Paths](#) on page 86.

Support for WORM

PowerVault ML6000 tape libraries support WORM (write once, read many) technology in LTO-3, LTO-4, LTO-5 and LTO-6 tape drives. WORM allows non-rewriteable and non-erasable data to be written and provides extra data security by prohibiting accidental data erasure. The WORM feature is supported whenever you use WORM cartridges.

Licensable Features

In addition to the standard features, the following additional, licensable features are available for the PowerVault ML6000:

- Advanced Reporting, described in [Chapter 6, Advanced Reporting](#)
- Capacity on Demand, described in [Chapter 7, Capacity on Demand](#)
- Library Managed Encryption, described in [Chapter 8, Library Managed Encryption](#)

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

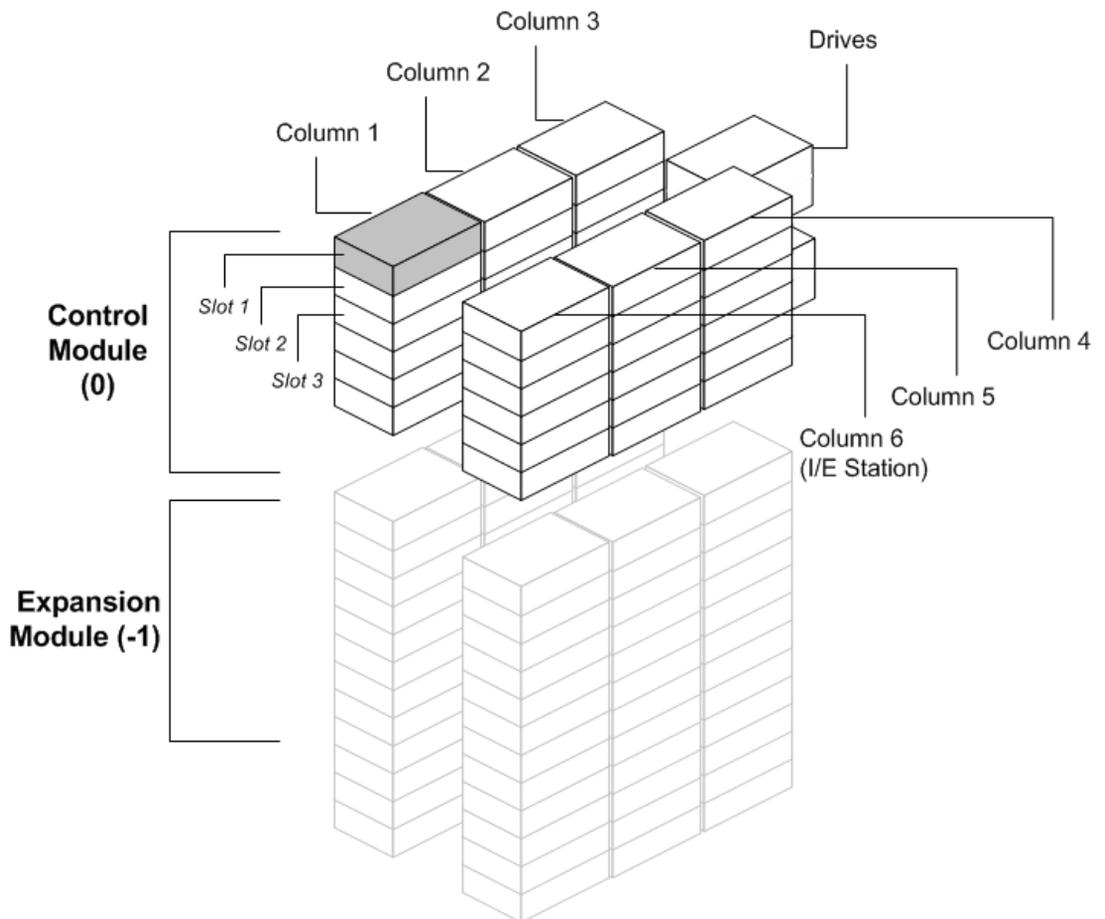
Understanding the Location Coordinates

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

library with a 5U Library Control Module and a 9U Library Expansion Module is numbered.

Note: The library location coordinates are different from the logical element addressing; see [Understanding Logical Element Addressing](#) on page 38 for more information.)

Figure 11 Library Location Coordinates



Modules

Library modules are represented by the first digit of a library coordinate. Modules are identified relative to the 5U Library Control Module.

The 5U Library Control Module is numbered 0 (zero). 9U Library Expansion Modules stacked above the 5U Library Control Module are addressed with positive integer digits depending on their position above the 5U Library Control Module. For example, the 9U Library Expansion Module stacked directly above the 5U Library Control Module is number 1. The 9U Library Expansion Module stacked directly above module 1 is number 2, and so on.

Modules stacked below the 5U Library Control Module are numbered with negative integer digits, also depending on their relative position to the 5U Library Control Module. For example, the 9U Library Expansion Module stacked directly below the 5U Library Control Module is number -1. The 9U Library Expansion Module stacked directly below module -1 is number -2, and so on.

Columns

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

Slots

Fixed storage slots are represented by the third digit of the library location coordinate. Within each column, slots are numbered from top to bottom, starting at 1. For example, in [Figure 11](#) on page 36, 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 9U Library 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 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.

Understanding Logical Element Addressing

The library uses standard industry conventions to logically number every storage slot, I/E station slot, and tape drive in the library. Host software is designed to understand this addressing system, and generally there are no problems relating to tape cartridge slots. However, hosts sometimes have problems relating to tape drives, particularly when tape drives, 5U Library Control Modules, or 9U Library Expansion Modules are added or removed, or empty tape drive slots exist. This section explains how the library logically addresses tape drives and slots, so that you can avoid common problems with host software.

Note: The logical element addressing described in this section is different from the library-specific location coordinates described in [Understanding the Location Coordinates](#) on page 35.)

Tape Drive Logical Element Addressing

Tape drive logical element addresses are assigned by partition. The numbering is sequential within a partition and starts over with each partition. The addresses start with the lowest library module in a partition. The top tape drive in the module and partition is always number 256. The tape drive beneath that is 257, and so on until all tape drives in that module/partition have been accounted for. Numbering continues with the top tape drive in the next module up. Empty tape drive slots are skipped (they are not given an element address).

Host software may have problems recognizing tape drives when tape drives, 5U Library Control Modules, or 9U Library Expansion Modules are added, removed, or replaced; or when partitions are added, deleted, or modified, because existing logical element addresses can change. Therefore, after making any of these types of modifications, you must refresh the configuration of any backup application that manages the library to reflect new tape drive positions. In addition, you may need to reboot the host server(s) or rescan the bus to detect the changes.

See [Figure 12](#) on page 41 for a simple example of element addressing in a 14U library with a single partition, six tape drives installed and no empty tape drive slots. Note that multiple partition can create complexity. If you need help with the element addressing in your library, contact Dell Technical Support (see [Appendix C, Contacting Dell](#)).

Cartridge Slot Logical Element Addressing

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

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

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

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

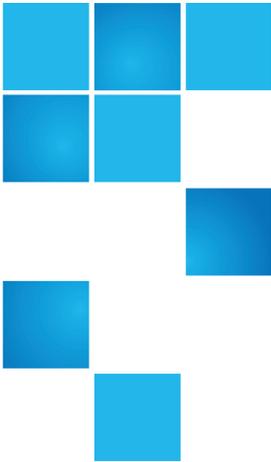
Generally, host software easily recognizes logical slot element addresses, even when they change. The next time the host issues a READ ELEMENT STATUS command, it will process the new number and recalculate all of the slot addresses.

See [Figure 12](#) on page 41 for a simple example of element addressing in a 14U library with a single partition.

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

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

- Tape cartridge slots in partition
- I/E station slots
- Tape drives
- Unused slots



Understanding the User Interface

The user interface of PowerVault ML6000 libraries is available in two formats: the operator panel and the Web client. Operations on the library can be performed locally on the 5U Library Control Module using the operator panel or remotely on your computer using the Web client. Similar functionality with common elements is used for both formats.

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

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

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 45 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 386 for more information on “Library Not Ready” messages displayed in the header.

[Figure 13](#) and [Figure 14](#) show the operator panel and the Web client interfaces.

Figure 13 Operator Panel User Interface

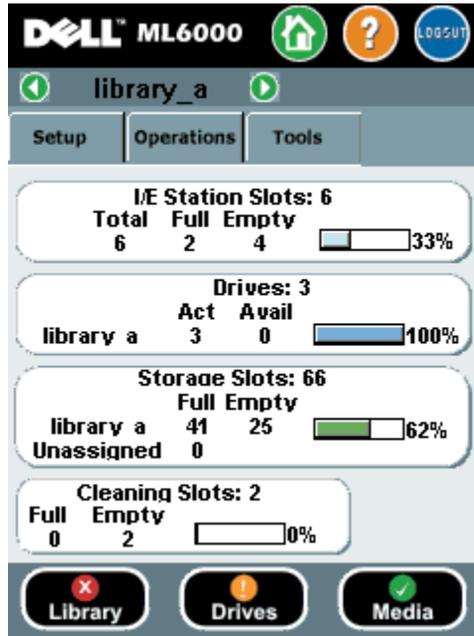


Figure 14 Web Client User Interface



System Summary and Subsystem Status

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

The three subsystems are:

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

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

- **Green** – No RAS tickets exist for this subsystem, or, if any tickets do exist, they have all been closed.
- **Yellow** – The library contains open or unopened, low-severity (Severity 3) or high-severity (Severity 2) RAS tickets for this subsystem.
- **Red** – The library contains open or unopened urgent (Severity 1) RAS tickets for this subsystem.

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

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

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

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

You can also open the **All RAS Tickets** screen by selecting **Tools > All RAS Tickets**. See [About RAS Tickets](#) on page 377 for more information about RAS tickets.

Home Page

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

Details about the home page include:

- On the Web client, users see the partitions (in alphabetical order) to which they have access.
- On the operator panel, if users have access to more than one partition, they can navigate to other partitions using the arrows next to the partition name in the title bar at the top of the screen.

For more information about user privileges, see [User Privileges](#) on page 54 and [Working With User Accounts](#) on page 96.

Operator Panel

The operator panel is physically attached to the front door of the 5U Library Control Module. The user interface appears on the touch-screen LCD display of the operator panel for executing basic library management functions. Audible feedback, or “key click” sounds, are generated when a user presses a button on the operator panel. Users can choose to disable the audible feedback. See [Configuring System Settings](#) on page 126.

Operator Panel Keypads

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

Operator Panel Indicates Intervention Required

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

Web Client

The Web client user interface is similar to the operator panel user interface. The Web client interface is accessible from supported Web browsers. See [Library Capacity](#) on page 423 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 124 for information on setting the network configuration settings for remote use.

You must disable Web browser popup blockers to use the Web client interface and the library's online Help. Add the PowerVault ML6000's Internet Protocol (IP) address to the list of trusted/allowed sites on your PowerVault ML6000-supported browser, so the Web client pages will automatically refresh.

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

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

Menu Trees

The following menus organize operations and commands into logical groupings:

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

- The **Operations** menu consists of commands that enable users to change the library's mode of operations, import and export cartridges, load and unload tape drives, move media, perform diagnostics, and log off. Administrators can also access commands to lock or unlock the I/E station and to shut the library down.
- The **Tools** menu consists of commands that you can use to maintain your library, such as viewing RAS Tickets, generating diagnostic logs, identifying drives, configuring the internal network, saving and restoring the library configuration, setting system and security settings, and updating firmware.
- The **Reports** menu (Web client only) consists of summaries of library information.

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

[Table 1](#) lists the Web client menus. Some menu commands are available only to administrators.

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

Table 1 Web Client Menus

Setup Menu *	Operations Menu	Tools Menu *	Reports Menu
<ul style="list-style-type: none"> • Setup Wizard • Partitions • Cleaning Slots • I/E Station Slots • Drive Settings • Control Path • License • Notifications <ul style="list-style-type: none"> • E-mail Configuration • Advanced Reporting (if licensed) <ul style="list-style-type: none"> • Receiver Addresses • Media Security • RAS <ul style="list-style-type: none"> • Receiver Addresses • Contact Information • Network Management <ul style="list-style-type: none"> • Network • SNMP • SNMP Trap Registrations 	<ul style="list-style-type: none"> • Media <ul style="list-style-type: none"> • Move • Import • Export • Cleaning Media <ul style="list-style-type: none"> • Import • Export • Partitions <ul style="list-style-type: none"> • Change Mode • Drive <ul style="list-style-type: none"> • Load • Unload • Change Mode • I/E Station Lock/Unlock* • System Shutdown* • Logout 	<ul style="list-style-type: none"> • All RAS Tickets • Capture Snapshot • Save/Restore Configuration • E-mail Configuration Record • Save Configuration Record • Identify Drives • Drive Operations • Download SNMP MIB • FC I/O Blade Info** • FC I/O Blade Port Info** • Update Library Firmware • Reset Factory Defaults • Diagnostics 	<ul style="list-style-type: none"> • System Information • Library Configuration • Network Settings • Logged In Users* • All Slots • Log Viewer* • Advanced Reporting* <ul style="list-style-type: none"> • Drive Resource Utilization • Media Integrity Analysis • About

Setup Menu [*]	Operations Menu	Tools Menu [*]	Reports Menu
<ul style="list-style-type: none"> • User Management <ul style="list-style-type: none"> • User Accounts • Remote Authentication • FC I/O Blades** <ul style="list-style-type: none"> • Port Configuration • Channel Zoning • Host Mapping • Host Management • Host Port Failover • Data Path Conditioning • FC I/O Blade Control • Encryption (if licensed) <ul style="list-style-type: none"> • System Configuration • Partition Configuration • System Settings • Date & Time 			

^{*} Administrators only. ^{**} Available only when the library contains I/O blades.

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

Table 2 Operator Panel
Menus

Setup Menu ^a	Operations Menu	Tools Menu
<ul style="list-style-type: none"> • Partition Mgmt <ul style="list-style-type: none"> • Create Partition • Delete Partition • Configure I/E Station Slots • Configure Cleaning Slots • User Mgmt <ul style="list-style-type: none"> • Create User • Modify User • Drive Settings <ul style="list-style-type: none"> • Fibre • SCSI • SAS • Notification <ul style="list-style-type: none"> • E-mail Alerts • E-mail Account • Customer Contact • Licenses • Date & Time • Network Mgmt <ul style="list-style-type: none"> • IP version 4 • IP version 6 (if enabled) • Port Settings • Control Path 	<ul style="list-style-type: none"> • Move Media • Import Media • Export Media • Import Cleaning Media • Export Cleaning Media • Change Partition Mode • Load Drive • Unload Drive • Change Drive Mode • Lock/Unlock I/E Station^a • Shutdown^a 	<ul style="list-style-type: none"> • All RAS Tickets^a • Capture Snapshot^a • Drive Mgmt^a <ul style="list-style-type: none"> • Create a firmware tape • Update drive firmware from tape • Erase a firmware tape • Clean drive • Reset drives • Drive Info • About Library <ul style="list-style-type: none"> • Network Info • View Drive Info • Partition Info • Internal Network^a • System Settings <ul style="list-style-type: none"> • 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 • Unlabeled Media Detection

Setup Menu ^a	Operations Menu	Tools Menu
<ul style="list-style-type: none"> • FC I/O Blades^b <ul style="list-style-type: none"> • Port Configuration • Channel Zoning • Host Mapping^c • Host Management^c • Host Port Failover • Data Path Conditioning • FC I/O Blade Control 		<ul style="list-style-type: none"> • Security^a <ul style="list-style-type: none"> • Network Interface • SSH Services • ICMP • Remote UI • SNMP • SMI-S • Display Settings <ul style="list-style-type: none"> • Brightness • Contrast • Defaults • Library Tests^a <ul style="list-style-type: none"> • Installation & Verification Tests • Library Demo • View Last Summary Log • View Last Detailed Log • E-mail Last Detailed Log • Blade Info^b <ul style="list-style-type: none"> • Port Info • Command History Log^{ab} • Factory Defaults^a

^aAdministrators only. ^bAvailable only when the library contains I/O blades. ^cVisible 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 96 for more information on setting user privilege levels.

Two types of users are defined in PowerVault ML6000 libraries:

- **Administrators** have access to the entire physical library and all of its partitions, and can configure the library and set up user and administrator accounts. The library ships with a default administrator account. The user name for the default administrator account is **admin** and the password is **password**. You cannot modify or delete the user name for the default administrator account, but you can modify the password. If you misplace the password for the default administrator account, contact Dell Technical Support (see [Appendix C, Contacting Dell](#)).
- **Users** have access to one or more assigned partitions, as well as portions of the **Operations** and **Reports** menus. Users cannot access the **Setup** and **Tools** menus. Users can perform functions within a partition (such as performing cartridge and tape drive operations), but cannot set up or configure the library (for example, creating or deleting partitions).

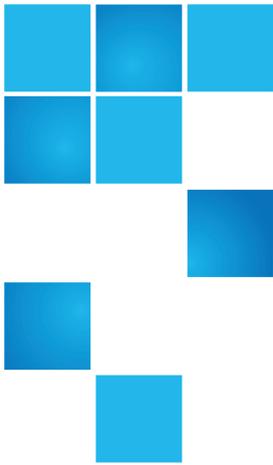
Details on user privileges include:

- The library can contain eighteen user accounts (user or administrator or both), including the default administrator account.
- Eighteen user (user or administrator or both) sessions can be active at one time.
- The same user can be logged in to a library from multiple remote locations.
- Clicking the close button (**X**) in the upper-right corner of the Web client closes the browser window but does not log the user or administrator out.

- All users are logged out automatically after a configurable period of inactivity. The default user session timeout period is 30 minutes, but administrators can change the user session timeout to a value from 15 minutes to 480 minutes (eight hours). See [Configuring System Settings](#) on page 126.
- A screen saver is invoked after 10 minutes of inactivity on the operator panel. After an hour of inactivity, the screen will appear black. If the user has not been logged out for inactivity, touching the operator panel will reactivate it, returning the user to the screen last in use. (The Web client does not use a screen saver.)
- An administrator can disable any access to the library from the Web client. For more information, see [Configuring System Settings](#) on page 126.

User Access

Administrators have access to the entire library. Users with user privileges can only access some of the menus. See [Table 1 on page 50](#) for the Web client menu tree and privilege level information. See [Table 2 on page 52](#) for the operator panel menu tree and privilege level information.



Configuring Your Library

Once you have installed the hardware as described in [Chapter 2, Setting Up the PowerVault ML6000 Library](#), 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 [Saving and Restoring the Library Configuration](#) on page 384.

About the Setup Wizard

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

The Setup Wizard on the operator panel only runs once, at initial startup. After that, administrators access the Setup Wizard any time via the Web client or use commands on the **Setup** and **Operations** menus to modify all library settings, including network settings. See [Completing the Library Configuration With Menu Commands](#) on page 57.

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 60.

For additional information, see [Using the Setup Wizard](#) on page 58.

Using the Default Administrator Account

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

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

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

Note: If you misplace the password for the default administrator account, contact Dell Technical Support (see [Appendix C, Contacting Dell](#)).

Completing the Library Configuration With Menu Commands

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

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

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

For the menu trees on both the operator panel and Web client, see [Menu Trees](#) on page 48.

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 60).
- 3 When you get to the network configuration screens, configure the network settings as follows:

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

- **If you are using IPv4:** On the **Setup Wizard: Enable IPv6** screen, do NOT select the **Enable IPv6** check box. Click **Next**. Configure the network settings.
 - **If you are using IPv6:** On the **Setup Wizard: Enable IPv6** screen, select the **Enable IPv6** check box and click **Next**. You have enabled IPv6 but you will not be prompted to configure IPv6 settings here. Continue with the Setup Wizard screens. Then, when you are finished using the Setup Wizard, configure the IPv6 network settings by going to **Setup > Network Mgmt** on the operator panel.
- 4 Log out of the operator panel.
 - 5 Using the default administrator account, log in to the Web client. Type **admin** in the **User Name** text box and **password** in the **Password** text box.
 - 6 Complete the **Setup Wizard** screens on the Web client interface. The final **Setup Wizard** screen will prompt you to apply your settings.

When you have completed the **Setup Wizard**, the Library Configuration report appears on the Web client. The Library Configuration report provides information on the library's tape drives, partitions, I/E stations, storage slots, cleaning slots, and loaded media. See [Viewing the Library Configuration Report](#) on page 190 for more information on the Library Configuration report.

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

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

- The only time that you do not need to log in to the library is when the Setup Wizard appears on the operator panel the first time the library is powered on.
- After a timeout period of one hour, the Setup Wizard will close, and you will be logged out of the library. Use the default administrator account to log in to the operator panel.
- If you time out of the Setup Wizard or do not complete all the Setup Wizard screens, the library will apply the default configuration settings plus whatever modifications you made (see [Default Configuration Settings](#) on page 60).

- You cannot log in to the library from the Web client until you have configured network settings on the operator panel. To change IPv4 settings and configure IPv6 settings, go to **Setup > Network Mgmt.**
- You can return to the **Setup Wizard** from the Web client.
- Any administrators you create will also be able to use the Setup Wizard from the Web client as well as **Setup** and **Operations** menu commands to reconfigure the library.
- If necessary, you can cancel out of the **Setup Wizard** on the operator panel and begin using the library locally with the default settings in place. If you accept the default network configuration settings, you will not be able to access the library remotely from the Web client. You can, however, use **Setup > Network Mgmt** on the operator panel at any time to modify network settings. See [Default Configuration Settings](#) on page 60 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 media type. To mix tape drive types/media types within a partition, create partitions manually. See [Manually Creating Partitions](#) on page 74.

See also [About the Setup Wizard](#) on page 56 above.

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 license keys for licensable features. For more information, see [Obtaining and Installing a License Key](#) on page 88.
- [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 problems, the library snapshot will help technical support personnel to troubleshoot the problem. Saving the library configuration will allow you to restore the most current settings if necessary. For more information on taking a library snapshot and saving and restoring the library configuration, see [Saving and Restoring the Library Configuration](#) on page 384.

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

The paths to open the appropriate screens are as follows:

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

Accessing the Web Client

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

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

Managing the Network

Administrators can configure the following:

- Network settings that allow remote access to the library. For more information, see [Modifying Network Settings](#) on page 63.
- 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 65.
- 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 66.

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

Modifying Network Settings

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

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

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

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

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

Note: Make sure that the library is connected to the network before modifying network settings. If the Ethernet cable is not installed properly, you cannot configure the network settings. Install one end of the Ethernet cable in the top Ethernet port of the library control blade (LCB) just below the three LEDs. The LCB is located at the back of the 5U Library Control Module. Make sure the other end of the Ethernet cable is installed in the appropriate LAN port on your LAN.

Details on network settings include:

- **Library Name** is the network name you want to assign to the library. The library name is limited to 12 lowercase alphanumeric characters and dashes (-).
- **DHCP** defaults to enabled. When DHCP is enabled, the library obtains an IP address automatically. If DHCP is not enabled, you must manually enter an IP address, default gateway, and subnet mask/net prefix.
- **IPv4 addresses** must be entered in dot notation (for example, 192.168.0.1). They are limited to numeric characters and do not allow values exceeding 255 for dot-separated values.
- **IPv6 addresses** must be entered in the proper notation. IPv6 address can be entered in the most common notation, as eight groups of four hexadecimal digits. 2001:0ff8:55cc:033b:1319:8a2e:01de:1374 is an example of a valid IPv6 address. Also, if one or more of the four-digit groups contains 0000, you can omit the zeros and replace them with two colons (::), as long as there is only one double colon used in an address. Using this notation, 2001:0ff8:0000:0000:0000:0000:01de:1374 is the same as 2001:0ff8::01de:1374.
- **IP Address** is the IP address of the library. For IPv4, this text box is available only if DHCP is disabled.
- **Default Gateway Address** is the IP address of the default gateway for your portion of the Ethernet network. For IPv4, this text box is available only if DHCP is disabled.
- **Subnet Mask** (IPv4 only). Text box is available only if DHCP is disabled.
- **Network Prefix** (IPv6 only).

- **Primary DNS Address** (optional, Web client only) must be entered as an IP address. This text box is available only if DHCP is disabled.
- **Secondary DNS Address** (optional, Web client only) must be entered as an IP address. This text box is available only if DHCP is disabled.
- **Port Settings** (operator panel only) allows you to change the autonegotiate mode, speed, and duplex settings on the Ethernet port.

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

Note: Be sure to add the PowerVault ML6000's IP address to the list of trusted/allowed sites on your PowerVault ML6000-supported browser, so the Web client pages automatically refresh.

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

The paths to open the appropriate screens are as follows:

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

Enabling SSL

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

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

See the *Dell PowerVault ML6000 SMI-S Reference Guide* (document number HK592) 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 *Dell PowerVault ML6000 Basic SNMP Reference Guide*. For information on integrating MIBs with an SNMP management application, contact your network management application vendor.

Administrators can perform the following SNMP procedures:

- Register the IP addresses and port numbers of external management applications, enabling them to receive SNMP traps from the library. For more information, see [Registering External Management Applications](#) on page 67.
- Enable or disable support for SNMP v1 and v2c. SNMP v3 is enabled by default and cannot be disabled. For more information, see [Enabling SNMP Versions](#) on page 68.

- Choose which version of SNMP the library uses to report traps. You can choose SNMPv1 or SNMPv2. The default is SNMPv1.
- Modify the default SNMP community string, which is used as a password to authenticate GET and GET-NEXT SNMP v1 and SNMP v2c messages exchanged between the library and a remote management application. For more information, see [Modifying the SNMP Community String](#) on page 69.
- 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 70.
- 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 70.

Registering External Management Applications

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

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

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

- **Transport** – The transport protocol. This should be the same as the transport protocol configured on the SNMP trap receiver. Select one of the following:
 - UDP/UDP6 – User Datagram Protocol. For IPv4, select UDP; for IPv6, select UDP6.
 - TCP/TCP6 – Transmission Control Protocol. For IPv4, select TCP; for IPv6, select TCP6.
- **Host Name/IP Address** – The host name or the IP address of the external management application you want to register. A host name may be entered only if DNS is enabled. Otherwise, IP addresses must be entered. For information on DNS, see [Modifying Network Settings](#) on page 63.

- **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 *Dell PowerVault ML6000 Basic SNMP Reference Guide* for further configuration and access details.

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

The path to open the appropriate screen is as follows:

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

Enabling SNMP Versions

The library supports SNMP v1, v2c, and v3.

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

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

See the *Dell PowerVault ML6000 Basic SNMP Reference Guide* for further configuration and access details.

The paths to open the appropriate screens are as follows:

- From the Web client select **Setup > Network Management > SNMP**.
- From the operator panel select **Tools > System Settings > Enable SNMP V1/V2**.

Choosing SNMP Trap Versions

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

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

The path to open the appropriate screen is as follows:

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

Modifying the SNMP Community String

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

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

See the *Dell PowerVault ML6000 Basic SNMP Reference Guide* for further configuration and access details.

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

The path to open the appropriate screen is as follows:

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

Enabling and Disabling SNMP Authentication Traps

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

See the *Dell PowerVault ML6000 Basic SNMP Reference Guide* for further configuration and access details.

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

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

Downloading the SNMP MIB

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

For more information about the library MIB, see the *Dell PowerVault ML6000 Basic SNMP Reference Guide* or contact Dell Technical Support (see [Appendix C, Contacting Dell](#)). For information on integrating MIBs with an SNMP management application, contact your network management application vendor.

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

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

Working With Partitions

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

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

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

There are two ways to create partitions:

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

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

Table 3 Number of Partitions Supported

Available Configurations	Tape Drives Minimum, Maximum	Partitions Minimum, Maximum
ML6010	1, 2	1, 2
ML6020	1, 6	1, 6
ML6030	1, 10	1, 10
ML6030 CM + 1 ML6000 EM	1, 14	1, 14
ML6030 CM + 2 ML6000 EMs	1, 18	1, 18

Details on partitions include:

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

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

- The maximum number of partitions that can be created is equal to the number of tape drives in the library.
- At minimum, a partition consists of one tape drive and one slot. The tape drive or slot cannot be shared with another partition.
- I/E station slots are shared between all partitions. Partitions take temporary ownership of I/E station slots when importing or exporting tape cartridges.

Caution: Before permanently removing a 9U Library Expansion Module from your library, you need to perform a set of configuration operations that includes deleting all partitions. See [Deleting Partitions](#) on page 76 and [Removing the 9U Library Expansion Module](#) on page 286.

Automatically Creating Partitions

At any time after the initial configuration of the library, administrators can add to the number of existing partitions by using the automatic partitioning process. Automatic partitioning assigns available library resources proportionately among the partitions, grouping tape drives according to their interface type (SCSI, FC, or SAS) and media generation. The default number of partitions created is the number of distinct tape drive interface/media type combinations of the tape drives that are not currently assigned to a partition. You cannot mix tape drive interface types or media generations in partitions that you create automatically. To create a partition with mixed interface types and media generations you must create the partition manually (see [Manually Creating Partitions](#) on page 74).

For example:

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

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

The library must contain at least one unassigned tape drive and one unassigned slot to automatically create a partition. If no unassigned tape drives or slots exist, you must modify or delete one or more partitions to free up resources. For more information, see [Modifying Partitions](#) on page 75 and [Deleting Partitions](#) on page 76.

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

By default, the library applies the Standard barcode format to each partition. You can change this setting by modifying the partitions after it has been created. For information on modifying partitions, see [Modifying Partitions](#) on page 75.

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

The paths to open the appropriate screens are as follows:

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

Manually Creating Partitions

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

You can mix tape drive interface type and media generation in partitions that you create manually.

The library must contain at least one unassigned tape drive and slot to create a partition. If no tape drives or slots are available, you must modify or delete an existing partition to free up resources. For more information, see [Modifying Partitions](#) on page 75 and [Deleting Partitions](#) on page 76. When you manually create partitions, the library creates control paths. See [Working With Control Paths](#) on page 86 for a description of the default control paths and how to change them.

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

- **Partition Name** – Limited to a maximum of 12 lower-case alphanumeric characters and underscores (_)
- **Media Barcode Format** – This setting tells the library how to read and report barcodes of the tape cartridges in the partition. The library supports the following options (for definitions of each of the options, see [Supported Barcode Formats](#) on page 418).
 - **Standard** (default)
 - **Standard Six**
 - **Plus Six**
 - **Extended**
 - **Media ID Last**
 - **Media ID First**

- **Number of Slots** – The number of storage slots allocated to the new partition.
- **Drives** – The tape drive or drives assigned to the partition.

Note: Before creating partitions, verify that all tape drives are unloaded. For information on unloading tape drives, see [Unloading Tape Drives](#) on page 175.

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

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

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

Modifying Partitions

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

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

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

Note: If the operation does not complete successfully, the partition remains offline until you turn it back online manually or restart the library (see [Taking a Partition Online or Offline](#) on page 78).

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

- **Partition Name** – limited to a maximum of 12 lower-case alphanumeric characters and underscores (_).
- **Media Barcode Format** – This setting tells the library how to read and report barcodes of the tape cartridges in the partition. The default selection is **Standard** (for definitions of each of the options, see).
- **Number of Slots** – the number of tape cartridge slots allocated to the partition.
- **Drives** – the tape drive or drives assigned to the partition.

Note: Before deleting a tape drive from a partition, verify that it is unloaded. For information on unloading tape drives, see [Unloading Tape Drives](#) on page 175.

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

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

Deleting Partitions

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

Unload all tape drives and export all cartridges assigned to the partition that is to be deleted. After exporting the cartridges, remove them from the I/E station. For more information, see [Unloading Tape Drives](#) on page 175 and [Exporting Media](#) on page 172.

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 77.

- Because partitions may extend across the library's physical modules and share resources, the library will report errors if you permanently remove or replace a module in your library without first deleting or modifying partitions and modifying shared resources such as cleaning slots and I/E slots. See [Preparing to Remove or Replace a Module](#) on page 277 for detailed instructions on preparing your library for the permanent removal or replacement of a module.

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

The paths to open the appropriate screens are as follows:

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

Changing Partition Access

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

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

- **Password** – A unique password that can be viewed and modified by the administrator.
- **Privilege Level** – Determines the user's access privileges. See [User Privileges](#) on page 54 for more information on user privilege levels.
- **Partition Access** – the partitions to which the user has access.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Setup > User Management > User Accounts**.
- From the operator panel, select **Setup > User Mgmt > Modify User**.

Taking a Partition Online or Offline

There are two partition modes: online and offline.

- **Online** – SCSI hosts control the partition. In this mode, all host application SCSI commands are processed.
- **Offline** – SCSI hosts cannot control the partition. In this mode, library operations can be performed via the operator panel or Web client.

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

Details about changing the partition mode include:

- When you access the **Change Partition Mode** screens, you will see only partitions to which you have been given access.
- The **Online/Offline** buttons toggle between modes.
- If a partition is in use, the **Online/Offline** button is grayed out.
- Restarting the library will bring all offline partitions back online (see [Restarting the Library](#) on page 162).

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

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

The paths to open the appropriate screens are as follows:

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

Disabling/Enabling Manual Cartridge Assignment

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

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

For more information on how manual cartridge assignment affects importing of media, see [Importing Media](#) on page 165.

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, see [Configuring System Settings](#) on page 126.

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.

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

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

it notifies the library. If AutoClean is enabled, the library automatically cleans the tape drive using a cleaning cartridge loaded in a cleaning slot.

Note: If you configure zero I/E station slots, you will not be able to import or export cleaning cartridges using I/E stations. See [Configuring I/E Station Slots](#) on page 81.

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

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

Administrators can configure cleaning slots during the initial library configuration and at any time after that, as long as unassigned slots are available. If no slots are available in the library, you must modify or delete a partition to free up slots. For more information see [Modifying Partitions](#) on page 75 and [Deleting Partitions](#) on page 76.

Administrators can also clean tape drives manually. For information, see [Manually Cleaning Tape Drives](#) on page 183.

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

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

The paths to open the appropriate screens are as follows:

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

Configuring I/E Station Slots

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

Each 5U Library Control Module contains six I/E station slots, and each 9U Library Expansion Module contains 12 I/E station slots. The available library configurations support a minimum of six I/E slots in the 5U library to a maximum of 54 I/E slots in the 41U library configuration. You can also choose to configure zero I/E station slots and use all slots in all I/E stations for tape cartridge storage. For more information on configuring zero I/E slots, see [Configuring Zero I/E Station Slots](#) on page 83.

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 an ML6010 CM, all six I/E station slots must be configured either as storage or as I/E station slots. The ML6020 CM consists of a 5U Library Control Module (with six I/E station slots) and a 9U Library Expansion Module (with 12 I/E station slots). All 12 of the slots in the 9U Library Expansion Module must be configured the same way, as either I/E station slots or storage slots. Therefore, the ML6020 CM can contain a minimum of six and a maximum of 18 dedicated I/E station slots. [Table 4](#) lists the number of I/E station slots available per library for all base library configurations.

Table 4 Number of I/E Station
Slots Available

Details on configuring I/E station slots include:

Library Configuration	5U Library Control Control Module		9U Library Expansion Module		Library Total	
	I/E Stations	I/E Slots	I/E Stations	I/E Slots	I/E Stations	I/E Slots
ML6010 CM	1	6	-	-	1	6
ML6020 CM	1	6	1	12	2	18
ML6030 CM	1	6	2	24	3	30
ML6030 CM + 1 ML6000 EM	1	6	3	36	4	42
ML6030 CM + 2 ML6000 EMs	1	6	4	48	5	54

- 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 5U Library Control Module.
- If you increase the size of your library by adding 9U Library 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 5U Library Control Module I/E station first and then works outward to the I/E stations in the 9U Library Expansion Modules. I/E stations in 9U Library Expansion Modules below the 5U Library Control Module have precedence over

I/E stations in 9U Library Expansion Modules above the 5U Library 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 9U Library Expansion Modules, and you configure an even number of I/E slots greater than six, the 5U Library 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 185.
- I/E station slots are shared by all partitions within a library.
- To identify how a specific I/E station magazine is configured, view the **Library Configuration** report available from the **Reports** menu on the Web client. See [Viewing the Library Configuration Report](#) on page 190.

Configuring Zero I/E Station Slots

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

- You will not be able to use the I/E station to import and export tape cartridges, including cleaning media.
- You will be required to open the library access door to bulk load and unload tape cartridges, disrupting library operations. See [Bulk Loading](#) on page 169.
- 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 161.

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

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

The paths to open the appropriate screens are as follows:

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

Setting Tape Drive Parameters

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

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

Note: If the operation does not complete successfully, the partition remains offline until you turn it back online manually or restart the library (see [Taking a Partition Online or Offline](#) on page 78).

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

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

- 5U Library Control Module: 1 and 2
- Each 9U Library 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 5U Library Control Module is assigned a default loop ID of 61. The tape drive installed in the 5U Library Control Module's bottom drive bay is assigned a default loop ID of 63.

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

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

- The requested topology connection mode can be set to one of the following:
 - **Auto (LN)** – Auto-configure trying L-Port first
 - **Loop (L)** – Force L-Port
 - **Point to Point** – Force N-Port
 - **Auto (NL)** – Auto-configure trying N-Port first (default)

Notes About Point to Point:

- You can use Point to Point if the tape drive is connected via a switch.
- You cannot use Point to Point if the tape drive is connected to an FC I/O blade or connected directly to a host.

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

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

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

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

The paths to open the appropriate screens are as follows:

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

Working With Control Paths

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

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

Table 5 Control Path
Assignment During Partition
Creation

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

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

different tape drive. You can also disable a partition's control path by clearing the current control path selection.

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

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

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

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

The paths to open the appropriate screens are as follows:

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

Obtaining and Installing a License Key

Several features can be added to the standard library configuration either with your initial purchase or afterward (see [Licensable Features](#) on page 35).

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

- [About License Keys](#)
- [Viewing Licenses and License Keys](#)
- [Obtaining a License Key](#)
- [Applying a License Key](#)

About License Keys

If you purchase a licensable feature with your library, the license will be installed when you receive the library. If you upgrade or add new features after the initial purchase, Dell issues you a license key certificate. The license key certificate contains an authorization code that enables you to retrieve your license key from the PowerVault ML6000 Web site. Once you install the license key on the library, the feature becomes available.

Details about license keys include:

- An authorization code to obtain a license key can be used one time only.
- The license key may contain up to 12 alphanumeric characters. The license key can also contain the “at” (@), hyphen (-), or underscore (_) symbols. Alpha characters must be lowercase. The user interface automatically converts entries to lowercase.
- A given license key can only be used on the library to which it is assigned and cannot be transferred to another library. The key is verified when it is applied to the library to make sure it is the proper key associated with the library serial number.
- License keys do not expire.
- Once installed on the library, license keys cannot be removed (unless you replace the control 5U Library Control Module or the library control blade (LCB) compact flash card).
 - **If you replace the 5U Library Control Module:** The license key is associated with the serial number of the 5U Library Control Module. If you replace your 5U Library Control Module, you must replace all your installed license keys. Request replacement license keys from Dell.
 - **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 site listed above. In some cases, factory installed license keys will not be listed on the Web site and you will need to contact Dell for a replacement. If you cannot retrieve your license keys or need assistance, contact Dell.

Viewing Licenses and License Keys

To see the license keys you have purchased and obtained, go to <http://www.dell.com/tapeautomation> and select from the list of ML6000 licensable options.

The license history for each feature is listed (feature licensed, amount licensed, authorization code, and date license key was obtained). The most recent license contains the full amount of the license for that feature (for example, the most recent COD license contains the total number of COD slots licensed) and replaces previous license keys.

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

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

Obtaining a License Key

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

- 1 Contact your Dell technical sales representative to submit your order for the feature or upgrade. See [Appendix C, Contacting Dell](#).
- 2 Upon receipt of your order, Dell will ship you a license key certificate containing your authorization code.
- 3 On your PowerVault ML6000, locate your Dell Service Tag and serial number. Make note of these items. You will need them to retrieve your license key from the Web site. To view the Dell Service Tag and serial number:
 - On the operator panel, select **Tools > About Library**, or
 - On the Web client, select **Reports > About > ML6000**.
- 4 Access the features Web site at: <http://www.dell.com/tapeautomation>. Under ML6000, select the feature you want.
- 5 In the **Service Tag** box, enter your Dell Service Tag number.

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

Note: The serial number you enter here cannot be transferred to another Dell Service Tag at a later time

- 7 Click the **Search** button (=>).

If you have entered a valid Service Tag/serial number combination, the Web site displays existing license keys for this feature. Exception: If the license was applied at the factory, the word "**Factory**" may appear instead of the actual license key. If you need to retrieve the license key in this case, contact Dell Technical Support (see [Appendix C, Contacting Dell](#)).

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

- 9 Click the **Get License Key** button(=>).

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

- 10 To enter another authorization code for another license key, click **Enter Additional Authorization Code**.

You are now ready to apply the license key to the PowerVault ML6000. 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 increased capacity is purchased, the new license key will replace the current license key.

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

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

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

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

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

The paths to open the appropriate screens are as follows:

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

Setting Customer Contact Information

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

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

The paths to open the appropriate screens are as follows:

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

Configuring the Library E-mail Account

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

Before configuring the e-mail account, ask your network administrator for an IP address, valid login account (optional), and valid password (optional) for your SMTP server. The login account name and password can contain the following special characters: @ and #. E-mail account settings are not case-sensitive.

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

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

- **SMTP Server** includes the IP address or host name of the SMTP server. IP addresses must be entered in dot notation (for example, 192.168.0.1) and cannot exceed 255.
- **Sender E-mail Address** includes an e-mail address for the library (for example, "libraryname@mycompany.com"). The library uses this address in the **From** field of e-mail messages that it sends out, indicating the originator of the message.

Send snapshot with e-mail notifications instructs the library to automatically attach a library snapshot file (ASCII format) to certain RAS ticket e-mail notifications (see [Working With RAS E-mail Notifications](#) on page 94). (Snapshots are only auto-generated for this purpose if they help to clarify or diagnose the problem.) This feature is turned off by default. Library snapshot files can also be sent to specified e-mail addresses using the **Capture Snapshot** operation (see [Capturing Snapshots of Library Information](#) on page 381). If the library is in the process of capturing an automatic snapshot, you will not be able to manually capture a snapshot via the Web client until the automatic snapshot is complete. If this happens, an error message will display. Wait about 10 minutes and try again.

- **Authentication** includes a means to enter the login account name and password for the library. Selecting the box enables use authentication. Clearing the box disables use authentication. The following fields are only available if use authentication is enabled:
 - **Login Account** includes the name of a valid account on the SMTP server (for example, "John.User"). The login account name can contain the following special characters: @ and #.
 - **Password** is the password for the account that you specified in the **Login Account** text box. The password can contain the following special characters: @ and #.

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

After configuring the e-mail account, save the library configuration. For information, see [Saving and Restoring the Library Configuration](#) on page 384.

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

The paths to open the appropriate screens are as follows:

- From the Web client, select **Setup > Notifications > E-mail Configuration**.
- From the operator panel, select **Setup > Notification > E-Mail Account**.

Working With RAS E-mail Notifications

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

Before you can configure e-mail notifications, you must configure the library's e-mail account so that the library can send notifications to the designated recipients. See [Configuring the Library E-mail Account](#) on page 92 for information on how to configure the e-mail account.

See [Creating RAS E-mail Notifications](#) on page 95 for information on setting up additional e-mail notifications. The library supports a maximum of 20 e-mail notification recipients.

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

There are three e-mail notification filter levels:

- **Low Filter** – Notifies e-mail recipients of all RAS tickets and information notifications.
- **Medium Filter** – Notifies e-mail recipients of high-severity (Severity 2) and urgent (Severity 1) RAS tickets.
- **High Filter** – Notifies e-mail recipients of urgent (Severity 1) RAS tickets only.

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

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

The paths to open the appropriate screens are as follows:

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

Creating RAS E-mail Notifications

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

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

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

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

The path to open the appropriate screen is as follows:

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

Modifying RAS E-mail Notifications

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

The path to open the appropriate screen is as follows:

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

Deleting RAS E-mail Notifications

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

The path to open the appropriate screen is as follows:

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

Working With User Accounts

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

Local Authentication vs. Remote Authentication

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

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

To use remote authentication, you must enable LDAP on the library. Once LDAP is enabled, users can log into the library using either LDAP or local authentication. See [Logging In When LDAP or Kerberos is Enabled](#) on page 164 for more information.

About Local User Accounts

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

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

The library ships with a default administrator account. The user name for this account is **admin** and the password is **password**. You cannot delete this user account or change the user name, but you can change the password. The default administrator account is used to perform the initial configuration of the library. If you misplace the password for the default administrator account, contact Dell Technical Support. See [Appendix C, Contacting Dell](#).

See [User Privileges](#) on page 54 for more information on library permission levels. For information on changing passwords, see [Modifying Local User Accounts](#) on page 98.

Creating Local User Accounts

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

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

- **User Name** – the login name of the user account you are creating. User names are limited to 1-12 lower-case letters, numbers, and underscores (_). For example: **john_usa**.
- **Password** – the unique password for the user account you are creating. Passwords are limited to 6-16 lower-case alphanumeric characters and can include also include underscores (_), periods (.), hyphens (-), asterisks (*), and the “at” symbol (@). For example: **pass_19**.
- **Privilege** – is set to either **User** or **Admin**. See [User Privileges](#) on page 54 for more information on user privilege levels.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Setup > User Management > User Accounts**.
- From the operator panel, select **Setup > User Mgmt> Create User**.

Modifying Local User Accounts

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

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

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

- **Privilege** — set to either **User** or **Admin**. See [User Privileges](#) on page 54 for more information on user privilege levels.
- **Partition Access** — the partitions to which this user has access. Any user assigned to a partition that has been deleted can be reassigned to other partitions.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Setup > User Management > User Accounts**.
- From the operator panel, select **Setup > User Mgmt > Modify User**.

Deleting Local User Accounts

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

Note: The default administrator account cannot be deleted.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Setup > User Management > User Accounts**.
- From the operator panel, select **Setup > User Mgmt > Modify User**.

Configuring LDAP

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

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

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

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

LDAP Server Guidelines

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

- **Library user group** — Assign users to this group who need user-privilege access to the library. Enter the name of this group in the **Library User Group** field on the **Setup - Remote Authentication** screen on the library Web client (see [Configuring LDAP on the Library](#) on page 101).
- **Partition groups** — For LDAP users with user privileges, access to library partitions is determined by group assignment on the LDAP server. Groups must be created on the LDAP server with names that match the library partition names (names must match but are not case sensitive). Users with user privileges must be assigned to these groups on the LDAP server to have access to the corresponding partitions on the library.
- **Library admin group** — Assign users to this group who need administrator-privilege access to the library. LDAP users with administrator privileges have access to all partitions and administrator functions and do not need to be assigned to partition-related groups on the LDAP server. Enter the name of this group in the **Library Admin Group** field on the **Setup - Remote Authentication** screen on the library Web client (see [Configuring LDAP on the Library](#) on page 101).

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

Configuring Secure LDAP on the Library

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

- **LDAPS** — Uses Secure Sockets Layer (SSL) over a specific port for LDAP (636). You may enable LDAP over SSL (LDAPS) by entering a URI in the form of “ldaps://hostname” in the Server URI field. This will use SSL to send secure communication via port 636. If the LDAP server does not support LDAPS or does not have LDAPS enabled,

then login operations will fail. LDAPS has been deprecated in favor of using StartTLS (see option below). Do not use LDAPS if you are using StartTLS. Once you apply LDAPS, StartTLS will not be available.

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

Installing an LDAP TLS CA Certificate

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

Configuring LDAP on the Library

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

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

Examples:

ldap://hostname:389

ldap://10.50.91.103

ldap://mycompany.com

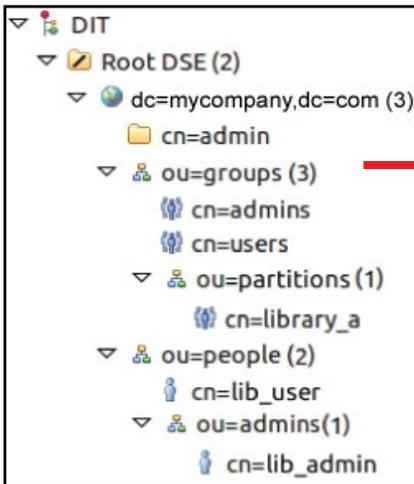
- **LDAPS** — Optional. See [Configuring Secure LDAP on the Library](#) on page 100.

- **StartTLS** — Optional. See [Configuring Secure LDAP on the Library](#) on page 100.
- **Install TLS CA Certificate** — Optional. See [Installing an LDAP TLS CA Certificate](#) on page 101.
- **Remove TLS CA Certificate** — This check box is available if a TLS CA certificate is installed. You can remove the certificate by selecting this check box. The certificate will be removed after you click **Apply**.
- **Principal** — An LDAP user login ID with permissions to search the LDAP directory. The library logs on to LDAP using this ID. For an example, see [Figure 15](#) on page 103.
- **Password** — The password for the principal authorization login ID.
- **User DN** — The Fully Qualified Distinguished Name that contains the users. For an example, see [Figure 15](#) on page 103.
- **Group DN** — The Fully Qualified Distinguished Name that contains the groups. For an example, see [Figure 15](#) on page 103.
- **Library User Group** — The value of the Common Name attribute for the group entry on the LDAP server associated with library users who have user-level privileges (see [User Privileges](#) on page 54 for information on privilege levels). This group must exist on your LDAP server (see [LDAP Server Guidelines](#) on page 100). For an example, see [Figure 15](#) on page 103.
- **Library Admin Group** — The value of the Common Name attribute for the group entry on the LDAP server associated with library users who have administrator-level privileges (see [User Privileges](#) on page 54 for information on privilege levels). This group must exist on your LDAP server (see [LDAP Server Guidelines](#) on page 100). For an example, see [Figure 15](#).

Figure 15 LDAP Setup
Example

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

Simple LDAP Server Configuration:



Setup - Remote Authentication
Authenticate logins against a third-party service.

Authentication Type:
Local Only: LDAP: LDAP with Kerberos:

LDAP Server

Server URI:
 StartTLS:
 Install TLS CA Certificate:
 Remove TLS CA Certificate:
 Principal:
 Password:
 Confirm Password:

Authorization

User DN:
 Group DN:
 Library User Group:
 Library Admin Group:

User: Password:

*Apply any changes to the settings before
Test with a user that belongs to both the User*

Testing LDAP Settings

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

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

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

After configuring LDAP settings, save the library configuration.

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

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

The path to open the appropriate screen is as follows:

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

Configuring Kerberos

Use Kerberos if you want extra security with remote authentication.

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

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

- **Realm** – The Kerberos realm name, typed in all uppercase letters. Usually the realm name is the DNS domain name.
Example: MYCOMPANY.COM
- **KDC (AD Server)** – The key distribution center (in other words, the server on which Kerberos/ Active Directory is installed).
Example: mycompany.com:88
- **Domain Mapping** – The domain portion of the library's fully qualified domain name.
Example: mycompany.com
- **Service Keytab** – Click the **Browse** button to select the service keytab file. The service keytab file is a file you generate on your Kerberos/ Active Directory server. See [Generating the Service Keytab file](#) on page 105.

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

The path to open the appropriate screen is as follows:

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

Generating the Service Keytab file

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

- 1 Set up an Active Directory domain on the Windows server.
- 2 If Active Directory is not already configured, run **dcpromo**.
- 3 **Windows 2003 servers only:** Install Windows Support Tools on the Windows 2003 server as follows:
 - a Go to www.microsoft.com and search for “windows server 2003 support tools sp2” or click on the following link:
<http://www.microsoft.com/downloads/details.aspx?FamilyID=96a35011-fd83-419d-939b-9a772ea2df90&DisplayLang=en>
 - b Download both **support.cab** and **suptools.msi**.
 - c Run **suptools.msi** to begin installation.
- 4 Create a computer account in Active Directory.
 - Do not select any of the check boxes during creation.
 - The account name will be used for <computer account> fields shown in the following steps.
- 5 At the command prompt, map SPN to the computer account. Use the following format:

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

For example:

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

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

- **For Windows 2003:**

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

For example:

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

- **For Windows 2008:**

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

For example:

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

Setting the Date, Time, and Time Zone

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

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

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

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

Setting the Date and Time Manually

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

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

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

Setting the Date and Time Using the Network Time Protocol

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

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

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

Details on NTP settings include:

- NTP servers must be configured in available in groups of 3 or more, with one exception: a single NTP server configuration is also allowed.
- NTP is enabled on the **Date & Time** screen. When NTP is enabled, you cannot manually configure date and time. For more information on setting date and time manually, see [Setting the Date and Time Manually](#) on page 107.
- You can enter an IP address for a primary and an alternate (optional) NTP server.
- NTP server IP addresses must be entered in the proper format. See [Modifying Network Settings](#) on page 63 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-3, LTO-4, LTO-5 and LTO-6 FC drives. The number of FC I/O blades in any library configuration cannot exceed four, and each FC I/O blade in the library supports up to four FC tape drives.

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

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

- **Channel zoning** allows you to control access between FC I/O blade ports configured for host servers and ports configured for target devices. For more information, see [Configuring FC I/O Blade Channel Zoning](#) on page 111.
- **Host Mapping** allows you to control visibility to target devices and access from individual host servers to target devices. For more information, see [Managing FC Hosts and Host Mapping](#) on page 113.

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

- [Fibre-Channel Input/Output Blades](#) on page 29
- [Controlling FC I/O Blade Power](#) on page 187
- [Viewing FC I/O Blade Information](#) on page 197
- [Viewing FC I/O Blade Port Information](#) on page 197
- [Cabling Libraries With Fibre Channel Tape Drives Connected to Fibre Channel I/O Blades](#) on page 228
- [Recommended Library Cabling for FC I/O Blades](#) on page 234

- [Identifying FC I/O Blades](#) on page 393
- [Resetting FC I/O Blade Ports](#) on page 394

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

Configuring FC I/O Blade Ports

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

Each FC I/O blade has six ports. Ports 1 and 2 are always target ports and are configurable. Ports 3 through 6 are always initiator ports and are not configurable. For information on viewing the current configured settings for all I/O blade ports, see [Viewing FC I/O Blade Port Information](#) on page 197.

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 384.

The paths to open the appropriate screens are as follows:

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

FC I/O Blade Internal Virtual Port for Media Changers

FC I/O blades use an internal virtual port to access the media changer devices (partitions). Each FC I/O blade can access all media changer devices, except those that are defined in association with drive-based access (also known as “LUN-1”). The PowerVault ML6000 library can have up to 18 partitions. These internal virtual ports are not configurable via channel zoning; thus, all media changer devices are accessible via ports 1 and 2 of each FC I/O blade present within the library. This may lead to one or more media changer devices being discovered multiple times, depending on how the system is connected to host servers (for example, if four partitions are defined in a system that has two FC I/O blades, there would be four media changer devices visible on ports 1 and 2 of both FC I/O blades, for a total of 16). To minimize unnecessary discovery of media changer devices, you need to configure host mapping. See [Managing FC Hosts and Host Mapping](#) on page 113.

Configuring FC I/O Blade Channel Zoning

When FC I/O blades are installed in the library, administrators can configure channel zoning for selected FC I/O blades. Channel zoning, also called port zoning, configures access to an entire FC and all the LUNs on that channel for the exclusive use of a host or group of hosts on a single port. Channel zoning enables you to control access between specific target ports 1 and 2 and initiator ports 3–6 on an FC I/O blade.

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

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

Details on configuring channel zoning include:

- By default, all target FC ports (ports 1 and 2) on an FC I/O blade have access to all initiator ports (ports 3–6).
- Changing channel zoning setting will cause the affected FC I/O blade to reboot.
- If host port failover is enabled on the FC I/O blade, channel zoning must be configured so that all target FC ports have access to all initiator ports. For information on host port failover, see [Configuring FC Host Port Failover](#) on page 119.
- The **Setup - FC I/O Blade Channel Zoning** screen on the Web client lists all FC I/O blades found in the library. FC I/O blades are listed by the following: location in the library, WWNN, and status. The corresponding **Channel Zoning Select Blade** screen on the operator panel lists the location in the library and state. You can select the FC I/O blade you want to configure for channel zoning and proceed to the next screen.
- The two FC target ports (ports 1 and 2) and the four FC initiator ports (ports 3–6) are displayed in a grid, with the target ports listed in columns and the initiator ports listed in rows. Check boxes allow you to associate a target port with an initiator port.
 - To permit access, select the check box at the intersection of the target port and the initiator port. You can associate each initiator port with more than one target port.
 - To restrict access, clear the check box at the intersection of the target port and the initiator port.
 - When you select a check box, the entire FC channel is zoned. This zoning affects any host application that might be accessing the FC I/O blade. If both channel zoning and host mapping are enabled, the channel zoning settings supersede any host LUN mapping on the FC I/O blade.
 - After configuring channel zoning, save the library configuration. For instructions on how to save the library configuration, see [Saving and Restoring the Library Configuration](#) on page 384.

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

The paths to open the appropriate screens are as follows:

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

Managing FC Hosts and Host Mapping

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

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

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

Enabling/Disabling FC Host Mapping

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

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

The paths to open the appropriate screens are as follows:

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

Viewing FC Host Information

The following information is provided for FC hosts:

- **Host Name** – The host device name
- **I/O Blade** – The location of the FC I/O blade in the library
- **Status** – The online/offline (connectivity) status of the host (Web client only)
- **Host Port** – The host port number
- **WWPN** – The World Wide Port Name of the host device
- **Type** – The operating system of the host device

The paths to open the appropriate screens are as follows:

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

Creating, Modifying, and Deleting an FC Host Connection

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

After creating, modifying, or deleting an FC host connection, save the library configuration. For instructions on how to save the library configuration, see [Saving and Restoring the Library Configuration](#) on page 384.

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

Creating an FC Host Connection

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

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

Modifying an FC Host Connection

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

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

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

Deleting an FC Host Connection

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

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

Note: If the host application is connected through an FC switch, a power cycle of the I/O blade might be required to make the host go offline. For instructions on how to power cycle an I/O blade, see [Controlling FC I/O Blade Power](#) on page 187.

The paths to open the appropriate screens are as follows:

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

Host Mapping - Overview

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

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

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

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

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

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

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

Host Mapping Vs. Channel Zoning

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

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

Note: On the operator panel, the host mapping screens (**Setup > FC I/O Blades > Host Mapping**) are not available unless FC host mapping is enabled. See [Enabling/Disabling FC Host Mapping](#) on page 113.

Configuring Host Mapping

To configure host mapping, you need to select the media changer device (partition) or tape drive you want to map and assign a new LUN number for the device.

Note: Depending on host operating system constraints, it might be necessary to reboot or reconfigure the host due to device mapping changes that result from configuring host mapping.

Details on configuring host mapping include:

- Host mapping is an optional feature and is disabled by default. For instructions on how to enable or disable host mapping, see [Enabling/Disabling FC Host Mapping](#) on page 113.
- The **Setup - I/O Blade Host Mapping** screen on the Web client lists the host name, I/O blade location, World Wide Port Name (WWPN), and operating system type of each available FC host. You can select the FC host to configure and proceed to the next screen.

The screen lists the available partitions and tape drives connected to the FC I/O blade to which the FC host is attached. For each available partition and tape drive, the screen lists the following:

- **Description** – For tape drives: Drive [location coordinates] [(associated partition)]. For partitions: the name assigned to the partition during the partition creation process.
- **Type** – Device type, for example, processor, media changer (partition), tape drive.
- **Serial Number** – Serial number of the partition or tape drive.
- **Vendor** – Device manufacturer.
- **Product** – Name of the device.
- **LUN** – Current logical unit number (LUN) assignment. Assign a new LUN number for the device.

Note: The operator panel host mapping configuration screens show less information about each device; however, you still select the host and device(s) and configure the LUN number(s.).

- After configuring FC host mapping, save the library configuration. For instructions on how to save the library configuration, see [Saving and Restoring the Library Configuration](#) on page 384.

Note: A warning message will display if the command and control LUN (CCL) or another device is not mapped to LUN 0 (zero). LUN 0 is typically occupied by the command and control LUN (CCL), unless it has been manually mapped to another LUN. Make sure at least one device is mapped to LUN 0.

Note: If an FC switch is attached to an FC I/O blade target port, the FC switch will appear in the Blade Host Management list as if it were an FC host. Do not map library devices to an FC switch. To avoid confusion, it is recommended that you modify the FC switch host name and type using Blade Host Management. See [Modifying an FC Host Connection](#) on page 115.

Note: If both channel zoning and host mapping are enabled, the channel zoning settings supersede any host LUN mapping on the FC I/O blade. For information on channel zoning, see [Configuring FC I/O Blade Channel Zoning](#) on page 111.

The paths to open the appropriate screens are as follows:

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

Configuring FC Host Port Failover

When FC I/O blades are installed in the library, administrators can enable and configure the optional FC host port failover feature. This feature is disabled by default.

You can configure the FC host port failover feature so that a “standby” target port (1 or 2) on an I/O blade can assume the identity and LUN mapping configuration of the designated “active” target port if the active port fails. Host port failover enables the library to continue operations without requiring you to reconfigure the host or the SAN.

To enable host port failover, you must configure target ports 1 and 2 on the FC I/O blade as point-to-point connections (**Setup > FC I/O Blades > Port Configuration**). FC I/O blade target ports 1 and 2 must be attached to the same SAN fabric to provide host access. The primary active port is used for host communications, while the passive standby port is kept idle. In addition, channel zoning must be configured so that target ports 1 and 2 have access to all initiator ports (ports 3–6) (**Setup > FC I/O Blades > Channel Zoning**). If these conditions are not met, an error message will display when you attempt to enable host port failover.

Note: The current feature implementation does not support arbitrated loop or target/initiator mode.

Note: Ports on the 4 Gb FC I/O blade used for failover must connect to the same SAN fabric.

Note: When both target ports on the FC I/O blade are attached to the same SAN fabric, you may see duplicate media changer devices (partitions) being reported. To stop this from happening, you need to enable host port mapping and configure host mapping. For more information, see [Configuring Host Mapping](#) on page 118.

Note: When Fibre Channel port 2 is selected to be the active port in a host port failover configuration, the active port can switch to the default setting, port 1, following a reboot. Reconfigure the host port failover settings so that the intended port is the active port.

For information on configuring FC I/O blade ports and channel zoning, see [Configuring FC I/O Blade Ports](#) on page 110 and [Configuring FC I/O Blade Channel Zoning](#) on page 111.

The library generates a Reliability, Availability, and Serviceability (RAS) ticket when port failover occurs. Examine the ticket to determine the reason for the failover. When the failed port is repaired, the port must be re-enabled to make it available for host port failover as the standby or active port. For more information, see [Repairing and Enabling a Failed Target Port](#) on page 121.

Details on configuring host port failover include:

- The **Setup - Host Port Failover** screen displays all the FC I/O blades found in the library. FC I/O blades are listed by the following: location in the library, WWNN (Web client only), and status/state. You can select the FC I/O blade you want to configure for host port failover and proceed to the next screen.
- To enable FC host port failover for the selected FC I/O blade, you can select a check box to enable FC Host Port Failover. Clearing the check box disables FC host port failover for the selected FC I/O blade.
- If you are enabling FC host port failover, select one target port on the FC I/O blade as the **Active Port**. The selected target port becomes active by default. The other target port will go on passive standby until failover occurs.
- After enabling or disabling FC host port failover, save the library configuration. For instructions on how to save the library configuration, see [Saving and Restoring the Library Configuration](#) on page 384.

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

- The paths to open the appropriate screens are as follows:
- From the Web client, select **Setup > I/O Blades > Host Port Failover**.
- From the operator panel, **Setup > I/O Blades > Host Port Failover**.

Repairing and Enabling a Failed Target Port

After host port failover occurs, the failed target port must be repaired and enabled before it can be configured as an active or standby port for the host port failover feature. To repair the failed port, use the information in the RAS ticket that was generated when the host port failover occurred. For information on viewing and resolving RAS tickets, see [About RAS Tickets](#) on page 377.

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 384.

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

For information on how to configure the repaired port as the standby or active target port, see [Configuring FC Host Port Failover](#) on page 119.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Setup > I/O Blades > Host Port Failover**.
- From the operator panel, **Setup > I/O Blades > Host Port Failover**.

Working With Data Path Conditioning

When I/O blades are installed, administrators can configure data path conditioning, an automatic means of verifying, monitoring, and protecting data path integrity between FC I/O blades and FC tape drives. Data path conditioning allows you to proactively detect and resolve data path problems before they affect backup, restore, and other data transfer operations.

The I/O blade does not manage data path conditioning along the path between the host and the I/O blade. It does manage data path conditioning along the path between itself and the FC tape drives. Data path monitoring automatically occurs at regular, configurable intervals. The I/O blade generates a RAS ticket if the monitoring tests fail for two intervals.

To configure data path conditioning, set the following parameters for the selected I/O blade:

- The level at which the data path is monitored between an I/O blade and the FC tape drives connected to it. The two levels are as follows:
 - **Interface Test** – performs tests to verify that FC controllers on I/O blades are responsive to commands. This is the default level.
 - **Device Datapath Test** – performs tests at the Interface Test level and also performs a device inquiry on each target device.
- **Test Interval** – the time interval between monitoring checks. You can configure the test interval. It can range from 5 to 2,880 minutes (48 hours). If you do not configure the test interval, the default test interval is 60 minutes. If you disable data path conditioning and then re-enable it in the future, the interval reverts to the default of 60 minutes regardless of whether you changed the interval previously.

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

The paths to open the appropriate screens are as follows:

- From the Web client, select **Setup > I/O Blades > Data Path Conditioning**.
- From the operator panel, select **Setup > I/O Blades > Data Path Conditioning**.

Configuring Library Security Settings

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

- **Network Interface** – Enables external access to the library over Ethernet. This setting is enabled by default to allow external access.
- **SSH Services** – Opens port 22 to allow Secure Shell (SSH) services, to access the library. This setting is enabled by default.
- **ICMP** – Enables external attempts to discover the library by pinging it (by means of the Internet Control Message Protocol [ICMP] Echo packets). This setting is enabled by default.
- **Remote UI** – Opens port 80 to allow remote access to the library via the Web client. This setting is enabled by default.
- **SNMP** – Opens port 161 to allow SNMP communication to the library. This setting is enabled by default.

Note: This setting differs from enabling SNMP services in the **Tools > System Settings** menu (see [Enable SNMP V1/V2](#) on page 129). In order to run SNMP, the port must be open and the SNMP services must be enabled.

- **SMI-S** – Opens port 5988 to allow SMI-S communication to the library. This setting is enabled by default.

Note: This setting differs from enabling the SMI-S service in the **Tools > System Settings** menu (see [Enable SMI-S](#) on page 129). In order to run SMI-S, the port must be open and the SMI-S service must be enabled.

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

- From the operator panel, select **Tools > Security**.

Configuring the Internal Network

Use the **Internal Network Configuration** screen to configure your library's internal network setting. The default internal network address is **10.10.10.X**.

The library's internal network enables communication among library components. While rare, it is possible that the default addressing of the internal network could conflict with your network, potentially causing the library to become confused. When installing the PowerVault ML6000 library, make sure that the external network setting is different from the internal network setting on the library. If DHCP is enabled or you do not know what your external network setting is, check with your network administrator.

Caution: Do not change the library's internal IP address during backup/restore operations.

From the operator panel, administrators can change the setting of the internal network using the **Internal Network Configuration** screen. Select the new internal IP address from the list on the screen. You can select from nine IP addresses.

The **Internal Network Configuration** screen is only accessible from the operator panel. The path to open the appropriate screen is as follows:

- From the operator panel, select **Tools > Internal Network**.

Configuring System Settings

This section describes the system-wide settings you can configure on the library. Each setting is described in detail below.

Details on the system settings include:

- The only setting users with User privileges can configure is the **Touch screen audio** setting.
- Administrators can configure all the system settings.
- All of the system settings are available on the operator panel. The only settings available on the Web client are user session timeout and unlabeled media detection.

The paths to open the appropriate screens are as follows:

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

User Session Timeout (minutes)

The library automatically logs out a user or administrator when the library has detected no activity for a specified length of time. You can adjust the user session timeout by entering a numeric value in the **User session timeout (minutes)** text box. Valid user session timeout values are 15 minutes to 480 minutes. You can change this setting from either the operator panel or the Web client. When you change the setting on the operator panel, the Web client is updated at the same time, and vice versa.

- **Touch Screen Audio** — Allows you to enable or disable the beep sound that occurs each time you press a button on the operator panel. The **Touch screen audio** setting is enabled by default.
- **Unload Assist** — Allows you to specify whether the library should automatically eject cartridges from tape drives. When the setting is enabled, the library will assist with tape drive unload operations in the event that a tape drive is not unloaded by a host command. When the setting is disabled, the library will not assist with tape drive unload operations and reject a move request from a tape drive, if the cartridge is not already unloaded. The **Unload Assist** setting is enabled by default.

The paths to open the appropriate screens are as follows:

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

Tape Drive Logical SN Addressing

The library assigns a fixed logical serial number to each tape drive slot in the library (whether it is occupied or not). When the **Logical SN Addressing** setting is enabled, the library reports only the logical serial number to the host instead of the tape drive's physical serial number. If the tape drive is later replaced by another tape drive in the same slot, the logical serial number remains the same. From the host application's perspective, the replacement tape drive is the same as the original. Logical SN Addressing is enabled by default.

When the Logical SN Addressing setting is disabled, the library reports only the tape drive physical serial number to the host.

The library System Information Report shows both the logical and physical serial numbers on installed tape drives for your convenience (**Reports > System Information**).

Caution: If you change the logical serial number addressing setting, you must power cycle the library in order for the change to take effect.

Caution: Use caution with this feature, as it can be accessed by both Admin and Service login users. Enabling this feature in an existing installation will change the presentation of the tape drive serial numbers to the host computer and host applications. Some host operating systems, and some application software, will no longer see a tape drive if the serial number changes (by use of this feature) from a previously set host configuration. If this happens, you will need to reconfigure the tape drives in your backup application.

The path to open the appropriate screen is as follows:

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

Manual Cartridge Assignment

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

For more information on manual cartridge assignment, see [Disabling/Enabling Manual Cartridge Assignment](#) on page 79.

The path to open the appropriate screen is as follows:

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

Disable Remote Service User

For security purposes, prevents a service user from logging in to the library remotely, from either the Web client or over the Ethernet service port. The service user will still be able to log in to the library from the operator panel interface. This option is disabled by default.

The path to open the appropriate screen is as follows:

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

Enable SSL

Enables Secure Socket Layer (SSL) for secure data transmission between the library and remote clients. This option is disabled by default.

The path to open the appropriate screen is as follows:

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

Enable SNMP V1/V2

Enables Simple Network Management Protocol (SNMP) V1 and V2c services to run on the library. This option is disabled by default.

Note: SNMP v3 is always enabled. For more information on SNMP, see [Configuring SNMP Settings on the Library](#) on page 66.

Note: This setting differs from opening the SNMP port in the **Tools > Security** menu (see [Configuring Library Security Settings](#) on page 124). In order to run SNMP, the port must be open and the SNMP service must be enabled.

Enable IPv6

Enables support for IPv6. This option is disabled by default.

The path to open the appropriate screen is as follows:

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

Enable SMI-S

Enables the SMI-S service to run on the library. This setting is disabled by default.

Note: This setting differs from opening the SMI-S port in the **Tools > Security** menu (see [Configuring Library Security Settings](#) on page 124). In order to run SMI-S, the port must be open and the SMI-S service must be enabled.

The path to open the appropriate screen is as follows:

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

Unlabeled Media Detection

At bootup and other times the library performs an inventory of all slots and media. If a slot contains media with an unreadable barcode label (for example, the label is missing, torn, or marked up), the scanner cannot identify it, so the library normally reports the slot as empty.

With the Unlabeled Media Detection feature, you can configure the library to detect and report which slots contain media with unreadable barcodes. Since cartridges with unreadable barcodes will not work for

some library functions, knowing which labels are bad enables you to replace them with good ones as soon as possible.

When you enable Unlabeled Media Detection, the calibration sensor re-scans slots identified as empty in the inventory to see if a cartridge is physically in the slot. If so, the library reports the cartridge as having an unreadable barcode.

Note: The library always re-scans “empty” slots in the top and bottom rows of the library, even if you don’t enable the Unlabeled Media Detection feature. This is because occasionally a small or poorly placed label cannot be read by the barcode scanner in those two rows. The calibration sensor re-scans the bottom row, and the picker physically checks the top row because the calibration sensor cannot reach it.

“Bottom row” here means the bottommost available row as indicated in the library configuration report.

This feature is disabled by default. When enabled, the following occurs:

- The re-scan may take up to several minutes to complete.
- You can configure the library to re-scan only the I/E station slots that were identified as empty, or all the slots in the library that were identified as empty.
- The library configuration report indicates media with unreadable barcodes by displaying a red triangle in the corner of the slot.
- The library user interface lists **No_Label** as the barcode for all cartridges with unreadable labels.
- The library posts a RAS ticket (T143) when an unreadable barcode label is detected. As long as that ticket remains open, no more T143 tickets will be issued, even if more unreadable barcode labels are found.
- An unreadable barcode label is re-scanned every time the cartridge moves to a new location to check if it is readable in the new location.

The paths to open the appropriate screens are as follows:

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

Auto-Ticket Closure

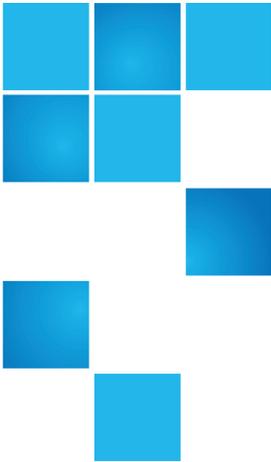
For information about this feature, see [Closing RAS Tickets Automatically](#) on page 380.

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**.



Advanced Reporting

Advanced Reporting is a licensable feature. You must have an Advanced Reporting license installed on your library in order to use the features described in this chapter. For more information on licensing, see [Obtaining and Installing a License Key](#) on page 88.

Advanced Reporting provides the following reports that you can configure, view, save, and e-mail:

- **Drive Resource Utilization Report** – Provides tape drive usage information, showing you which tape drives are working at optimum capacity and which are under-utilized. This can help you allocate your tape drive resources properly.
- **Media Integrity Analysis Report** – Provides TapeAlert count for various combinations of tape drives, tape cartridges, and TapeAlert flags. This can help you determine if a problem is due to a specific tape drive or tape cartridge.

Advanced Reporting provides the following logs that you can view, save, and e-mail:

- **Media Security Log** – Lists media that has been removed from the library.
- **Media Usage Log** – Lists information on all media that have ever been in the library.

In addition, you can automatically e-mail any of the reports and logs to designated recipients at specified, scheduled times.

Note: To use all the features of Advanced Reporting, your library firmware must be at version 580G or higher.

About the Advanced Reporting License

The Advanced Reporting license applies to your entire library, regardless of library size. This means you only need to purchase the license once. If you increase the size of your library, your existing license applies to your new library configuration.

Working With Advanced Reporting Reports

Details about Advanced Reporting reports include:

- The data for the reports is collected in log files. When the log files reach their maximum size, the oldest information is deleted as new information is added. This may affect how much historical data you can access.
- The on-screen reports contain a chart and a data table. When the log files are large, it would take an excessively long time to load all the historical data into the data table. For this reason, the table displays a maximum of 1000 rows of data, beginning with the most recent, even if more data is available. (The graph displays information for the entire range.) To view all of the data, you need to save or e-mail the data file. See [Saving and E-mailing Report Data Files](#) on page 139.

- The reports are built according to data in the log files, not your current library configuration. For this reason, your library may contain tape drives or cartridges that do not show up in the report. Similarly, the report may contain tape drives and cartridges that no longer reside in the library.
- Information about a tape drive, cartridge, or operation is not recorded in the Drive Resource Utilization log file until after a tape cartridge has been mounted (loaded) *and* unmounted (unloaded) from the tape drive.

Configuring the Drive Resource Utilization Report

This report identifies how tape drive resources are utilized in your library. You can use this report to help you determine the proper work load distribution between the tape drives in your library.

The following information is collected for each tape drive installed in the library:

- Drive location (module, row)
- Drive serial number
- Partition
- Megabytes read
- Megabytes written
- Time and date of mount (UTC)
- Time and date of dismount (UTC)
- Media motion time (in seconds)
- Tape cartridge barcode

To configure the report, specify the following:

- **Date Range** – Specifies the range of time covered in the report. Choose one of the following:
 - Last 7 days
 - Last 4 weeks (default)
 - Last 3 months
 - All History (as far back as there is data in the log file)

- **Attribute** – Specifies which values are included in the report. Select one of the following:
 - Data Written/Read (default) – The amount of data written to and read from each tape drive, shown separately in the chart.
 - Total Read and Write – The combined total amount of data written to and read from each tape drive.
 - Media Mount Count – The number of tape cartridge mounts.
 - Media Mount Time – The total amount of time media spent in the selected drive(s).
 - Media Motion Time – The total amount of time media spent in motion while in the tape drive (writing, reading, rewinding, etc.).
- **Chart** – How the data is displayed in the chart. Select Area, Bar (default), Line, or Pie.
- **Type** – The chart type. Select one of the following:
 - Rollup (default) – Displays the Grouping on the x-axis and the Attribute amount on the y-axis.
 - Trend – Shows how the Attribute amount changes over time for the selected Grouping.
- **Grouping** – Specifies which tape drive(s) or partition(s) to include in the report. Select one of the following:
 - All Drives by Coordinate (default) – Presents the sum total of the selected Attribute for all tape drives according to their location in the library. If more than one tape drive resided in that location during the selected Date Range, then the Attribute values for all the tape drives that resided in that location are combined in the chart.
 - All Drives by Physical SN – Presents the sum total of the selected attribute for all drives according to the physical tape drive serial number.
 - All Partitions – Presents a comparison of all drives grouped by partition in the physical library.
 - Selected Drive by Coordinate – The report chart is based on an individual tape drive location in the library. If more than one tape drive resided in that location during the selected Date Range, then the attribute values for all the tape drives that resided in that location are combined in the chart.

- Selected Drive by Physical SN – The report chart is based on an individual tape drive identified by its physical drive serial number.
- Selected Partition – The report chart is based on an individual partition in the physical library.

You can only access this report from the Web client. The path to open the report is **Reports > Advanced Reporting > Drive Resource Utilization**.

Configuring the Media Integrity Analysis Report

This report provides TapeAlert counts for various combinations of tape drives, tape cartridges, and TapeAlert flags. You can use this report to help determine if a problem is due to a specific tape drive or tape cartridge.

The report displays the number of TapeAlerts for the selected Grouping and combination of Attributes. Additionally, the downloaded report includes the last 10 tape drive error codes for each TapeAlert, displayed in columns with the headings **Error #1**, **Error #2**, and so on. (The onscreen report does not contain the tape drive error codes.)

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

- Date and time (UTC) of TapeAlert occurrences
- Tape drive physical serial number
- Cartridge barcode
- TapeAlert value
- Occurrence count of each TapeAlert
- Tape drive error codes for each TapeAlert

To configure the report, specify the following:

- **Date Range** – Specifies the range of time covered in the report. Choose one of the following:
 - Last 7 days
 - Last 4 weeks (default)
 - Last 3 months
 - All History (as far back as there is data in the log file)

- **Attribute**—Specifies which values are included in the report, and how they are combined. Select in any combination, including all (default). If you select no attributes, the report uses Cartridge Barcode.
 - Cartridge Barcode — All relevant tape cartridges.
 - Drive Physical SN — All relevant tape drives.
 - TapeAlert — All TapeAlert flags that were issued. For a description of all TapeAlert flags, see [Appendix B, TapeAlert Flag Descriptions](#).
- **Chart** — Specifies how the data is displayed in the chart. Choose Area, Bar (default), Line, or Pie.
- **Type** — Specifies the chart type. Select one of the following:
 - Rollup (default) — Displays the number of TapeAlerts for the combination of Grouping and Attributes you selected (default).
 - Trend — Shows the occurrence of TapeAlerts over time.
- **Grouping**—Specifies which drive(s) or tape cartridge(s) on which to base the report. Choose one of the following:
 - All (default) — All tape drives and tape cartridges for which a TapeAlert was issued during the specified Date Range.
 - Selected Drive by Physical SN — An individual tape drive. Only tape drives which issued a TapeAlert during the specified Date Range appear in the report.
 - Selected Cartridge by Barcode — An individual tape cartridge. Only tape cartridges that were associated with a TapeAlert during the specified Date Range appear in the report.
- **Sorting**— Specifies how the data will be sorted. Choose from the following:
 - Alphabetical
 - Count (ascending)
 - Last Occurrence (default)

You can only access this report from the Web client. The path to open the report is **Reports > Advanced Reporting > Media Integrity Analysis**.

Using Advanced Reporting Templates

If you want to use the same configuration repeatedly, you can save it as a template. You can save up to 20 templates for each type of advanced report.

Creating a Template

- 1 From the report configuration page, make the selections you want.
- 2 In the **Report Templates** box at the bottom of the screen, type a name for the template in the empty field next to the **Save** button. The name can have a maximum of 15 characters. You can use only lowercase letters, numbers, and the underscore character (_) in template names.
- 3 Click **Save**.

The report appears in the drop-down list next to the **Load** button.

Using a Template

To use a saved template, select the template from the drop-down list and click **Load**.

Deleting a Template

To delete a template, select the template from the drop-down list and click **Delete**.

Loading and Reloading Advanced Reporting Data

When you first open an Advanced Report configuration page, the system loads all the data from the library log file for that report to the Internet browser in preparation for creating your reports. If there is a lot of information in the log files, this may take several minutes.

The data that is loaded in the Internet browser remains unchanged until you log out of your library session or reload the data. If new data is added to the library log file during your session (for instance, a TapeAlert occurs), it will not appear in the onscreen report until you either log out of the library and log on again, or reload the data. To reload the data without logging out, click the **Reload** button. This reloads the entire data set, which may again take several minutes.

You can see how many records were loaded from the log files for this report by looking at the Report Data section of the report configuration page. A note says “XX records read,” where XX is the number of records (see [Figure 16](#)).

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 Report Data Files](#)).

Figure 16 Report Data Buttons



Saving and E-mailing Report Data Files

You cannot save the report as it appears on the screen, but you can save or e-mail the report data as a comma-separated values (.csv) file. You can then import the .csv data into a spreadsheet program and manipulate it to create your own reports for analysis. The .csv file contains all of the data in the log file that falls within the date range you specify.

- 1 Generate a report.
- 2 Scroll down to the bottom of the report viewing screen to a box titled **Retrieve the Report Data File**.
- 3 To save the report data as a .csv file, click **Save**.

Note: To e-mail a saved report from the Web client, you must save the report, and then go to another page in the web client. Return to the report viewer page, scroll down to the bottom of the report viewing screen to a box titled **Retrieve the Report Data File**, and click **E-mail**.

- 4 To e-mail the report data as a .csv file, type the name of a recipient in the empty field next to the **E-mail** button, then click **E-mail**.

Figure 17 Saving and E-mailing the Report Data



The screenshot shows a dialog box titled "Retrieve the report data file:". Inside the dialog, there are two buttons: "Save" and "E-mail". To the right of the "E-mail" button is a text input field containing the email address "recipient@company.com".

Configuring and Viewing the Media Security Log

Media removal is detected by the library when it performs an inventory (at boot up; after an open door is closed, etc.). The media security log lists media that have been removed from the library. You can enable the library to collect information about media removal, and then view, save, and/or e-mail the log.

You can configure the library to collect any or all of the following information. By default, the library collects nothing and the log is empty. You must select each item you want the library to collect:

- **Unexpected Removal Detection After Power-up and Reboot Only**
- **Unexpected Removal Detection During Library Operation**
- **Expected Removal Detection From I/E Slots During Library Operation**

Note: **Unexpected removal** refers to tape cartridges that were removed from the library without being properly exported via the I/E station.
Expected removal refers to tape cartridges that were exported properly via the I/E station.

The log file contains the following information:

- Date and time of media removal
- Tape cartridge barcode
- Type of removal (expected or unexpected)
- Slot location coordinates (of the slot the cartridge is missing from)
- Slot type (I/E, storage, or cleaning)

When the log file reaches its maximum size, the oldest information is replaced as new information is added.

To configure what information gets tracked in the log, select **Setup > Notifications > Advanced Reporting > Media Security** from the Web client.

To view, save, or e-mail the report, select **Reports > Log Viewer** from the Web client. Select **Media Security Log** from the list of logs and click **Next**.

Viewing the Media Usage Log

The Media usage report lists information regarding data written and read on the media and lists statistics pertaining to soft and hard read and write errors. The media usage log collects information on all media that have ever been in the library, including media that are no longer in the library. Lifetime media usage metrics are associated with the cartridge and are kept on the embedded cartridge memory. The log reflects what the drive reports from the embedded cartridge memory whenever the media is unloaded. If the tape cartridge was never mounted and unloaded, it will not appear in the log. When the log file reaches its maximum size, old information is deleted as new information is added. This may affect the amount of available historical data.

The log provides the following information:

- **Volser** – Media cartridge barcode label
- **SN** – Media cartridge serial number
- **Mfr** – Media cartridge manufacturer
- **Date** – Media cartridge manufacturing date (format: YYYYMMDD)

- **Type** – Media type
- **Mounts** – Cartridge mount count
- **RRE** – Recovered read errors
- **URE** – Unrecovered read errors
- **RWE** – Recovered write errors
- **UWE** – Unrecovered write errors
- **LW** – Cartridge lifetime MB written
- **LR** – Cartridge lifetime MB read
- **Enc** – Cartridge encryption status (U=Unknown, E=Encrypted, N=Not Encrypted)

To view, save, or e-mail the report, select **Reports > Log Viewer** from the Web client. Select **Media Usage Log** from the list of logs and click **Next**.

Automatically E-mailing Advanced Reporting Reports and Logs

You can configure the library to automatically e-mail Advanced Reporting logs and reports to specified recipients on a daily or weekly basis.

You can create up to 20 e-mail recipients. If you want to send the same recipient a different set of reports, you can enter the same e-mail address more than once, with different reports selected for each. Each entry counts as a unique recipient toward the 20 total.

Note: Duplicate entries are not allowed. A duplicate entry means the same recipient is set to receive the exact same reports in two different entries, regardless of the day or time. If you have duplicate recipients, make sure that the reports selected in each entry are not an exact match.

For example, if you have one entry in which Recipient A receives the Drive Utilization and Media Integrity reports on Monday, you cannot create another entry to send Recipient A the Drive Utilization and Media Integrity reports on Thursday. Instead, you can create one entry for Recipient A and send the reports every day (select **Daily** as the day to send the report), or you can change the reports you are sending so that they are not the same as the first entry. You could create three entries for Recipient A as follows: 1) send both reports out on Monday; 2) send Drive Utilization out on Thursday; and 3) send Media Integrity out on Thursday (in a different entry). The recipient is the same, but the reports sent in each entry are different.

Each e-mail notification includes an optional comment text box you can use to enter information about the library or the reports and logs that you want the recipient to know. This information appears in the body of the e-mail.

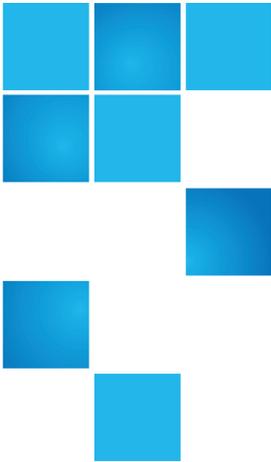
You can modify the settings of an existing e-mail notification at any time after it is created. If an e-mail notification is no longer needed, you can delete it.

Before the library can send e-mail notifications, you must configure the library e-mail account. For information on how to configure the e-mail account, see [Configuring the Library E-mail Account](#) on page 92.

Administrators can configure the library e-mail account and e-mail notifications. Users with user privileges can receive e-mail notifications, but they cannot configure the library e-mail account or e-mail notifications.

The path to open the appropriate screen is as follows:

- From the Web client, select **Setup > Notifications > Advanced Reporting > Receiver Addresses**.



Capacity on Demand

All PowerVault ML6000 library configurations ship with the purchased number of slots pre-activated. The ML6010 CM (5U) and ML6020 CM(14U) library configurations ship with a minimum of 41* active slots, and the ML6030 CM (23U) configuration ships with a minimum of 87* active slots.

* A base license of 41 slots requires 520G or later library firmware.

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, an ML6020 CM could have 87 slots licensed at the time of the initial purchase (41 default + 46 purchased = 87). The remaining 46 slots of the ML6020 CM can be activated at a later time by purchasing an upgrade. The full 133 slots would then be available for use.

If you upgrade to more slots, your new license key contains the entire license corresponding to your expanded slot count. The new license key replaces your current license key. For more information on licensing, see [Obtaining and Installing a License Key](#) on page 88.

It is possible to license more slots than are physically available in the library. In that case, when 9U Library Expansion Modules are added, the extra licensed slots then become available for use.

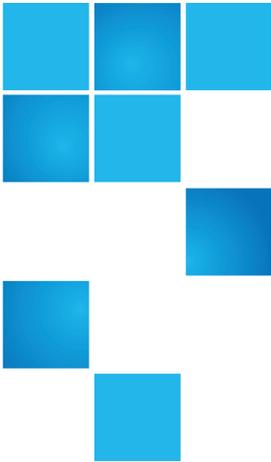
To see your library's current configuration and slot availability, open the Library Configuration Report (choose **Reports > Library Configuration** from the Web).

[Table 6](#) shows the number of default and available pre-activated slots available for purchase and the number of slots you can activate with a COD license key for each library configuration.

**Table 6 Available Slots and
COD Upgrades Per
Configuration**

	ML6010 CM	ML6020 CM	ML6030 CM	ML6030 CM + 1 ML6000 EM	ML6030 CM + 2 ML6000 EMs
Minimum*, Maximum Available Slots (including I/E station slots)	41, 41	41, 133	87, 225	87, 317	87, 409
Default* Pre-Activated Slots	41	41	87	87	87
Available* Pre-Activated Slots	41	41, 87, 133	87, 133, 179, 225	87, 133, 179, 225, 271, 317	87, 133, 179, 225, 271, 317, 363, 409
Available COD Slot Upgrades	NA	87, 133	133, 179, 225	133, 179, 225, 271, 317	133, 179, 225, 271, 317, 363, 409

* A base license of 41 slots requires 520G or later library firmware.



Library Managed Encryption

The Dell PowerVault ML6000 requires the use of an external encryption key management (EKM) server for library managed encryption. The encryption key management software is installed on a server or servers. The encryption key management software program generates, protects, stores, and manages encryption keys. These keys are used by LTO-4, LTO-5, and LTO-6 Fibre Channel and SAS tape drives to encrypt information being written to, and decrypt information being read from, tape media. The library is configured to communicate with these server(s). The encryption keys pass through the library, so that encryption is "transparent" to the applications.

When you purchase library managed encryption, you receive the encryption key management software application along with installation and configuration instructions. This chapter describes how to configure library managed encryption (LME) on the library. This chapter also describes all of the LME functions available on the library.

Refer to the documentation supplied with the encryption key management software or located at <http://support.dell.com> for information on how to manage the software application outside of the library.

Library Managed Encryption is a licensable feature. You must have a library managed encryption license installed on your library in order to use the encryption key management features described in this chapter.

Note: The *Dell™ Encryption Key Manager 3.0 Deployment Guide* will be used to support the Encryption Key Manager (EKM) 3.0 application shipped with the license key certificate and should be referred to instead of the current EKM documentation references on the license key certificate in this kit or the *Dell™ PowerVault™ ML6000 Tape Library User's Guide*. The deployment guide is posted under **Manuals > Software > Key Management** at <http://support.dell.com/support/edocs/SOFTWARE/ekm>.

Note: These three solutions are not interoperable. The Scalar i500 library does not support more than one encryption key management system on a single library.

The Dell PowerVault ML6000 supports the Dell Encryption Key Manager (EKM). The Dell EKM is a Java software program that generates, protects, stores, and manages encryption keys. These keys are used by LTO-4, LTO-5, and LTO-6 Fibre Channel and SAS tape drives to encrypt information being written to, and decrypt information being read from, tape media. 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, so that encryption is “transparent” to the applications.

When you purchase library managed encryption, you receive the Dell EKM software application along with installation and configuration instructions.

This chapter describes how to configure your encryption key management (EKM) solution on the library. This chapter also describes all of the EKM functions available on the library.

Refer to the *Dell Encryption Key Manager Deployment Guide* for information on how to manage the Dell EKM outside of the library.

General Notes About Encryption on the Library

Keep the following points in mind when using encryption on the library:

- Data written to encryption-supported and encryption-capable media in LME-supported tape drives will be encrypted *unless* data was previously written to the media in a non-encrypted format. In order for data to be encrypted, the media must be blank or have been written to using library managed encryption at the first write operation at the beginning of tape (BOT).
- You cannot append encrypted data to a non-encrypted tape.
- You cannot append non-encrypted data to an encrypted tape.
- Only one data encryption key can be used per tape cartridge.
- Encryption is configured by partition. Partitions must be configured for “Library Managed Encryption.” EKM partitions must contain only the tape drives supported by the encryption system you are using. (For more information, see [Step 5: Configuring Partitions for Library Managed Encryption](#) on page 152.

About the EKM License

If you purchase an LME license after you purchased your library, you must install the license key on your library to enable the LME functionality. The LME license is sold on a per-drive basis. The license corresponds to the number of tape drives that you can enable for library managed encryption. If your library contains more encryption-enabled tape drives than are covered by the license, you will need to purchase an additional license to cover them. Your new license key replaces your current license key and contains the entire license for the total number of tape drives.

Configuring the Dell Encryption Key Manager (EKM) on the Library

Make sure your Dell EKM servers are installed and running before configuring the library (see the *Dell Encryption Key Manager Deployment Guide* for instructions).

Then follow these steps, in order, to configure the library:

- [Step 1: Installing the EKM License Key on the Library](#) on page 149
- [Step 2: Preparing Partitions for Library Managed Encryption](#) on page 149
- [Step 3: Configuring Encryption Settings and Key Server Addresses](#) on page 150

Step 1: Installing the EKM License Key on the Library

If your LME license key is not already installed on the library, install it now.

Step 2: Preparing Partitions for Library Managed Encryption

For each partition on which you want to enable library managed encryption, do the following:

- 1 Make sure the partition contains encryption-supported and encryption-capable tape drives and media.

Note: If you enable a partition for library managed encryption, all library managed encryption-supported tape drives in that partition are enabled for encryption, and all data written to supported media in the partition is encrypted. Any tape drives not supported by library managed encryption in that partition are not enabled for encryption, and data written to non-supported media is not encrypted.

- 1 On the tape drives, install the latest version of firmware that is qualified for the library firmware installed on your library. Refer to the library release notes for the correct version of tape drive firmware. (It is recommended that you upgrade library firmware to the latest release.) The latest firmware and installation instructions are available on <http://support.dell.com>.
- 2 Unload tape cartridges from all tape drives in the partitions on which you are configuring Dell EKM.

Step 3: Configuring Encryption Settings and Key Server Addresses

Configure encryption settings and key server information as follows:

- 1 From the Web client, select **Setup > Encryption > System Configuration**.
- 2 **Automatic EKM Path Diagnostics** — Enable or disable as desired; however, it is recommended you leave the default. For more information, see [Using Automatic EKM Path Diagnostics](#) on page 158). When enabled, this feature performs a check, at specified intervals, to make sure both key servers are connected to the library and functioning properly. The library generates a RAS ticket if there are problems.
- 3 **Interval** — If Automatic EKM Path Diagnostics is enabled, select the interval at which the library performs the diagnostics.
- 4 **Test Warning Threshold** — If Automatic EKM Path Diagnostics is enabled, specify the number of consecutive missed test intervals required to generate a RAS ticket.
- 5 **Secure Sockets Layer (SSL)**: To enable SSL for communication between the library and the EKM key servers, select the **SSL Connection** checkbox. This feature is disabled by default. If you enable SSL, you must make sure that the **Primary** and **Secondary Key Server Port Numbers** (see below) match the SSL port numbers set on the EKM key servers. The default SSL port number is 443.

Note: Keys are always encrypted before being sent from the EKM key server to a tape drive, whether SSL is enabled or not. Enabling SSL provides additional security.

- 6 In the **Primary Key Server Port Number** text box, enter the port number for the primary key server. 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 setting on the library, you must also change the port number on the key server to match or EKM will not work properly.

- 7 If you are using a secondary key server for failover purposes, enter the IP address or host name of the secondary key server into the **Secondary Key Server IP Address or Host** text box.

Note: If you do not plan to use a secondary key server, you may type a zero IP address, 0.0.0.0, in the **Secondary Key Server IP Address or Host** text box, or you may leave the text box blank.

- 8 If you configured a secondary key server (previous step), enter the port number for the secondary key server into the **Secondary Key Server 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 key server, then the port numbers for both the primary and secondary key servers must be set to the same value. If they are not, synchronization and failover will not occur.

- 9 Click **Apply**.

Note: You cannot edit the encryption system configuration settings when any partition is enabled for library managed encryption. If this happens, go to **Setup > Encryption > Partition Configuration**, change all Dell EKM partition settings from **Library Managed** to **Application Managed**. Then make your changes to the system configuration settings. Finally, go back and change all the Dell LME partition settings to **Library Managed**.

- 10 Ensure all ports corresponding to the EKM servers are open on your firewall to allow the library to connect to the servers.

Step 4: Running EKM Path Diagnostics

Perform EKM Path Diagnostics as described in [Using EKM Path Diagnostics](#) on page 156.

Step 5: Configuring Partitions for Library Managed Encryption

Encryption on the Dell PowerVault ML6000 tape library is enabled by partition only. You cannot select individual tape drives for encryption; you must select an entire partition to be encrypted.

Configure the partitions as follows:

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

A list of all your partitions displays, along with a drop-down list displaying the encryption method for each partition. The Encryption Method applies to all encryption-capable tape drives and media in that partition. [Table 7](#) on page 152 describes the partition encryption methods.

Table 7 Partition Encryption
Methods

Encryption Method	Description
Library Managed	For use with EKM. Enables encryption support via a connected Dell EKM key server for all tape drives and encryption-capable media assigned to the partition.

Application Managed	<p>Not for use with EKM. Allows an external backup application to provide encryption support to all encryption-capable tape drives and media within the partition. The library will NOT communicate with the Dell EKM key server on this partition.</p> <p>This is the default setting if you have encryption-capable tape drives in the partition. This option should remain selected <i>unless</i> you want the EKM server to manage encryption.</p> <p>Note: If you want an application to manage encryption, you must specifically configure the application to do so. The library will not participate in performing this type of encryption.</p>
None	Disables encryption on the partition.
Unsupported	<p>Means that no tape drives in the partition support encryption.</p> <p>If Unsupported is shown, it will be greyed out and you will not be able to change the setting.</p>

- 2 For each partition on which you are configuring Dell EKM, change the Encryption Method to **Enable Library Managed**. (To disable EKM, select **Allow Application Managed**).

Note: When you change the encryption method on a partition, the partition is taken offline. When the change completes successfully, the partition comes back online automatically. If the operation does not complete successfully, the partition remains offline until you turn it back online manually or restart the library.

Note: When you change a partition from **Library Managed** to **Application Managed**, the data that was written to the tapes while the partition was configured for library managed encryption can no longer be read, until you change the partition back to **Library Managed**.

- 3 If you want different partitions to use different EKM key servers, fill in the Library Managed Encryption Server Overrides section as follows. The settings in the overrides section supersede the default settings listed in the **Setup > Encryption > System Configuration** screen. (However, the overrides settings do not change the settings listed in the **Setup > Encryption > System Configuration** screen. Those settings are the default configuration settings for any partition that does not use overrides.) Overrides are only available on partitions that have **Library Managed** set as the encryption method.

Caution: Only fill in the overrides section if you want different partitions to use different EKM key servers. Otherwise, leave this section alone and allow the values from the **Setup > Encryption > System Configuration** screen to populate these fields. Once you make any changes to the overrides section, the default values from the **Setup > Encryption > System Configuration** screen will no longer automatically populate these fields. If you want to return to the default settings after changing the overrides, you must enter them manually.

For each partition that has Library Managed as the encryption method, do the following:

- Type the IP address (if DNS is not enabled) or the host name (if DNS is enabled) of the primary EKM key server in the **Primary Host** text box.
- Type the port number for the primary EKM key server into the **Port** text box. The default port number is 3801, unless SSL is enabled. If SSL is enabled, the default port number is 443.
- If you are using a secondary EKM server, type the address/host name and port number of the secondary EKM key server in the **Secondary Host** and **Port** text boxes.

- Select the **SSL** checkbox if you want to enable Secure Sockets Layer (SSL) for communication between that partition and the EKM servers. The default is Disabled. If you enable SSL, you must make sure that the primary and secondary EKM Port numbers in the overrides section match the SSL port numbers set on the EKM servers. The default SSL port number is 443.

Note: Keys are always encrypted before being sent from the EKM server to a tape drive, whether SSL is enabled or not. Enabling SSL provides additional security.

Note: Restriction on EKM servers used for overrides: If you are using primary and secondary servers for overrides, the following restriction applies. (If you are not using a secondary server, there are no restrictions.)

Restriction: A given primary server and secondary server must be “paired” and cannot be used in different combinations. For example:

- You can have Server1 as primary and Server2 as secondary for any or all partitions.
- If Server1 is primary and Server2 is secondary on one partition, then in any other partition that you use Server1, Server1 can only be primary and it must be “paired” with Server2 as secondary. You cannot have Server1 as primary and Server3 as secondary on another partition.
- You cannot have Server1 be both primary on PartitionA and secondary on PartitionB.
- You cannot have Server2 be both secondary on PartitionA and primary on PartitionB.

If you use overrides, make sure that you install the EKM software on all the servers you specify. Then run EKM Path Diagnostics on each tape drive in every partition configured for EKM to make sure that each tape drive can communicate with and receive keys from the specified EKM server. For more information, see [Using EKM Path](#)

[Diagnostics](#) on page 156.

- 4 Click **Apply**.
- 5 Save the library configuration.

Using EKM Path Diagnostics

The EKM Path Diagnostics consists of a series of short tests to validate whether the key servers are running, connected, and able to serve keys as required.

Run the Manual EKM Path Diagnostics any time you change the key server settings or library encryption settings, and when you replace a tape drive. It is recommended that you test each drive that communicates with key manager servers.

The diagnostics consists of the following tests:

- **Ping** – Verifies the Ethernet communication link between the library and the key servers. If the partition in which the selected tape drive resides uses EKM server overrides, then the override IP addresses are tested (see **Setup > Encryption > Partition Configuration**). If the partition does not use overrides, the default system IP addresses are tested (see **Setup > Encryption > System Configuration**).
- **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). The tape drive must be unloaded, ready, and online in order to run this test. If this test fails, the Path and Config tests are not performed.
- **Path** – Verifies that EKM services are running on the key servers.
- **Config** – Verifies that the key servers are capable of serving encryption keys.

Note: This test cannot run if the Drive test fails.

If any of the tests fail, try the following resolutions and run the test again to make sure it passes:

- **Ping Test Failure** – Verify that the key server host is running and accessible from the network to which the library is connected.
- **Drive Test Failure** – Look for any tape drive RAS tickets and follow the resolution instructions in the ticket.

Differences Between Manual and Automatic EKM Path Diagnostics

There are two ways to perform EKM Path Diagnostics:

- [Using Manual EKM Path Diagnostics](#) on page 157
- [Using Automatic EKM Path Diagnostics](#) on page 158

The Manual diagnostics differs from the Automatic diagnostics in the following ways:

- The Manual diagnostics takes affected partitions offline during the tests. When the tests complete, the partitions are returned to the online/offline state they were in before the tests began.
- The Automatic diagnostics does not take partitions offline, but it may delay moves to tape drives while they are being tested.
- The Manual diagnostics requires that you select one tape drive to use for the test. Since the test only validates the selected drive, if you want to test the path for each tape drive, you must run the test multiple times (once for each drive). To test all servers, you must run the diagnostics once for each Library Managed Encryption enabled partition (each server pair is connected to a unique partition and tape drive). In addition, if the tape drive is not available (it must be unloaded, ready, and online), the Drive, Path, and Config tests are not performed.
- The Automatic diagnostics tests every connected EKM server in turn, and the library selects the tape drive to use for each test. If the selected tape drive is not available (it must be unloaded, ready, and online), then the library tries another tape drive that is connected to the key server until it finds one that is available. If no tape drives connected to a particular key server are available, then that server is skipped and the tests are not performed. If a server is skipped for “X” number of consecutive test intervals (where “X” is configurable on the Web client), the library generates a RAS ticket. If a tape drive remains loaded for a long time, it is possible that it will never be tested. If you want to test a specific tape drive, then you should use the Manual EKM Path Diagnostics. In particular, if you replace a tape drive, run the Manual EKM Path Diagnostics.

Using Manual EKM Path Diagnostics

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

- Enter library Diagnostics. From the Web client select **Tools > Diagnostics**, and click **OK** to the message that appears. From the Diagnostics menu, select **EKM > EKM Path Diagnostics**.

Note: Performing Diagnostics will log off all other users of the same or lower privileges and take your partitions offline. When you exit Diagnostics, the partitions automatically come back online.

- Select **Setup > Encryption > System Configuration** or **Setup > Encryption > Partition Configuration** and click the link that says “Click here to run EKM Path Diagnostics.”
- 2 Click **OK** to start the diagnostics.
 - 3 The library performs the diagnostics and displays pass/fail results on each of the tests in the Progress Window.

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

- 4 Do one of the following:
 - If **Completed** appears in the Progress Window, the diagnostics were performed (this does not mean that the diagnostics passed, just that the diagnostics were performed). Click **Close** to close the Progress Window.
 - If **Failure** appears in the Progress Window, the diagnostics were not performed. Follow the instructions listed in the Progress Window to resolve any issues that occurred during the operation.
- 5 If you are entered the Diagnostics menu, select **Exit** from the menu bar and then click **OK** in the dialog box that appears.

Using Automatic EKM Path Diagnostics

You can enable the library to automatically perform EKM Path Diagnostics at selected intervals. During each interval, the library tests every configured key server. The default test interval is four hours. The library generates a RAS ticket if there are problems.

- Automatic EKM Path Diagnostics is disabled by default. It is recommended that you leave Automatic EKM Path Diagnostics disabled, unless network interruptions are a common cause of encryption failures at your site.

Caution: Running Automatic EKM Path Diagnostics may cause an increase in RAS tickets if tests are skipped due to tape drives being unavailable for a configurable number of consecutive test intervals. To reduce the occurrences of RAS tickets, you can specify the number of consecutive test intervals required to generate a RAS ticket to a higher number, or you can set the library to never generate a RAS ticket for missed test intervals.

For a list of tests performed, see [Using EKM Path Diagnostics](#) on page 156.

To enable Automatic EKM Path Diagnostics:

- 1 From the Web client, select **Setup > Encryption > System Configuration**.
- 2 Select the **Automatic EKM Path Diagnostics** check box.
- 3 Select a test interval from the **Interval** drop-down list.
- 4 From the **Test Warning Threshold** drop-down list, select the number of consecutive, missed test intervals required before the library generates a RAS ticket informing you that the test could not be performed within the specified number of test intervals. You can select "Off" or any value from 1 to 24. If you select "Off," the library will never generate a RAS ticket, no matter how many tests are missed. The default threshold is 3.

Viewing and Changing the Active Key Server

The **Key Manager Status** screen shows you which encryption key server is currently active, and allows you to change the active server. When you change the active server, it means that the next key server operation and all subsequent key server operations will be performed using the new active server until that server fails or the key server settings are changed.

- 1 From the Web client, select **Tools > EKM Management > Server Status**.

The **Key Manager Status** screen appears. A list of all your connected EKM servers displays. The currently active server displays in bold green type with the word “(Active)” after it.

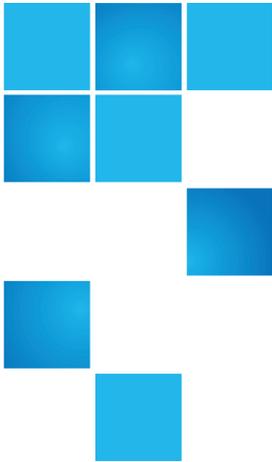
- 2 To choose a different server to be the active server, select that server’s radio button and click **Apply**.

Viewing Tape Drive Encryption Settings

You can view the encryption settings in the following ways:

- **System Information Report** – To view encryption information on all key servers, partitions, and tape drives, select **Reports > System Information** from the Web client.
- **Library Configuration Report** – To view the encryption status of a selected tape drive or tape cartridge, select **Reports > Library Configuration** from the Web client and click a tape drive or slot. The encryption status is displayed in a pop-up status window.
- **Partition Encryption** – From the Web client, select **Setup > Encryption > Partition Configuration** to view and change the encryption settings of partitions. See [Step 5: Configuring Partitions for Library Managed Encryption](#) on page 152 for more details.

Avoid manually generating keys on more than five libraries simultaneously as the key generation process is resource-intensive on the server. Generating keys manually on more than five libraries at once could result in a failure to complete the key generation operation, or interfere with key retrieval operations. If a failure does occur during key generation, wait 10 minutes, then try to start it again. The key generation process will resume from where the error was encountered.



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.

Powering on the Library

To power on the library:

- 1 Connect all power cords to their electrical source.
- 2 Turn on each power supply using the switch on the rear of the power supply.
- 3 Press the power button located on the front door of the 5U Library Control Module.

When you power on the library, the library performs a self-test to ensure that all of its parts are functioning properly. All tape drives and partitions are brought online.

Shutting Down, Powering Off, and Completely Removing Power

The **Shutdown** command shuts down the library's operating system and firmware. When performing a shutdown, the library finishes the current command and lowers the robot to the floor of the library.

Caution: Always perform a shutdown before powering off the library or completely removing power from the library.

Before performing a shutdown, make sure the connected host applications are not sending commands to the library.

To power off the library: Perform the shutdown sequence and then press the power button on the front of the 5U Library Control Module.

To completely remove power: Perform the shutdown sequence and power off the library. Then turn off the power switch on each power supply, located at the rear of the library. Finally, disconnect the power supply cables from their electrical source.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Operations > System Shutdown**.
- From the operator panel, select **Operations > Shutdown**.

Restarting the Library

The **Restart** command shuts down and restarts the library's operating system and firmware. When performing a restart, the library finishes the current command, then shuts down the library and restarts it. During the restart, the library brings all tape drives and partitions online and performs an inventory of cartridges, tape drives, and slots.

Before performing a restart, make sure the connected host applications are not sending commands to the library.

Restarting takes approximately 5 minutes for the 5U Library Control Module and longer for the 14U and higher library configurations.

If the “Not Initialized” message appears on the operator panel after the restart process is complete, the library did not properly initialize. View the **All RAS Tickets** screen to find the problem that is preventing the library from properly initializing. See [Viewing RAS Tickets](#) on page 378.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Operations > System Shutdown**.
- From the operator panel, select **Operations > Shutdown**.

Logging In

All users and administrators must log in to the library to perform library functions or view library operations.

If you are logging in to the library for the first time using the default administrator account, type **admin** in the **User Name** text box and **password** in the **Password** text box.

After you log on for the first time, change the password for the default administrator account. Passwords are limited to 6–16 lower-case alphanumeric characters and can also include underscores (_), periods (.), hyphens (-), asterisks (*), and the “at” symbol (@). For example: **pass_1**. For information on changing passwords, see [Modifying Local User Accounts](#) on page 98.

Note: If you misplace the password for the default administrator account, contact Dell Technical Support. For contact information, see [Appendix C, Contacting Dell](#).

Logging In When LDAP or Kerberos is Enabled

When LDAP or Kerberos is enabled, the **Login** screen displays a **Remote Authentication** check box. Log in on either the operator panel or Web client as follows:

- Select the **Remote Authentication** check box to log in using a directory service user name and password.
- Clear the **Remote Authentication** check box to log in using a local user name and password.

For more information on LDAP, see [Configuring LDAP](#) on page 99.

For more information on Kerberos, see [Configuring Kerberos](#) on page 104.

Logging Out

Logging out secures the library from being accessed by unauthorized users. Log out whenever you have finished accessing the library through either the Web client or the operator panel.

From the Web client or the operator panel, you can click the **LOGOUT** button at the top right of the screen to log out. From the Web client, you can also select **Operations > Logout**.

Performing Media Operations

Administrators and users can use commands on the Web client and operator panel **Operations** menu to perform the following media operations:

- Import data cartridges into the library
- Export data cartridges from the library
- Move data cartridges between tape drives, I/E stations, and storage slots within a partition

- Import cleaning cartridges into the library (AutoClean is enabled)
- Export cleaning cartridges from the library (AutoClean is enabled)
- Load cartridges into tape drives
- Unload cartridges from tape drives
- Change the tape drive mode from online to offline and back as needed

In addition, administrators can:

- Clean tape drives manually, using the **Tools > Drive Mgmt > Clean Drive** command on the operator panel or **Tools > Drive Operations > Clean a tape drive** from the Web client.

The following topics provide an overview of these media operations. For step-by-step procedures, see the library's online Help. To access the online Help system, click the **Help** icon at the top right of the Web client or operator panel.

Note: The information and procedures in this user's guide apply specifically to the library Web client and the operator panel user interface, not to the host application. Performing media operations through the library user interface may affect your host application. See your host application documentation for information.

Importing Media

The Import Media operation allows you to use the I/E station to import data cartridges into the library. The library's scanner automatically reads the barcode on new cartridges imported into the library.

Note: If your library has zero I/E station slots, you cannot import or export media. See [Configuring I/E Station Slots](#) on page 81.

This topic focuses on using the library user interface, not the host application, to import media. Using the library to import media may necessitate performing an inventory of the library with the host application. See your host application documentation for more information.

There are two ways to import tape cartridges via the library: with manual cartridge assignment enabled or disabled. Manual cartridge assignment

is enabled on the library by default. For information on disabling/enabling this feature, see [Disabling/Enabling Manual Cartridge Assignment](#) on page 79.

This section contains the following sub-sections

- [Importing Media with Manual Cartridge Assignment Enabled](#) on page 166
- [Importing with Manual Cartridge Assignment Disabled](#) on page 167
- [Process for Importing Media](#) on page 167

The table below describes the differences in what you can do depending on manual cartridge assignment status:

Manual Cartridge Assignment	Cartridge Assignment in I/E Station	Is Importing Unassigned Media Allowed?
Enabled (default)	You are asked to assign cartridges to a partition immediately upon placing them in the I/E station. You may “cancel” out of this window without assigning them to a partition.	From operator panel: NO From Web client: YES
Disabled	You are not asked to assign cartridges to a partition and the cartridges remain unassigned until imported into the library.	From operator panel: YES From Web client: YES

Importing Media with Manual Cartridge Assignment Enabled

- When Manual Cartridge Assignment is enabled (default), once you load tape cartridges into the I/E station and close the I/E station door, the **Assign I/E** screen automatically appears on the operator panel. The **Assign I/E** screen prompts you to use the operator panel to assign the cartridges to a specific partition or to the system partition. The cartridges can be used only by the assigned partition. All of the cartridges you placed in the I/E station are assigned to the same partition that you selected.

- If you cancel out of the **Assign I/E** screen (or forget to assign the inserted cartridge to a partition), the cartridges remain unassigned until you either import them via the Web UI or open and close the I/E station so the **Assign I/E** screen displays again.
- You cannot import unassigned media into the library via the operator panel.
- You can import unassigned media into the library via the Web client. When importing unassigned tape cartridges via the Web client, only the cartridges you actually import into a partition will be assigned to that partition. The rest of the cartridges will remain unassigned in the I/E station.
- Unassigned cartridges are not visible to host applications.

Importing with Manual Cartridge Assignment Disabled

- Disabling manual cartridge assignment allows you to load several tape cartridges into the I/E station and assign them to different partitions.
- The **Assign I/E** screen does not appear on the operator panel. The cartridges in the I/E station are available for use by any partition, including the system partition. The cartridges in the I/E station remain unassigned until you import them into a partition (importing assigns them to the partition).
- You can import unassigned tape cartridges via the operator panel or the Web client. When importing unassigned tape cartridges, only the cartridges you actually import into a partition will be assigned to that partition. The rest of the cartridges will remain unassigned in the I/E station.
- Unassigned cartridges are visible to host applications and can be claimed by any host application on a first-come, first-served basis.

Process for Importing Media

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

If you have AutoClean enabled, you can also import cleaning cartridges into the library. For information, see [Importing Cleaning Media](#) on page 180. In addition, you can bulk load cartridges into the library rather

than use the I/E station to import media. For information, see [Bulk Loading](#) on page 169.

Note: Once the import operation has started, do not interfere with the operation by opening and closing the I/E station door.

The process for importing cartridges includes the following steps:

- 1 Go to the front of the library and insert cartridges into the I/E station.
- 2 Close the I/E station door.

The **Assign I/E** screen appears on the operator panel if the **Manual Cartridge Assignment** setting is enabled on the operator panel **System Settings** screen (**Tools > System Settings**).

If the **Assign I/E** screen appears, do the following:

- a Assign the cartridges to the appropriate partition by selecting a partition listed on the **Assign I/E** screen.

The partition button turns blue after it has been selected.

Caution: If you select the wrong partition, open the I/E station door. Move the cartridge to a different I/E station slot and close the I/E station door. The library will rescan the I/E station, and the **Assign I/E** screen will appear again.

- b Select **Apply**.

If the selected partition is online, it will be taken offline before the import operation is performed, and brought back online after the operation is complete. If the library contains multiple partitions, the import operation will not affect operations in other partitions.

Note: If the operation does not complete successfully, the partition remains offline until you turn it back online manually or restart the library (see [Taking a Partition Online or Offline](#) on page 78).

- 3 Use the **Import Media** screens on either the operator panel or the Web client to import the cartridges into the partition. Follow the on-screen prompts, or see the library's online Help for step-by-step procedures. To access the online Help system, click the **Help** icon at the top right of the Web client or operator panel user interface.

You need to provide the following information in the **Import Media** screens to import media:

- **Partition** – The partition into which you want to import the cartridges. The screen lists only the partitions to which you have been given access. The screen includes information about the partition mode (online or offline) and the number of empty slots in the partition. The number of cartridges you can import is limited to the number of empty slots.
- **Media** – The cartridges that you want to import.

Note: You can filter the list of media by entering all or part of a barcode in the **Search** text box. Use an asterisk (*) to search with wildcards. You can also sort the list by clicking on columns with bold headings. For example, selecting the **Location** column heading sorts the list by location coordinates.

The paths to open the appropriate screens are as follows:

- **From the Web client**, select **Operations > Media > Import**.
- **From the operator panel**, select **Operations > Import Media**.

For step-by-step procedures, see the library's online Help. To access the online Help system, click the **Help** icon at the top right of the Web client or operator panel user interface.

Bulk Loading

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

Before bulk loading, print out the Library Configuration report from the Web client to see how the physical slots of the library are configured. The report shows what slots are unavailable or configured as cleaning slots or

as I/E station slots. For information on accessing the report, see [Viewing the Library Configuration Report](#) on page 190.

Caution: Place cartridges in their appropriately configured slot location; for example, cleaning cartridges should not be placed in slots configured for storage.

When I/E station slots have been configured as I/E slots, the I/E station door is unlocked, and you can open the main access door to the library. When all I/E station slots are configured as storage, the I/E station door is always locked. You will not be able to open the main access door to bulk load tape cartridges into the library without first unlocking the I/E station door. If possible, bulk load the library before configuring the I/E station slots as storage. Otherwise, unlock the I/E station door. For information on locking and unlocking the I/E stations, see [Locking and Unlocking the I/E Stations](#) on page 185. For information on configuring I/E station slots, see [Configuring I/E Station Slots](#) on page 81.

To perform an initial bulk load, open the access door and manually insert directly into storage slots as many cartridges as you plan to use. The cartridges will not go in all the way if they are inserted incorrectly.

Note: A small number of physical storage slots are inaccessible to the robot and should not be used for any tape cartridges. These slots appear as unavailable in the Library Configuration report. For detailed information on these slots, see [Unused Slots](#) on page 171.

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 377.

After the initial bulk load, you can use the **Import Media** screen to add cartridges without interrupting library operations, as long as I/E station slots have been configured. For more information, see [Importing Media](#) on page 165.

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.

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 81.

This topic focuses on using the library user interface, not the host application, to move media. Using the library to move media may necessitate performing an inventory of the library with the host application. See your host application documentation for more information.

Details on using the library to move media include:

- If the partition is online, it will be taken offline before the move is performed and brought back online after the move is complete. You will be asked to confirm that you want to take the partition offline.

Note: If the operation does not complete successfully, the partition remains offline until you turn it back online manually or restart the library (see [Taking a Partition Online or Offline](#) on page 78).

- 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 81.

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 181.

Note: Once the export operation has started, do not interfere with the operation by opening and closing the I/E station door.

Caution: Some host applications may fail import/export operations when the I/E station contains cartridges that are assigned to another partition. Move cartridges from the I/E station as soon as possible to avoid possible conflicts with the other partitions.

Details on exporting cartridges include:

- If the partition is online, it will be taken offline before the export operation is performed and brought back online after the operation is complete. You will be asked to confirm that you want to take the partition offline.

Note: If the operation does not complete successfully, the partition remains offline until you turn it back online manually or restart the library (see [Taking a Partition Online or Offline](#) on page 78).

- You can select only the partitions to which you have been given access.
- You can only export cartridges if empty I/E station slots are available.
- You must have access to the library's I/E station and the operator panel to import cleaning cartridges.

You need to provide the following information in the **Export Media** screens to export media:

- **Partition** – The partition from which you want to export cartridges. The screens include information about the partition mode (online or offline) and the number of empty I/E station slots. The number of cartridges you can export is limited to the number of empty slots.
- **Media** – The tape cartridges that you want to export.

Note: You can filter the list of media by entering all or part of a barcode in the **Search** text box. Use an asterisk (*) to search with wildcards. You can also sort the list by clicking on columns with bold headings. For example, selecting the **Location** column heading sorts the list by location coordinates.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Operations > Media > Export**.
- From the operator panel, select **Operations > Export Media**.

For step-by-step procedures, see the library's online Help. To access the online Help system, click the **Help** icon at the top right of the Web client or operator panel user interface.

Loading Tape Drives

The Load Drive operation enables you to load a cartridge from a storage slot into a tape drive. The storage slot and tape drive must be assigned to the same partition.

This topic focuses on using the library user interface, not the host application, to load tape drives. Using the library to load tape drives may necessitate performing an inventory with the host application. See your host application documentation for more information.

Details on loading tape drives include:

- If the partition is online, it will be taken offline before the load operation is performed and brought back online after the operation is complete. You will be asked to confirm that you want to take the partition offline.

Note: If the operation does not complete successfully, the partition remains offline until you turn it back online manually or restart the library (see [Taking a Partition Online or Offline](#) on page 78).

- You can select only partitions to which you have been given access.
- Default tape drive locations are highlighted if the barcode field is empty or the field is cleared.

You need to provide the following information in the **Load Drive** screens to load tape cartridges into tape drives:

- **Partition** – The partition containing the cartridge you want to load into a tape drive. The screens include information about the partition mode (online or offline).
- **Media** – The tape cartridges that you want to move.

Note: You can filter the list of media by entering all or part of a barcode in the **Search** text box. Use an asterisk (*) to search with wildcards. You can also sort the list by clicking on columns with bold headings. For example, selecting the **Location** column heading sorts the list by location coordinates.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Operations > Drive > Load**.
- From the operator panel, select **Operations > Load Drive**.

For step-by-step procedures, see the library's online Help. To access the online Help system, click the **Help** icon at the top right of the Web client or operator panel user interface.

Unloading Tape Drives

The Unload Drive operation allows you to unload a cartridge from a tape drive to a storage slot. The storage slot and tape drive must be assigned to the same partition.

This topic focuses on using the library user interface, not the host application, to unload tape drives. Using the library to unload tape drives may necessitate performing an inventory with the host application. See your host application documentation for more information.

Details about unloading tape drives include:

- Only drives with media loaded appear on the screen.
- You can select only partitions to which you have been given access.
- If the affected partition is online, it will be taken offline before the unload operation is performed, and brought back online after it is complete.

Note: If the operation does not complete successfully, the partition remains offline until you turn it back online manually or restart the library (see [Taking a Partition Online or Offline](#) on page 78).

You need to provide the following information in the **Unload Drive** screens to unload tape cartridges from tape drives:

- **Partition** — The partition containing the tape drive that you want to unload. The screens include information about the partition mode (online or offline).
- **Tape drive** — The tape drive that contains the cartridge that you want to unload.

Note: You can sort the list of tape drives by clicking on columns with bold headings. For example, selecting the **Location** column heading sorts the list by location coordinates.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Operations > Drive > Unload**.
- From the operator panel, select **Operations > Unload Drive**.

For step-by-step procedures, see the library's online Help. To access the online Help system, click the **Help** icon at the top right of the Web client or operator panel user interface.

Taking a Tape Drive Online or Offline

There are two tape drive modes: online and offline.

- **Online** — Tape drive is available for use. This is the normal operating mode for the tape drive.
- **Offline** — Tape drive is offline to the host application and is not available for cartridge load and unload (move) operations initiated by the host application, but it remains available for Web client or operator panel initiated move commands.

Note: If a cartridge is already in the tape drive when you take the tape drive offline, then the host can still read and write data on the tape.

Some operations require that the tape drive be offline. You can take a tape drive offline rather than the entire library or partition so as to minimize disruption of library operations.

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

Details on changing the tape drive mode include:

- The default tape drive mode is online.
- You can select only tape drives in partitions to which you have been given access.
- The **Online/Offline** buttons toggle between modes.
- Once taken offline, tape drives remain offline until they are turned online again, or the library is restarted. Restarting the library will bring all offline tape drives back online.

Note: If you change the mode of a control path tape drive to offline, a caution dialog appears asking you to confirm the mode change. For information on control path tape drives, see [Working With Control Paths](#) on page 86.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Operations > Drive > Change Mode**.
- From the operator panel, select **Operations > Change Drive Mode**.

For step-by-step procedures, see the library's online Help. To access the online Help system, click the **Help** icon at the top right of the Web client or operator panel user interface.

About Cleaning Tape Drives

Library tape drives require occasional cleaning. Cleaning cartridges are used to remove accumulated residue from each tape drive's read/write head.

The library supports two methods for cleaning tape drives with cleaning cartridges: AutoClean and Manual.

AutoClean – Configuring one or more dedicated cleaning slots automatically enables AutoClean. Cleaning cartridges are stored in the designated cleaning slots. When a tape drive needs cleaning, it notifies the library, and the library automatically cleans the tape drive using a cleaning cartridge loaded in a cleaning slot. Automatic cleaning is integrated into routine library operations. The host application requests the library to move a tape cartridge. If the tape drive performing the operation needs cleaning, the library will perform the move operation and then automatically clean the tape drive with a cleaning cartridge before informing the host application that the move operation is complete.

When a cleaning cartridge has expired, a RAS ticket informs the user to export the expired tape from the library. If more cleaning cartridges are present, the next cleaning cartridge will be used for the next cleaning request. If no more cleaning cartridges are available, a RAS ticket will inform the user that the tape drive needs cleaning and that a cleaning tape needs to be imported.

Only administrators can configure cleaning slots, thus enabling AutoClean. When AutoClean is enabled, the library allows you to import and export cleaning media through the I/E Station.

For information on configuring cleaning slots, see [Configuring Cleaning Slots](#) on page 79. For information on importing and exporting cleaning media, see [Importing Cleaning Media](#) on page 180 and [Exporting Cleaning Media](#) on page 181.

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

Manual Cleaning – When a tape drive needs cleaning, it notifies the library. If the library’s AutoClean feature is not enabled (no cleaning slots have been configured), the library generates a RAS ticket informing the user that the tape drive needs cleaning. Administrators can clean tape drives manually at any time, using commands on the operator panel or Web client. For more information, see [Manually Cleaning Tape Drives](#) on page 183.

Enabling AutoClean

To enable AutoClean, an administrator must configure at least one cleaning slot in the library. For information on configuring cleaning slots, see [Configuring Cleaning Slots](#) on page 79. For a description of AutoClean, see [About Cleaning Tape Drives](#) on page 178.

Viewing the Cleaning Count

The cleaning count is the number of times a cleaning cartridge has been used to clean a tape drive. Knowing this can help you decide when to replace a cleaning cartridge. The cleaning count is now listed in two locations:

- Library Configuration Report (from the Web client, select **Reports > Library Configuration**)
- Export Cleaning Media screen (from the Web client, select **Operations > Cleaning Media > Export**)

Using Valid Cleaning Media

The preferred method of labeling a cleaning cartridge is to have **CLN** or **CLNU** as the prefix on the label. Any cartridge detected with a **CLN** or **CLNU** prefix will be considered a universal cleaning cartridge, regardless of any media identification extension. Cartridges containing a media identification of **C1**, **C2**, **C3**, **C4**, **C5**, and **CU** will be considered cleaning cartridges and will be tracked and treated as if the media label contained the prefix **CLN** or **CLNU**.

Importing Cleaning Media

When AutoClean is enabled (at least one cleaning slot has been configured), you can use the Import Cleaning Media operation to import cleaning cartridges from the I/E station to designated cleaning slots. For information on configuring cleaning slots, see [Configuring Cleaning Slots](#) on page 79. For a description of AutoClean, see [About Cleaning Tape Drives](#) on page 178.

When manual cartridge assignment is enabled (the default setting), you cannot import cartridges via the operator panel until you have assigned them to a specific partition or to the system partition. Cleaning cartridges should always be assigned to the system partition. Assigning cleaning cartridges to the system partition makes them available to all partitions in the library. For more information about manual cartridge assignment, see [Importing Media](#) on page 165 and [Disabling/Enabling Manual Cartridge Assignment](#) on page 79.

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: Once the import operation has started, do not interfere with the operation by opening and closing the I/E station door.

The process for importing cleaning cartridges includes the following steps:

- 1 Go to the front of the library and insert the cartridges into the I/E station.

Note: Do not insert cartridges into the I/E station during the restart process.

- 2 Close the I/E station door.

The **Assign I/E** screen appears on the operator panel if the **Manual Cartridge Assignment** setting is enabled on the operator panel **System Settings** screen (**Tools > System Settings**).

If the **Assign I/E** screen appears, do the following:

- a On the **Assign I/E** screen, select **System**.

The **System** button turns blue 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 79. For a description of AutoClean, see [About Cleaning Tape Drives](#) on page 178.

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: Once the export operation has started, do not interfere with the operation by opening and closing the I/E station door.

Details on exporting cleaning cartridges include:

- You must have access to the library's I/E station and the operator panel to export cleaning cartridges.
- You can only export cartridges if empty I/E station slots are available.

You need to provide the following information in the **Export Cleaning Media** screens to export cleaning media:

- **Media** – The tape cartridges that you want to export.

The screen includes information about the number of empty I/E station slots in the library. The number of cleaning cartridges you can export is limited to the number of empty I/E station slots. The screen also displays the cleaning status (usable/expired) and cleaning count (the number of times the cartridge was used to clean a tape drive) for each cleaning cartridge in the library.

Note: You can filter the list of media by entering all or part of a barcode in the **Search** text box. Use an asterisk (*) to search with wildcards. You can also sort the list by clicking on columns with bold headings. For example, selecting the **Location** column heading sorts the list by location coordinates.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Operations > Cleaning Media > Export**.
- From the operator panel, select **Operations > Export Cleaning Media**.

For step-by-step procedures, see the library's online Help. To access the online Help system, click the **Help** icon at the top right of the Web client or operator panel user interface.

Manually Cleaning Tape Drives

The **Clean Drive** screens allow administrators to manually clean tape drives.

Note: Be sure to unload the tape drive before attempting to clean it. If the tape drive is loaded with a cartridge, it will not be available for this operation.

If you have at least one cleaning slot configured (see [Configuring Cleaning Slots](#) on page 79), and you are using the Web client, you can choose to use a cleaning tape from either a configured cleaning slot or the topmost I/E station slot. If two or more cleaning slots are configured and have cleaning tapes in them, the library chooses which cleaning tape to use. If you have zero cleaning slots configured, or if you are using the operator panel, you must use a cleaning tape in the topmost I/E station slot. You are prompted to insert a cleaning cartridge in the appropriate slot and select the tape drive you want to clean. The library then takes the associated partition offline, moves the cleaning cartridge from the I/E station slot to the designated tape drive, and cleans the tape drive. You will be asked to confirm that you want to take the partition offline.

When the operation is complete, the library moves the cleaning cartridge back to the I/E station slot and takes the partition back online.

Note: If the operation does not complete successfully, the partition remains offline until you turn it back online manually or restart the library (see [Taking a Partition Online or Offline](#) on page 78).

Note: If your library has zero I/E station slots, you will not be able to manually clean tape drives. See [Configuring I/E Station Slots](#) on page 81.

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:

- Create a firmware upgrade (FUP) tape. A FUP tape can be created of a tape drive firmware version already in use in your library. For more information, see [Using an Image File to Upgrade Tape Drive Firmware](#) on page 202.
- Erase a FUP tape. When a FUP tape is no longer needed, you can erase it and reuse it as a data cartridge or again as a FUP tape. For more information, see [Erasing a FUP Tape](#) on page 205.
- Upgrade tape drive firmware using a FUP tape. For more information, see [Using a FUP Tape to Upgrade Tape Drive Firmware](#) on page 206.
- Upgrade tape drive firmware using a firmware image file. For more information, see [Using an Image File to Upgrade Tape Drive Firmware](#) on page 202.
- Retrieve tape drive logs. Tape drive logs can be retrieved from any tape drive installed in the library. For more information, see [Retrieving Tape Drive Logs](#) on page 391.
- 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 392.
- Clean tape drives. Tape drive can be cleaned manually at any time. For more information, see [About Cleaning Tape Drives](#) on page 178.

- 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 208.
- 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 411.

Locking and Unlocking the I/E Stations

Each 5U Library Control Module and 9U Library Expansion Module has an I/E station door with multiple open and close sensors. A secondary door located behind the I/E station door acts as a redundant indicator as to whether the I/E station is opened or closed. When you are finished accessing the I/E station, make sure the station door is fully closed.

Administrators can use this operation to lock or unlock the doors for all I/E stations that are configured as I/E station slots. If all I/E station slots are configured as storage, this operation unlocks the 5U Library 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 5U Library Control Module. When the I/E station is unlocked, you can open the main access door on the 5U Library 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**.

Manually Unlocking the I/E Station Door

While the recommended procedure is to unlock the I/E station door using the **Operations > I/E Station Lock/Unlock** command, you can, if necessary, unlock the I/E station door manually.

The process for manually unlocking the I/E station door includes the following steps:

- 1 Standing in front of the library, look for the small (0.25 inches in diameter) access hole on the front of the I/E station door.
- 2 Insert a pencil-shaped object into the access hole and press inward.

If an I/E station is configured as storage, the station door will lock automatically when you close it, assuming that the library is powered on. If you unlocked the door while the library was powered off, the door will lock automatically during power up.

Controlling FC I/O Blade Power

Administrators can turn on, turn off, or power cycle individual FC I/O blades in the library. Turning off or power cycling the FC I/O blade will cause a temporary loss of communication with connected hosts. The screen will display a warning message about the communication loss and ask you to confirm that you want to proceed.

The **Setup - Blade Control** screen allows you to perform the following operations on the selected FC I/O blades:

On the Web client:

- Click **On** to turn on the FC I/O blade.
- Click **Off** to turn off the FC I/O blade.
- Click **Cycle** to power cycle the FC I/O blade. It takes approximately 3 minutes to power cycle a blade.

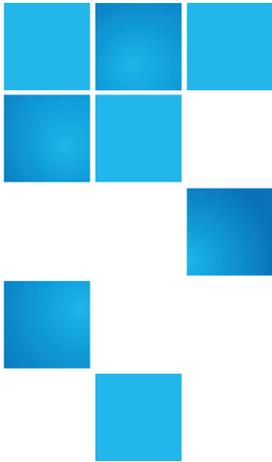
On the operator panel, select the option you want:

- Power Cycle Blade
- Power On Blade
- Power Off Blade

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

The paths to open the appropriate screens are as follows:

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



Getting Information – Logs and Reports

This chapter describes how to find information about your library.

From the operator panel, you can find system information in the **About ML6000** screen (**Tools > About Library**). From the Web client, you can find information in the **Reports** and **Tools** menus.

Note: Users without administrator privileges can view only certain reports. See [User Privileges](#) on page 54 for information about user privileges.

Viewing Information About the PowerVault ML6000

The **About** screen gives you a quick glance at your library settings.

From the Web client, you can view the **About ML6000** report, which provides the following information about the library:

- Serial Number
- Service Tag
- Firmware Version Number

From the operator panel, the **About** screen provides the following information about the library:

- Library name
- State
- Serial number
- Service Tag
- 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 > ML6000**.
- From the operator panel, select **Tools > About Library**.

Viewing the System Information Report

The System Information Report contains information on the following library settings:

- **Date and time** – current date, time, and time zone settings
- **Physical library** – host name, Internet Protocol (IP) address(es), serial number, firmware version, board support package (BSP) level, the date the BSP was last updated, and robot firmware version.
- **Encryption** (this section displays only if encryption key management is licensed and configured on the library) – key server type; encryption software version; SSL connection (enabled/ disabled); primary host (primary key server IP address or host name), primary

key server port number; primary key server serial number; secondary host (secondary key server IP address or host name); secondary key server port number; secondary key server serial number.

- **Library Partitions** – name, serial number, control path, mode, encryption method, encryption system type, number of slots, number of media, and number of tape drives configured for each partition.
Tape drives – location coordinates, vendor name, model, type, physical serial number (P-SN), logical serial number (L-SN), firmware level, sled boot version, sled application version, encryption method, and whether the tape drive is connected to an I/O blade.
- **FC I/O blades** – if the library contains FC I/O blades, this table lists the location coordinates, World Wide Node Name (WWNN), firmware level, and ready status.

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

Viewing the Library Configuration Report

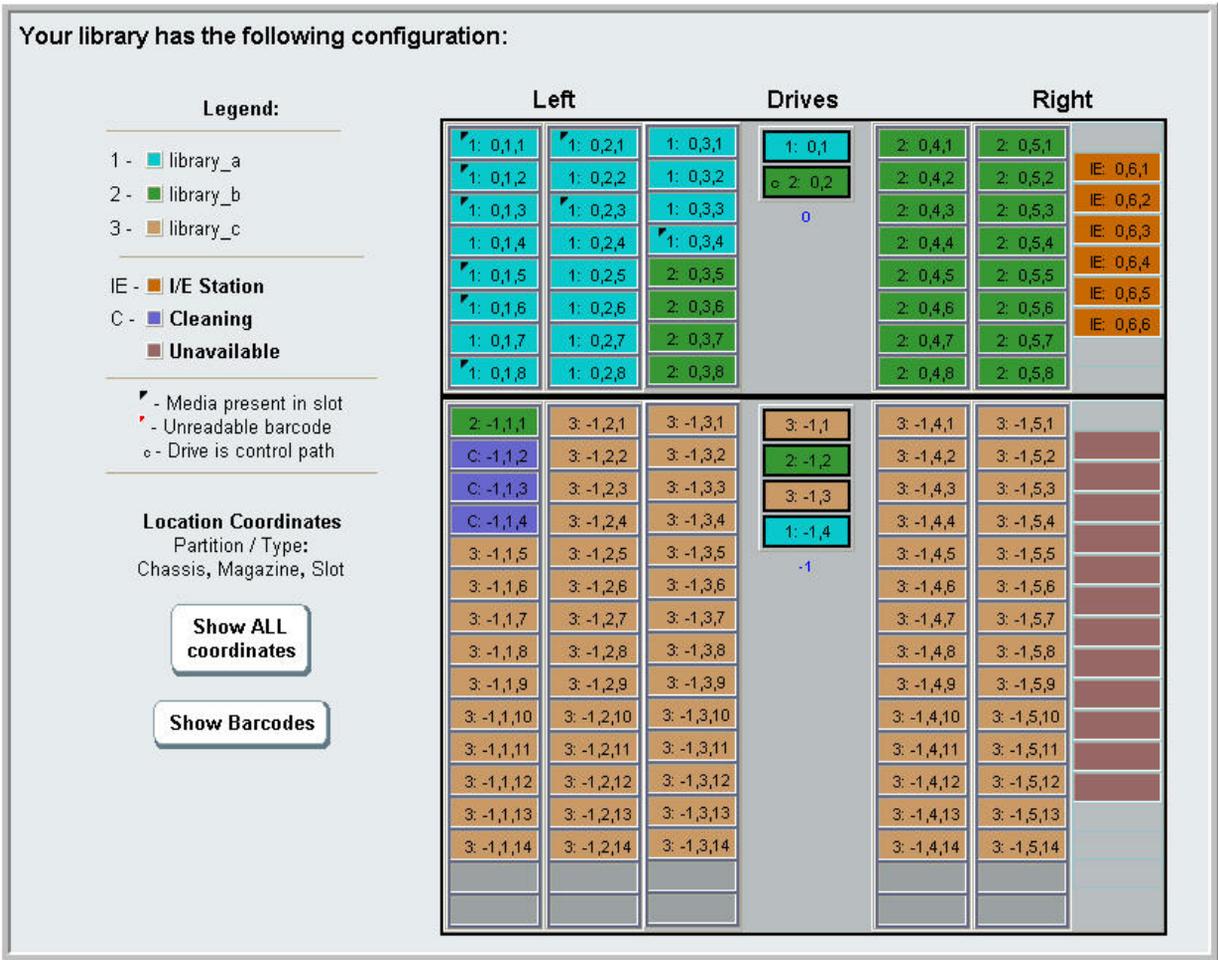
The Library Configuration Report is a dynamic representation of the physical locations of various library resources, including tape drives, slots, partitions, and modules.

Each partition's slots are displayed in a unique color, indicated in the legend. I/E station slots, cleaning slots, and unavailable slots are also displayed in unique colors. A black triangle in the upper left corner of a slot indicates media is present in the slot. A red triangle indicates media is present but the media barcode label is unreadable. A "c" in a tape drive indicates the drive is the control path for the partition.

By default, the Library Configuration Report displays the coordinates for all licensed slots that are assigned to a partition. To view all library slot coordinates, click **Show ALL coordinates**. To display the barcodes for all imported cartridges, click **Show Barcodes**.

[Figure 18](#) shows an example of the Library Configuration Report.

Figure 18 Library Configuration Report



Use the report to view detailed information on the following resources. Click on the item you want to view and the information appears in a box to the right of the library diagram.

- **Tape drives** – Depending on the interface type, the information provided may not include all of the following: interface type, tape drive type, ready state, mode (online/offline), assigned partition name, location coordinates, media barcode (“No_Label” means unreadable barcode), media type, element address, vendor, model,

physical SN, logical SN, World Wide Node Name (WWNN), World Wide Port Name (WWPN), loop ID, topology request, speed request, actual topology, actual speed, maximum speed, active port (if the drive has more than one FC port), 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, and put retries. If the slot is a cleaning slot, the cleaning status (usable/expired) and cleaning count (the number of times the cartridge was used to clean a tape drive) are also displayed. For more details about slot data, see [Viewing the All Slots Report](#) on page 194.
- **Partitions** – Name, online status, barcode policy, number of total tape drives in the partition, number of active tape drives partition, total media, mounted media, total slots, full slots, total I/E stations, full I/E stations, and encryption method of each partition.
- **Modules (Chassis)** – Manufacturer, model type, and serial number of each module.

You can print the report by clicking on the printer icon in the report window.

The path to open the report from the Web client is **Reports > Library Configuration**.

Viewing the Network Settings Report

The Network 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.
 - **Access:** Indicates whether the SMI-S port for SMI-S traffic to the library (port 5988) is enabled or disabled. You can change the setting via the operator panel, **Tools > Security** menu. The default setting is enabled.
 - **State:** Indicates whether allowing SMI-S to run on the library is enabled or disabled. You can change this setting on the operator panel, **Tools > System Settings**. The default is disabled.
- **SNMP** – access enabled/disabled, V1 enabled/disabled, V2 enabled/disabled, V3 enabled/disabled, algorithm, encryption enabled/disabled, and port.
- **SNMP-Traps** – IP addresses and ports.

The path to open the report from the Web client is **Reports > Network Settings**.

Viewing Logged-in Users

The Logged-in User's Report report contains information about the users that are currently logged into the library. The report contains the following information:

- **User name** – Name of logged-in user.
- **Role name** – Privilege level of logged-in user (for example, **Admin** for administrator, **User** for non-administrator, non-service user).
- **Login date and time** – Date and time the user logged into the library.
- **Last activity date and time** – Date and time the user last logged into the library.
- **Login location** – IP address or host name of the system being used to access the system.

- **Management interface** – User interface being used to access the system (Web client or operator panel).

The path to open the report from the Web client is **Reports > Logged in Users**.

Viewing the All Slots Report

The All Slots Report contains information on all slots that are currently assigned to a partition and all I/E slots. A maximum of 20 responses displays per page. You can scroll between the pages using the page arrows at the bottom left of the screen. The report contains the following information about each slot:

- **Slot type** – Drive, I/E station, cleaning, or storage slot.
- **Barcode** – Barcode number of the cartridge installed in the slot (no barcode number means the slot is empty).
- **Partition** – The partition that owns the slot.
- **Location** – Location coordinates of the slot. (For a description of location coordinates, see [Understanding the Location Coordinates](#) on page 35.)
- **Element Address** – Element address of the slot.
- **Encryption** – The encryption state of the media in the slot. In order for the library to know the encryption state, the tape must have been placed into an encryption-capable tape drive in the library. The encryption-capable tape drive reads and records the encryption state of the tape, and the encryption state displays as “Encrypted” or “Not Encrypted.” If the tape was not placed into an encryption-capable tape drive in the library, or if the slot is empty, the encryption state displays as “Unknown.”
- **Get Count** – The number of times the picker successfully removed a tape from the slot.
- **Get Retries** – The number of times the picker had to perform a recovery operation to remove a tape from the slot.
- **Put Count** – The number of times the picker successfully placed a tape into the slot.

- **Put Retries** – The number of times the picker had to perform a recovery operation to place a tape into the slot.

Note: “Get” and “put” counts and retries are counted from the beginning of library use to the present. If the LCB compact flash card is replaced, the count starts over at zero.

The path to open the report from the Web client is **Reports > All Slots**.

Viewing, Saving, and E-mailing Library Logs

The library collects specific information in log files that you can view onscreen, save to your computer, or e-mail to a recipient. The following library logs are available:

- **Installation Verification Test Summary Log** – This log is saved each time you run the Installation Verification Test (IVT). The log saves only the information from the most recently run test. If you run the test again, the new information overwrites the previous information. This option presents the summary log. For more information, see [Using the Installation Verification Test](#) on page 405.
- **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 405.
- **Command History Log** – Available only if you are using FC I/O blades. When you select this report, you choose the FC I/O blade and device for which you want to run the report. The **Blade** menu lists all FC I/O blades installed in the library (if more than one are installed). The **Devices** menu lists the devices associated with the selected FC I/O blade. The report shows all commands from the selected device to the selected blade. When the log file reaches its maximum size, the oldest information is replaced as new information is added.

- **Cleaning Log** – Shows all cleanings that have been performed in the library since firmware version 520G was installed. When the log reaches its maximum size, the oldest information is replaced as new information is added. The comma-separated values (csv) file provides the following information:

Date Time (date and time); Barcode (barcode of the cleaning cartridge); Tape (location coordinates of the cleaning cartridge); Drive (location coordinates of the tape drive that was cleaned); Status (pass/fail); Return Code (service use only), Cleaning Type (Manual, Auto, MoveMedium), Expired (“Invalid” if the tape is expired or a data tape was improperly used to clean; “-” if not applicable); Usage Count (“N/A” if the cleaning did not complete); Reserved.
- **Slot Position Log** – Shows current information for all slots in the library. The comma-separated values (csv) file provides the following information for each slot:

Date and Time, Slot Type (Picker, Drive, Storage, or IE), Object Present? (Y, N), Location Coordinates, X Position, Y Position, Angle Position, X Calibration Offset, Y Calibration Offset.
- **RAS Tickets Log** – Records all RAS tickets for the library. When the log file reaches its maximum size, the oldest information is replaced as new information is added.
- **Media Security Log** – Lists media that have been completely removed from the library. This log is only available if you have an Advanced Reporting license installed on the library (see [Obtaining and Installing a License Key](#) on page 88), and you have enabled the library to collect data for the log file. For more information about this log and how to enable the library to collect data for the log, see [Configuring and Viewing the Media Security Log](#) on page 140.
- **Media Usage Log** – Lists information regarding data written and read on the medium and lists statistics pertaining to soft and hard read and write errors. This log is only available if you have an Advanced Reporting license installed on the library (see [Obtaining and Installing a License Key](#) on page 88). For more information about the information displayed in this log, see [Viewing the Media Usage Log](#) on page 141.

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

Viewing FC I/O Blade Information

Administrators can view information about all the FC I/O blades installed in the library. The **Tools - Blade Information** screen lists the following FC I/O blade information:

- **Location** – Library location coordinates of the blade: [module,blade#], where blade# is 1 for the top blade in the module and 2 for the bottom blade in the module.
- **Firmware Version** – Firmware version of the blade (part of the library firmware).
- **Serial Number** – Serial number of the blade.
- **WWNN** – World Wide Node Name of the blade.
- **CCL** – Command control LUN.
- **Status/State** – The status of the blade can be: Ready, Not Ready, Auto Level Failed, Auto Leveling Booting, and Unknown.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Tools > I/O Blade Info**.
- From the operator panel, select **Tools > Blade Info**.

Viewing FC I/O Blade Port Information

Administrators can view information about all the FC I/O blades installed in the library. The **Tools - Blade Port Information** screen lists the following port information for each FC I/O blade:

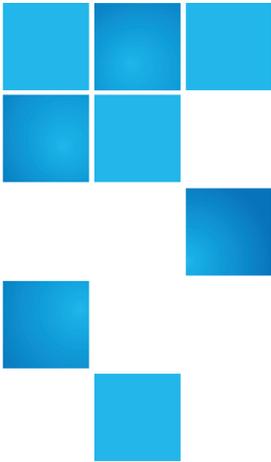
- **Port number** – The port number: 1–6.
- **WWPN** – World Wide Port Name of the port.
- **Status** – The status of the blade: Config wait, Loop init, Login, Ready, Lost Sync, Error, Re-Init, Non part, and Failed.

- **Actual Speed** – Negotiated speed of the port: 1 Gb/s, 2 Gb/s, or 4 Gb/s. If the port is not in a ready state, “N/A” displays.
- **Actual Loop ID** – Negotiated loop ID of the port: 0-125. On the Web client, if the port connection type is Point to Point, or if the port is not in a ready state, “N/A” displays. On the operator panel, if the port is not in a ready state, “N/A” displays.
- **Requested Speed** – Requested speed of the port: Auto, 1 Gb/s, 2 Gb/s, 4 Gb/s, or 8 Gb/s (Web client only).
- **Requested Loop ID** – Requested loop ID of the port: Auto or 0-125 (Web client only).
- **Framesize** – Framesize setting of the port: 528, 1024, or 2048.
- **Mode** – Mode of the port: Public or Private.
- **Role** – Role of the port: Target (ports 1-2) or Initiator (ports 3-6).
- **Connection** – Connection type of the port: Loop, Point to Point, or Loop Preferred.

For information about configuring FC I/O blade ports, see [Configuring FC I/O Blade Ports](#) on page 110.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Tools > I/O Blade Port Info**.
- From the operator panel, select **Tools > Blade Info > Port Info**.



Updating Library and Tape Drive Firmware

There are two types of firmware that can be upgraded on the library: library firmware (including drive sled firmware) and tape drive firmware. There may be times when you will need to upgrade your library and tape drive firmware as directed by Dell Technical Support. You can also regularly monitor the Dell Support Website at <http://support.dell.com> for firmware upgrades, but you need to make sure that the firmware you download is compatible with your library and tape drives.

Note: Check the information provided on the Dell Support Website at <http://support.dell.com> to verify 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. You can download library firmware upgrades from the Dell Support Website: <http://support.dell.com>. Library firmware version 200G.GSxxx and 210G.GSxxx support library configurations of up to 14U. Library firmware 300G.GSxxx supports library configurations up to 23U. Library firmware versions 320G.GSxxx

and higher support library configurations up to 41U. Make sure you are running the appropriate firmware version to support the size of your library. It is recommended that you use the most current version of firmware regardless of library size.

It is recommended that you resolve and close all open RAS tickets before upgrading library firmware. If Auto-Ticket Closure is enabled, all open RAS tickets will be closed during the reboot which occurs after firmware is upgraded (see [Closing RAS Tickets Automatically](#) on page 380).

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 384.

It is also a good idea to capture a library snapshot information before making any significant change to your system such as upgrading library firmware. Technical support personnel can, if necessary, use the snapshot file to troubleshoot the library. For more information, see [Capturing Snapshots of Library Information](#) on page 381.

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 384.

Note: If you are running firmware code level 400G or later and your library has Fibre Channel (FC) I/O blades installed, you can downgrade to level 400G or later. 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 code.

Note: If your library is running firmware version 600G or later, you can only downgrade library firmware to version 410G or later. If you need to downgrade to a version earlier than 410G, contact Dell Technical Support (see [Appendix C, Contacting Dell](#)) for assistance.

Note: If you purchased your library after October 15, 2008, you cannot downgrade library firmware to below version 520G.

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

Note: The library automatically restarts after the firmware upgrade is complete. Before logging into the library, clear the Web browser cache. See your Web browser's documentation for instructions on how to clear the cache.

You can find instructions on updating library firmware in the library firmware upgrade package you download from the Dell 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**.

Upgrading Tape Drive Firmware

Dell provides tape drive firmware upgrades that allow you to upgrade your tape drive firmware over the SCSI, FC, FC I/O blade, or SAS connection from the host application. This is the Dell-recommended method for updating tape drive firmware. You can download the firmware upgrade package from the Dell Support Website. For more information, see [Downloading Tape Drive Firmware From the Dell Support Website](#) on page 207.

If necessary, you can use the Web client to upgrade one or more tape drives in your library with an image file downloaded from the Dell Support Website.

You can also create a Firmware Upgrade (FUP) tape of a tape drive firmware version already installed in your library. A FUP tape contains a specific version of tape drive firmware. You can then use the tape to transfer firmware to one or more tape drives installed in the library.

The following topics provide information on these procedures.

Using an Image File to Upgrade Tape Drive Firmware

The Web client allows you to upgrade tape drive firmware using a firmware image file. The firmware upgrade can take up to 40 minutes .

Tape drive firmware and updating instructions are available at the Dell Support Website: <http://support.dell.com>. You can navigate to your product's firmware from the home page. Select the appropriate firmware version and download the file to your computer hard drive. The Dell Support Website provides information that can help you to verify that the library is running the appropriate level of tape drive firmware, compatible with the tape drive type.

Details on using an image file to upgrade tape drive firmware include:

- The library allows you to upgrade firmware on multiple tape drives at one time. Upgrade firmware on all tape drives of the same interface type at the same time to make sure that all drives are at the same firmware level. Having different levels of drive firmware in the library is not recommended.
- Each tape drive interface type requires unique firmware. The image file must contain the appropriate SCSI, FC, or Serial Attached SCSI (SAS) firmware image for the corresponding SCSI, FC or SAS drive type.
- The tape drive and associated partition are automatically taken offline during the operation and brought back online when the operation completes. You will be asked to confirm that you want to take the tape drive and partition offline.

Note: If the operation does not complete successfully, the partition remains offline until you turn it back online manually or restart the library (see [Taking a Partition Online or Offline](#) on page 78).

You can find detailed instructions on updating library firmware on the Dell 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: Since tape drives restart after a firmware upgrade, make sure that cartridges are not loaded in the applicable tape drives before upgrading firmware.

Caution: Do not turn off power to the library during the upgrade process. Turning off power to the library during the upgrade can cause problems with the library.

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

You cannot upgrade tape drive firmware with an image file from the operator panel. The path to the appropriate screen is as follows:

- From the Web client, select **Tools > Drive Operations**.

Creating a FUP Tape

A FUP tape is a tape cartridge that is used to transfer upgraded tape drive firmware code to the library. When you create a FUP tape, you save a copy of a tape drive firmware version already in use in your library. The drive code image is copied onto the FUP tape, which you can then use to upgrade the drive firmware on all of the specified drives within the library. Drive code versions are independent of the library versions.

The entire process of creating a FUP tape can be performed using the operator panel. If you choose to create the tape using the Web client, be aware that part of the process must be performed on the operator panel and that you will need access to the physical library.

Details on creating FUP tapes include:

- FUP tapes are created using a blank, or scratch, tape.
- FUP tapes can be reused.
- Each tape drive interface type requires a unique firmware image. FUP tapes must contain the appropriate SCSI, FC, or SAS firmware image for the corresponding SCSI, FC, or SAS drive type.
- You cannot use an LTO-1 tape in LTO-3 tape drives, or LTO-1 or LTO-2 tapes in LTO-4 tape drives, or LTO-1, LTO-2, or LTO-3 tapes in LTO-5 tape drives, to create FUP tapes.
- You can select only empty tape drives to perform this operation. If the tape drive you want to use contains a tape cartridge, you will need to unload it first.
- The tape drive and associated partition are automatically taken offline during the operation and brought back online when the operation completes. You will be asked to confirm that you want to take the tape drive and partition offline.

Note: If the operation does not complete successfully, the partition remains offline until you turn it back online manually or restart the library (see [Taking a Partition Online or Offline](#) on page 78).

You can find step-by-step instructions for FUP tape operations 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: Any data on the scratch tape will be overwritten when you create the FUP tape.

The paths to open the appropriate screens are as follows:

- From the operator panel, select **Tools > Drive Mgmt.**
- From the Web client, select **Tools > Drive Operations.**

Erasing a FUP Tape

When the tape drive firmware version on a FUP tape is no longer needed, it can be erased and the tape can be reused as a data cartridge.

Use this operation only when you need to reuse a FUP tape as a data cartridge. It is not necessary to erase a FUP before updating it with new tape drive firmware. In addition, this operation should not be used to erase information on data cartridges.

The entire process of erasing a FUP tape can be performed using the operator panel. If you choose to create the tape using the Web client, be aware that part of the process must be performed on the operator panel and that you will need access to the physical library.

Details on erasing FUP tapes include:

- The tape drive and associated partition are automatically taken offline during the operation and brought back online when the operation completes. You will be asked to confirm that you want to take the tape drive and partition offline.

Note: If the operation does not complete successfully, the partition remains offline until you turn it back online manually or restart the library (see [Taking a Partition Online or Offline](#) on page 78).

- You can select only empty tape drives to perform this operation. If the tape drive you want to use contains a tape cartridge, you will need to unload it first.

You can find step-by-step instructions on erasing FUP tapes 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.

The paths to open the appropriate screens are as follows:

- From the operator panel, select **Tools > Drive Mgmt.**
- From the Web client, select **Tools > Drive Operations.**

Using a FUP Tape to Upgrade Tape Drive Firmware

You can upgrade tape drive firmware using a FUP tape. A FUP tape contains a specific version of tape drive firmware and is used to transfer the firmware to one or more tape drives within the library. For information on creating FUP tapes, see [Creating a FUP Tape](#) on page 204.

Make sure to upgrade the library with the appropriate level of tape drive firmware, compatible with the tape drive type. To determine the appropriate drive firmware, see the library's release notes or contact Dell Technical Support. The Dell Support Website, <http://support.dell.com>, provides information that can help you to verify that the library is running the appropriate level of tape drive firmware, compatible with the tape drive type.

The entire process of updating tape drive firmware with a FUP tape can be performed using the operator panel. If you choose to perform the operation using the Web client, be aware that part of the process must be performed on the operator panel and that you will need access to the physical library.

Details on using a FUP tape to upgrade tape drive firmware include:

- Upgrade firmware on all of the drives in the library at the same time to make sure that all of the 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 a unique firmware image. FUP tapes must contain the appropriate SCSI, FC, or SAS firmware image for the corresponding SCSI, FC, or SAS drive type.
- You cannot use an LTO-1 tape in LTO-3 tape drives, or LTO-1 or LTO-2 tapes in LTO-4 tape drives, or LTO-1, LTO-2, or LTO-3 tapes in LTO-5 tape drives, to create FUP tapes. See [Creating a FUP Tape](#) on page 204 for more information.

- 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 logical library offline.

Note: If the operation does not complete successfully, the partition remains offline until you turn it back online manually or restart the library (see [Taking a Partition Online or Offline](#) on page 78).

You can find step-by-step instructions for FUP tape operations in your library's online Help. To access the online Help system, click the **Help** icon at the top right of the Web client.

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 administrators. You can access the appropriate screens, but you cannot apply changes while another administrator is performing the same operation.

The paths to open the appropriate screens are as follows:

- From the operator panel, select **Tools > Drive Mgmt.**
- From the Web client, select **Tools > Drive Operations.**

Downloading Tape Drive Firmware From the Dell Support Website

Dell provides tape drive firmware upgrades that allow you to upgrade your tape drive firmware over the SCSI, FC, FC I/O blade, or SAS connection from the host. You can upgrade all of your tape drives

through the host connection. Alternatively, once you have upgraded at least one tape drive through the host connection, you can create a FUP tape to upgrade other tape drives to the same level.

You can download tape drive firmware from the Dell Support Web site: <http://support.dell.com>. The firmware upgrade package contains an image file, a drive vendor tool, and instructions for using the tool to upgrade the tape drive firmware over the SCSI, FC, FC I/O blade, or SAS connection from the host. This is the Dell-recommended method for updating tape drive firmware.

Downgrading LTO-4 Tape Drive Firmware

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 Dell Technical Support for instructions and assistance.

Autoleveling Tape Drive Firmware

The autoleveling feature enables you to automatically upgrade firmware on all FC tape drives that are connected to the FC I/O blades. This allows you to keep all FC tape drives of the same type (for example, LTO-5) at the same firmware level. Tape drive firmware is checked whenever a tape drive is reset, such as when the library is power cycled or restarted, or whenever a tape drive is added or replaced. If the firmware does not match, the tape drive firmware is autoleveled.

FC tape drives must be connected to an FC I/O blade to participate in autoleveling operations. The library does not support autoleveling FC tape drives connected directly to an FC host or switch. In addition, the library does not support autoleveling SCSI or SAS tape drives.

To enable autoleveling, you must upload a firmware image file to the library. If you have multiple versions of FC tape drives installed in your library (for example, LTO-4 and LTO-5), you must upload a unique firmware image file for each version. You can also delete a firmware image file when you no longer want to autolevel tape drive firmware.

Uploading Tape Drive Firmware Used in Autoleveling

Before uploading tape drive firmware, verify with published release notes or Dell Technical Support that you are uploading the correct version of firmware. For contact information, see [Appendix C, Contacting Dell](#).

You must have access to a tape drive firmware image file to enable autoleveling. Tape drive firmware is available at <http://support.dell.com>. 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 > Upload/remove tape drive firmware for autoleveling**.

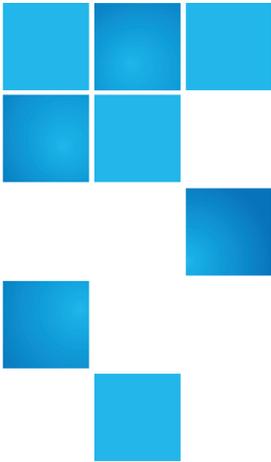
Deleting Tape Drive Firmware Used in Autoleveling

The library allows you to delete a firmware image file if you no longer want to autolevel tape drive firmware. In addition, you might want to delete a firmware image file if your library no longer contains a specific version of tape drives. For example, if you replace all LTO-3 tape drives with LTO-4 tape drives, you no longer need the LTO-3 firmware.

You can find step-by-step instructions in your library's online Help. To access the online Help system, click the **Help** icon at the top right of the Web client or operator panel user interface.

You cannot upload tape drive firmware from the operator panel. The path to the appropriate screen is as follows:

- From the Web client, select **Tools > Drive Operations > Upload/remove tape drive firmware for autoleveling**.



Chapter 12

Installing, Removing, and Replacing

This chapter describes how to add, remove, and replace hardware within your library. Adding, removing, or replacing library components may require you to power off the entire library. There are a few components, however, that you can service without powering off the library, such as replacing tape drives. Instead, you may only need to take a specific partition offline, or you may not need to impact the status of the library at all.

Warning: All libraries taller than 14U must be installed in a rack having a main protective earthing (grounding) terminal, and power must be supplied via an industrial plug and socket-outlet and/or an appliance coupler complying with IEC 60309 (or an equivalent national standard) and having a protective earth (ground) conductor with a cross sectional area of at least 1.5 mm² (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 5U Library Control Module weighs approximately 60 lbs (27.2 kg). A 9U Library Expansion Module, without tape drives, tape cartridges, or power supplies, exceeds 65 lbs (29.5 kg).

To avoid serious injury, at least two people are required to safely lift the modules.

Caution: ML6030 (and higher) CM and Expansion Modules require professional installation. Professional installation may have been included with your purchase. Please call 1-800-945-3355 to schedule professional installation of your PowerVault library.

- [Cabling Libraries With Fibre Channel Tape Drives Connected to Fibre Channel I/O Blades](#)
- [Recommended Library Cabling for FC I/O Blades](#)

Taking the Library Online/Offline

An online library allows a host application to fully control library operations. Taking a library offline switches library control to the user interfaces and limits host application command requests.

Taking a Library Online

To take an entire library online, take all of its partitions online.

- 1 Using the library's operator panel, select **Operations > Change Partition Mode**; or, using the Web client, select **Operations > Partitions > Change Mode**.
- 2 For each partition that you want to take online, click **Online**.
- 3 Click **Apply**.

Taking a Library Offline

To take an entire library offline, take all of its partitions offline.

- 1 Using the library's operator panel, select **Operations > Change Partition Mode**; or, using the Web client, select **Operations > Partitions > Change Mode**.
- 2 For each partition that you want to take offline, click **Offline**.
- 3 Click **Apply**.

Cabling the Library

Use the following cabling procedure appropriate for your drive type.

- [Specific Instructions for LTO-5 and LTO-6 Tape Drives](#) on page 212
- [Cabling Libraries With SCSI Tape Drives](#) on page 214
- [Cabling Libraries With SAS Tape Drives](#) on page 219
- [Cabling Libraries With Fibre Channel Tape Drives Connected Directly to a Host or Switch](#) on page 224
- [Cabling Libraries With Fibre Channel Tape Drives Connected to Fibre Channel I/O Blades](#) on page 228
- [Recommended Library Cabling for FC I/O Blades](#) on page 234

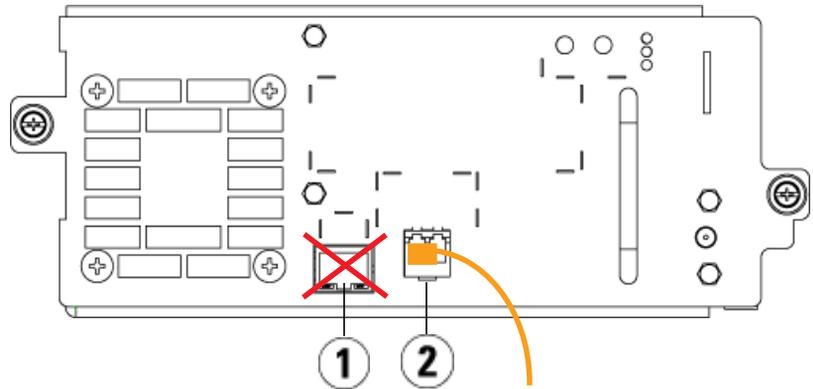
Specific Instructions for LTO-5 and LTO-6 Tape Drives

The library handles the Ethernet and Fibre Channel data ports on LTO-5 and LTO-6 tape drives differently depending on the tape drive. See [Figure 19](#) and [Figure 20](#) for details.

Figure 19 LTO-5 Single Port

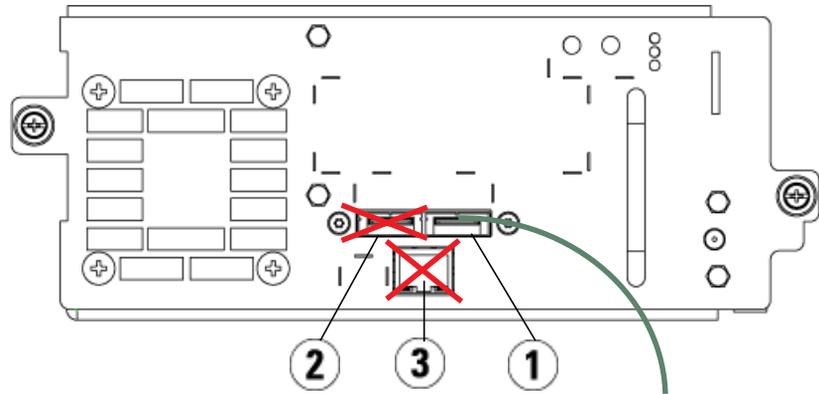
Caution: LTO-5 Fibre Channel tape drives can be configured for speeds of up to 8 GB per second and support auto-negotiation to 8 Gb/s, 4 Gb/s, and 2 Gb/s. If they are configured for 8 Gb/s, you should connect them directly to a host or switch and not to an FC I/O blade, because the FC I/O blade only allows speeds up to 4 Gb/s. If you connect an LTO-5 Fibre Channel tape drive to an FC I/O blade, the speed will autonegotiate to 4 Gb/s (see [Setting Tape Drive Parameters](#) on page 84). Speeds less than 2 Gb/s are not supported.

Fibre Channel Tape Drive



-
- 1 Ethernet port - do not use
 - 2 Fibre Channel port - use this port
-

Figure 20 LTO-5 Dual Port
SAS Tape Drive



-
- 1 SAS port 1 - use this port
 - 2 SAS port 2 - do not use
 - 3 Ethernet port - do not use
-

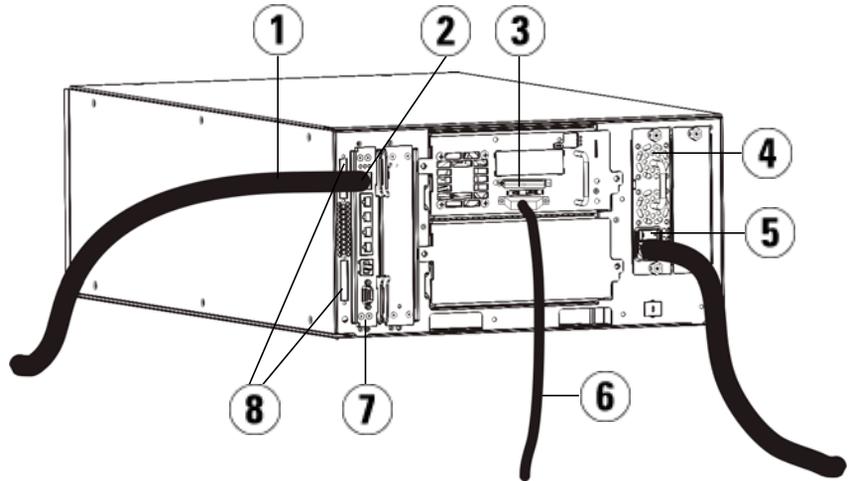
Cabling Libraries With SCSI Tape Drives

Use this procedure, along with [Figure 21](#) and [Figure 22](#), 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 mm² (14 AWG).

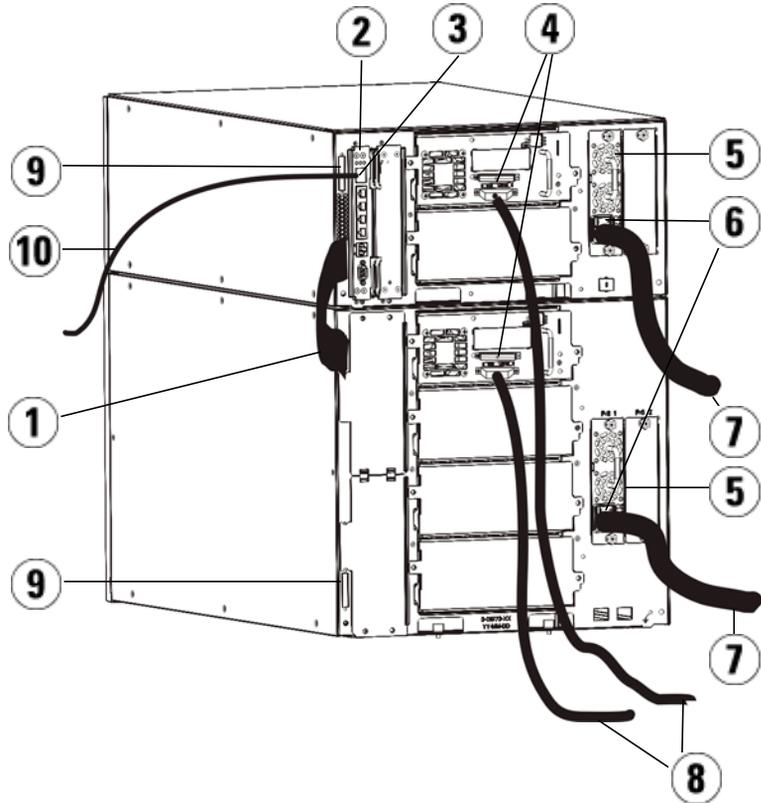
To ensure proper airflow and access space, Allow 60 cm (24 inches) in the front and back of the library.

Figure 21 Stand-Alone 5U
Library 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 22 Multi-Module SCSI
Cabling



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

- 1 If your library is larger than 14U, install it in a rack. See [Installing the Library in a Rack](#) on page 333 for instructions. The instructions include procedures for removing and replacing tape drives.
- 2 Connect the SCSI cables to the tape drives. There are two recommended ways to cable SCSI tape drives: one tape drive per SCSI bus or two tape drives per SCSI bus (see [Figure 23](#)).

Note: To avoid possible performance issues, do not connect more than two SCSI drives per SCSI bus.

Caution: The library supports a maximum cable length of 12 meters (including internal wiring) for Ultra 160 SCSI and Ultra 320 SCSI cables.

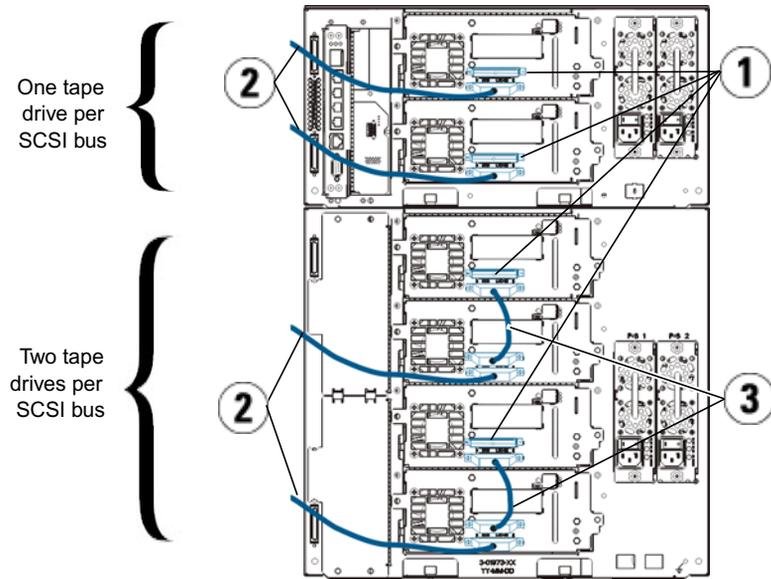
To connect one tape drive per SCSI bus:

- a Use a SCSI cable to connect the bottom port of the tape drive to your host.
- b Use a SCSI terminator to terminate the top port of the tape drive.

To connect two tape drives per SCSI bus:

- a Connect one end of the SCSI cable to the top SCSI port of the bottom tape drive. Then connect the other end of the cable to the bottom SCSI port of the tape drive above. The SCSI cable connecting the two tape drives should be at least 30 cm in length.
- b Use another SCSI cable to connect the bottom tape drive of the SCSI bus to your host.
- c Use a SCSI terminator to terminate the top tape drive of the SCSI bus.

Figure 23 Cabling One or Two
Tape Drives Per SCSI Bus



-
- 1 SCSI terminator
 - 2 SCSI drive-to-host cable
 - 3 SCSI cable connecting two SCSI tape drives
-

3 Connect the module terminators.

Caution: The module terminator is not the same as a SCSI terminator. Using a SCSI terminator instead of a module terminator will damage the library.

- a** Using the module terminators, terminate the top and bottom modules in the library stack. Install one module terminator in the top terminator connector on the topmost module and one in the bottom terminator connector on the bottommost module.

If your library configuration consists of a single module, place module terminators in the module's top and bottom module terminator connector.

- b** If you need to add 9U Library Expansion Modules to the 5U Library Control Module, remove the module terminator from the 5U Library Control Module terminator connection that is closest to the 9U Library Expansion Module.
 - c** Replace the module terminator in the 9U Library Expansion Module in the terminator connection that is furthest from the 5U Library Control Module.
- 4** Connect the module-to-module cable from the 5U Library Control Module to the 9U Library 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 5U Library Control Module. If redundant power supplies are used, connect a power cord to each of the additional power supply outlets.

- 7** Power on the library.
 - a** Turn on the rear power switch of each of the power supplies.
 - b** Turn on the front power button.
 - c** Power up the host system.
- 8** Verify communication with all devices on the bus.
- 9** Configure the library using the commands on the operator panel. See configuration information in [Configuring Your Library](#) on page 56.

Cabling Libraries With SAS Tape Drives

Each SAS tape drive should be connected directly to the host bus adapter (HBA) using one SAS cable. The LTO-4 and LTO-5 SAS tape drives in the Dell PowerVault ML6000 library use the SFF-8088 type SAS connector. The connector needed on the host end of the cable depends on the type of Host Bus Adapter (HBA) being used.

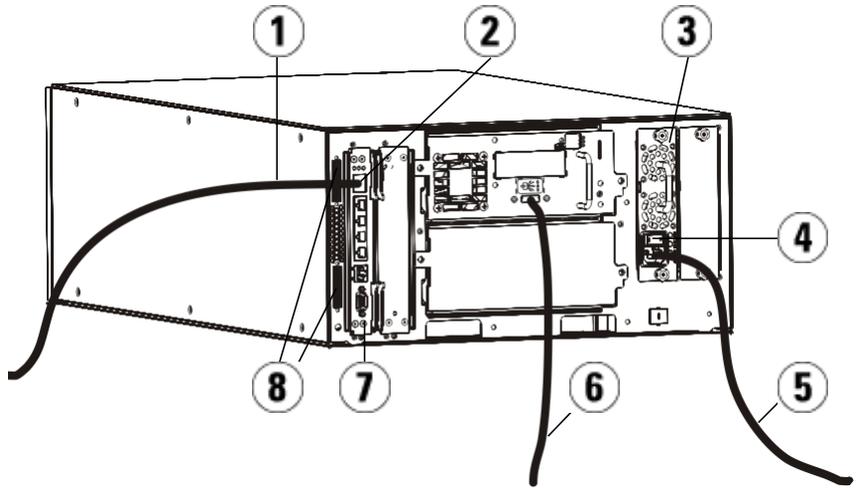
The library does not support daisy-chaining SAS cables. The library does not support the use of SAS expander devices or cables at this time.

Use this procedure, along with [Figure 24](#) and [Figure 25](#), 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 mm² (14 AWG).

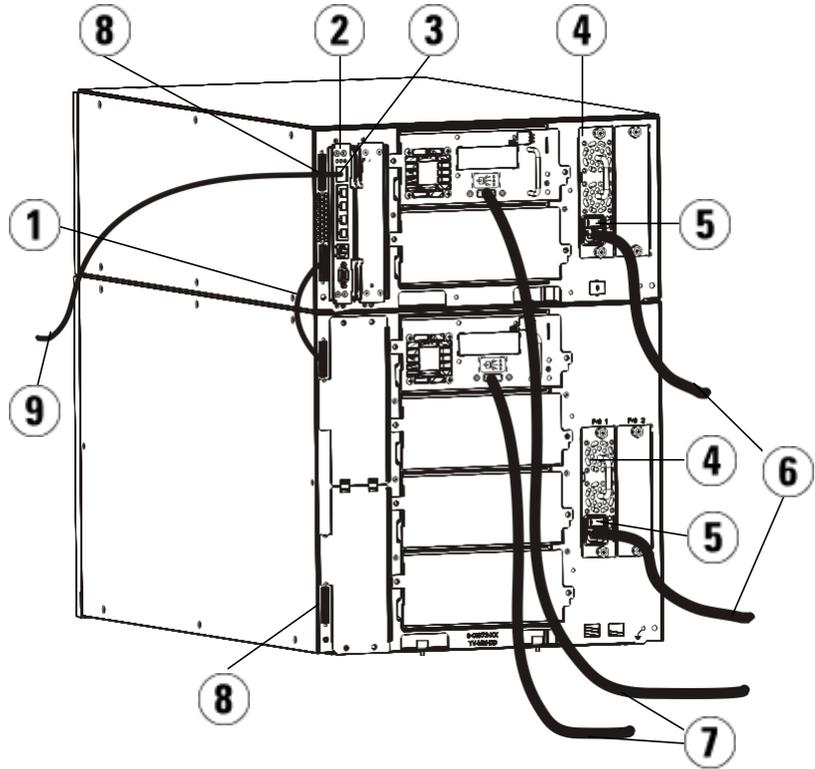
To ensure proper airflow and access space, Allow 60 cm (24 inches) in the front and back of the library.

Figure 24 Stand-Alone 5U
Library 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 25 Multi-Module SAS
Cabling



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

- 1 If your library is larger than 14U, install it in a rack. See [Installing the Library in a Rack](#) on page 333 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 9U Library Expansion Modules to the 5U Library Control Module, remove the module terminator from the 5U Library Control Module terminator connection that is closest to the 9U Library Expansion Module.
 - c Replace the module terminator in the 9U Library Expansion Module in the terminator connection that is furthest from the 5U Library Control Module.
 - d Connect the module-to-module cable from the 5U Library Control Module to the 9U Library 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.

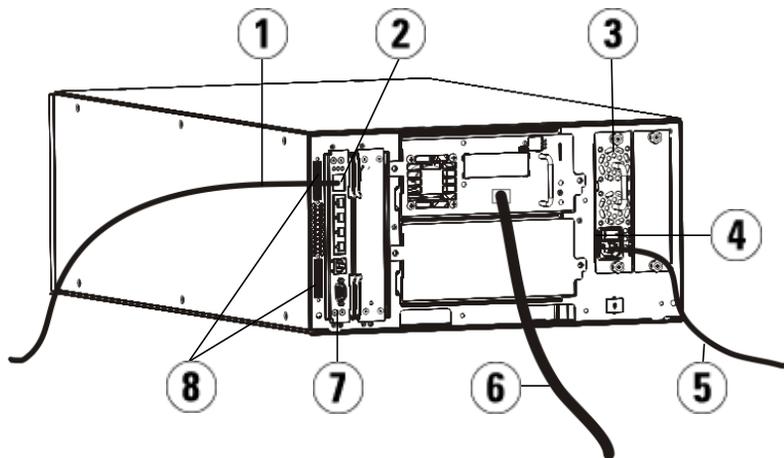
There should always be a power cord connected to the power supply on the 5U Library Control Module. If redundant power supplies are used, connect a power cord to each of the additional power supply outlets.

- 7 Plug the power cord into a nearby AC power source.
- 8 Power on the library.
 - a Turn on the rear power switch of each of the power supplies.
 - b Turn on the front power button.
 - c Power up the host system.
- 9 Verify communication with all devices on the bus.
- 10 Configure the library using the commands on the operator panel. See configuration information in [Configuring Your Library](#) on page 56.

Cabling Libraries With Fibre Channel Tape Drives Connected Directly to a Host or Switch

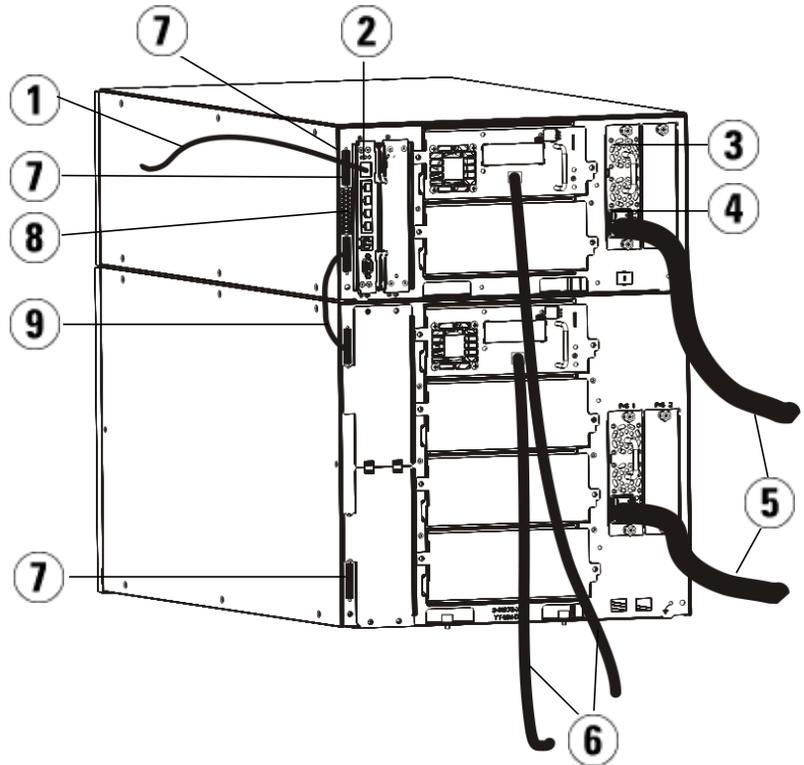
Use this procedure, along with [Figure 26](#) and [Figure 27](#), if you are installing a library that includes FC tape drives that are connected directly to a host or switch.

Figure 26 Stand-Alone 5U
Library 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 27 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 mm² (14 AWG).

To ensure proper airflow and access space, Allow 60 cm (24 inches) in the front and back of the library.

Note: Pay attention to where the operator panel is positioned in the rack for optimum usability.

- 1 If your library is larger than 14U, install it in a rack.
See [Installing the Library in a Rack](#) on page 333 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.

Caution: LTO-5 Fibre Channel tape drives can be configured for speeds of up to 8 GB per second and support auto-negotiation to 8 Gb/s, 4 Gb/s, and 2 Gb/s. If they are configured for 8 Gb/s, you should connect them directly to a host or switch and not to an FC I/O blade, because the FC I/O blade only allows speeds up to 4 Gb/s. If you connect an LTO-5 Fibre Channel tape drive to an FC I/O blade, the speed will autonegotiate to 4 Gb/s (see [Setting Tape Drive Parameters](#) on page 84). Speeds less than 2 Gb/s are not supported.

For information on installing FC I/O blades, see [Adding, Removing, and Replacing FC I/O Blades](#) on page 359.

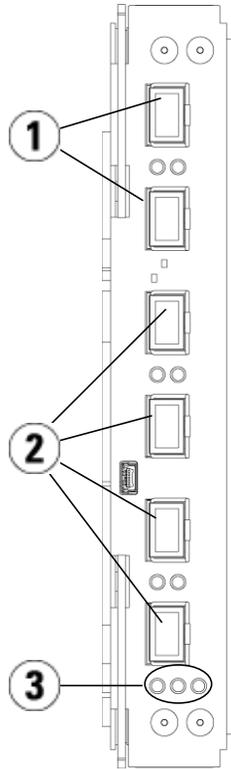
Cabling may be affected by partitioning or zoning changes made as part of configuration. When cabling to drives, ensure that they are cabled to the correct hosts for the defined partitions. If the FC I/O blades have active channel zoning, ensure that the drives are attached to ports that are accessible to the defined zone. For information on partitioning, configuring FC I/O blade ports, channel zoning, and host mapping, see [Chapter 5, Configuring Your Library](#).

Details about cabling FC I/O blades include:

- Each 9U Library 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 28](#).
- 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 9U Library Expansion Module as the tape drive.

Note: See [Cable Management Guidelines](#) on page 237 for best-practice guidelines for cabling a library.

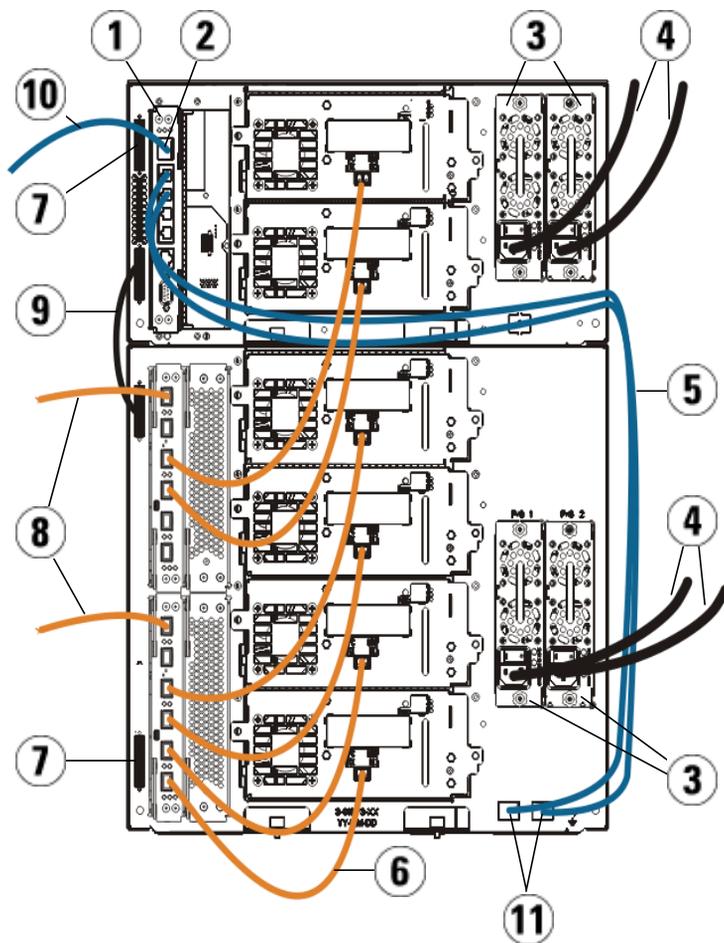
Figure 28 FC I/O Blade



-
- 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 29](#), if you are installing a library that includes FC tape drives that are connected to FC I/O blades.

Figure 29 FC With I/O Blade
Cabling



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

Required tools: None

- 1 If your library is larger than 14U, install it in a rack. See [Installing the Library in a Rack](#) on page 333 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 mm² (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 a 9U Library Expansion Module, connect the 9U Library 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 9U Library Expansion Module, connect one end of an Ethernet cable to the Ethernet port labeled **LOWER** in the lower right corner of the 9U Library 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 9U Library Expansion Module, connect one end of an Ethernet cable to the Ethernet port labeled **UPPER** in the lower right corner of the 9U Library 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 237 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 237 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 9U Library Expansion Modules to the 5U Library Control Module, remove the module terminator from the 5U Library Control Module terminator connection that is closest to the 9U Library Expansion Module.

- c** Replace the module terminator in the 9U Library Expansion Module terminator connection furthest from the 5U Library Control Module.
- 10** Connect the module-to-module cable from the 5U Library Control Module to the 9U Library 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 5U Library Control Module. If redundant power supplies are used, connect a power cord to each of the additional power supply outlets.

- 13** Power on the library.
 - a** Turn on the rear power switch of each of the power supplies.
 - b** Turn on the front power button.
 - c** Power up the host system.
- 14** Verify communication with all devices on the bus.
- 15** Configure the library using the commands on the operator panel. See configuration information in [Configuring Your Library](#) on page 56.

Recommended Library Cabling for FC I/O Blades

Fibre optic cables connect Fibre Channel tape drives to FC I/O blades and FC I/O blades to a Storage Area Network (SAN) fabric or host. Correctly managing these cables on the rear of the library can prevent damage to the cables and Fibre Channel ports and ensure optimal data throughput.

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

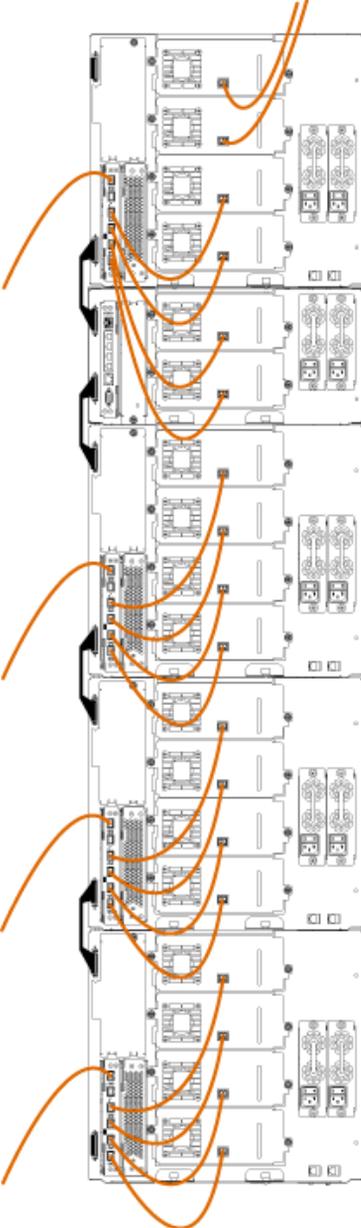
Ideally, an installed tape drive should be cabled to a port on the nearest FC I/O blade to eliminate the need to manage excessively long cables.

The nearest FC I/O blade is usually located in the same expansion module as the tape drive.

You will need to provide fibre cables long enough to connect a host or a SAN switch to a target port on an FC I/O blade.

It is important to consider how drives are assigned to partitions when cabling tape drives and hosts to an FC I/O blade. If you want a host to be able to communicate with a tape drive that is assigned to a particular partition, both the drive and the host that has access to the partition should communicate through the same FC I/O blade.

The following table provides an example of an ML6030 Control Module plus two ML600 9U Expansion Modules with FC I/O blade-attached tape drives. The information next to the image shows each tape drive and the FC I/O blade and port to which each tape drive is connected.

Recommended Cabling With FC I/O Blades In Maximum Capacity Library	Tape Drive	FC I/O Blade	FC I/O Blade Port
	[1,1]	N/A (direct attached)	
	[1,2]	N/A (direct attached)	
	[1,3]	[1,2]	Port 3
	[1,4]	[1,2]	Port 4
	[0,1]	[1,2]	Port 5
	[0,2]	[1,2]	Port 6
	[-1,1]	[-1,2]	Port 3
	[-1,2]	[-1,2]	Port 4
	[-1,3]	[-1,2]	Port 5
	[-1,4]	[-1,2]	Port 6
	[-2,-1]	[-2,-2]	Port 3
	[-2,-2]	[-2,-2]	Port 4
	[-2,-3]	[-2,-2]	Port 5
	[-2,-4]	[-2,-2]	Port 6
	[-3,1]	[-3,2]	Port 3
	[-3,2]	[-3,2]	Port 4
	[-3,3]	[-3,2]	Port 5
	[-3,4]	[-3,2]	Port 6

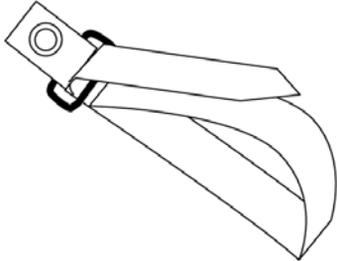
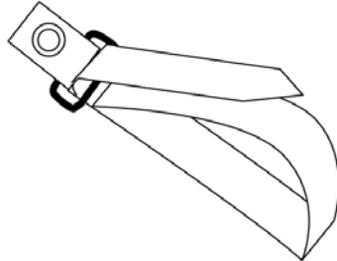
Cable Management Guidelines

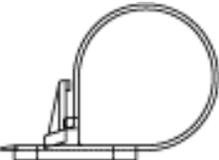
As the library expands to support larger configurations, it is important to restrain and organize cables and power cords on the rear of the library. Doing so ensures that the rear of the library remains accessible and reduces the possibility that cables become damaged.

Use this section to find cable management guidelines and best practices for power cords and Ethernet cables. Use the equipment specified in the [Cable Management Kit](#) section below.

Cable Management Kit

If you purchase a Fibre Channel I/O blade or, 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 Dell (see [Appendix C, Contacting Dell](#) for contact information). 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 9U Library Expansion Modules.	1
	Blue hook-and-loop fastener – Secures Ethernet cables to 9U Library Expansion Modules.	1

Component	Description	Quantity
	Push-in clip — to secure hook-and-loop fasteners to 9U Library 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 5U Library Control Module.	2
	Adhesive-backed wire saddle cable clamp — For older library models without drilled holes for push-in wire saddle clamps. The adhesive-backed wire saddle clamp secures Ethernet cables to the 5U Library Control Module.	2

Managing Power Cords

Power cord management is important especially for the larger, expanded library configurations. An ML6030 CM plus two PowerVault ML6000 9U Library Expansion Modules 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 9U Library 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 9U Library 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 9U Library Expansion Module near the right side of the library chassis. Refer to the illustration below to locate this hole.

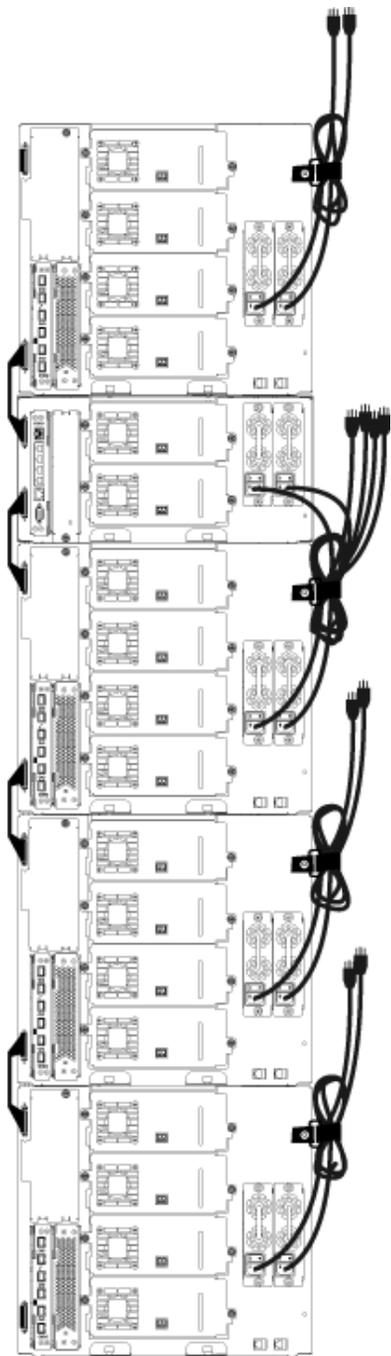
Note: If your module chassis does not have the drilled hole, use an M5 thumbscrew to attach the black hook-and-loop fastener to the nearest available M5 threaded hole on the lower right of any module chassis.

- 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 9U Library 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 9U Library 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 an ML6030 CM plus two PowerVault ML6000 9U Library Expansion Modules should look similar to [Figure 30](#) on page 240.

Figure 30 Power Cord
Management



Managing Ethernet Cables

A Dell PowerVault ML6000 library with FC I/O blades uses external Ethernet cables on the rear of the library to provide connectivity between the LCB in the 5U Library Control Module and a 9U Library Expansion Module. The upper and lower FC I/O blade bays within a 9U Library Expansion Module each have a corresponding Ethernet port on the back of the module. Running an Ethernet cable between this port and one of the Ethernet hub ports on the LCB establishes Ethernet connectivity between the blade and the LCB.

The LCB provides ports for up to four Ethernet cables on its internal Ethernet hub. This allows the library to support a total of four FC I/O blades.

To organize Ethernet cables on the rear of the library, mount two wire saddles on the 5U Library 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 9U Library Expansion Module and at least one FC 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 5U Library 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 5U Library Control Module's power supplies. See [Figure 31](#) on page 243 for the locations of these holes.

Note: If your 5U Library Control Module chassis does not have the drilled holes, use the adhesive -backed wire saddle cable clamps in the location shown in [Figure 31](#).

- 2 Locate a specific hole that is drilled into the back of the 9U Library 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 9U Library Expansion Module on the right side of the frame back plane. See [Figure 31](#) on page 243 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 9U Library 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 9U Library Expansion Module.

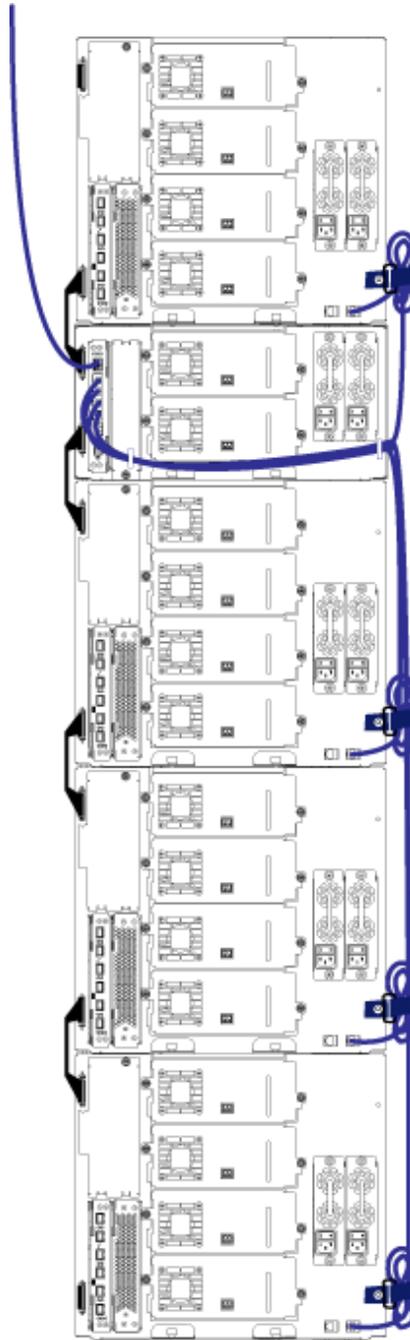
If the FC I/O blade is installed in the module's upper I/O blade bay, plug the cable into the Ethernet port labeled **UPPER**. If the FC I/O blade is installed in the module's lower I/O blade bay, plug the cable into the Ethernet port labeled **LOWER**.

- 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 9U Library Expansion Module. Repeat these steps to secure other Ethernet cables, if necessary.

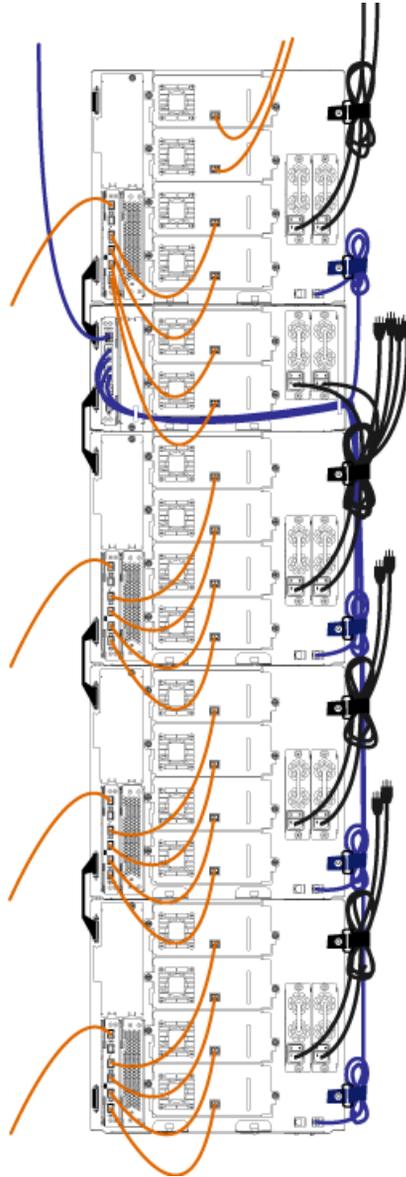
Once complete, the Ethernet cabling for an ML6030 Control Module plus two PowerVault ML6000 9U Library Expansion Modules containing four FC I/O blades should appear similar to [Figure 31](#) on page 243.

Figure 31 Ethernet Cable
Management



[Figure 32](#) shows how a 41U library with FC I/O blades installed would appear with power, Ethernet, and fibre cables installed and managed according to these guidelines.

Figure 32 Cable Management,
All Cables, FC I/O Blades
Installed



Installing a Stand-Alone 5U Library Control Module

Required tools: None

Use this procedure to install a 5U library configuration:

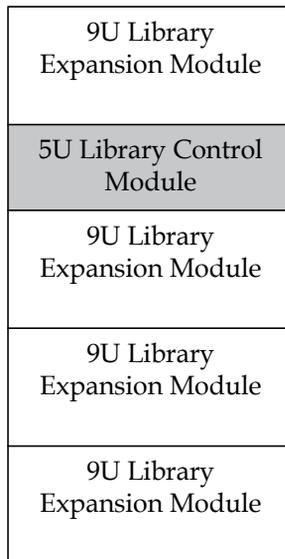
- 1 Prepare the rack to hold modules, if you want to install your library in a rack. See [Installing the Library in a Rack](#) on page 333 for instructions on installing a rack-mount kit.
- 2 Make sure all tape drives have been removed from the 5U Library Control Module. See [Adding, Removing, and Replacing Tape Drives](#) on page 354 for instructions on removing tape drives.
- 3 Make sure all power supplies have been removed from the 5U Library Control Module. See [Adding, Removing, and Replacing Power Supplies](#) on page 330 for instructions on removing power supplies.
- 4 Open the library's I/E station door and access door. Lift the 5U Library 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 5U Library Control Module to the rack. For instructions, see [Installing the Bottom Module in the Rack](#) on page 344.
- 6 If not already installed, install the library control blade (LCB) in the 5U Library Control Module. See [Removing and Replacing the Library Control Blade and LCB Compact Flash Card](#) on page 320 for instructions on installing the LCB.
- 7 Add the tape drives to the module.
- 8 Install the power supplies. See [Adding, Removing, and Replacing Power Supplies](#) on page 330 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 [Cabling the Library](#) on page 212.
- 11 Install module terminators in the top and bottom module terminator connectors. See [Cabling the Library](#) on page 212 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 5U Library Control Module and one or two 9U Library Expansion Modules.

There are no restrictions on where the 5U Library 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.



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.

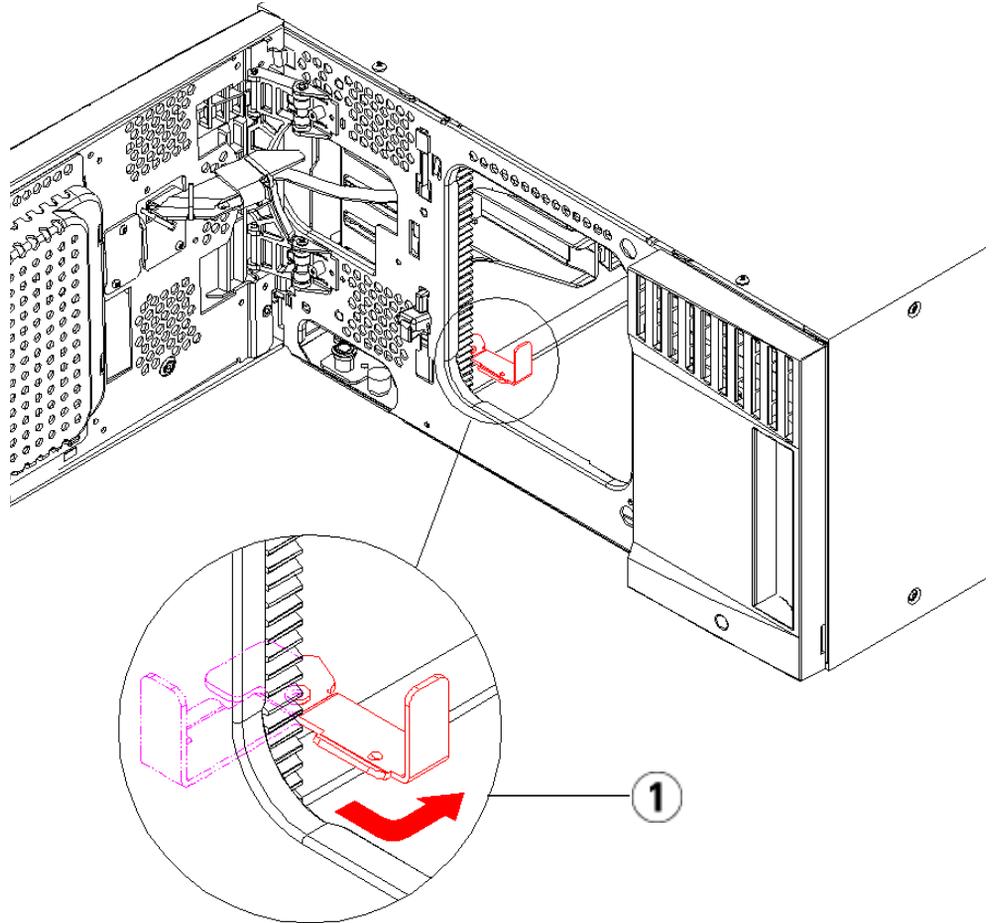
Preparing to Install a Multi-Module Library

Required tools:

- Phillips #2 screwdriver, for removing and replacing the top cover plate
 - T10 TORX screwdriver, for removing and replacing the bottom cover plate
- 1** Prepare the rack to hold modules, if you want to install your library in a rack. See [Installing the Library in a Rack](#) on page 333 for instructions on installing a rack-mount kit.
 - 2** Make sure all tape drives have been removed from all of the modules you plan to install. See [Adding, Removing, and Replacing Tape Drives](#) on page 354 for instructions on removing tape drives.
 - 3** Make sure all power supplies have been removed from all of the modules you plan to install. See [Adding, Removing, and Replacing Power Supplies](#) on page 330 for instructions on removing power supplies.
 - 4** Park the robot assembly in the 5U Library Control Module. Before unstacking the library, the robot assembly must be placed in the 5U Library 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 5U Library Control Module. The robot assembly should glide slowly and with some resistance.

Caution: Support the robot assembly by holding onto the broad metal X-axis plate. Lifting the robot by the thin metal rod will bend the rod. Lifting the robot by the black plastic picker body can damage the robot.

- c** After raising the robot assembly to the approximate middle of the 5U Library Control Module, hold it in place with one hand and, using your other hand, move the parking tab in a counter-clockwise direction until it stops in the “parked” position. The metal parking tab is located at the bottom of column 1.
- d** Gently lower the robot assembly to rest on the parking tab.

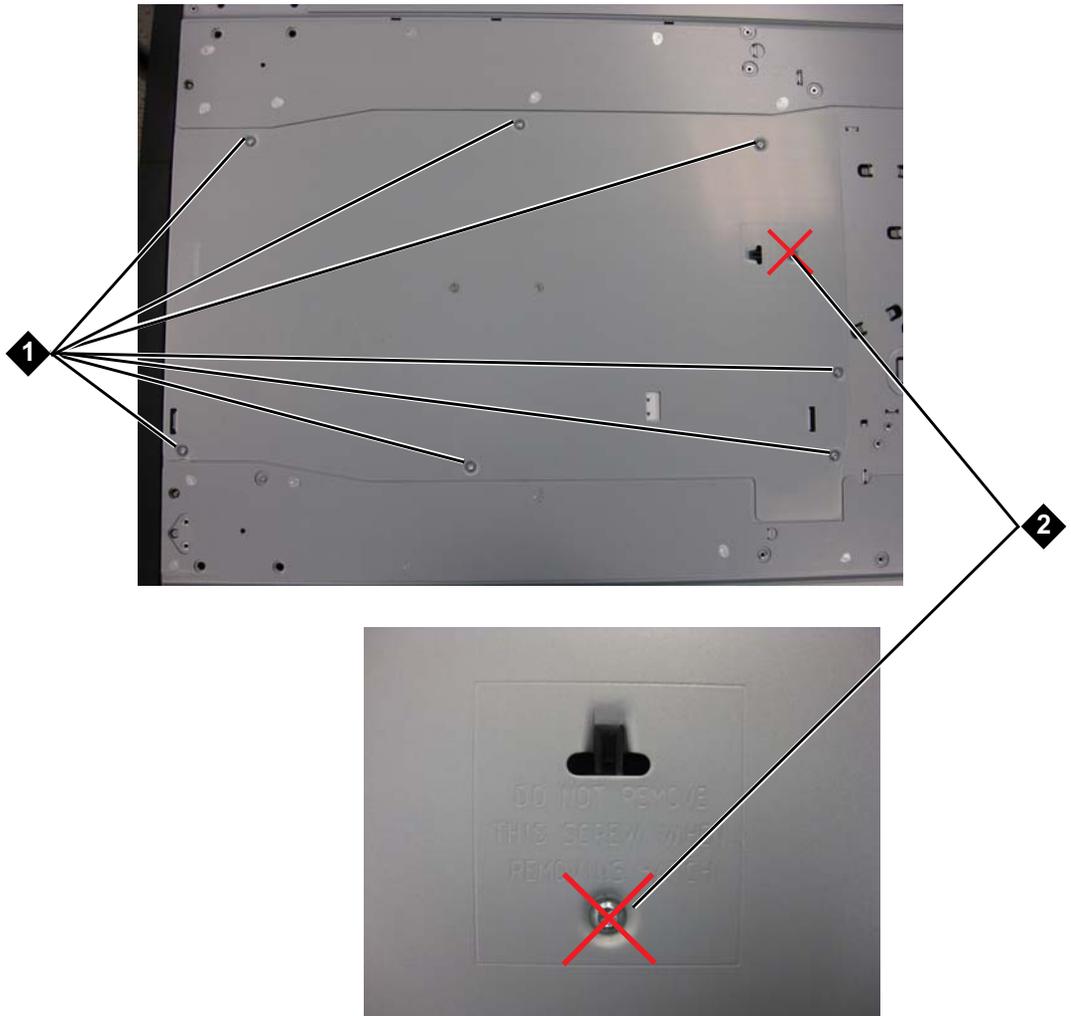


1 Parking tab in “parked” position

- 5 Remove and replace the cover plates, if appropriate. When removing the cover plate, ensure that you do not remove the y-home flag screw as shown in [Figure 33](#) on page 250.

Caution: Before removing the 5U Library Control Module’s bottom cover plate, the robot assembly must be parked as described in [Step 4](#) above.

Figure 33 Cover plate with Y-home flag



-
- 1 screws to remove
 - 2 Y-home flag screw - do not remove
-

- a** If you plan to stack the 5U Library Control Module at the top of the library, and if a 9U Library Expansion Module will be located below it, remove the 5U Library Control Module's bottom cover plate and the 9U Library Expansion Module's top plate.
- b** If you plan to stack the 5U Library Control Module between 9U Library Expansion Modules, remove both the top and bottom plates of the 5U Library Control Module. Also remove the top plate of the 9U Library Expansion Module located below the 5U Library Control Module and the bottom plate of the 9U Library Expansion Module located above the 5U Library Control Module.
- c** If you plan to stack the 5U Library Control Module at the bottom of the library, and if a 9U Library Expansion Module will be located above it, remove the 5U Library Control Module's top plate and the 9U Library Expansion Module's bottom plate.

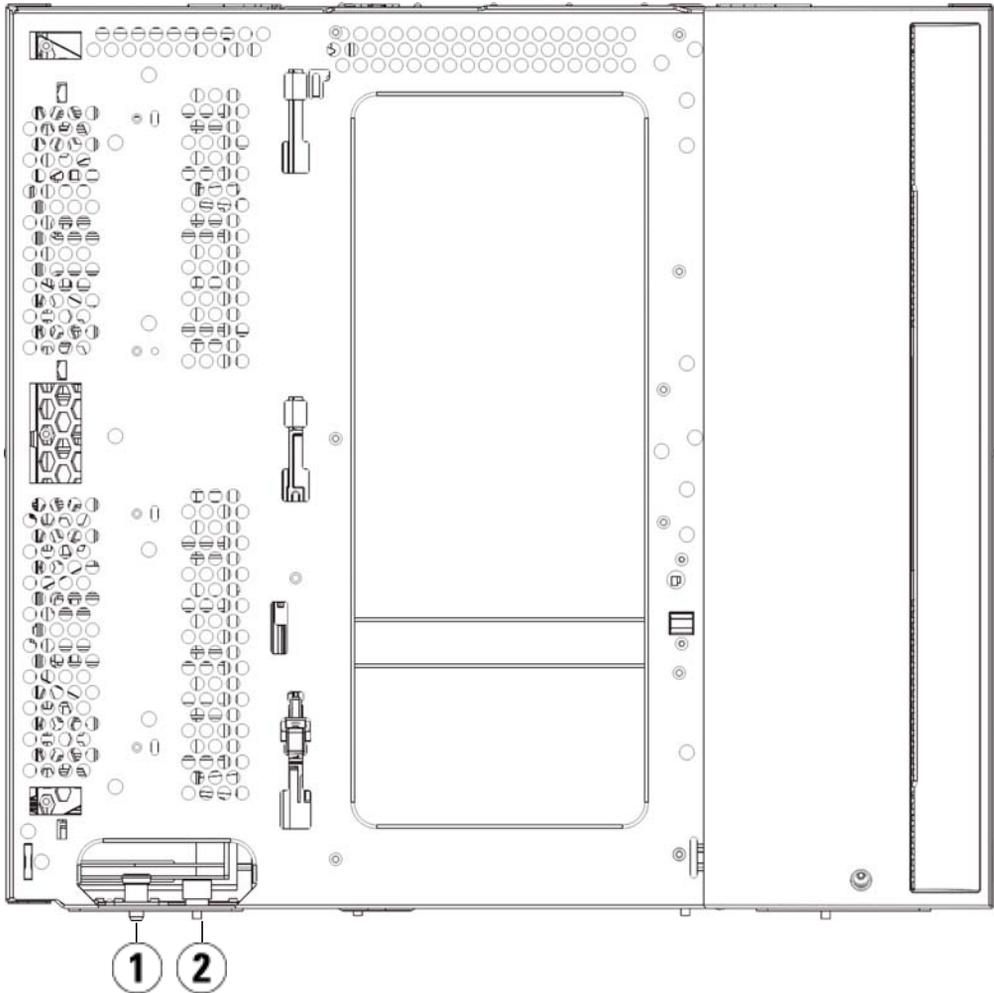
Figure 34 Recommended
Module Locations

ML6010	ML6020	ML6030	ML6030 CM + 1 9U Expansion Module	ML6030 CM + 2 9U Expansion Modules
				cover plate
			cover plate	9U Library Expansion Module
		cover plate	5U Library Control Module	5U Library Control Module
	cover plate	5U Library Control Module	9U Library Expansion Module	9U Library Expansion Module
cover plate	5U Library Control Module	9U Library Expansion Module	9U Library Expansion Module	9U Library Expansion Module
5U Library Control Module	9U Library Expansion Module	9U Library Expansion Module	9U Library Expansion Module	9U Library Expansion Module
cover plate	cover plate	cover plate	cover plate	cover plate

Installing the 9U Library Expansion Module

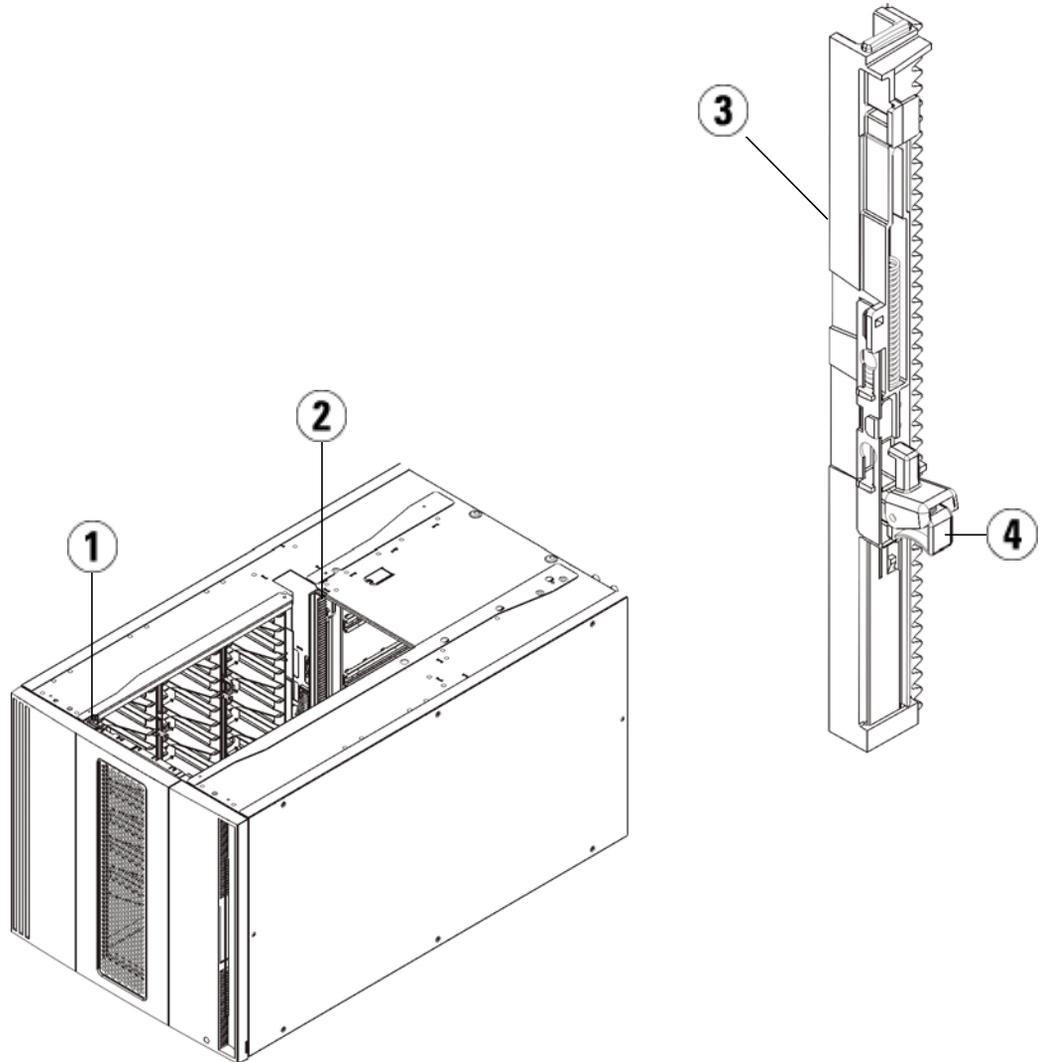
Install the expansion module as follows:

- 1 Open the 9U Library 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 9U Library Expansion Module and, from the front of the library, place it in the desired location.
- 3 If stacking the 9U Library Expansion Module on top of another module, secure the two modules together by tightening the two thumbscrews at the base of the front of the module and the two thumbscrews located at the base of the back of the module. Then lower the module's guide pin (located at the base of the front of the module) by turning it and pushing it down.
- 4 Tighten all thumbscrews located at the base of the front and back of the modules.
- 5 Fasten the module to the rack with rack ears. See [Installing the Library in a Rack](#) on page 333 for information on installing a rack-mount kit.
- 6 If stacking the 9U Library 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.



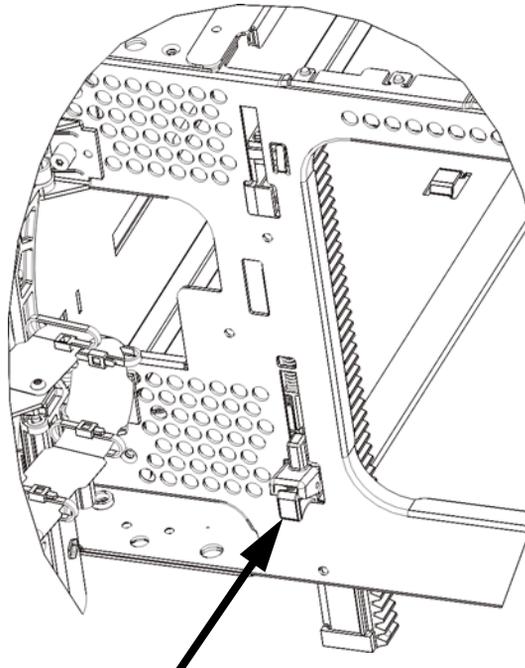
-
- 1 Front Y-rail
 - 2 Rear Y-rail
 - 3 Y-rail (this end up)
 - 4 Squeeze here to release
-

- a** From the front of the library, open the I/E station and access doors of the 9U Library 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 35 Y-Rail in Unlocked,
Functional Position



- 7** Repeat these steps for each 9U Library Expansion Module you are installing.

Installing the 5U Library Control Module

Install the 5U control module as follows:

- 1 Open the 5U Library Control Module's I/E station door and access door.
- 2 Lift the 5U Library Control Module and place it in the desired location.
- 3 If stacking the 5U Library 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 5U Library Control Module to the rack.
- 6 If not already installed, install the library control blade (LCB) in the 5U Library Control Module. See [Removing and Replacing the Library Control Blade and LCB Compact Flash Card](#) on page 320 for instructions on installing the LCB.

Preparing to Use the Multi-Module Library

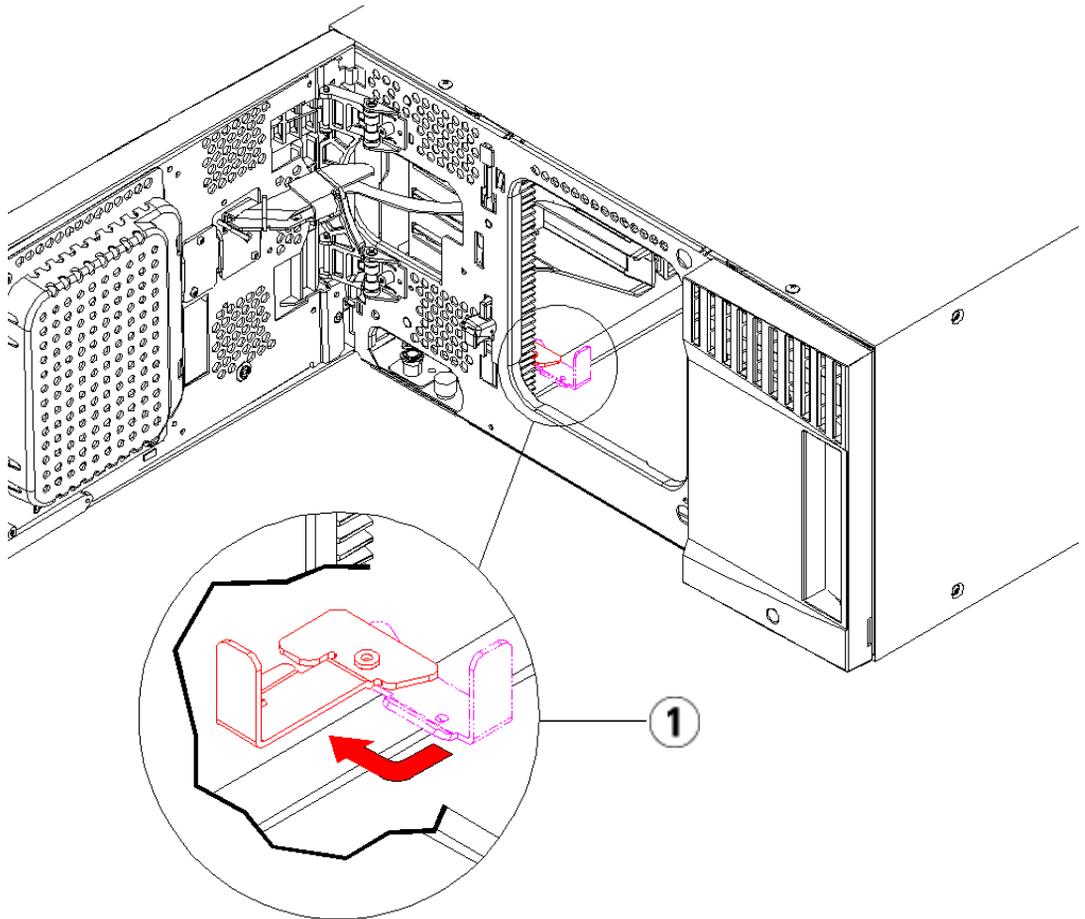
Prepare the library for use as follows:

- 1 Unpark the robot assembly.
 - a Gently raise the robot assembly so that it no longer rests on the parking tab.

Caution: Support the robot assembly by holding onto the broad metal X-axis plate. Lifting the robot by the thin metal rod will bend the rod. Lifting the robot by the black plastic picker body can damage the robot.

- b With your free hand, move the parking tab in a clockwise direction until it stops in the "unparked" position. When in the correct position, the parking tab is removed completely from the interior of the module and will not accidentally swing into the path of the robot.

- c Gently release the robot assembly. It will lower to the bottom module of the library.



1 Parking tab in “unparked” position

- 2 Close the library’s I/E station and access doors.
- 3 Add the tape drives to the modules. For details, see [Adding, Removing, and Replacing Tape Drives](#) on page 354.

- 4 If your library contains FC I/O blades, install both the I/O blades and the accompanying fan blades in the expansion module. For details, see and [Adding, Removing, and Replacing the FC I/O Fan Blade](#) on page 370.
- 5 Add the power supplies. For details, see [Adding, Removing, and Replacing Power Supplies](#) on page 330.
- 6 Connect all power cords, network data cables, and module-to-module cables. Make sure the module terminators are installed at the top and bottom of the stack of modules. For cabling instructions, see [Cabling the Library](#) on page 212.
- 7 Power on the library. For libraries larger than a ML6020, 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 9U Library Expansion Modules to an Existing Library

Adding 9U Library Expansion Modules to the library increases the number of data cartridges available within the library system. These instructions explain how to add a 9U Library Expansion Module to an existing library.

Note: The maximum number of 9U Library 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 on the Dell Support Web site. For the Dell Support Web site address, see Contacting Dell. See [Updating Library and Tape Drive Firmware](#) on page 199 for more information.

There are some configuration settings to take into account when adding a 9U Library Expansion Modules 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 9U Library Expansion Module has been added to the library.

A library can use up to four 9U Library 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 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 9U expansion module.

When adding additional 9U expansion modules to an existing library configuration, the recommended placement of the new 9U expansion module is at the bottom of the existing library configuration (except for the 41U library configurations, where recommended placement is on top). Installing the new 9U expansion module at the bottom of the existing library configuration will logically assign slot numbering within the library.

9U Library Expansion Module
5U Library Control Module
9U Library Expansion Module
9U Library Expansion Module
9U Library 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.

Warning: Without tape drives, tape cartridges, or power supplies, a 5U Library Control Module weighs approximately 60 lbs (27.2 kg). A 9U Library Expansion Module, without tape drives, tape cartridges, or power supplies, exceeds 65 lbs (29.5 kg).

To avoid serious injury, at least two people are required to safely lift the modules.

Preparing to Install an Additional 9U Library Expansion Module

Prepare to install an additional 9U Library Expansion Module as follows:

Warning: Without tape drives, tape cartridges, or power supplies, a 5U Library Control Module weighs approximately 60 lbs (27.2 kg). A 9U Expansion Module, without tape drives, tape cartridges, or power supplies, exceeds 65 lbs (29.5 kg).

To avoid serious injury, at least two people are required to safely lift the modules.

Caution: If the library contains a partition that spans modules, and you plan to install the new 9U Library Expansion Module between those modules, you must delete the partition before adding the new module, and re-create the partition after installing the module.

Required tools:

- Phillips #2 screwdriver, for removing and replacing the top cover plate
- T10 TORX screwdriver, for removing and replacing the bottom cover plate

You need to unstack the library to install the new 9U Library Expansion Module at the bottom of the new library configuration.

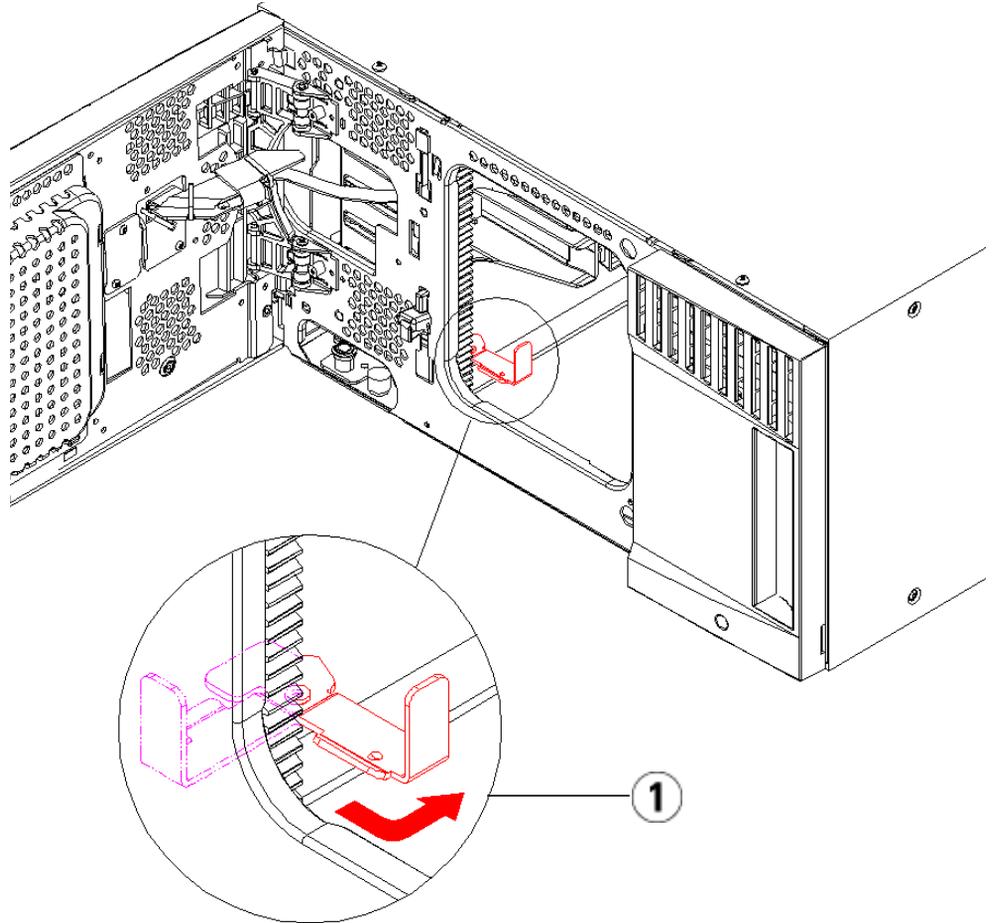
- 1 Upgrade the library firmware to a level that can support the number of modules you are adding. See [Updating Library and Tape Drive Firmware](#) on page 199 for information on upgrading firmware.
- 2 If you have a partition that spans modules, and you plan to add the new 9U Library Expansion Module between those modules, you must delete the partition before adding the new module (see [Deleting Partitions](#) on page 76).
- 3 Remove all tape cartridges from the library using the import and export commands of the operator panel or Web client.
- 4 Power off the library.
- 5 Disconnect all power cords, network data cables, and module-to-module cables from all of the modules.

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

- 6** Park the robot assembly in the 5U Library Control Module. Before unstacking the library, the robot assembly must be placed in the 5U Library 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 5U Library Control Module. The robot assembly should glide slowly and with some resistance.

Caution: Support the robot assembly by holding onto the broad metal X-axis plate. Lifting the robot by the thin metal rod will bend the rod. Lifting the robot by the black plastic picker body can damage the robot.

- c** After raising the robot assembly to the approximate middle of the 5U Library Control Module, hold it in place with one hand and, using your other hand, move the parking tab in a counter-clockwise direction until it stops in the “parked” position. The metal parking tab is located at the bottom of column 1.
- d** Gently lower the robot assembly to rest on the parking tab.



1 Parking tab in "parked" position

7 Remove all power supplies from each module.

8 Remove all tape drives from each module.

Unstacking the Existing Modules

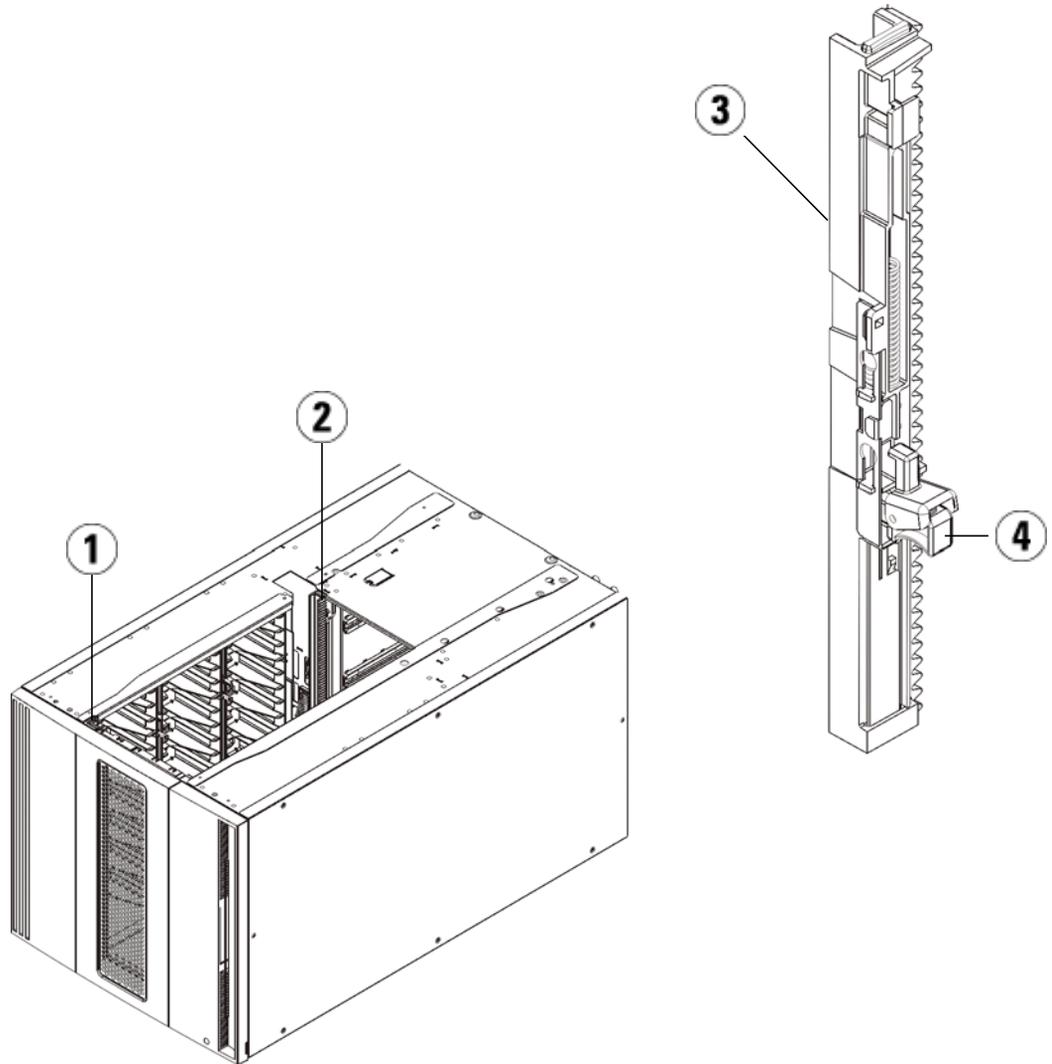
Unstack the modules as follows:

- 1 Starting with the topmost module of your library, open the I/E station and access doors.

Caution: Before unstacking the modules, the robot assembly must be parked as described in [Preparing to Install an Additional 9U Library Expansion Module](#) above.

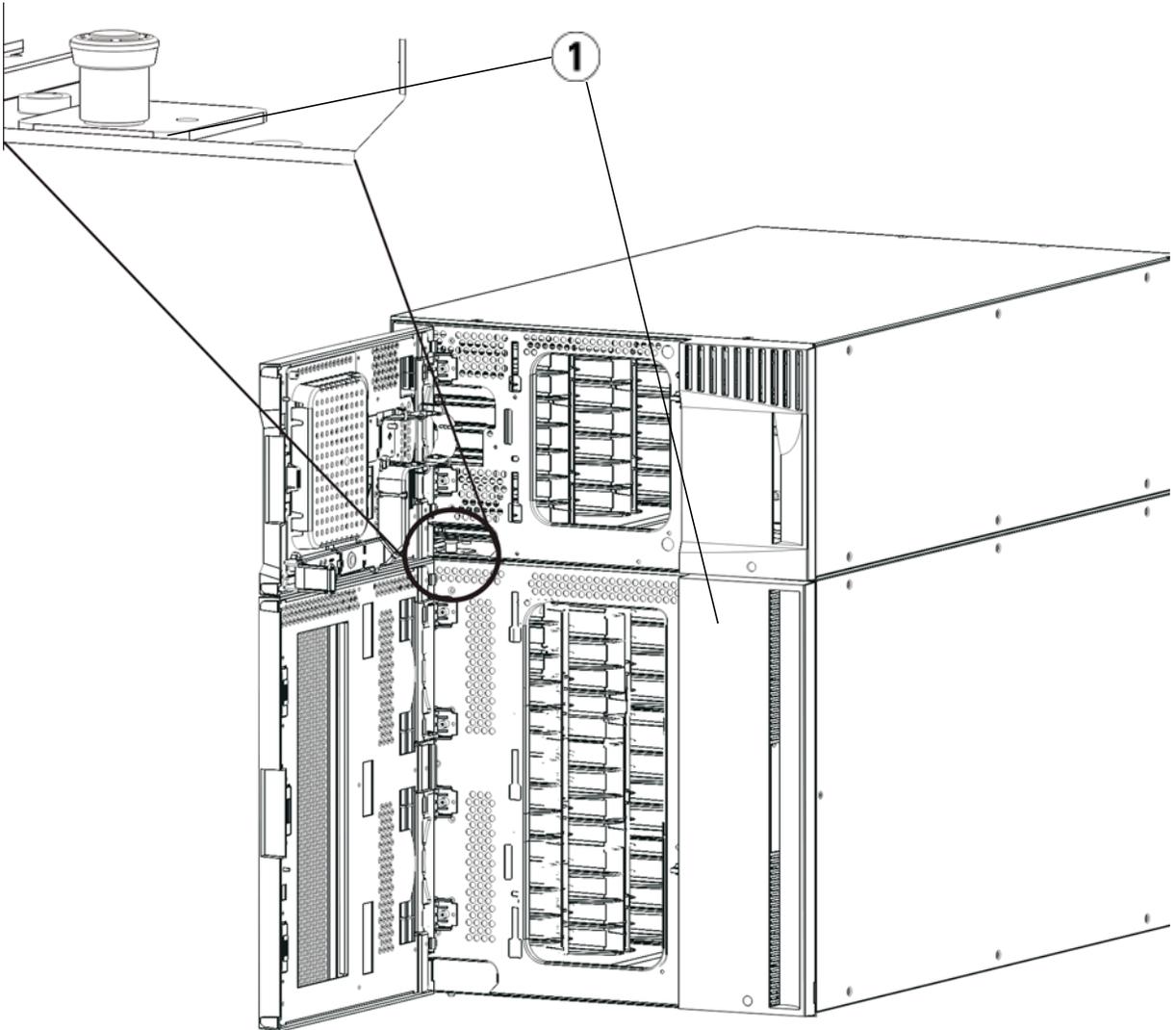
- 2 If your current configuration already uses a 9U Library Expansion Module, disengage the Y-rails so the modules can be safely unstacked.
 - a From the front of the library, find the Y-rail release mechanism, which is located on the left side of the module. Squeeze the handle of the Y-rail release 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.



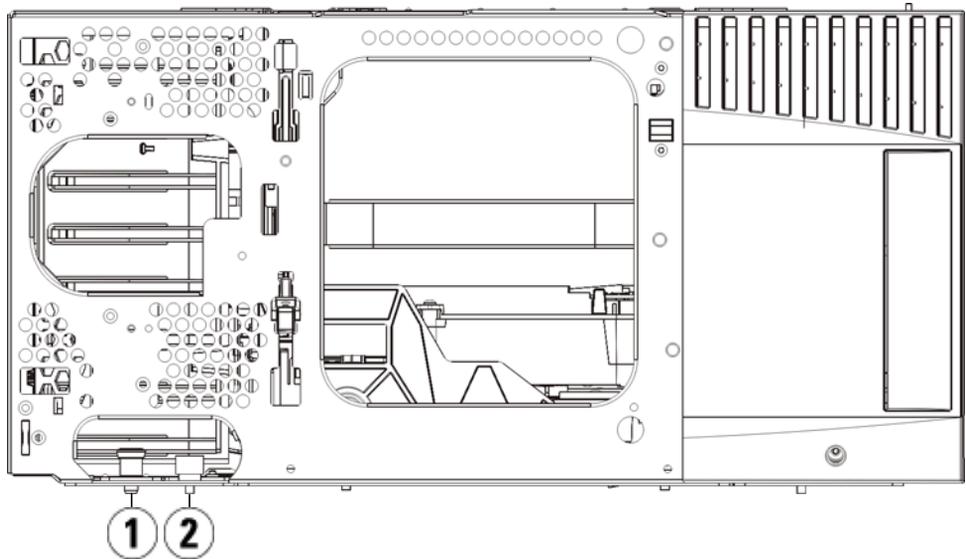
-
- 1 Front Y-rail
 - 2 Rear Y-rail
 - 3 Y-rail (this end up)
 - 4 Squeeze here to release
-

- 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 [Installing the Library in a Rack](#) on page 333 for instructions on installing a rack-mount kit.
- 2 Remove and replace the cover plates, if appropriate.

Caution: Before removing the 5U Library Control Module's bottom cover plate, the robot assembly must be parked as described in [Preparing to Install an Additional 9U Library Expansion Module](#) above.

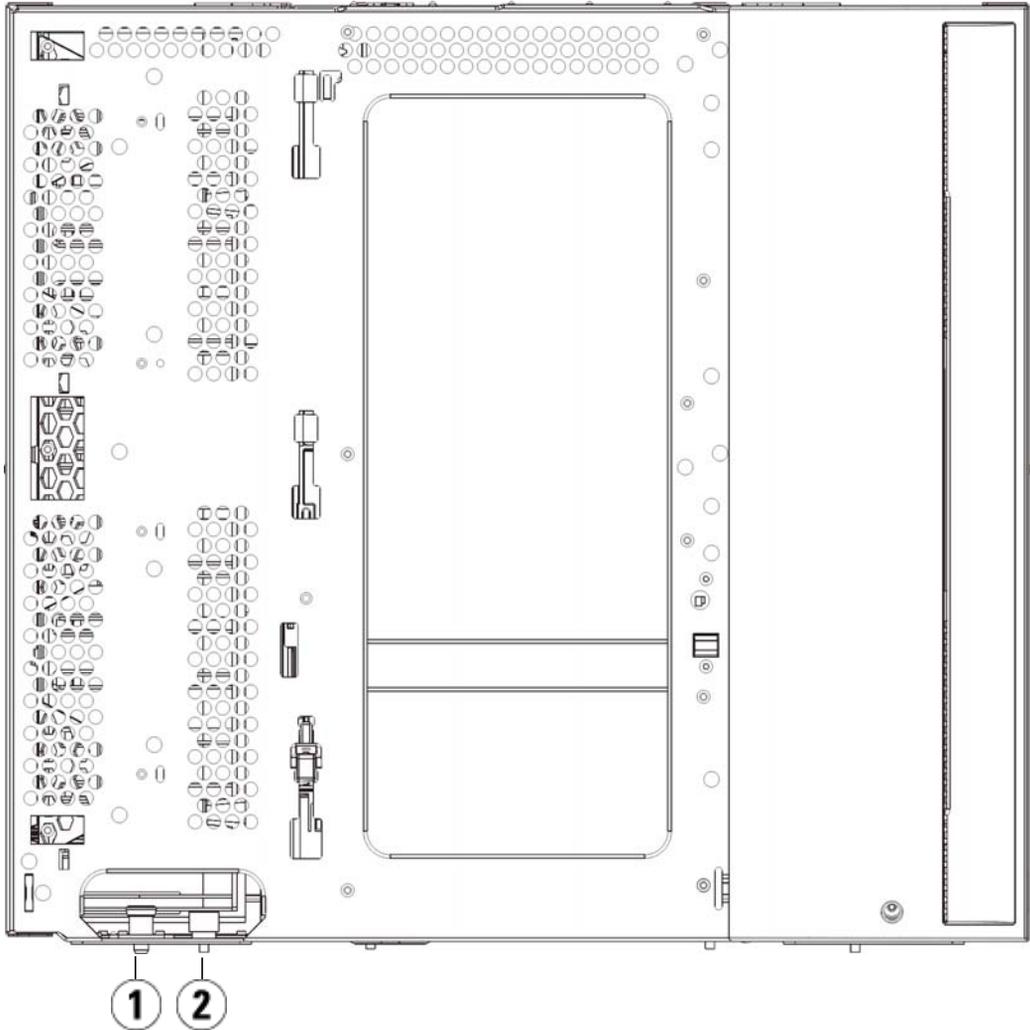
- a If you plan to stack the 5U Library Control Module at the top of the library, and if a 9U Library Expansion Module will be located below it, remove the 5U Library Control Module's bottom cover plate and the 9U Library Expansion Module top plate.
- b If you plan to stack the 5U Library Control Module between 9U Library Expansion Modules, remove both the top and bottom plates of the 5U Library Control Module. Also remove the top plate of the 9U Library Expansion Module, located below the 5U Library Control Module, and the bottom plate of the 9U Library Expansion Module, located above the 5U Library Control Module.
- c If you plan to stack the 5U Library Control Module at the bottom of the library, and if an 9U Library Expansion Module will be located above it, remove the 5U Library Control Module's top plate and the 9U Library Expansion Module's bottom plate.

Figure 36 Cover Plate Location
After Adding a 9U Library
Expansion Module

ML6010	ML6020	ML6030	ML6030 CM + 1 9U Expansion Module	ML6030 CM + 2 9U Expansion Modules
				cover plate
			cover plate	NEW 9U Library Expansion Module*
		cover plate	5U Library Control Module	5U Library Control Module
	cover plate	5U Library Control Module	9U Library Expansion Module	9U Library Expansion Module
cover plate	5U Library Control Module	9U Library Expansion Module	9U Library Expansion Module	9U Library Expansion Module
5U Library Control Module	NEW 9U Library Expansion Module*	NEW 9U Library Expansion Module*	NEW 9U Library Expansion Module*	9U Library Expansion Module
cover plate	cover plate	cover plate	cover plate	cover plate

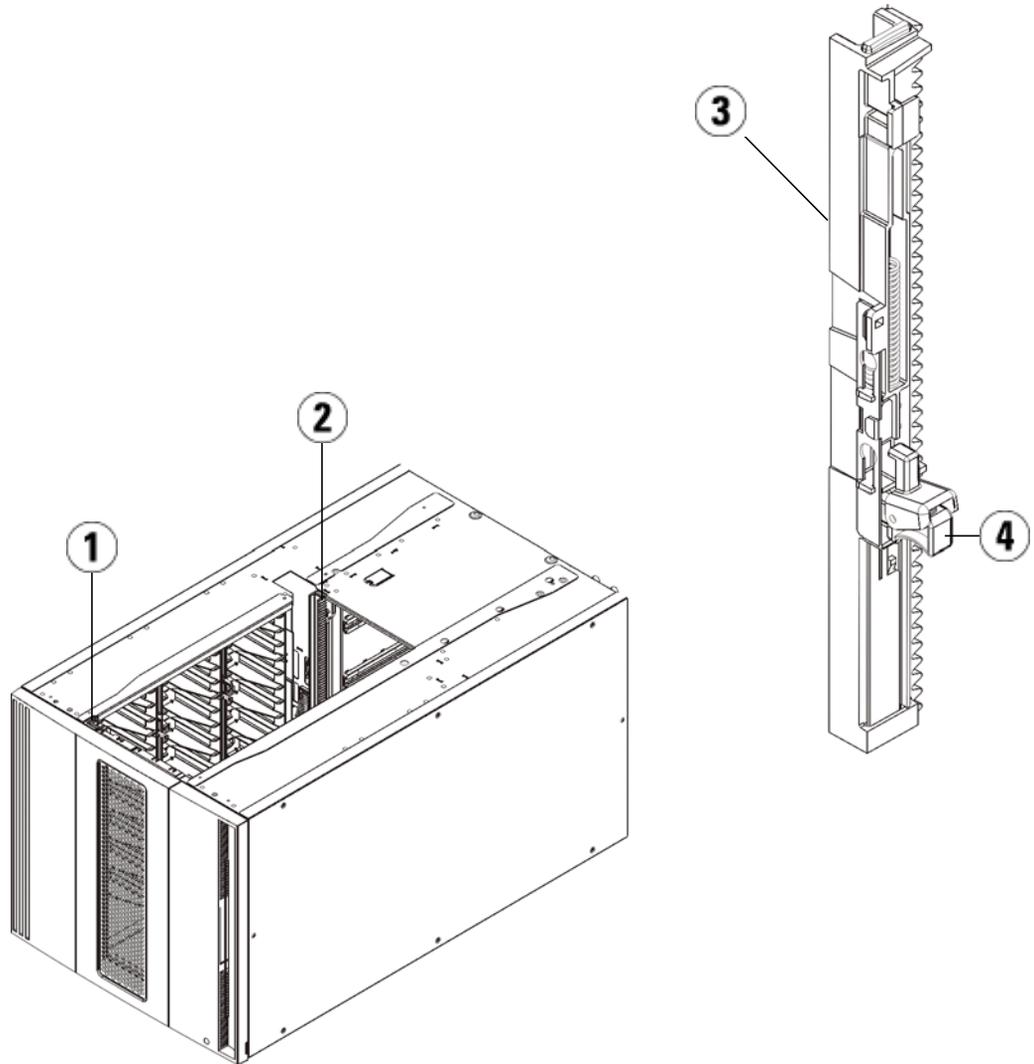
* Recommended location for adding a 9U Library Expansion Module.

- 3 Open the 9U Library 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 9U Library 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.

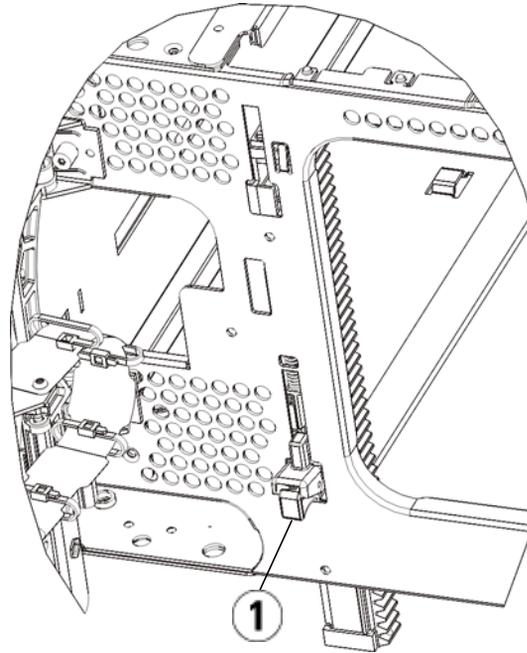


-
- 1 Front Y-rail
 - 2 Rear Y-rail
 - 3 Y-rail (this end up)
 - 4 Squeeze here to release
-

- a** From the front of the library, open the I/E station and access doors of the 9U Library 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

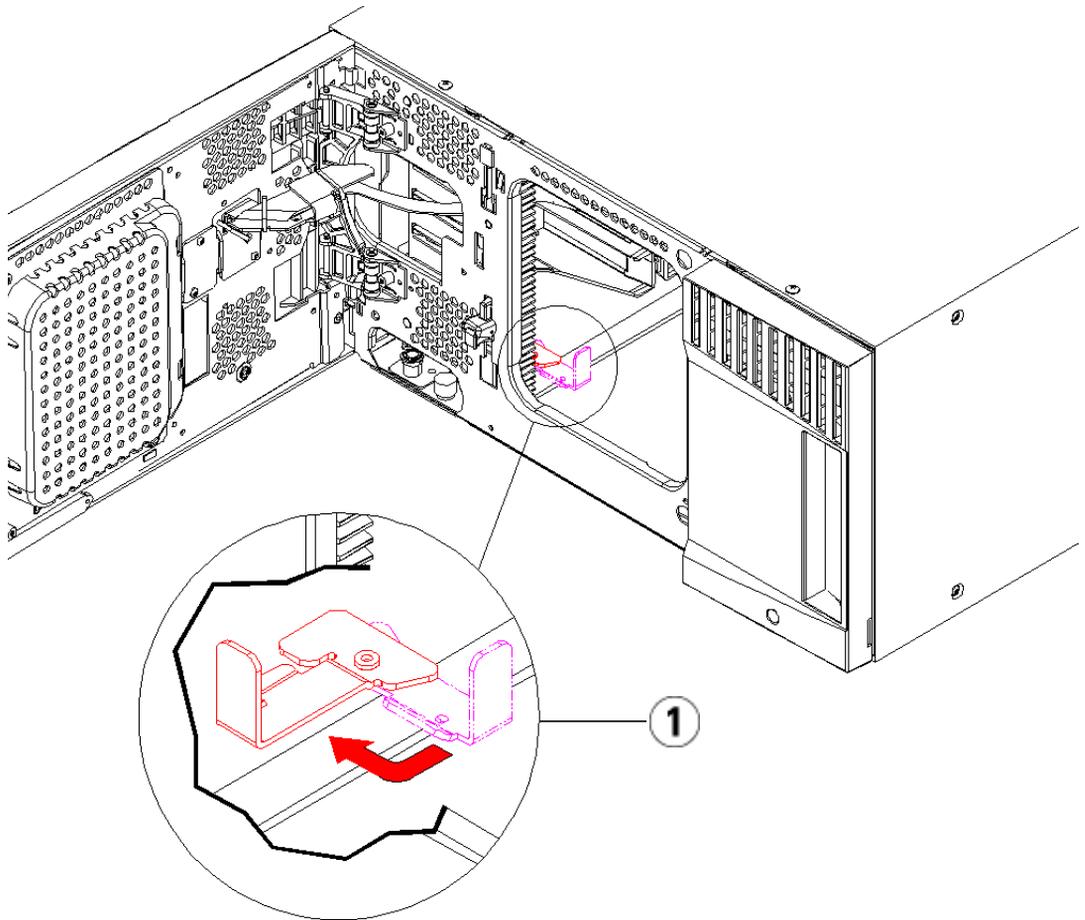
Prepare to use the library as follows:

- 1 Add the tape drives to the modules. For details, see [Adding, Removing, and Replacing Tape Drives](#) on page 354.
- 2 Add the power supplies. For details, see [Adding, Removing, and Replacing Power Supplies](#) on page 330.
- 3 Add the LCB to the 5U Library Control Module. For details, see [Removing and Replacing the Library Control Blade and LCB Compact Flash Card](#) on page 320.

- 4 If your library contains FC I/O blades, install both the I/O blades and the accompanying fan blades in the expansion module. For details, see [Adding, Removing, and Replacing FC I/O Blades](#) on page 359 and [Adding, Removing, and Replacing the FC I/O Fan Blade](#) on page 370.
- 5 Unpark the robot assembly.
 - a Gently raise the robot assembly so that it no longer rests on the parking tab.

Caution: Support the robot assembly by holding onto the broad metal X-axis plate. Lifting the robot by the thin metal rod will bend the rod. Lifting the robot by the black plastic picker body can damage the robot.

- b With your free hand, move the parking tab in a clockwise direction until it stops in the “unparked” position. When in the correct position, the parking tab is removed completely from the interior of the module and will not accidentally swing into the path of the robot.
 - c Gently release the robot assembly. It will lower to the bottom module of the library.



1 Parking tab in “unparked” position

- 6 Connect all power cords, network data cables, and module-to-module cables. Make sure the module terminators are installed at the top and bottom of the stack of modules. For cabling instructions, see [Cabling the Library](#) on page 212.
- 7 Power on the library.
- 8 Reconfigure the library, including applying the new COD license key, using the operator panel or Web client.
- 9 Recreate any partitions you deleted prior to installing the module.

- 10 Add the tape cartridges to the library's modules using the I/E station commands from the operator panel or Web client.
- 11 Open the host application and reinventory in order to synchronize its logical inventory with the physical inventory of the library. Due to the way the library logically addresses its tape drives and slots internally, adding an expansion module will change the element addresses, and this can affect proper communication to a controlling host. See [Understanding Logical Element Addressing](#) on page 38. Because of this, you must refresh the configuration of any backup application that manages the library to reflect the adjusted positions. In addition, you may need to reboot the host server(s) or rescan the bus to detect the changes.

Preparing to Remove or Replace a Module

Follow the instructions in this section before performing any of the following procedures:

- [Permanently Removing 9U Library Expansion Modules From an Existing Library](#) on page 285
- [Replacing the 5U Library Control Module](#) on page 297
- [Replacing a 9U Library Expansion Module](#) on page 307

Caution: If a 5U Library Control Module is replaced, all library configuration data will be invalidated and requires a new library configuration. Follow the instructions below to completely export all tape cartridges and completely delete all logical partition configuration and cleaning slot assignments.

Caution: If a 9U Library Expansion Module is removed or replaced, you must follow the steps below to modify or delete all the affected partitions before removing the module. Recreate the partitions after the removal or replacement is complete.

Required tools:

- Phillips #2 screwdriver, for removing and replacing the top cover plate
- T10 TORX screwdriver, for removing and replacing the bottom cover plate

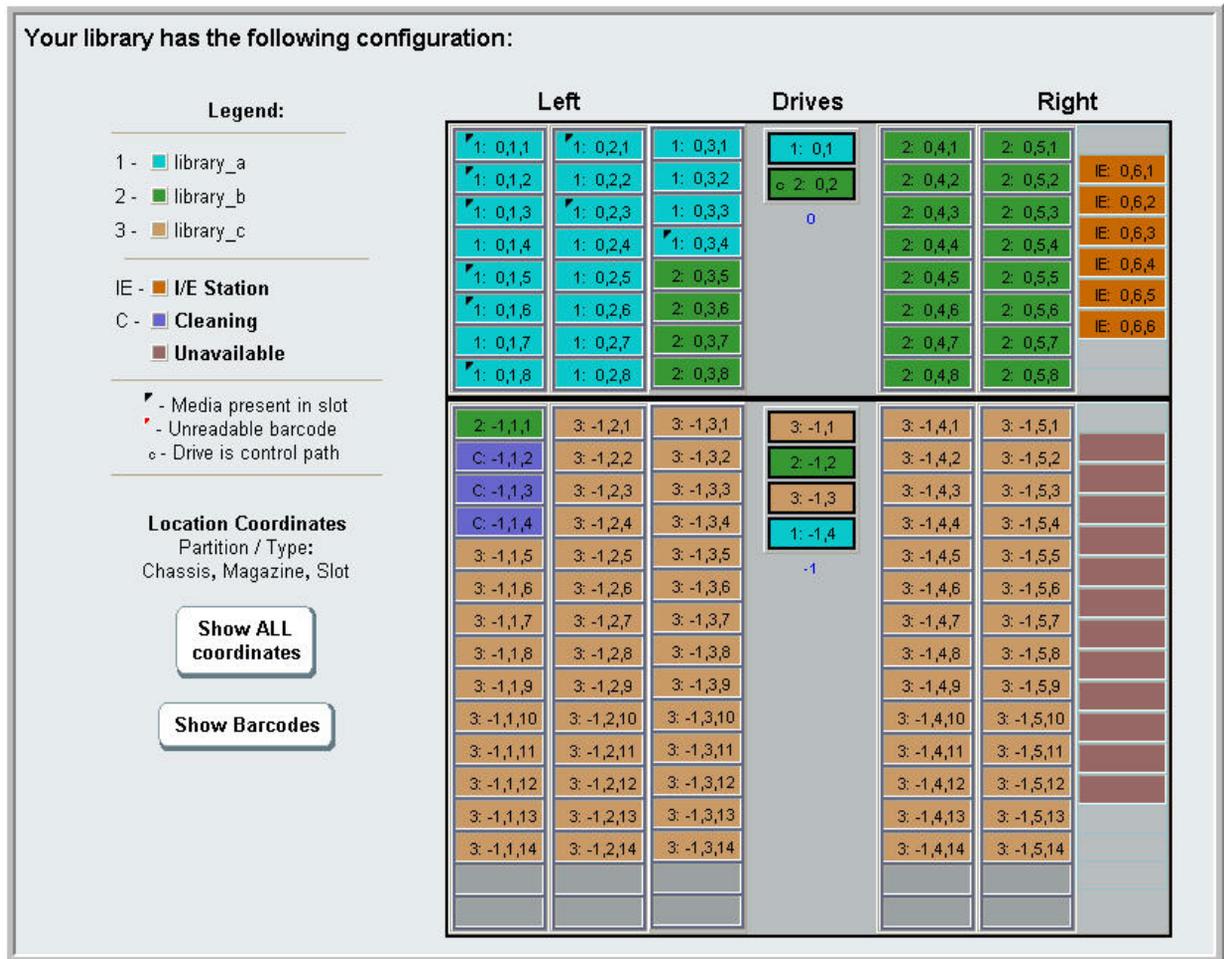
Instructions:

- 1 View your library's current configuration before removing or replacing any library modules to determine which partitions may be affected, which tape cartridges belong to which partition, and whether cleaning slots are configured within the library module you are removing or replacing. See [Viewing the Library Configuration Report](#) on page 190.

For example, in [Figure 37](#), the following library configuration may be observed. Note that there are three partitions configured. All three partitions share six I/E elements in the 5U Library Control Module. The library is configured for automatic cleaning and has three cleaning slots configured in the 9U Library Expansion Module.

- Library_a configured all storage elements in the 5U Library Control Module, and has one drive configured in the 5U Library Control Module, and one drive configured in the 9U Library Expansion Module.
- Library_b configured most storage elements in the 5U Library Control Module, but references its last storage element in the 9U Library Expansion Module. This partition has one drive configured in the 5U Library Control Module and one drive configured in the 9U Library Expansion Module.
- Library_c configured all storage elements in the 9U Library Expansion Module, and also configured two drives in this 9U Library Expansion Module.

Figure 37 Library Configuration
Example 1



- 2 If cleaning slots are configured for automatic, library-initiated cleaning operations, export all affected cleaning media from the elements contained within the module you are removing or replacing. See [Exporting Cleaning Media](#) on page 181.
- 3 If cleaning slots are affected and all cleaning media has been exported from the module you are removing or replacing, reduce or delete the cleaning slots so that cleaning slots are no longer configured within the module you are removing or replacing. You

can designate new cleaning slots after the module has been removed or replaced. See [Configuring Cleaning Slots](#) on page 79.

- 4 If the module you are removing or replacing contains tape drives, make sure that none of the tape drives have media mounted. See [Unloading Tape Drives](#) on page 175.
- 5 If the module you are removing or replacing contains I/E slots, remove all media from the affected I/E slots and store them separately for each partition so you can import them back into the same partition once the module removal or replacement is complete.
- 6 If one or more partitions reference any storage slots within the module you are removing or replacing, export all tape cartridges from the affected partitions and keep the exported cartridges separated by partition, so you can import them back into the same partition once the module removal or replacement is complete. See [Exporting Media](#) on page 172.

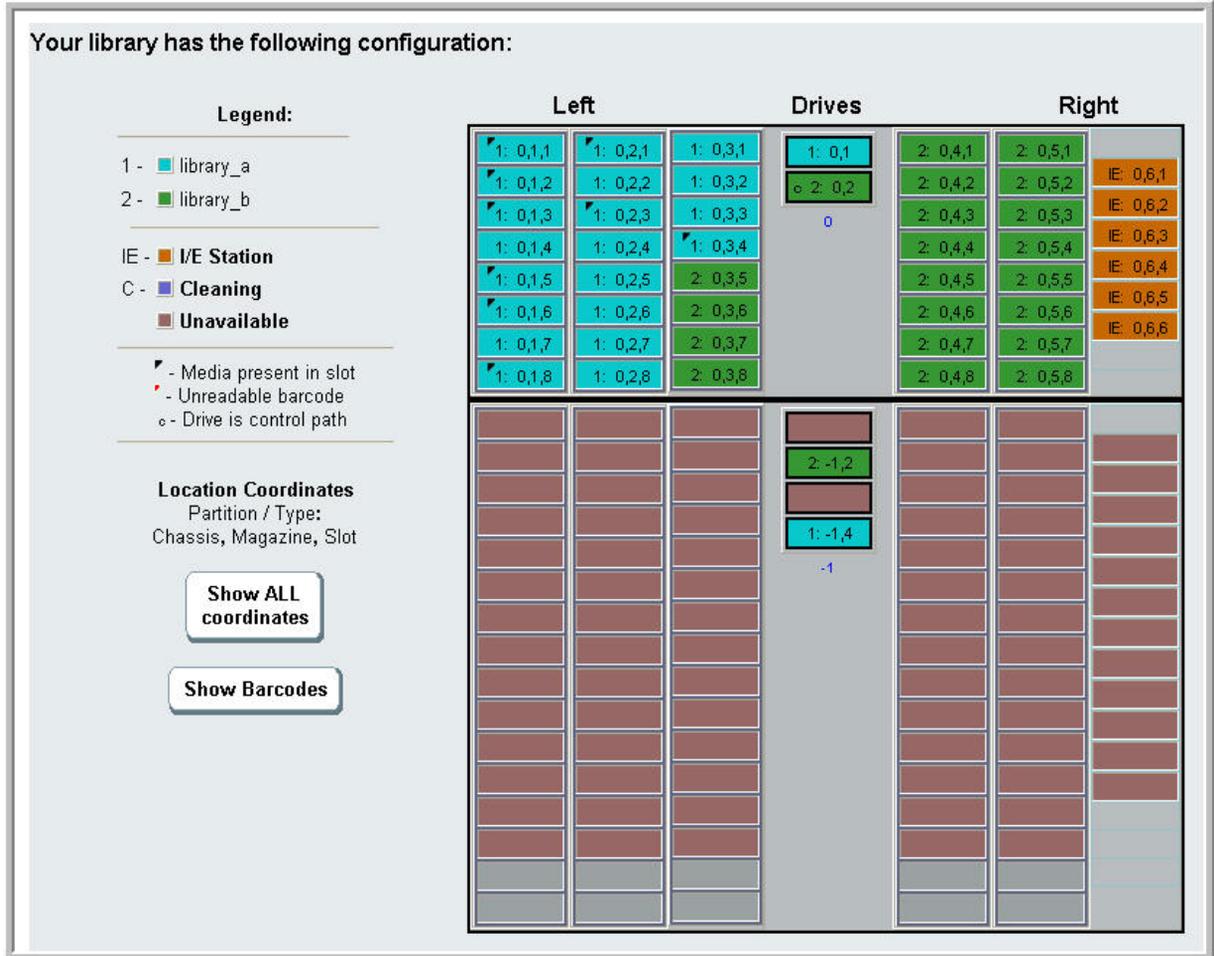
Caution: The library will not be able to locate tape cartridges that are removed from one partition and returned to a different partition. The tape cartridges must be returned to the same partition from which they were removed.

- 7 If a partition references storage slots within the module you are removing or replacing, delete such partition. You can create new partitions after modules have been removed or replaced. See [Working With Partitions](#) on page 71.

Note: If the last elements of a partition reside in the module you are removing or replacing, you may be able to modify the partition instead of deleting it. (See [Understanding Logical Element Addressing](#) on page 38 for more information on how the library logically addresses tape drives and slots.) In that case, you would 1) export those tape cartridges that reside in the module you are removing or replacing, and 2) modify the partition, instead of deleting it, so that the partition no longer references any storage or drive elements within the module you are removing or replacing. See [Modifying Partitions](#) on page 75.

For example, in [Figure 38](#), after exporting all affected tape cartridges from the module you are removing, the cleaning slots are deleted, then Library_c is completely deleted, and Library_b is modified to reduce its storage slot count by one, as this deletes the storage slot reference in the 9U Library Expansion Module. No storage element modifications are required for Library_a.

Figure 38 Library Configuration
Example 2



- 8 If a partition references tape drives within the module you are removing or replacing, modify any affected partition by removing the referenced drive elements from the partition. See [Modifying Partitions](#) on page 75.

For example, in [Figure 37](#) on page 279, all partitions reference drives in the 9U Library Expansion Modules. In [Figure 38](#) on page 282, Library_c was deleted, as well as its drive references in the 9U

Library Expansion Module. Library_a and Library_b still require partition modifications to remove the drive reference and hereby free the 9U Library Expansion Module of all partition resource references.

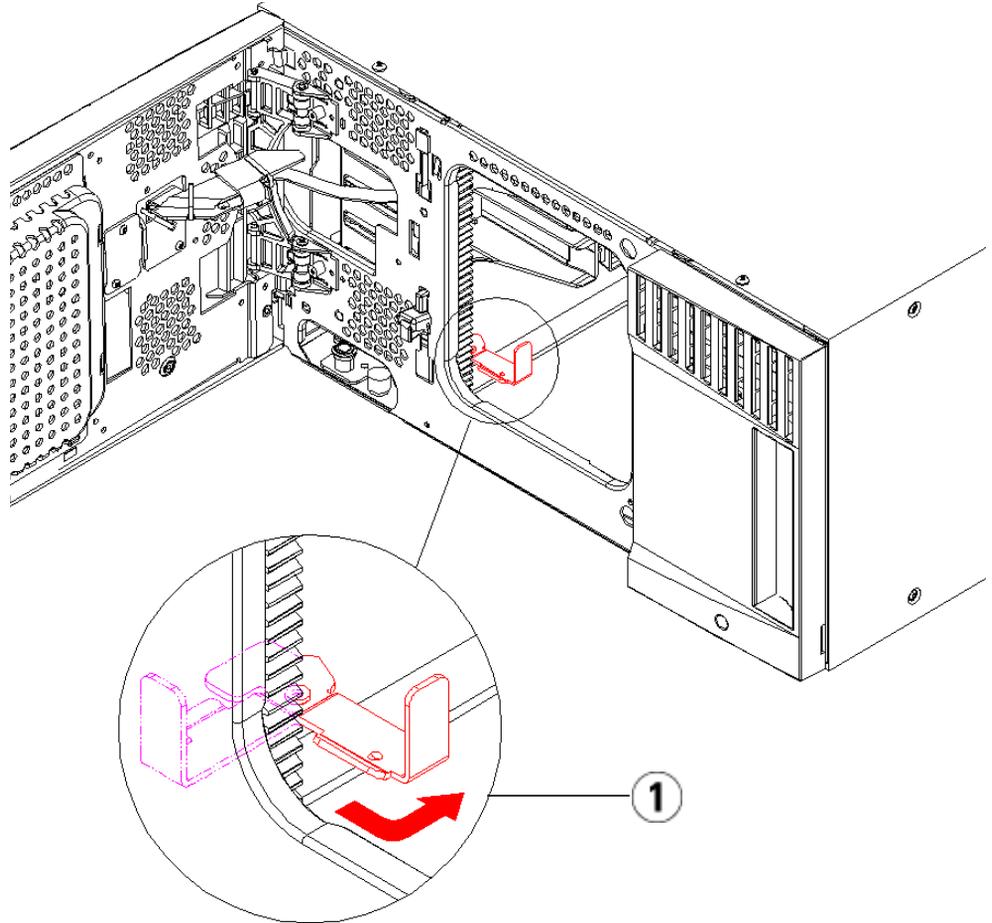
- 9 If you are removing or replacing a 9U Library Expansion Module, set the number of I/E station slots to six. You can reconfigure I/E station slots after the module removal or replacement is complete. See [Configuring I/E Station Slots](#) on page 81.
- 10 Power off the library.
- 11 Disconnect all power cords, network data cables, and module-to-module cables from each module you will be removing.

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

- 12 Park the robot assembly in the 5U Library Control Module. Before unstacking the library, the robot assembly must be placed in the 5U Library 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 5U Library Control Module. The robot assembly should glide slowly and with some resistance.

Caution: Support the robot assembly by holding onto the broad metal X-axis plate. Lifting the robot by the thin metal rod will bend the rod. Lifting the robot by the black plastic picker body can damage the robot.

- c After raising the robot assembly to the approximate middle of the 5U Library Control Module, hold it in place with one hand and, using your other hand, move the parking tab in a counter-clockwise direction until it stops in the “parked” position. The metal parking tab is located at the bottom of column 1.
- d Gently lower the robot assembly to rest on the parking tab.



1 Parking tab in “parked” position

- 13** Remove all power supplies from each module that you intend to remove. For details, see [Adding, Removing, and Replacing Power Supplies](#) on page 330.
- 14** Remove all tape drives from each module that you intend to remove. If you are going to replace the module, label the drives with their locations so you can re-install them in the same locations later. For details, see [Adding, Removing, and Replacing Tape Drives](#) on page 354.

- 15 If the module you are removing or replacing contains FC I/O blades, remove both the I/O blades and the accompanying fan blades from the 9U Library Expansion Module. For details, see [Adding, Removing, and Replacing FC I/O Blades](#) on page 359 and [Adding, Removing, and Replacing the FC I/O Fan Blade](#) on page 370.
- 16 Before removing a module, you must first remove all 9U Library Expansion Modules (if any) positioned above it. Disconnect all power cords, network data cables, and module-to-module cables from the module you are removing or replacing and all modules located above it. Then remove the modules.

Warning: Without tape drives, tape cartridges, or power supplies, a 5U Library Control Module weighs approximately 60 lbs (27.2 kg). A 9U Library Expansion Module, without tape drives, tape cartridges, or power supplies, exceeds 65 lbs (29.5 kg).

To avoid serious injury, at least two people are required to safely lift the modules.

Note: If the library is installed in a rack, you need to perform additional steps to remove modules from and place modules into the rack. See [Installing the Library in a Rack](#) on page 333 for more information.

Permanently Removing 9U Library Expansion Modules From an Existing Library

These instructions explain how to permanently remove a 9U Library Expansion Module from the library.

There are some configuration settings to take into account when removing a 9U Library Expansion Module from an existing library.

- COD licenses remain the same. After the 9U Library Expansion Module is removed, there may be more slots licensed than are available. Only the available slots appear on the **License** screen.
- All resources in the removed module(s) are removed. A partition with all resources in the removed module(s) will be present with no slots or drives. This partition can only be deleted.

Warning: All libraries taller than 14U must be installed in a rack having a main protective earthing (grounding) terminal, and power must be supplied via an industrial plug and socket-outlet and/or an appliance coupler complying with IEC 60309 (or an equivalent national standard) and having a protective earth (ground) conductor with a cross sectional area of at least 1.5 mm² (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 Library Control Module weighs approximately 60 lbs (27.2 kg). A 9U Library Expansion Module, without tape drives, tape cartridges, or power supplies, exceeds 65 lbs (29.5 kg).

To avoid serious injury, at least two people are required to safely lift the modules.

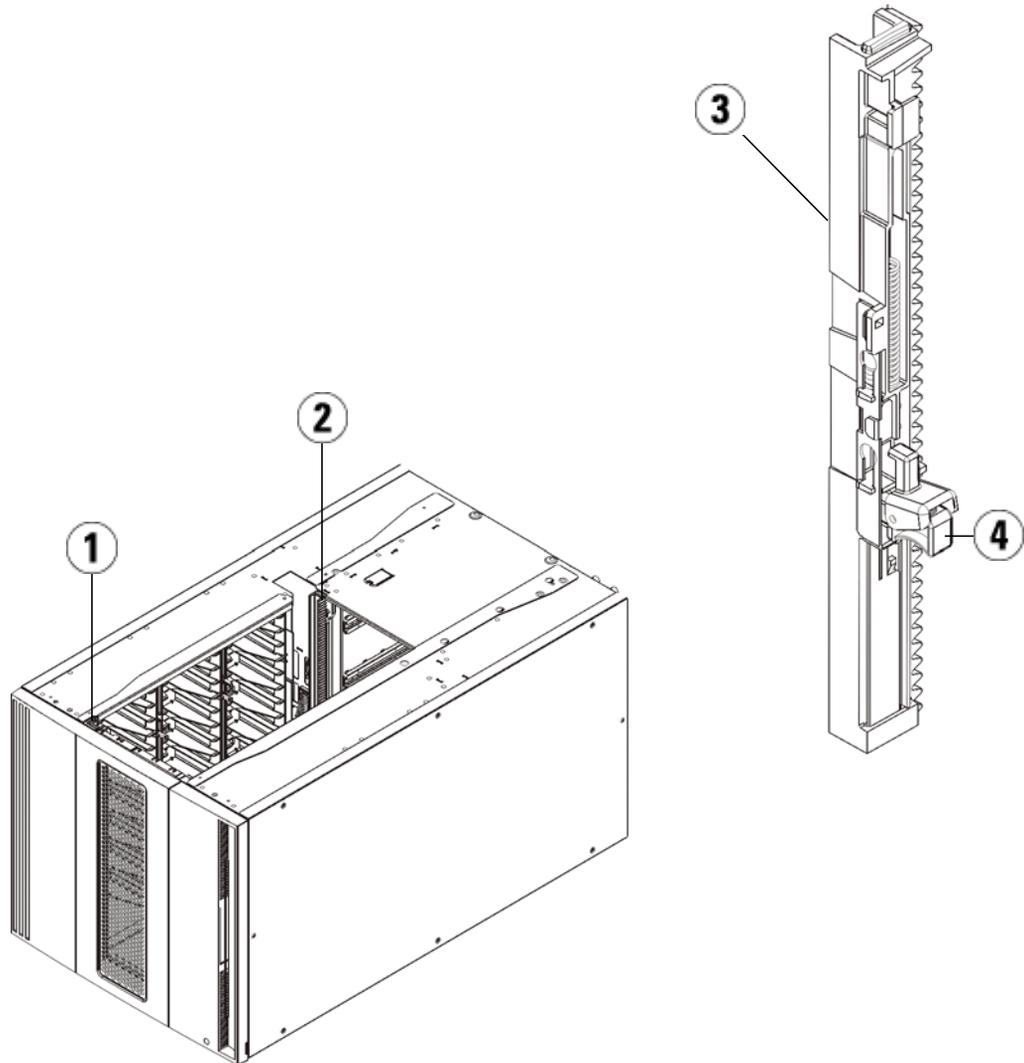
Removing the 9U Library Expansion Module

To remove the 9U Library Expansion Module:

- 1 Before removing a module, follow the instructions in [Preparing to Remove or Replace a Module](#) on page 277.
- 2 For each module that you plan to remove, open the I/E station and access doors of each module.

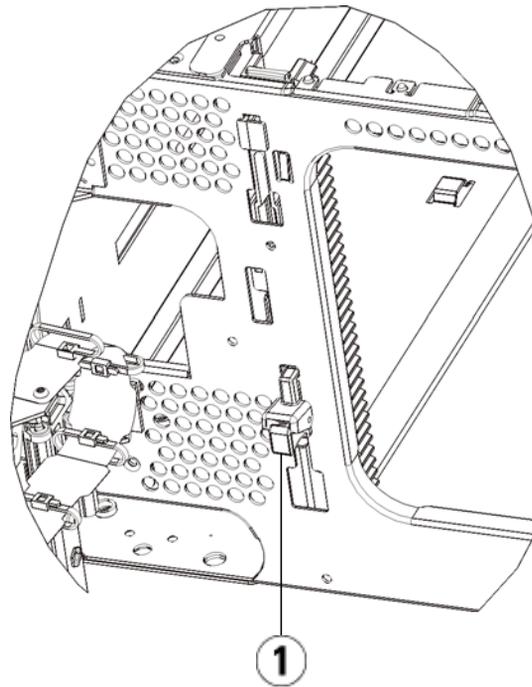
Caution: Before unstacking the modules, the robot assembly must be parked as described in [Preparing to Remove or Replace a Module](#) on page 277.

- 3 Disengage the Y-rails so the modules can be unstacked safely.



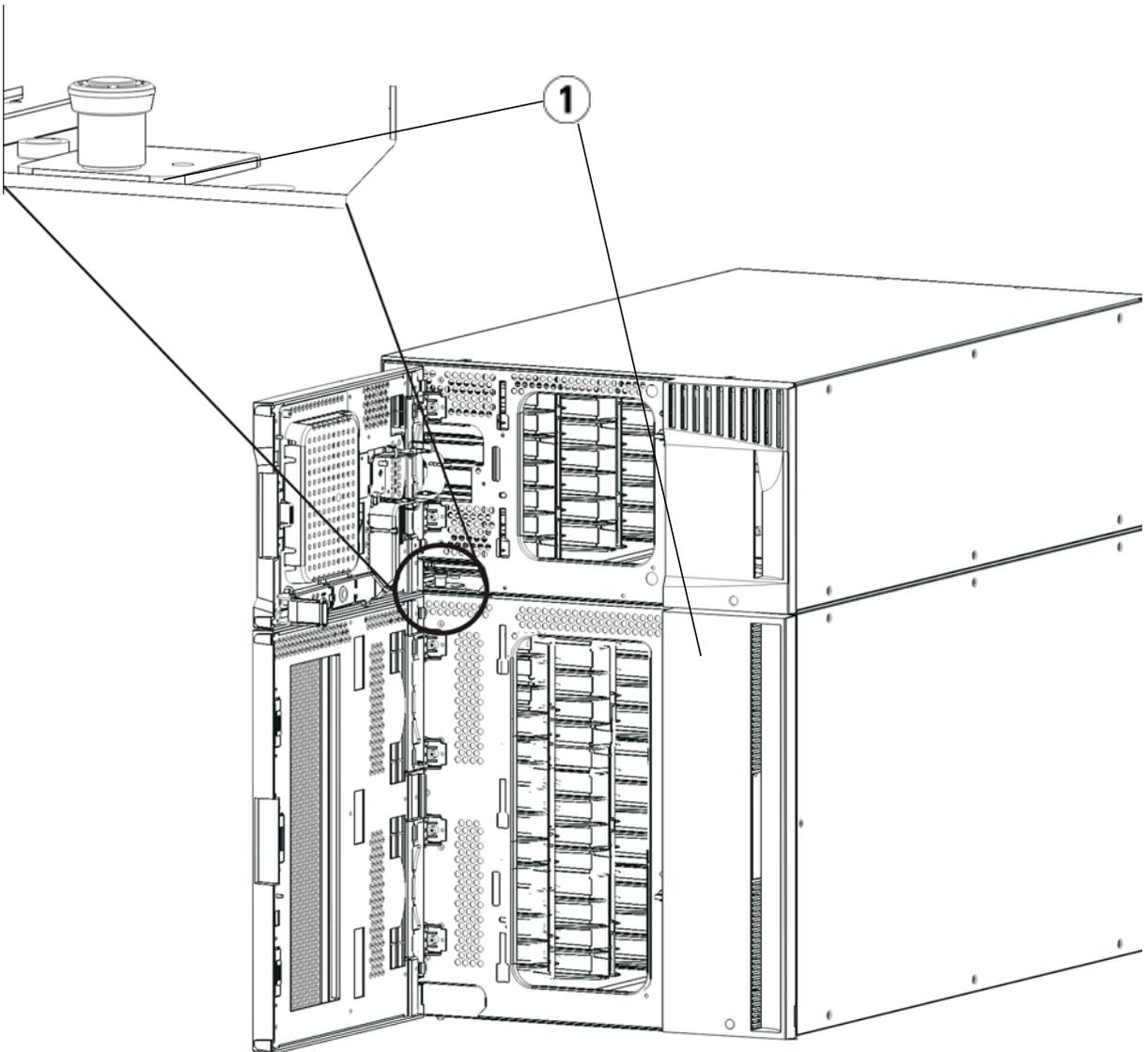
-
- 1 Front Y-rail
 - 2 Rear Y-rail
 - 3 Y-rail (this end up)
 - 4 Squeeze here to release
-

- a** From the front of the library, find the Y-rail release mechanism, which is located on the left side of the 5U Library Control Module. Squeeze the handle of the Y-rail release mechanism, lift it, and release it so that it locks into place.
- b** From the rear of the library, find the rear Y-rail release mechanism located in the interior of the right side of the module. Squeeze the handle of the Y-rail release mechanism, lift it, and release it so that it locks into place.



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

- 4** Remove the rack ears that fasten the module to the rack. See [Installing the Library in a Rack](#) on page 333 for detailed instructions on using the rack ears.
- 5** Loosen the thumbscrews located at the base of the front of the module.



1 Thumbscrews (behind doors)

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

- 7 Open the module's access door and raise the guide pin by pulling it up and turning it slightly as if it were a screw. Otherwise, the guide pin may scratch the front doors of the module beneath it.
- 8 From the front of the library, slide the entire module toward you and lift it off of the module below it.
- 9 Repeat these procedures for each module that you intend to remove.
- 10 Remove and replace the cover plates, if appropriate (see [Figure 39](#)).

Caution: Before removing the 5U Library Control Module's bottom cover plate, the robot assembly must be parked as described in [Preparing to Remove or Replace a Module](#) on page 277.

- a If you plan to stack the 5U Library Control Module at the top of the library, and if a 9U Library Expansion Module will be located below it, remove the 5U Library Control Module's bottom cover plate and the 9U Library Expansion Module's top plate.
- b If you plan to stack the 5U Library Control Module between 9U Library Expansion Modules, remove both the top and bottom plates of the 5U Library Control Module. Also remove the top plate of the 9U Library Expansion Module located below the 5U Library Control Module and the bottom plate of the 9U Library Expansion Module located above the 5U Library Control Module.
- c If you plan to stack the 5U Library Control Module at the bottom of the library, and if a 9U Library Expansion Module will be located above it, remove the 5U Library Control Module's bottom cover plate and the 9U Library Expansion Module's bottom plate.

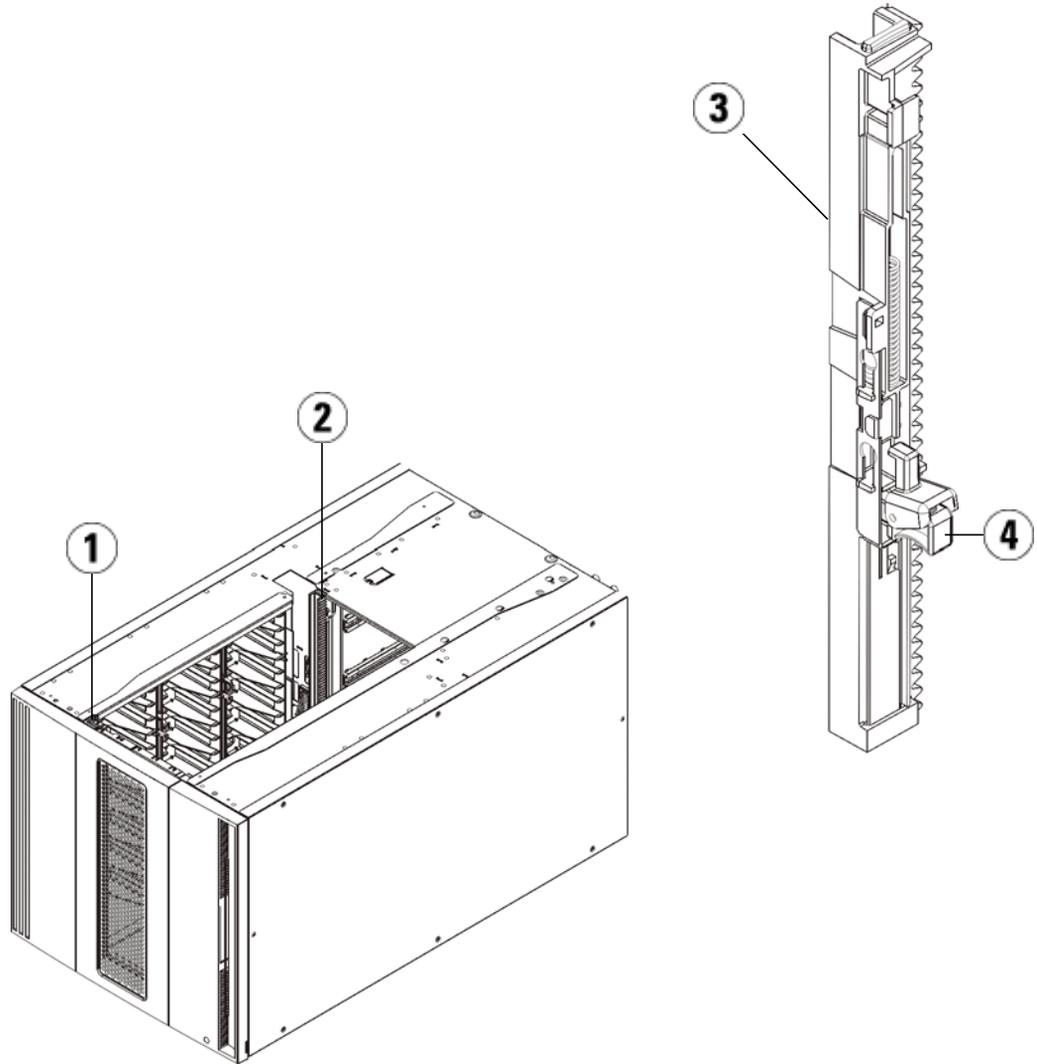
Figure 39 Cover Plate Location
 After Removing a 9U Library
 Expansion Module

5U	14U	23U	32U
			cover plate
		cover plate	5U Library Control Module
	cover plate	5U Library Control Module	9U Library Expansion Module
cover plate	5U Library Control Module	9U Library Expansion Module	9U Library Expansion Module
5U Library Control Module	9U Library Expansion Module	9U Library Expansion Module	9U Library 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.

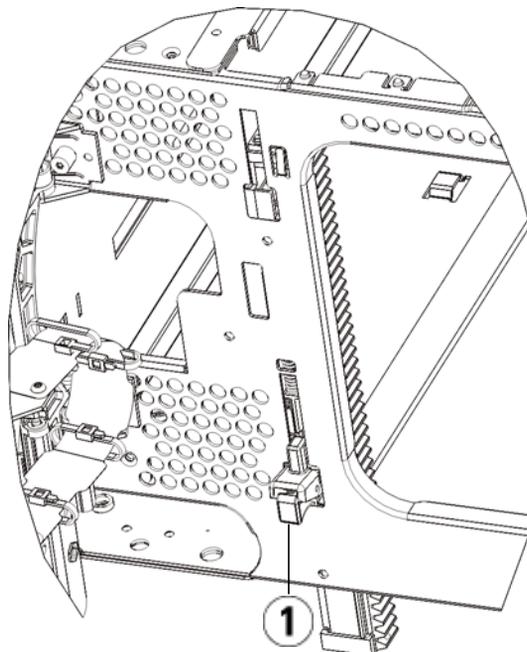


-
- 1 Front Y-rail
 - 2 Rear Y-rail
 - 3 Y-rail (this end up)
 - 4 Squeeze here to release
-

- a** From the front of the library, open the I/E station and access doors of the 9U Library 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.

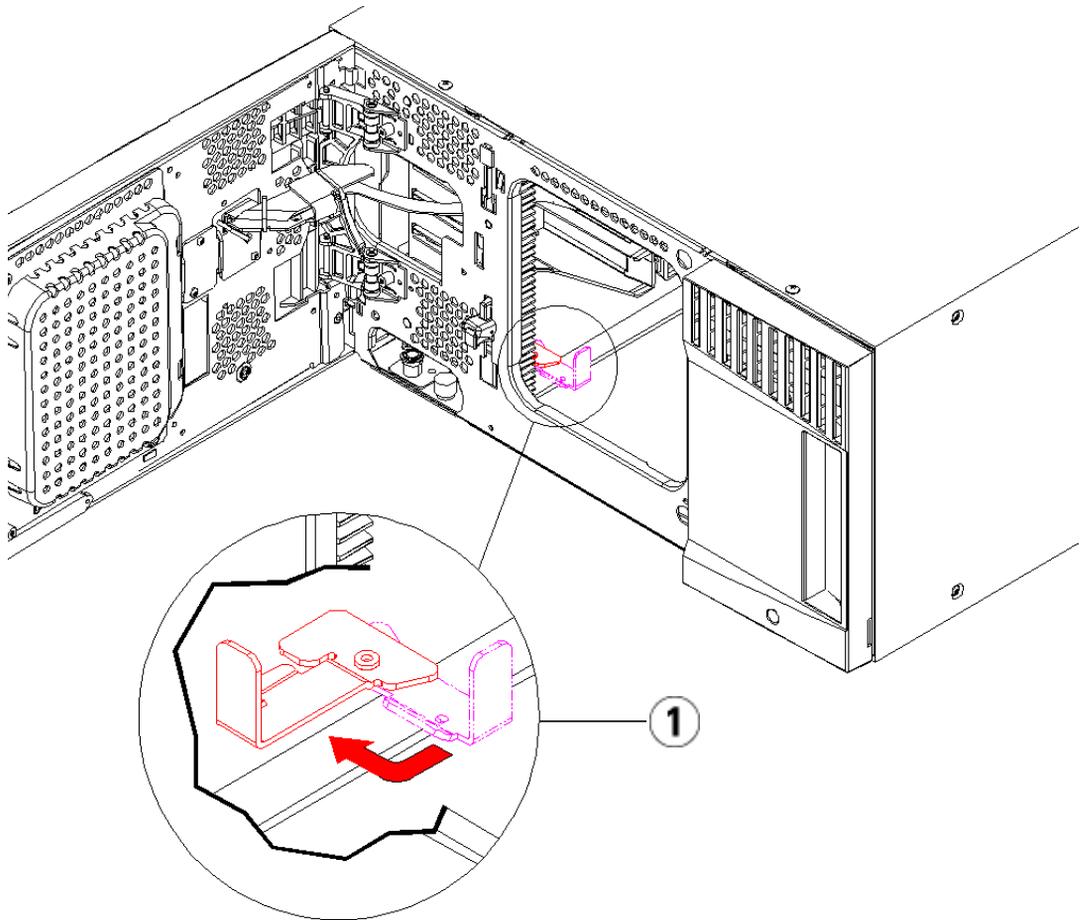


1 Y-rail in unlocked, functional position

- 2 Add the tape drives to the modules. For details, see [Adding, Removing, and Replacing Tape Drives](#) on page 354.
- 3 Add the power supplies. For details, see [Adding, Removing, and Replacing Power Supplies](#) on page 330.
- 4 If your library contains FC I/O blades, install both the I/O blades and the accompanying fan blades in the 9U Library Expansion Module. For details, see [Adding, Removing, and Replacing FC I/O Blades](#) on page 359 and [Adding, Removing, and Replacing the FC I/O Fan Blade](#) on page 370.
- 5 Unpark the robot assembly.
 - a Gently raise the robot assembly so that it no longer rests on the parking tab.

Caution: Support the robot assembly by holding onto the broad metal X-axis plate. Lifting the robot by the thin metal rod will bend the rod. Lifting the robot by the black plastic picker body can damage the robot.

- b** With your free hand, move the parking tab in a clockwise direction until it stops in the “unparked” position. When in the correct position, the parking tab is removed completely from the interior of the module and will not accidentally swing into the path of the robot.
- c** Gently release the robot assembly. It will lower to the bottom module of the library.



1 Parking tab in “unparked” position

- 6 Close the library’s I/E station and access doors.
- 7 Connect all power cords, network data cables, and module-to-module cables. Make sure the module terminators are installed at the top and bottom of the stack of modules. For cabling instructions, see [Cabling the Library](#) on page 212.
- 8 Power on the library.
- 9 Re-create and/or modify partitions, cleaning slots, and I/E station slots as desired.

- 10 Import tape cartridges to the correct library partitions as needed.
- 11 Save the library configuration (see [Saving the Library Configuration](#) on page 385).
- 12 If the host application inventories the location of each tape cartridge in the library, open the host application and reinventory in order to sync its logical inventory with the physical inventory of the library. Due to the way the library logically addresses its tape drives and slots internally, permanently removing an expansion module from the library will change the element addresses, and this can affect proper communication to a controlling host. See [Understanding Logical Element Addressing](#) on page 38. Because of this, you must refresh the configuration of any backup application that manages the library to reflect the adjusted positions. In addition, you may need to reboot the host server(s) or rescan the bus to detect the changes.

Replacing the 5U Library Control Module

These instructions explain how to remove a 5U Library Control Module and replace it with a 5U Library Control Module field replaceable unit (FRU). You may need to replace the 5U Library Control Module if its chassis is severely damaged. Typically, however, only certain customer replaceable units (CRUs) or FRUs within the 5U Library Control Module need to be replaced.

There are some configuration settings to take into account when replacing the 5U Library Control Module.

- If you have applied one or more license keys to the original 5U Library Control Module, you will need to replace each license key and apply it to the new 5U Library Control Module. For more information, see [Obtaining and Installing a License Key](#) on page 88.
- A partition with all resources in the removed module will be present with no slots or drives. This partition can only be deleted.

There are no restrictions on where the 5U Library Control Module can be installed in the library configuration. However, the recommended placement of the 5U Library Control Module for library configurations up to 32U is on top of all installed 9U Library Expansion Modules. The

recommended placement of the 5U Library Control Module for 41U library configurations is on top of three 9U Library Expansion Modules and below the top 9U Library Expansion Module.

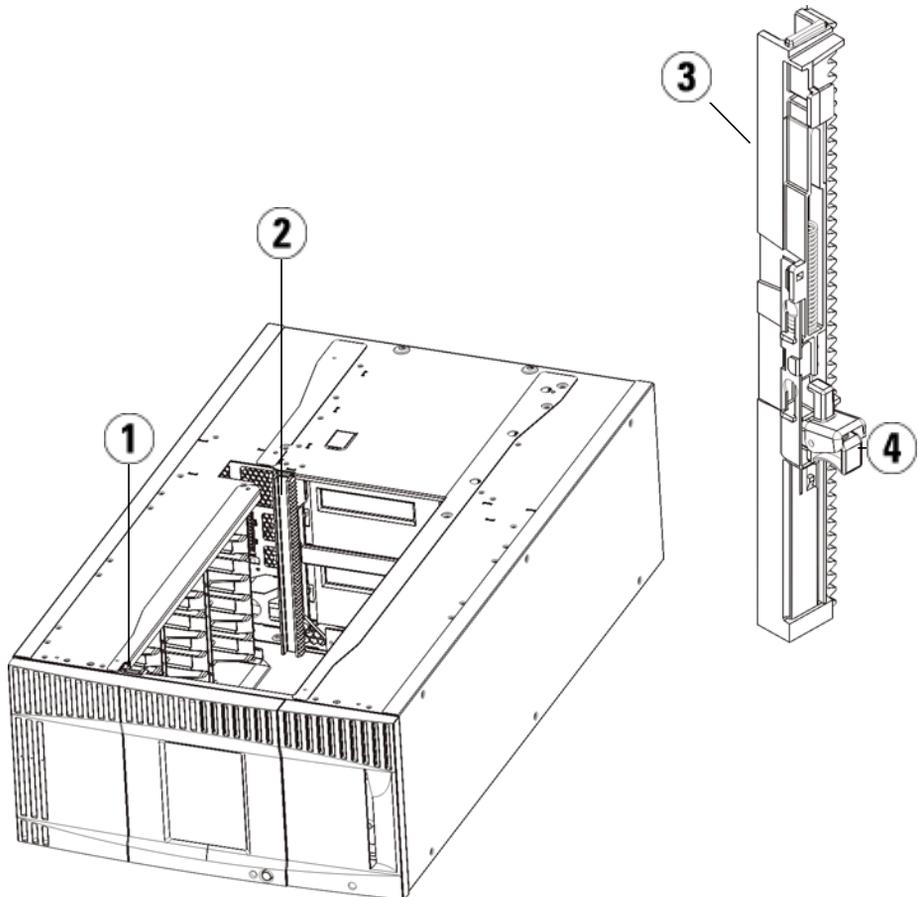
Removing the 5U Library Control Module

- 1 Before removing a module, follow the instructions in [Preparing to Remove or Replace a Module](#) on page 277.
- 2 Starting with the topmost module of your library, open the I/E station and access doors of the module.

Caution: Before unstacking the modules, the robot assembly must be parked as described in [Preparing to Remove or Replace a Module](#) on page 277.

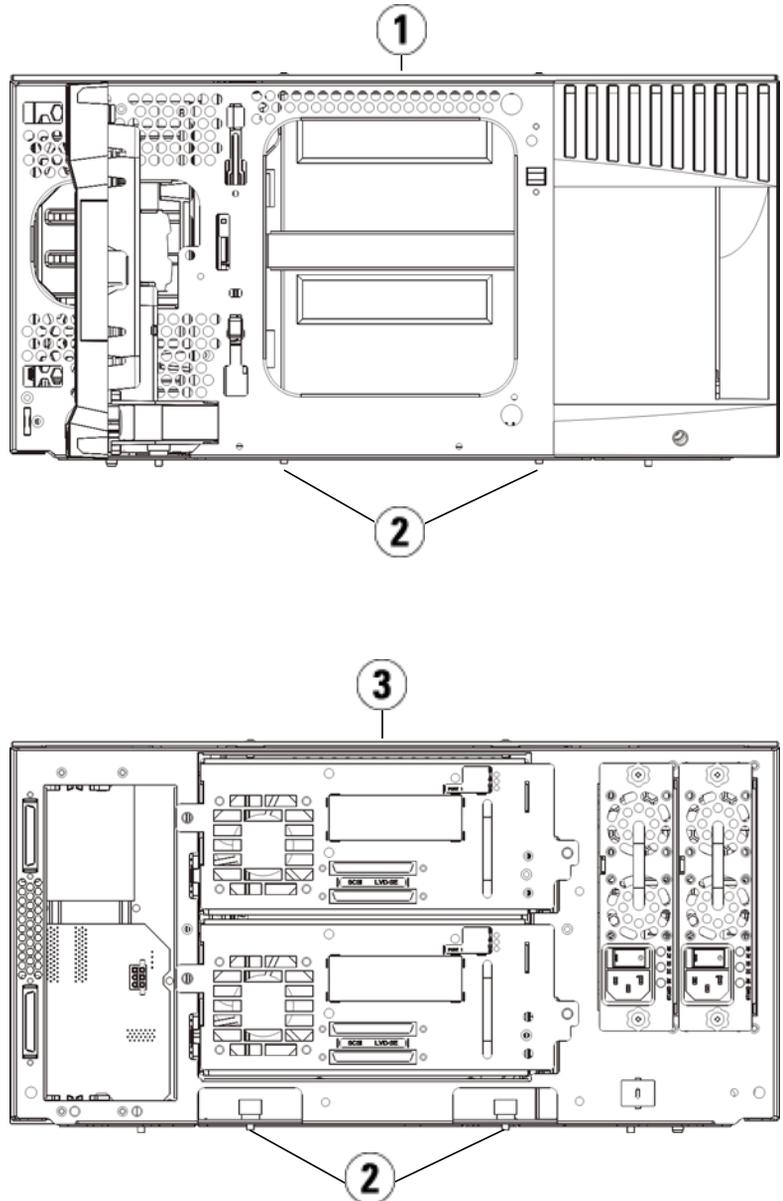
- 3 Disengage the Y-rails so the modules can be safely unstacked.
 - a From the front of the library, find the Y-rail release mechanism, which is located on the left side of the module. Squeeze the handle of the Y-rail release mechanism, lift it, and release it so that it locks into place.
 - b From the rear of the library, find the rear Y-rail release mechanism located in the interior of the right side of the module. Squeeze the handle of the Y-rail release mechanism, lift it, and release it so that it locks into place.

Note: The rear Y-rail is impossible to lift up with the tape drives installed.



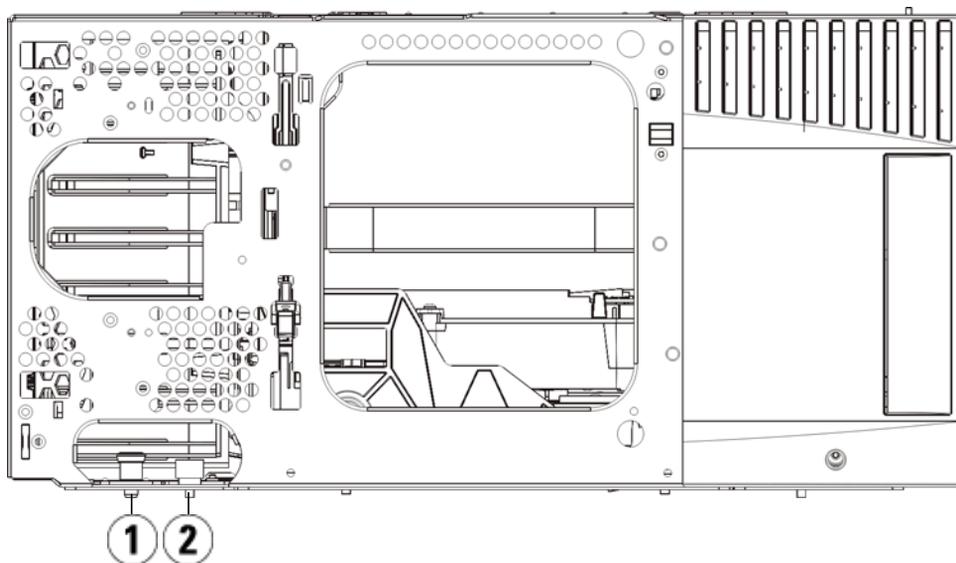
-
- 1 Front Y-rail
 - 2 Rear Y-rail
 - 3 Y-rail (this end up)
 - 4 Squeeze here to release
-

- 4 Remove the rack ears that fasten the module to the rack.
- 5 Loosen the thumbscrews located at the base of the front and rear of the module.



-
- 1 5U Library Control Module (front)
 - 2 Thumbscrews
 - 3 5U Library Control Module (rear)
-

- 6 Open the module's access door and raise the guide pin by pulling it up and turning it slightly as if it were a screw. Otherwise, the guide pin may scratch the front doors of the module beneath it.



-
- 1 Guide pin
 - 2 Thumbscrew
-

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

Replacing the 5U Library Control Module

- 1 If not already removed, remove the tape drives and power supplies from the 5U Library Control Module you are replacing.
- 2 Using the Phillips #2 screwdriver (for the top cover plate) and the T10 TORX screwdriver (for the bottom cover plate), remove the new 5U Library Control Module plates from the top and bottom of the module, as necessary.

Caution: Before removing the 5U Library Control Module's bottom cover plate, the robot assembly must be parked as described in [Preparing to Remove or Replace a Module](#) on page 277.

- a** If your library consists of only the 5U Library Control Module, do not remove the plates.
 - b** If you plan to stack the 5U Library Control Module at the top of the library, and if a 9U Library Expansion Module is located below it, remove the 5U Library Control Module's bottom cover plate.
 - c** If you plan to stack the 5U Library Control Module in the middle of the library, remove both the top and bottom cover plates.
 - d** If you plan to stack the 5U Library Control Module at the bottom of the library, and if a 9U Library Expansion Module is located above it, remove the 5U Library Control Module's top cover plate.
- 3** Remove the LCB from the removed 5U Library Control Module and set it aside.

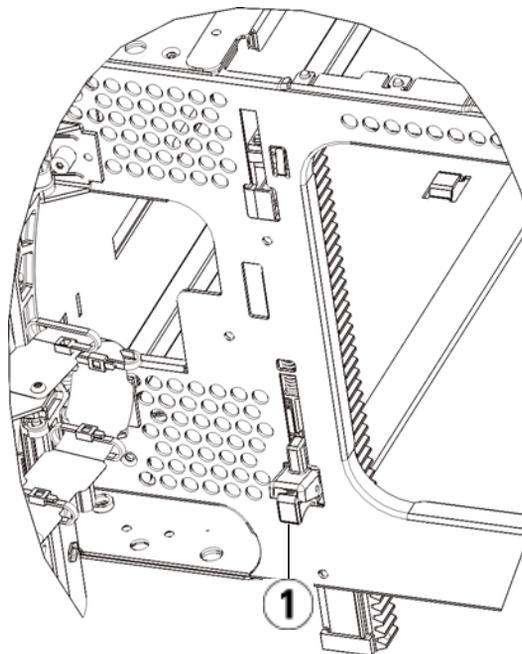
The LCB stores information about the library's contents and configuration, so you will probably want to install this LCB in the new 5U Library Control Module. For details about removing the LCB, see [Removing and Replacing the Library Control Blade and LCB Compact Flash Card](#) on page 320.

Note: If you plan to stack the 5U Library Control Module on top of a 9U Expansion Module, be sure to park the robot in the 5U Library Control Module first.

- 4** If the library configuration includes 9U Library Expansion Modules below the 5U Library Control Module, install them in the library now.
- 5** Install the new 5U Library Control Module in the library. Lift the 5U Library Control Module and, from the front of the library, place it in the desired location.

Place the 5U Library Control Module on top of the 9U Library Expansion Module and slide it to the rear of the unit. A small notch on the bottom of the 5U Library Control Module aligns it with the top of the 9U Expansion Module.

- 6** Use rack ears to fasten the 5U Library Control Module on top of a 9U Expansion Module.
- 7** If you placed the 5U Library Control Module on top of a 9U Library Expansion Module, secure the two modules by tightening the two thumbscrews at the base of the *front* of the module and the two thumbscrews located at the base of the *back* of the module. Then lower the module's guide pin (located at the base of the front of the module) by turning it and pushing it down.
- 8** Stack all 9U Library Expansion Modules (if any) in their original positions above the 5U Library Control Module. Use rack ears to fasten the modules to the rack. Then tighten all thumbscrews located at the base of the front and back of the modules.
- 9** Engage the Y-rails. Tighten the thumbscrews and lower the guide pin. Doing this aligns the Y-rail with the Y-rail of the module beneath it.
 - a** From the front of the library, open the I/E station and access doors of the 5U Library Control Module. Squeeze the handle of the Y-rail release mechanism, lift it out of its locked position, and slide it downward as far as it will go.

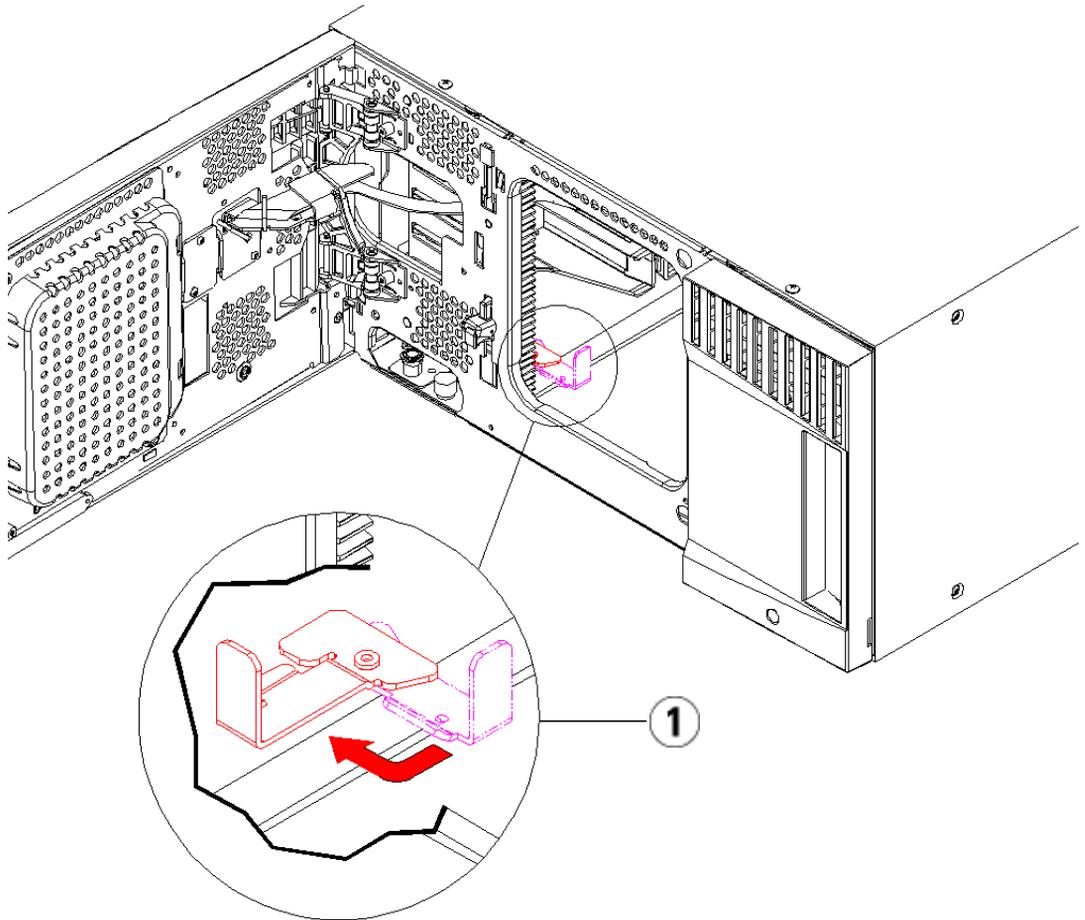


1 Y-rail in unlocked, functional position

- b** From the back of the library, find the rear Y-rail release mechanism, which is located in the interior of the right side of the module. Squeeze the handle of the Y-rail release mechanism, lift it out of its locked position, and slide it downward as far as it will go.
- 10** Unpark the robot assembly.
- a** Gently raise the robot assembly so that it no longer rests on the parking tab.

Caution: Support the robot assembly by holding onto the broad metal X-axis plate. Lifting the robot by the thin metal rod will bend the rod. Lifting the robot by the black plastic picker body can damage the robot.

- b** With your free hand, move the parking tab in a clockwise direction until it stops in the “unparked” position. When in the correct position, the parking tab is removed completely from the interior of the module and will not accidentally swing into the path of the robot.
- c** Gently release the robot assembly. It will lower to the bottom module of the library.



1 Parking tab in “unparked” position

Preparing to Use the 5U Library 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 354.
- 3 Add the power supplies. For details, see [Adding, Removing, and Replacing Power Supplies](#) on page 330.
- 4 Install the LCB from the removed 5U Library Control Module in the new 5U Library Control Module. For details, see [Removing and Replacing the Library Control Blade and LCB Compact Flash Card](#) on page 320.
- 5 Connect all power cords, network data cables, and module-to-module cables. Make sure the module terminators are installed in their previous positions at the top and bottom of the stack of modules. For cabling instructions, see [Cabling the Library](#) on page 212.
- 6 Power on the library.
- 7 Re-create and/or modify partitions, cleaning slots, and I/E station slots as desired.
- 8 Import tape cartridges into the correct partitions as needed.
- 9 Save the library configuration (see [Saving the Library Configuration](#) on page 385).
- 10 If the host application inventories the location of each tape cartridge in the library, open the host application and reinventory in order to sync its logical inventory with the physical inventory of the library. Due to the way the library logically addresses its tape drives and slots internally, replacing a control module may change the element addresses, and this can affect proper communication to a controlling host. See [Understanding Logical Element Addressing](#) on page 38. Because of this, you must refresh the configuration of any backup application that manages the library to reflect the adjusted positions. In addition, you may need to reboot the host server(s) or rescan the bus to detect the changes.

Replacing a 9U Library Expansion Module

These instructions explain how to remove and replace a 9U Library Expansion Module. You may need to replace the 9U Library Expansion Module if its chassis is severely damaged.

A library can use up to four 9U Library Expansion Modules to a maximum height of 41U.

There are some configuration settings to take into account when removing and replacing a 9U Library Expansion Module.

- COD licenses remain the same. After the 9U Library Expansion Module is removed, there may be more slots licensed than are available. Only the available slots appear on the **License** screen.
- All resources in the removed module(s) are removed. A partition with all resources in the removed module(s) will be present with no slots or drives. This partition can only be deleted.

Note: The maximum number of 9U Library Expansion Module supported in a library depends on the level of firmware the library is running. See [Updating Library and Tape Drive Firmware](#) on page 199 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 mm² (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 Library Control Module weighs approximately 60 lbs (27.2 kg). A 9U Library Expansion Module, without tape drives, tape cartridges, or power supplies, exceeds 65 lbs (29.5 kg).

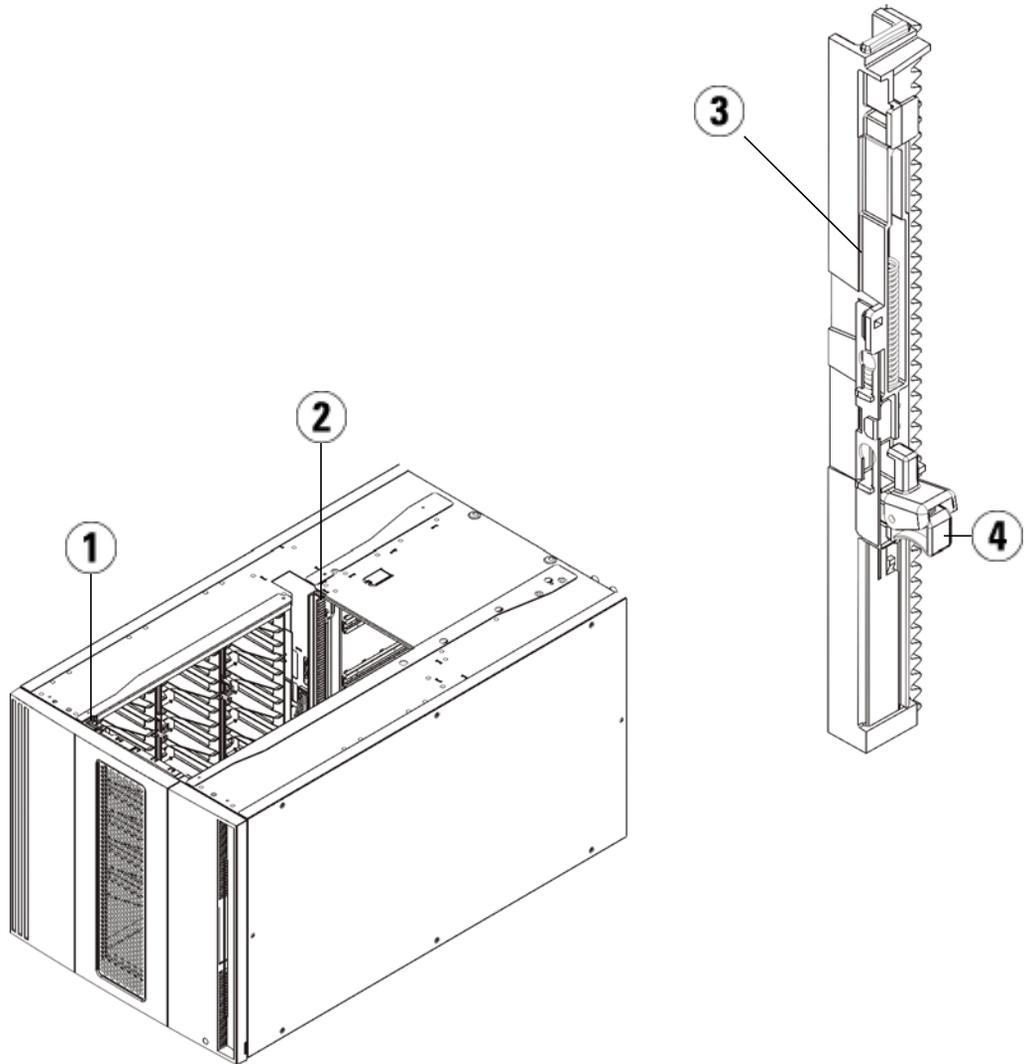
To avoid serious injury, at least two people are required to safely lift the modules.

Removing the 9U Library Expansion Module

- 1 Before removing the module, follow the instructions in [Preparing to Remove or Replace a Module](#) on page 277.
- 2 Starting with the topmost module of your library, open the I/E station and access doors of each module.

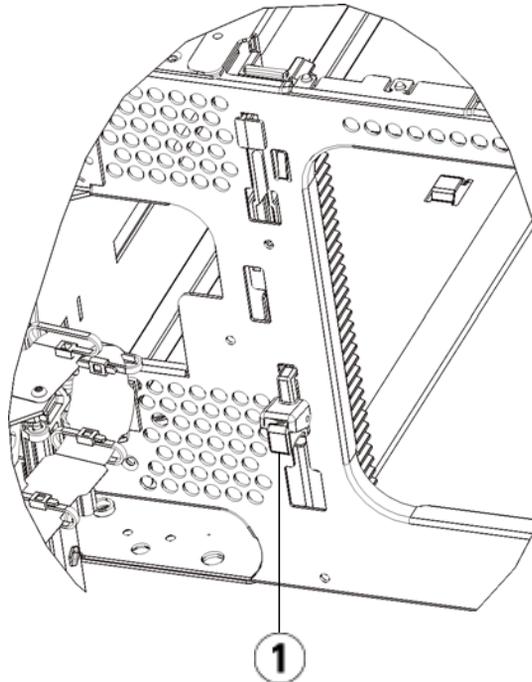
Caution: Before unstacking the modules, the robot assembly must be parked as described in [Preparing to Remove or Replace a Module](#) on page 277.

- 3 Disengage the Y-rails so the modules can be unstacked safely.



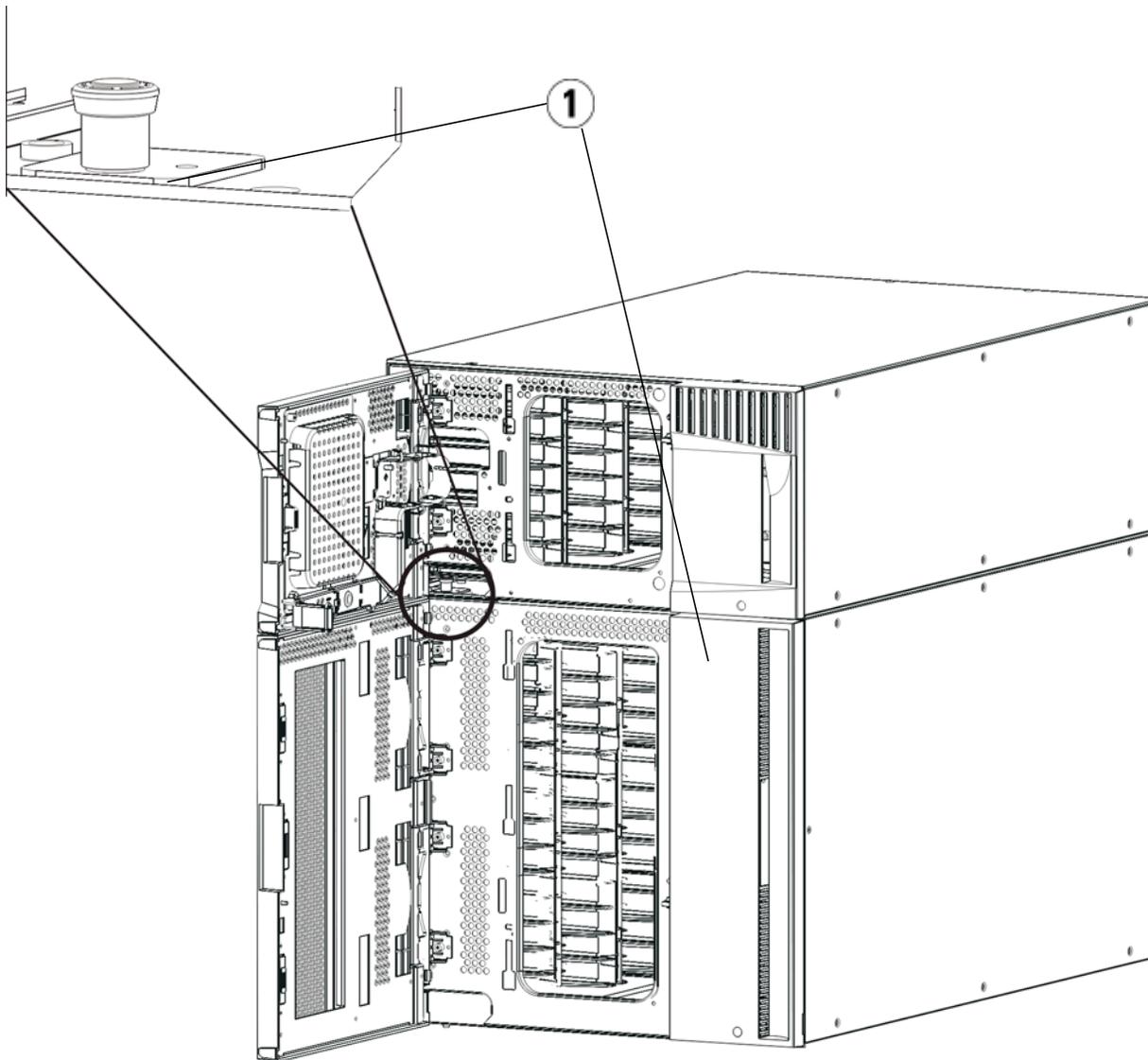
-
- 1 Front Y-rail
 - 2 Rear Y-rail
 - 3 Y-rail (this end up)
 - 4 Squeeze here to release
-

- a** From the front of the library, find the Y-rail release mechanism, which is located on the left side of the 5U Library Control Module. Squeeze the handle of the Y-rail release mechanism, lift it, and release it so that it locks into place.



1 Y-rail in locked, non-functional position

- b** From the rear of the library, find the rear Y-rail release mechanism located in the interior of the right side of the module. Squeeze the handle of the Y-rail release mechanism, lift it, and release it so that it locks into place.
- 4** Remove the rack ears that fasten the module to the rack. See [Installing the Library in a Rack](#) on page 333 for detailed instructions on using the rack ears.
- 5** Loosen the thumbscrews located at the base of the front of the module.



1 Thumbscrews (behind doors)

- 6 Loosen the two thumbscrews located at the base of the back of the module.
- 7 Open the module's access door and raise the guide pin by pulling it up and turning it slightly as if it were a screw. Otherwise, the guide pin may scratch the front doors of the module beneath it.
- 8 From the front of the library, slide the entire module toward you and lift it off of the module below it.
- 9 Repeat these procedures for each module that you need to remove.
- 10 Remove and replace the cover plates, if appropriate.

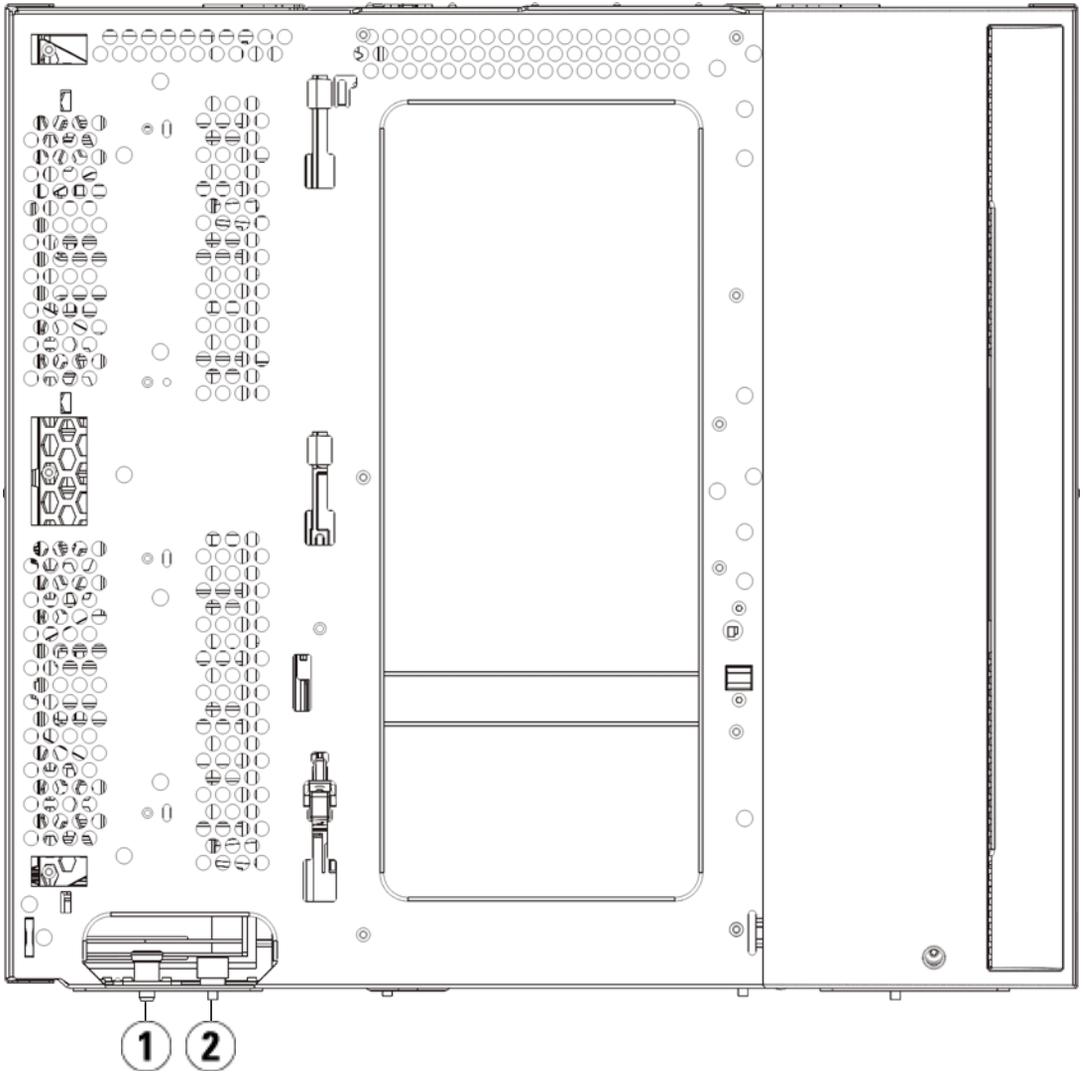
Caution: Before removing the 5U Library Control Module's bottom cover plate, the robot assembly must be parked as described in [Preparing to Remove or Replace a Module](#) on page 277.

- a If you plan to stack the 5U Library Control Module at the top of the library, and if a 9U Expansion Module will be located below it, remove the 5U Library Control Module's bottom cover plate and the 9U Expansion Module top plate.
- b If you plan to stack the 5U Library Control Module between 9U Expansion Modules, remove both the top and bottom plates of the 5U Library Control Module. Also remove the top plate of the 9U Expansion Module located below the 5U Library Control Module and the bottom plate of the 9U Expansion Module located above the 5U Library Control Module.
- c If you plan to stack the 5U Library Control Module at the bottom of the library, and if a 9U Expansion Module will be located above it, remove the 5U Library Control Module's top plate and the 9U Expansion Module's bottom plate.

Replacing the 9U Expansion Module

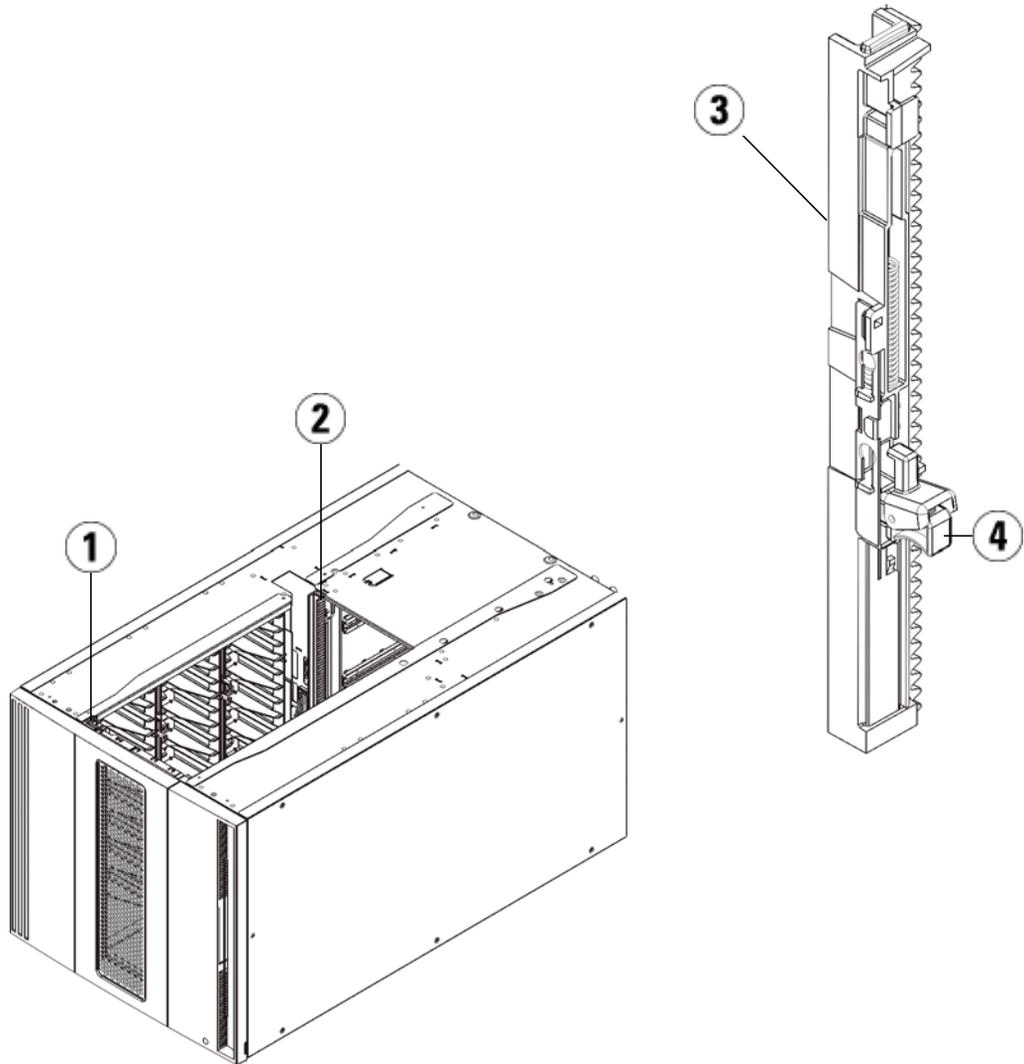
- 1 Remove all tape drives from the 9U Library Expansion Module that you are adding. See [Adding, Removing, and Replacing Tape Drives](#) on page 354 for instructions on removing tape drives.
- 2 Remove the power supplies from the 9U Library Expansion Module that you are adding. See [Adding, Removing, and Replacing Power Supplies](#) on page 330 for instructions on removing power supplies.

- 3** Open the 9U Library 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.



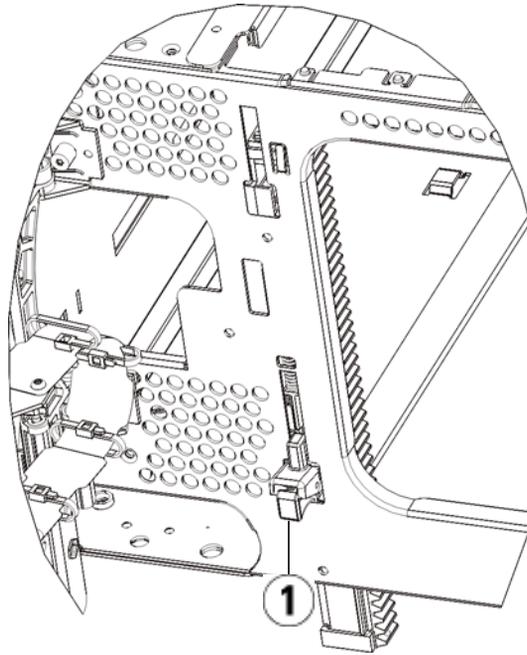
-
- 1 Guide pin
 - 2 Thumbscrew
-

- 4** Lift the new 9U Library 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 9U Library Expansion Module. Squeeze the handle of the Y-rail release mechanism, lift it out of its locked position, and slide it downward as far as it will go.



1 Y-rail in unlocked, functional position

- b** From the back of the library, find the rear Y-rail release mechanism, which is located in the interior of the right side of the module. Squeeze the handle of the Y-rail release mechanism, lift it out of its locked position, and slide it downward as far as it will go.

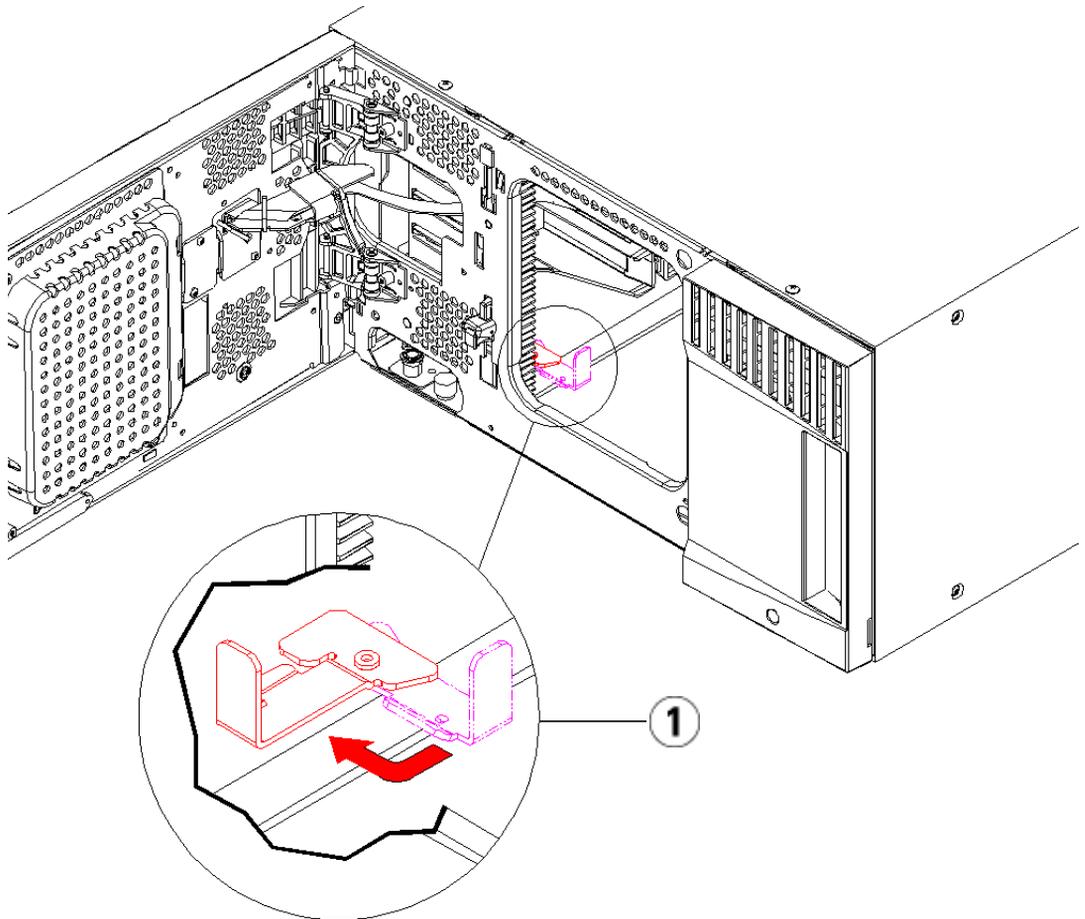
Doing this aligns the Y-rails with the Y-rails of the module beneath it.

Caution: Check to make sure that there is no gap between the top and bottom Y-rails on both the front and back of the library. If a gap exists, the library cannot mechanically initialize.

- 9 Unpark the robot assembly.
 - a Gently raise the robot assembly so that it no longer rests on the parking tab.

Caution: Support the robot assembly by holding onto the broad metal X-axis plate. Lifting the robot by the thin metal rod will bend the rod. Lifting the robot by the black plastic picker body can damage the robot.

- b With your free hand, move the parking tab in a clockwise direction until it stops in the “unparked” position. When in the correct position, the parking tab is removed completely from the interior of the module and will not accidentally swing into the path of the robot.
 - c Gently release the robot assembly. It will lower to the bottom module of the library.



-
- 1 Parking tab in “unparked” position
-

Preparing to Use the 9U Expansion Module

- 1 Close the library’s I/E station and access doors.
- 2 Add the tape drives to the modules. For details, see [Adding, Removing, and Replacing Tape Drives](#) on page 354.
- 3 Add the power supplies. For details, see [Adding, Removing, and Replacing Power Supplies](#) on page 330.

- 4 If your library contains FC I/O blades, install both the I/O blades and the accompanying fan blades in the expansion module. For details, see [Adding, Removing, and Replacing FC I/O Blades](#) on page 359 and [Adding, Removing, and Replacing the FC I/O Fan Blade](#) on page 370.
- 5 Connect all power cords, network data cables, and module-to-module cables. Make sure the module terminators are installed at the top and bottom of the stack of modules. For cabling instructions, see [Cabling the Library](#) on page 212.
- 6 Power on the library.
- 7 Re-create partitions, cleaning slots, and I/E station slots as desired.
- 8 Import tape cartridges to the correct partitions as needed.
- 9 Save the library configuration (see [Saving the Library Configuration](#) on page 385).
- 10 If the host application inventories the location of each tape cartridge in the library, open the host application and reinventory in order to sync its logical inventory with the physical inventory of the library.

Removing and Replacing the Library Control Blade and LCB Compact Flash Card

The library control blade (LCB) manages the entire library, including the operator panel and robot, and is responsible for running system tests to ensure that the library is functioning properly.

The LCB compact flash card contains important information about your library configuration. If you replace the compact flash card, then you need to reconfigure your library. You should always replace the LCB and LCB compact flash card together.

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.

Equipment Required

- Ethernet Cable.
- Host PC or laptop connected to the Dell PowerVault ML6000 library.
- Current Dell PowerVault ML6000 library firmware file saved to your host PC or laptop. Firmware downloads are available at <http://support.dell.com>.
- Latest library configuration saved on PC or laptop.

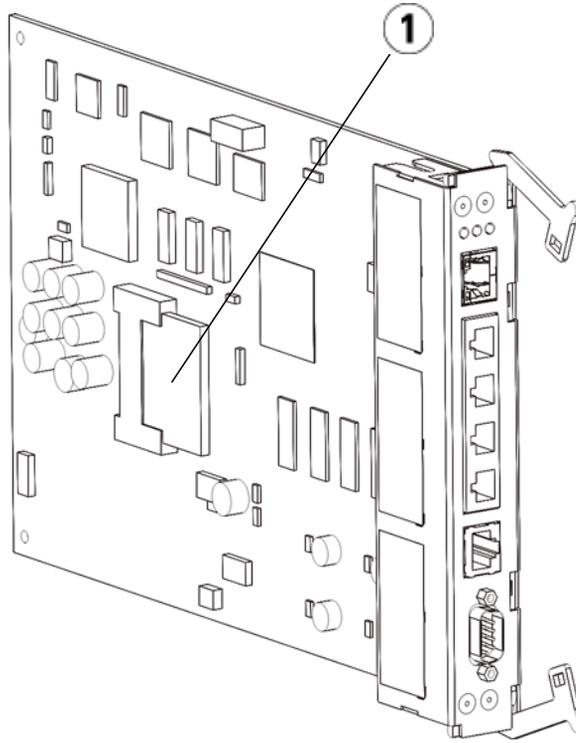
Instructions

The Compact Flash Card is new and has never been initialized. It contains only a minimal level of library firmware which allows the library to boot up and display an Upgrade Notification message. Once you install the LCB/compact flash card, you will need to upgrade firmware and reconfigure your network settings.

Note: Do not separate the old compact flash card from the library control blade.

- 1 If possible, save the library configuration (see [Saving the Library Configuration](#) on page 385).
- 2 Power off the library.
- 3 Disconnect all cables from the existing LCB. You may want to label each cable that is connected to the existing LCB to make sure that you can correctly reconnect them to the new LCB.
- 4 Remove the existing LCB from the library.

To remove the existing LCB, release both of the LCB latch hooks and, using the latch hooks as handles, pull the entire LCB toward you.



1 LCB compact flash card

- 5 If the new LCB and compact flash card came in discrete packages, insert the new compact flash card into the new LCB.
- 6 Insert the new LCB into the vacant LCB slot on the back of the library.

When inserting the new LCB into the slot, be sure that the LCB LEDs are located at the top of the blade, and that the latch hooks are on the right side of the blade.

When sliding the new LCB into the slot, there should be no resistance.

Caution: Do not force the LCB into the slot or damage may occur.

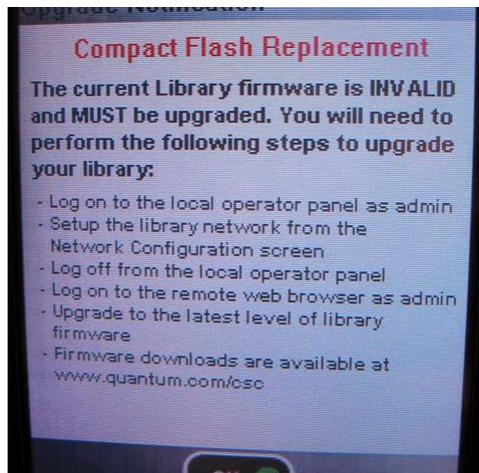
- 7 After inserting the new LCB, secure it by depressing both of the LCB latch hooks into the blade. The LCB will fit snugly into its slot.
- 8 Reconnect all cables to the new LCB.
- 9 Power on the library.

The green power light on the front panel turns on. The screen may remain dark for up to 5 minutes. Then an “Initialization In Progress” screen displays. The initialization process can take up to 30 minutes depending on library configuration.



Caution: From this point forward until the process is complete, do NOT remove power from the library! Doing so may cause failure and cause LCB to become unusable.

When initialization is complete, the screen will display “Upgrade Notification: Compact Flash Replacement” screen shown below.



10 Click **OK**.

The login screen appears.

11 Enter the following default user name and password:

- User name: **admin**
- Password: **password**

12 Press **OK**.

The Enable IPv6 screen appears.



13 Select the **Enable IPv6** check box if you are required to use IPv6 or leave the check box blank to not enable it.

14 Press **Next**.

The Network Configuration screen appears. The system defaults to DHCP. For IPv4 only, you can deselect the DHCP option and assign a static IP address. You cannot assign a static IP address for IPv6.



Setup Wizard: Network Configuration

Your library has the following name and network settings. You can edit these settings or accept them.

Library Name:

Network Settings:

Use DHCP:

OR

IP Address:

Subnet Mask:

Def. Gateway:

15 Accept the default settings by pressing **Apply**, or make any changes to the network settings, and then press **Apply**.

The progress window displays a “Success” message when complete.



- 16** Press **Close**.

The next screen lists one or more IP addresses assigned to the library.

- 17** Write down the IP addresses. You will need them to log in from your Web browser.

- 18** Click **Close**.

The system logs you out and you return to the login screen.

Caution: The installation is NOT complete at this point. Install current library firmware following the steps below. Firmware Installation can take up to 1 hour to complete. DO NOT remove power from the library during this process.

- 19** Open a Web browser on the host PC and type the following in the address bar:

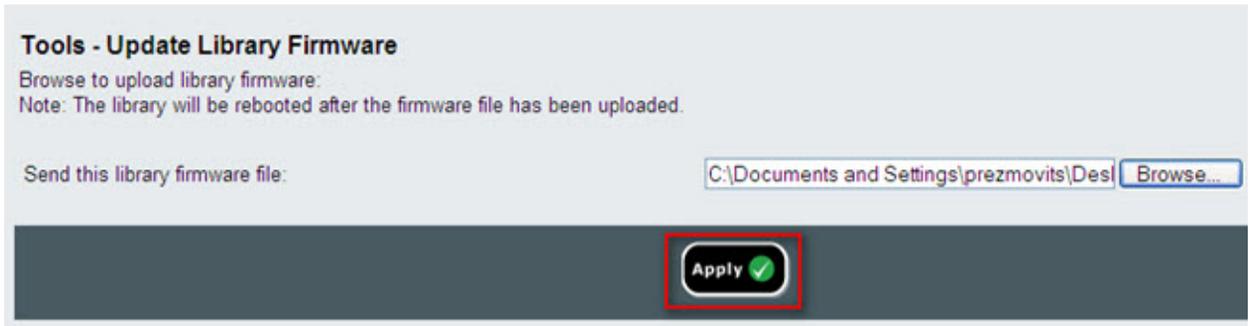
http://<ipaddress>/

where **ipaddress** is one of the IP addresses assigned to the library that you wrote down earlier.

A screen appears, displaying the current version of library firmware.

- 20 Click the **Click here to upgrade your library's firmware** link.

The Tools - Update Library Firmware screen appears.



- 21 Click **Browse** to retrieve the .tgz firmware file from the location on your computer, then click **Apply**.

A dialog box appears asking you to confirm it is OK to reboot the library.

- 22 Click **OK**.

The screen displays “WORKING” in the Progress Window.

Once the Firmware has been transferred from the computer to the library the login screen appears.

Caution: The appearance of the login screen on the Web browser does NOT mean the firmware upgrade has completed on the library; it is just an indication that the firmware image has been moved to the LCB/compact flash card. A 14U library with six tape drives installed can take up to 50 minutes to complete this process. Actual time may vary. You will not be able to log in until the firmware upgrade is complete.

Caution: Do NOT remove power from the library while the firmware is upgrading.

The library operator panel may display the following “upgrade in progress” message; or it may blank out or change multiple times during the firmware upgrade process.



- 23 When the firmware upgrade is complete, the login screen appears on the operator panel.
- 24 Enter the following default user name and password:
 - User name: **admin**
 - Password: **password**
- 25 Press **OK**.

The Setup Wizard screen appears.

Note: At this point the Scalar i500 Library is set up with factory default settings.

26 Reconfigure your library settings as they were before.

Caution: Contact Dell Support before restoring the configuration. In general, it is recommended that you use the setup wizard to manually reconfigure the library. It is not recommended to use the “restore configuration” tool to restore the previous settings. Doing so will completely reinstall the former library firmware level and potentially any defective configuration settings encountered prior to installing the new LCB/compact flash card combo. If you do restore a previous configuration and downrev firmware, you will need to install the latest version of firmware again.

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 5U Library Control Module provides power to all 5U Library 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 5U Library Control Module and each 9U Library 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 [Saving the Library Configuration](#) on page 385).
- 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 5U Library 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 [Saving the Library Configuration](#) on page 385).
- 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 385).
- 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 PowerVault ML6000 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 rack-mount kit secures your library within a rack. These instructions explain how to install your stand-alone library into a rack and how to install additional modules into an existing rack.

Installing the modules into the rack requires at least two people.

Warning: All libraries taller than 14U must be installed in a rack having a main protective earthing (grounding) terminal, and power must be supplied via an industrial plug and socket-outlet and/or an appliance coupler complying with IEC 60309 (or an equivalent national standard) and having a protective earth (ground) conductor with a cross sectional area of at least 1.5 mm² (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 5U Library Control Module weighs approximately 60 lbs (27.2 kg). A 9U Library Expansion Module, without tape drives, tape cartridges, or power supplies, exceeds 65 lbs (29.5 kg).

To avoid serious injury, at least two people are required to safely lift the modules.

Note: The rack-mount kit cannot be used with every type of rack. Racks with threaded rails or unique hole spacing, for example, may not support the rack-mount kit. In addition, the rack must have rail spacing (front to rear) of between 605 mm (23.8 in.) and 770 mm (30.3 in.).

Preparing for Installation

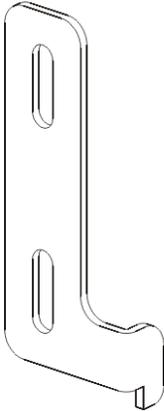
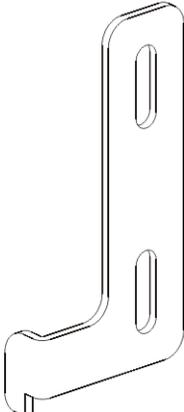
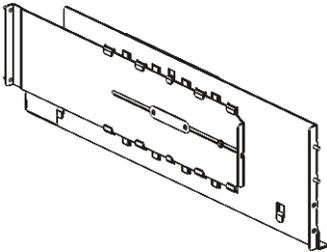
Required tools: None

- 1 Before beginning installation, verify the contents of the rack-mount kit (see [Table 8](#)) and the rack ear kit (see [Table 9](#)).
 - You only need one rack-mount kit per library. The rack-mount 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 Rack-mount 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
	<p>Rack ear, left – Holds the modules in the rack</p>	<p>1</p>
	<p>Rack ear, right – Holds the modules in the rack</p>	<p>1</p>
	<p>Rack shelf, left – Secures the modules in the rack</p>	<p>1</p>

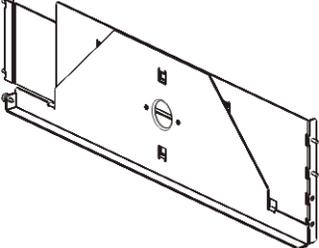
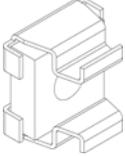
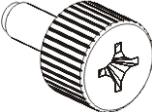
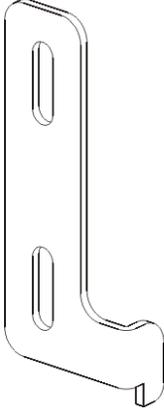
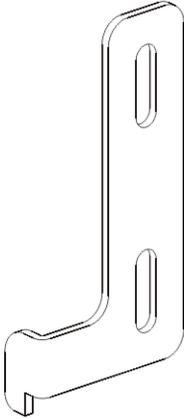
Component	Description	Quantity
	Rack shelf, right – Secures the modules in the rack	1

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 rack-mount 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 rack-mount kit. Different racks require different rack-mount parts. Although the rack-mount 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 rack-mount shelves.

Consider installing the shelves at a height that puts the base of the 5U Library Control Module anywhere between the 28U-32U alignment markers, which is usually a comfortable height for reading the operator panel. Remember, the 5U Library Control Module can be placed anywhere within the library configuration above, below, or between any 9U Library Expansion Modules. However, for recommended configuration, see [Installing a New Multi-Module Library Configuration](#) on page 246.

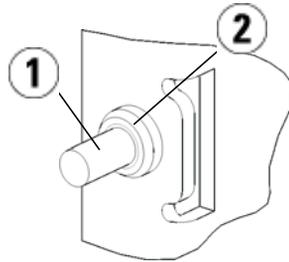
Installing the Rack-mount Shelves

Required parts: Rack-mount shelves, (8) ferrules, (8) thumbnuts

- 1 If the rack-mount 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.

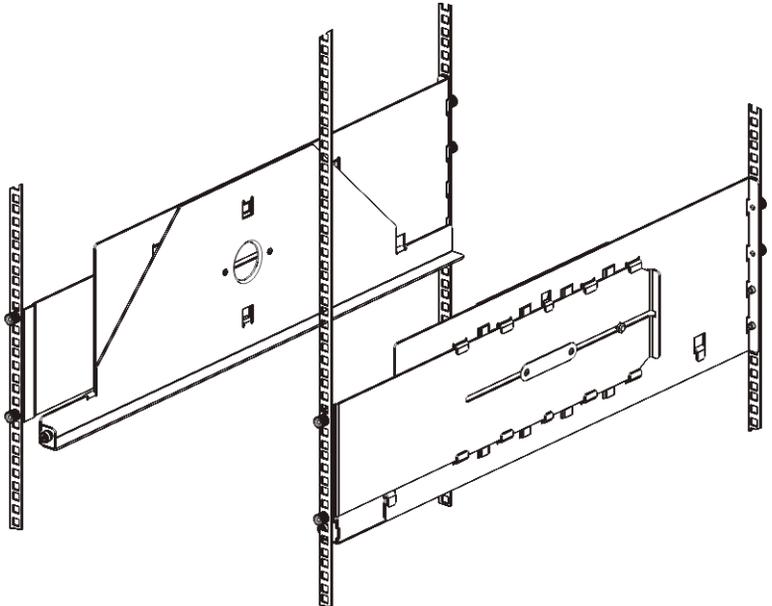
Note: Extending the shelves can be difficult, but they are designed to be resized by hand. Do not use tools to resize the shelves, and never take them apart.

- 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 334.



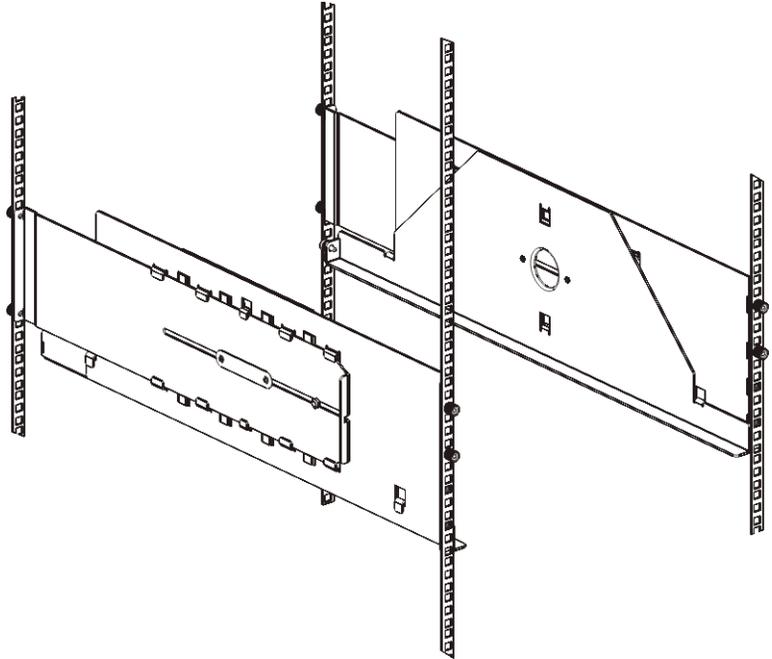
-
- 1 Stud
 - 2 Ferrule
-

- 3 Install the rack-mount shelves into the rack so that they are level with one another.
 - a Install the shelf's rear studs in the rack's rear mounting holes.



- b Position the shelf to the appropriate side of the rack (right or left) and align the shelf at the desired height.
 - c Insert the shelf's rear studs into the rack's rear mounting holes.

- d Fasten a thumbnut to the end of each stud. Secure the rack tightly, so that the ferrule fits snugly within the hole in the rack.
- e Next, install the shelf's front studs in the rack's front mounting holes.



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

Note: Extending the shelves can be difficult, but they are designed to be resized by hand. Do not use tools to resize the shelves, and never take them apart.

- g Insert the shelf's front studs into the rack's front mounting holes.
- h Fasten a thumbnut to the end of each stud. Secure the rack tightly, so that the ferrule fits snugly within the hole in the rack.

- 4 Visually make sure that both shelves are level, and that they are aligned properly within the rack.
- 5 Make sure that all thumbnuts are fastened tightly. Some thumbnuts may have loosened during installation.

Preparing Modules for Rack Installation

- 1 Power off your library and disconnect all power cords, network data cables, and module-to-module cables.
- 2 Remove all tape cartridges, tape drives, power supplies, and all cords and cables from the library modules. The modules are much easier to lift into the rack without the additional weight of the tape drives.

Warning: Without tape drives, tape cartridges, or power supplies, a 5U Library Control Module weighs approximately 60 lbs (27.2 kg). A 9U Library Expansion Module, without tape drives, tape cartridges, or power supplies, exceeds 65 lbs (29.5 kg).

To avoid serious injury, at least two people are required to safely lift the modules.

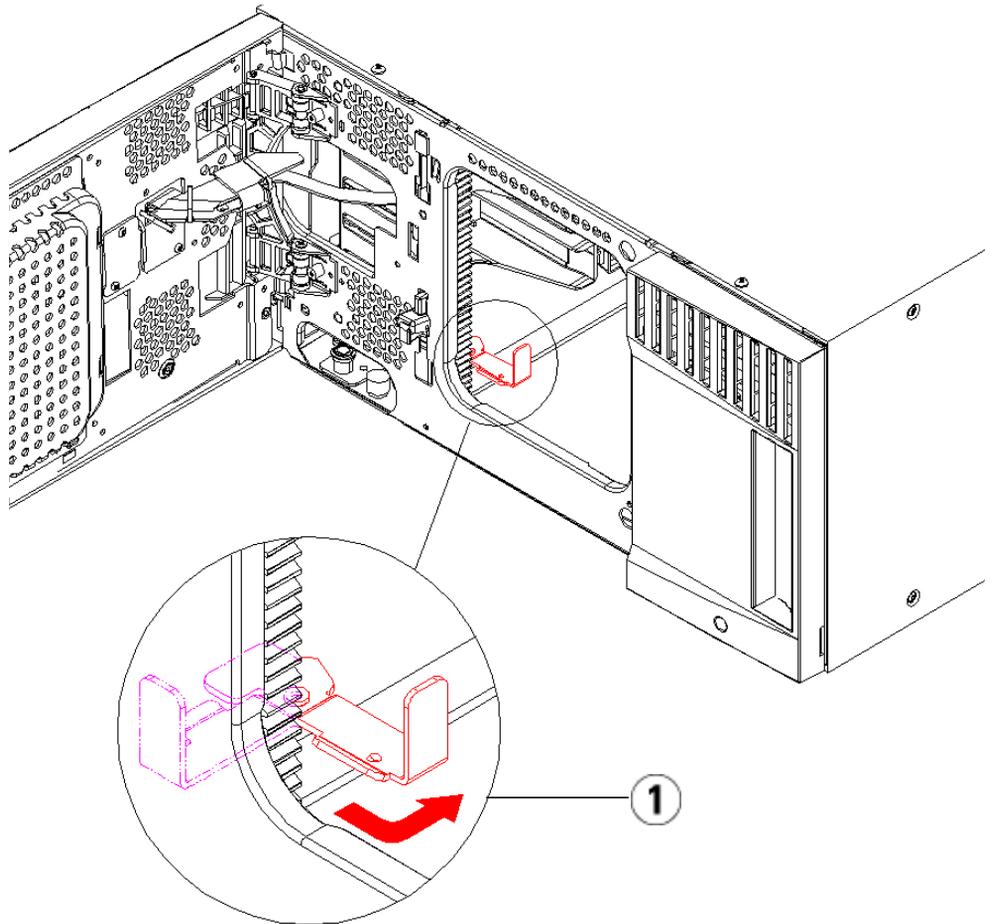
- 3 Park the robot assembly in the 5U Library Control Module. (Regardless of which module you are installing, the robot must be parked in the 5U Library Control Module before you begin moving the modules into the rack.)
 - a Open the I/E station and access doors of each module.
 - b Using your hands, gently lift the robot assembly into the 5U Library Control Module. The robot assembly should glide slowly and with some resistance.

Caution: Support the robot assembly by holding onto the broad metal X-axis plate. Lifting the robot by the thin metal rod will bend the rod. Lifting the robot by the black plastic picker body can damage the robot.

- c After raising the robot assembly to the approximate middle of the 5U Library Control Module, hold it in place with one hand and, using your other hand, move the parking tab in a counter-

clockwise direction until it stops in the “parked” position. The metal parking tab is located at the bottom of column 1.

- d Gently lower the robot assembly to rest on the parking tab.



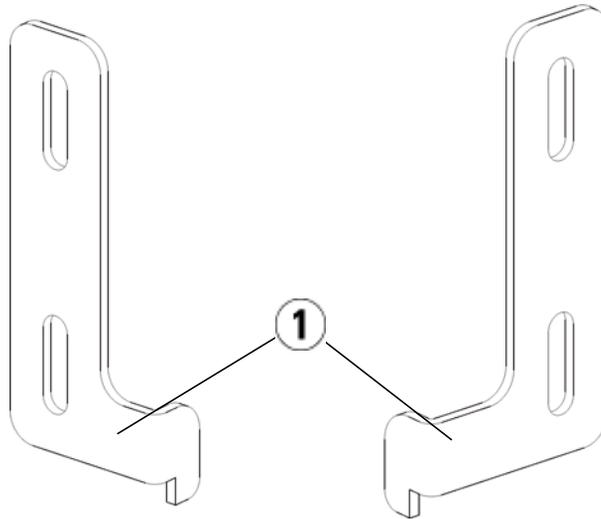
1 Parking tab in “parked” position

Installing the Bottom Module in the Rack

Required parts: Rack ears, (4) M5 thumbscrews

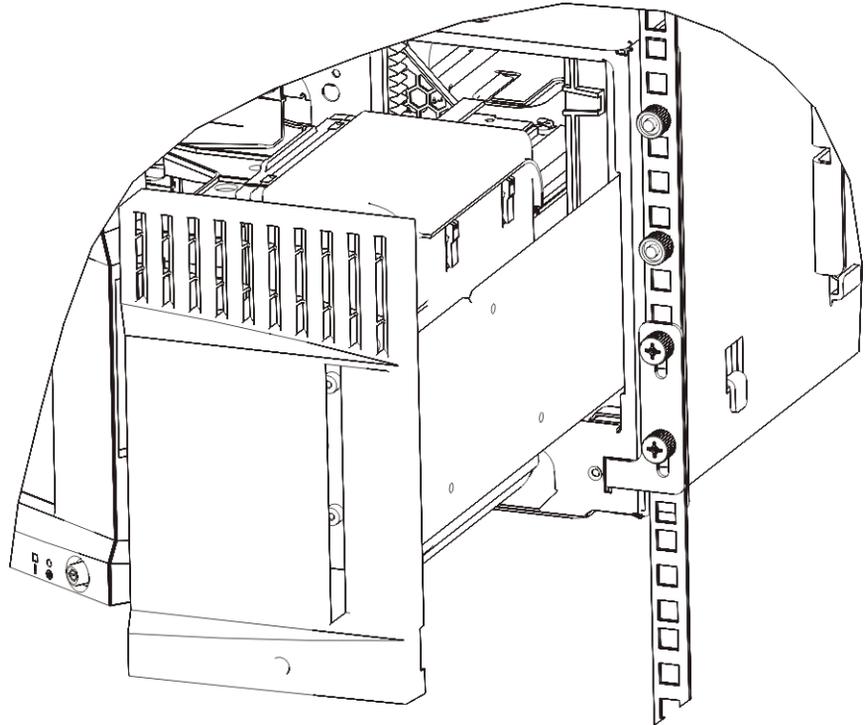
Explanation of parts: Each rack ear contains two elongated holes, enabling you to fasten it to the rack (using the M5 thumbscrews) in the most accessible mounting holes.

- 1 Place the desired module (whichever module you want to be the bottom module of the library) onto the rack-mount shelves. From the front of the rack, lift the module onto the shelf and gently slide it into the rack. Slide the module to the back of the rack, so that the front of the module is flush with the mounting holes.
- 2 From the back of the rack, secure the module to the rack-mount shelves by tightening the two silver thumbscrews that are attached to the rear of the rack-mount shelves.
- 3 Install the right rack ear. At the front of the library:
 - a Open the I/E station door. At the lower right corner of the module is a vertical slot. Insert the hinge of the right rack ear into the slot and then position the holes of the rack ear flush with the rack rail.



1 Hinge of rack ears

- b** Using two M5 thumbscrews, fasten the rack ear to the rack. The thumbscrews should thread through the holes in the rack shelves and fasten completely and evenly.

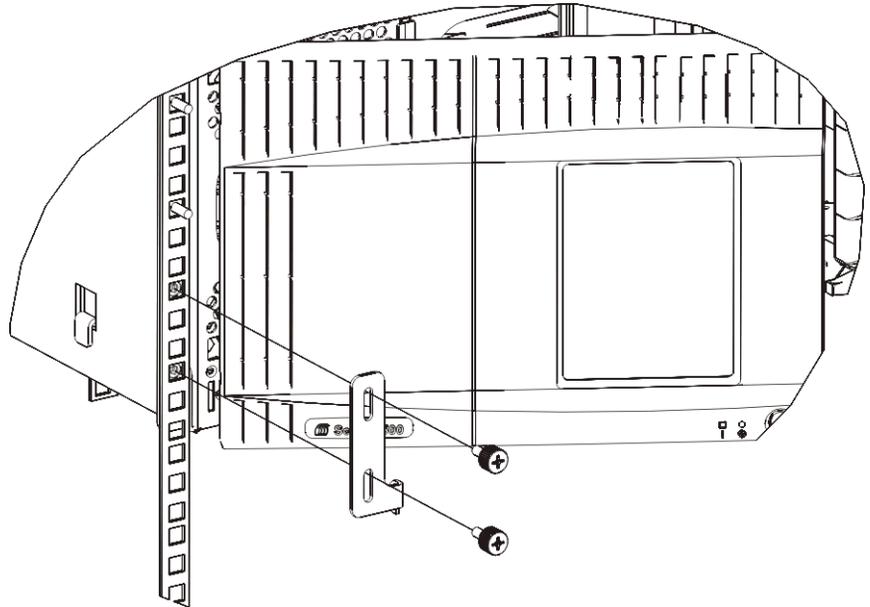


4 Install the left rack ear.

- a** With the I/E station door open, open the left door (the access door) of the module and locate the slot in the lower left corner of the module. (The flexible door hinge allows the door to be pulled away from the module, providing access to the slot.)

Note: You may need to pull the door toward you in order to access the slot.

- b** Install the left rack ear in the same manner as the right rack ear.
- c** Using two M5 thumbscrews, fasten the rack ear to the rack. The thumbscrews should thread through the holes in the rack shelves and fasten completely and evenly.



- 5** If you are only installing one module (a control module5U Library Control Module), unpark the robot assembly now. For instructions, see step 1 on page 256. If you are installing more modules, proceed to the next step and do not unpark the robot assembly yet.
- 6** Close the module's doors.
- 7** Install the remaining modules of your library (if any), following the instructions in [Installing Additional Modules Into the Rack](#) on page 347.
- 8** Reinstall the tape drives, power supplies, and tape cartridges in the library.
- 9** Cable your library as necessary, following the instructions provided in [Cabling the Library](#) on page 212.
- 10** Power on the library.

Installing Additional Modules Into the Rack

All modules that you add to the rack must be positioned above the module that you previously installed, since the bottom module must be secured to the rack-mount 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 268.
- 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 9U Library Expansion Module, count nine full units from the location of the 9U Library 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 9U Library 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 5U Library 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 5U Library 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 5U Library Control Module, count five full units from the location of the 5U Library 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 5U Library 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 5U Library 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 5U Library 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.)

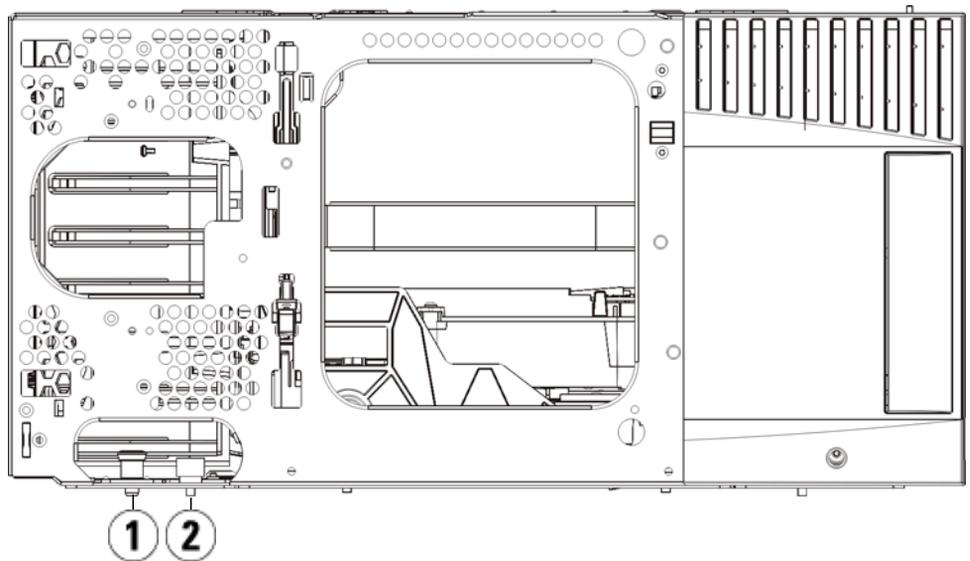
Installing cage nuts:

- 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.

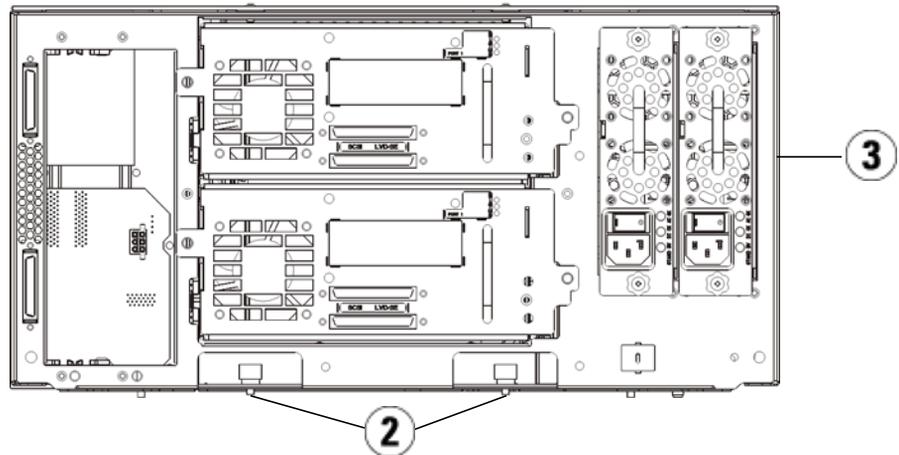
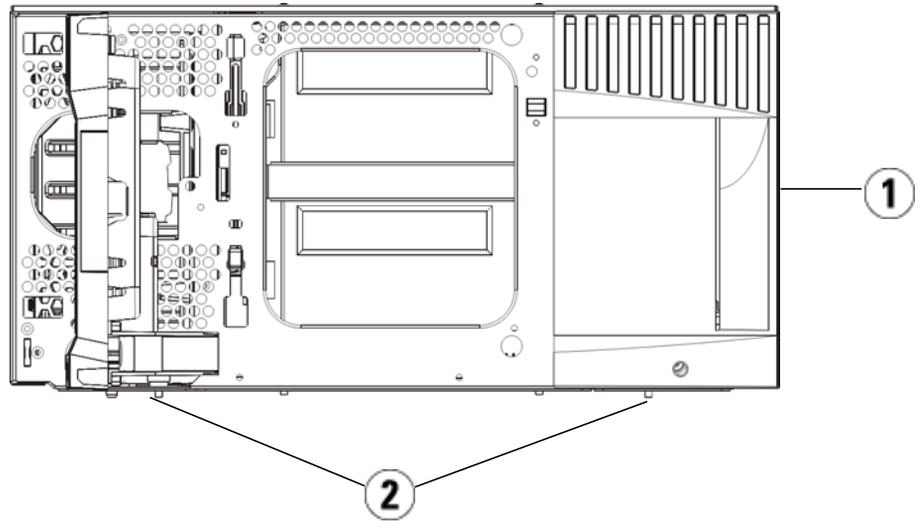
- a** Power off the module and disconnect all power cords, network data cables, and module-to-module cables.

- 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.



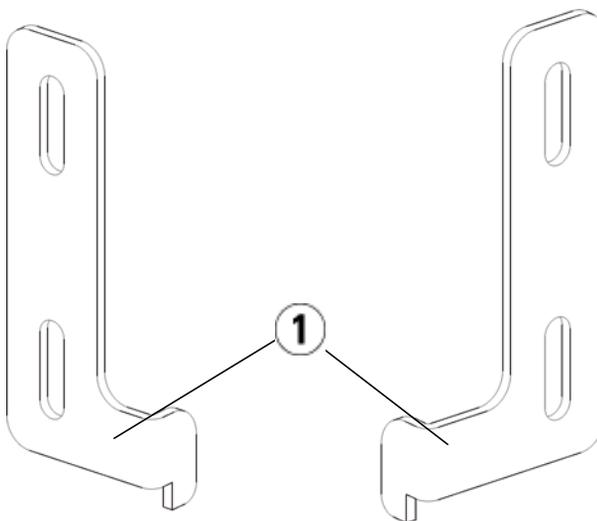
-
- 1 Guide pin
 - 2 Thumbscrew
-

- 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.



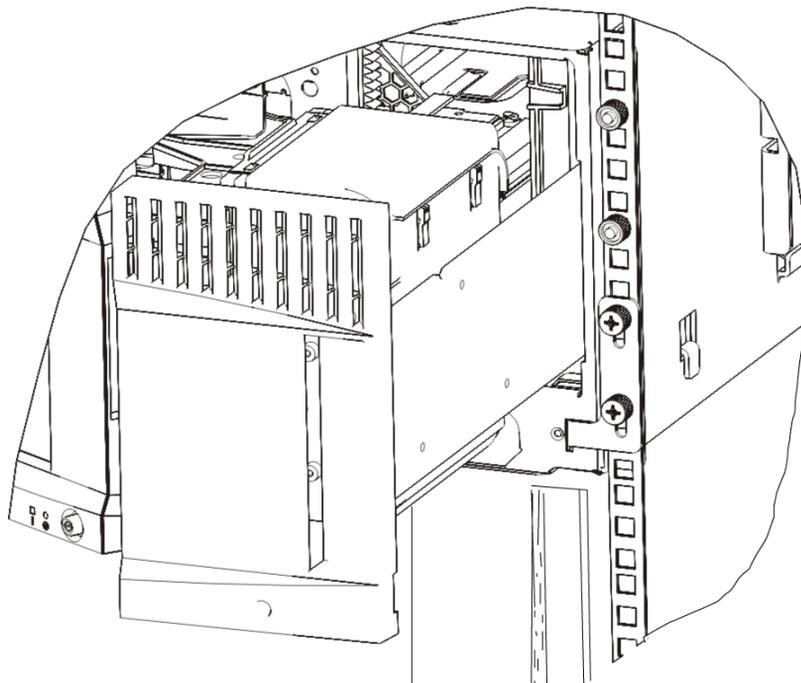
-
- 1 5U Library Control Module (front)
 - 2 Thumbscrews
 - 3 5U Library Control Module (rear)
-

- 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.

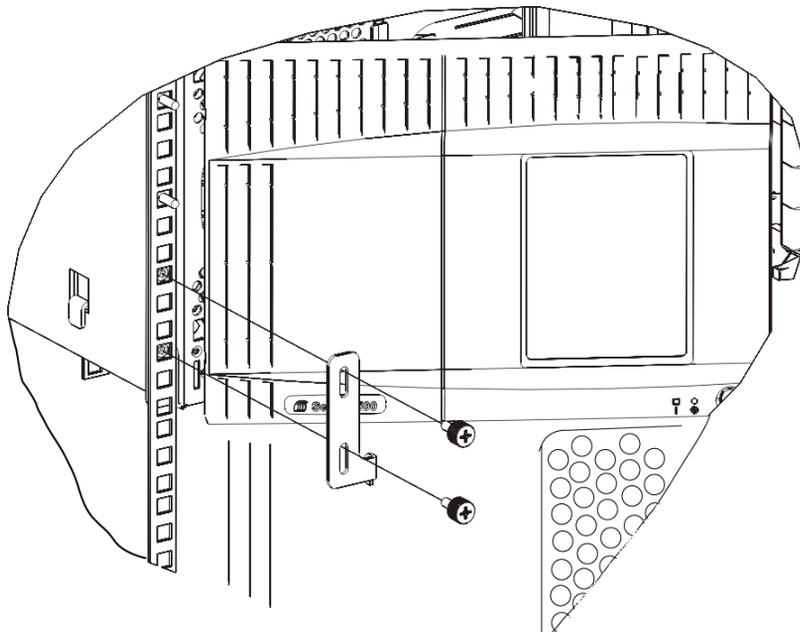


9 Install the left rack ear.

- 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 [Cabling the Library](#) on page 212.
- 13** Power on the library.

Adding, Removing, and Replacing Tape Drives

The tape drive always resides in a universal drive sled (UDS), and together they are effectively one unit. If you order a new or replacement tape drive, it will already be installed in a sled.

Note: If you are installing multiple tape drives with the library powered on, follow the special instructions in the note in [Step 3](#) below.

Adding a Tape Drive

These instructions explain how to add a tape drive to your library. You can add a tape drive while the library is powered on.

Required tools: None

- 1 Save the library configuration (see [Saving the Library Configuration](#) on page 385).
- 2 Detach the tape drive slot's cover plate. Loosen the cover plate's thumbscrews and remove the plate.

Store the cover plate in a separate cabinet. If you later decide to remove the tape drive, you will need to reinstall the cover plate.

- 3 Insert the tape drive into the drive slot. Using the guide rails on both the tape drive and in the tape drive slot, slowly slide the tape drive into the slot. The tape drive must be level to slide in smoothly.

Note: Special Instructions for Installing Multiple Tape Drives:

If you are installing multiple tape drives with the library powered on, do not push the drive in all the way yet. Instead, push it in almost all the way, leaving it out approximately 3 inches so that it does not connect with the library's backplane. Then partially insert all of the other new tape drives in the same manner. When all the new tape drives are partially inserted, push them all the way in at the same time.

- 4 Tighten the tape drive's thumbscrews to secure the tape drive to the module.

The thumbscrews must be aligned with the module's screw holes. If they are not aligned, the tape drive was not inserted correctly.

- 5 Power on the library (if it is not powered on already).
- 6 If the green LED is solidly lit for three seconds and then blinks twice, wait 10-15 minutes while the universal drive sled (UDS) firmware upgrades.

There are two types of firmware related to the tape drive: firmware for the tape drive itself, and firmware for the UDS that surrounds the tape drive. The UDS firmware is part of the library firmware. The library automatically upgrades the UDS firmware if the firmware on the newly inserted UDS is different than the library's current UDS firmware. Firmware downloads may take about 15 minutes.

- 7 Connect the host interface cables to the tape drive.
- 8 Take the tape drive online.
 - a From the **Operations** menu, select **Drive > Change Mode**.
The **Change Drive Mode** screen appears.
 - b Locate the tape drive that you want to take online.
 - c In the **New** column, click **Offline** to change the button status to **Online**.
- 9 Check the tape drive's LEDs to make sure that the drive functions correctly (see [Tape Drive LEDs](#) on page 400. If the blue or amber LED stays on solid, reseal the tape drive.
- 10 Add the new tape drive to an appropriate partition. You cannot use the tape drive until it is assigned to a partition.
- 11 If necessary, upgrade tape drive firmware by following the instructions provided in [Updating Library and Tape Drive Firmware](#) on page 199. The library can use the tape drive immediately after the firmware is upgraded.
- 12 Due to the way the library logically addresses its tape drives internally (see [Understanding Logical Element Addressing](#) on page 38), adding a tape drive to the library may change the tape drive ordering, and this can affect proper communication to a controlling host. Because of this, you must refresh the configuration of any backup application that manages the library to reflect the adjusted

tape drive positions and the presence of the new drive. In addition, you may need to reboot the host server(s) or rescan the bus to detect the changes.

Permanently Removing a Tape Drive

These instructions explain how to remove a tape drive that you do not intend to replace with another one. You may want to permanently remove a tape drive from your library if you are decreasing the size of your SAN or reducing the number of partitions in your library.

You can remove a tape drive while the library is powered on. Do not, however, remove a tape drive that is currently in use.

Required tools: None

- 1 Prepare host applications for tape drive removal.
- 2 Save the library configuration.
- 3 If there is a tape cartridge in the target tape drive, use the Web client to unload it.
- 4 Using the Web client, delete the partition that uses the target tape drive. Then re-create the partition, if desired, using another tape drive.
- 5 Disconnect the host interface cables from the tape drive that you want to remove.
- 6 From the back of the library, loosen the tape drive's thumbscrews.
- 7 Remove the tape drive by gripping the tape drive handle and pulling the entire tape drive toward you.
- 8 Install a cover plate over the vacant tape drive slot.

If you cannot find a cover plate, order one. It is important that all vacant slots have a cover plate to keep unwanted materials out of the library.

Warning: Running the library without a cover plate can be dangerous. Doing so also causes the library to run at a reduced speed.

- 9 Due to the way the library logically addresses its tape drives internally (see [Understanding Logical Element Addressing](#) on page 38), permanently removing a tape drive from the library may

change the tape drive ordering, and this can affect proper communication to a controlling host. Because of this, you must refresh the configuration of any backup application that manages the library to reflect the adjusted tape drive positions and the presence of the new drive. In addition, you may need to reboot the host server(s) or rescan the bus to detect the changes.

Removing and Replacing a Tape Drive

These instructions explain how to remove a tape drive and replace it with a new one. You may need to replace a tape drive if you are experiencing problems with one that is currently in use.

You can remove a tape drive while the library is powered on. Do not, however, remove a tape drive that is currently in use.

The new tape drive replaces the old tape drive in the partition. You do not need to delete the old tape drive or add the new tape drive to the partition, unless the replacement tape drive is of a different type (generation or interface) than the original. If the original tape drive is in a partition, and the replacement tape drive is of a different type, the library generates a RAS ticket will not activate the tape drive. If this happens, you must either replace the tape drive with one of the same type, or delete the old tape drive from the partition and then add the new tape drive to the partition (see [Modifying Partitions](#) on page 75).

Required tools: None

- 1 Prepare host applications for tape drive removal.
- 2 Save the library configuration.
- 3 If there is a cartridge in the tape drive, use the Web client to unload it.
- 4 Using the Web client, take the tape drive offline. When the tape drive is ready for removal, its blue LED will be solidly lit.
 - a From the **Operations** menu, select **Drive > Change Mode**.
The **Change Drive Mode** screen appears.
 - b Locate the tape drive that you want to take offline.
 - c In the **New** column, click **Online** to change the mode to **Offline**.
- 5 Disconnect the host interface cables from the tape drive that you want to remove.
- 6 From the back of the library, loosen the tape drive's thumbscrews.

- 7 Remove the tape drive by gripping the tape drive handle and pulling the entire tape drive toward you.
- 8 Add the new tape drive in the vacant slot. Using the guide rails on both the tape drive and the tape drive slot, slowly slide the tape drive into the slot. The tape drive must be level to slide in smoothly.
- 9 Tighten the tape drive's thumbscrews to secure the tape drive to the module.

The thumbscrews must be aligned with the module's screw holes. If they are not aligned, the tape drive was not inserted correctly.

- 10 Power on the library (if it is not powered on already) and wait for initialization to complete.
- 11 If the green LED is solidly lit for three seconds and then blinks twice, wait 10-15 minutes while the universal drive sled (UDS) firmware upgrades.

There are two types of firmware related to the tape drive: firmware for the tape drive itself, and firmware for the UDS that surrounds the tape drive. The UDS firmware is part of the library firmware. The library automatically upgrades the UDS firmware if the firmware on the newly inserted UDS is different than the library's current UDS firmware. Firmware downloads may take about 15 minutes.

- 12 Connect the host interface cables to the tape drive.
- 13 Take the tape drive online.
 - a From the **Operations** menu, select **Drive > Change Mode**.
The **Change Drive Mode** screen appears.
 - b Locate the tape drive that you want to take online.
 - c In the **New** column, click **Offline** to change the mode to **Online**.
- 14 Check the tape drive's LEDs to make sure that the drive functions correctly (see [Tape Drive LEDs](#) on page 400. If the blue or amber LED stays on solid, reseal the tape drive.
- 15 If necessary, upgrade tape drive firmware by following the instructions provided in the [Updating Library and Tape Drive Firmware](#) on page 199. The library can use the tape drive immediately after the tape drive firmware is upgraded.
- 16 When swapping out a tape drive, if the **Logical SN Addressing** feature is enabled, the library reports a logical tape drive serial number to the host that remains with the slot, so a replacement tape drive in the

same slot reports the same logical serial number and the host recognizes it immediately (see [Tape Drive Logical SN Addressing](#) on page 127). If **Logical SN Addressing** is disabled, the library reports the actual tape drive serial number to the host, so a swapped tape drive will not be registered by the host unless you refresh the configuration of any backup application that manages the library. In addition, you may need to reboot the host server(s) or rescan the bus to detect the changes.

Adding, Removing, and Replacing FC I/O Blades

This section describes adding, removing, and replacing FC I/O blades. The FC I/O blades support connections to LTO-3, LTO-4, LTO-5 and LTO-6 FC drives.

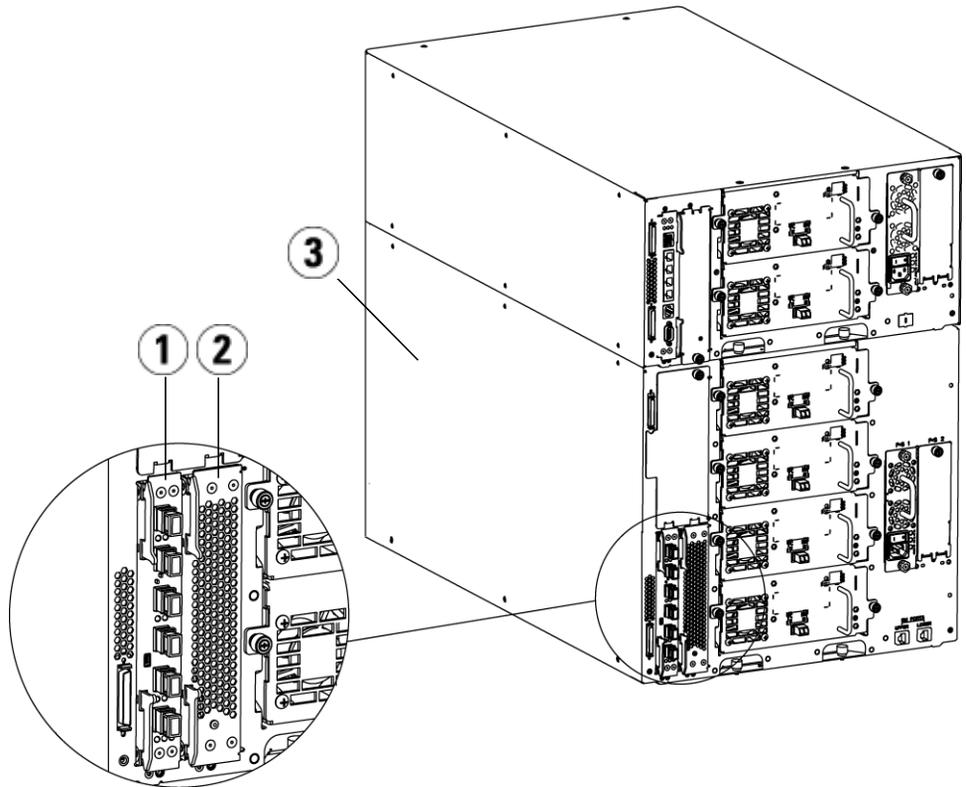
Caution: If you are adding a new FC I/O blade or completely removing an FC I/O blade, be sure to read [Working With Control Paths](#) on page 86. If you do not configure control paths correctly, you will experience communication problems with tape drives and media changer devices (partitions).

Details about FC I/O blades include:

- You must be running 400-level code or above in order to use FC I/O blades.
- Each 9U Library 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 5U Library Control Modules. However, FC tape drives in the 5U Library Control Module can be connected to FC I/O blades in a 9U Library Expansion Module.

- Each FC I/O blade is accompanied by a fan blade that cools the FC I/O blade. The fan blade is installed to the right of the FC I/O blade in the 9U Library Expansion Module. Each 9U Library Expansion Module has four bays and can accommodate two FC I/O blades and two fan blades. [Figure 40](#) shows the FC I/O blade and fan blade installed in the 9U Library Expansion Module. For instructions on installing the fan blade, see [Adding, Removing, and Replacing the FC I/O Fan Blade](#) on page 370.
- The recommended order of installing the FC I/O blade and fan blade in any 9U Library Expansion Module is starting from the bottom two bays and moving up.

Figure 40 FC I/O Blade and
Fan Blade Bays in a 9U Library
Expansion Module



-
- 1 FC I/O blade
 - 2 Fan blade
 - 3 9U Library Expansion module
-

**Read This First:
Complete Installation
Steps**

When installing an FC I/O blade, you must follow the installation steps in this order or communication with the FC I/O blade and tape drives in the library will not work properly.

Caution: If you are adding a new FC I/O blade or completely removing an FC I/O blade, be sure to read [Working With Control Paths](#) on page 86. If you do not configure control paths correctly, you will experience communication problems with tape drives and media changer devices (partitions).

You may perform the following steps with the library powered on.

- 1 Ensure you are running 400-level firmware or above.
- 2 Save the library configuration (see [Saving the Library Configuration](#) on page 385).
- 3 Connect the Ethernet cable from the Library Control Blade to the 9U Library Expansion Module(s). For each FC I/O blade installed in a 9U Library Expansion Module, connect the 9U Library Expansion Module containing the FC I/O blade(s) to a port in the Ethernet hub on the LCB (see [Figure 29](#) on page 231).

Caution: If the Ethernet cable between the LCB and the 9U Library 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 9U Library Expansion Module, connect one end of an Ethernet cable to the Ethernet port labeled **LOWER** in the lower right corner of the 9U Library 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 9U Library Expansion Module, connect one end of an Ethernet cable to the Ethernet port labeled **UPPER** in the lower right corner of the 9U Library 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 FC I/O Fan Blade](#) on page 370. The fan blade is required to prevent overheating of the FC I/O blade.
- 6 Add or replace the FC I/O blade(s) following the instructions in [Adding an FC I/O Blade](#) on page 364 or [Replacing an FC I/O Blade](#) on page 369. 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 9U Library Expansion Module.
- 8 Connect the library and tape drive cables to the FC I/O blade (see [Figure 29](#) on page 231). See also [Recommended Library Cabling for FC I/O Blades](#) on page 234.
- 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 86 for more important information about control paths. To modify the control path, select **Setup > Control Path** from the operator panel or Web client.
- 11 Configure host mapping (optional). If you have more than one FC I/O blade in the library, each FC I/O blade will present each partition that does not have a tape drive as the control path as a target

device to the host. Thus the host may see the same partition multiple times. To minimize confusion, you should configure host mapping so that each host sees each device only once. For more information, see the [Host Mapping - Overview](#) on page 116 and [Configuring Host Mapping](#) on page 118. To configure host mapping:

- a From the operator panel or Web client, select **Setup > FC I/O Blades > FC I/O Blade Control** and enable host mapping.
 - b From the operator panel or Web client, select **Setup > FC I/O Blades > Host Mapping**.
- 12** Configure host port failover on the FC I/O blade (optional). From the Web client, select **Setup > FC I/O Blades > Host Port Failover**. To enable host port failover, you must configure target ports 1 and 2 on the FC I/O blade as point-to-point connections (**Setup > FC I/O Blades > Port Configuration**). For more information, see [Configuring FC Host Port Failover](#) on page 119.
- 13** Save the library configuration (see [Saving the Library Configuration](#) on page 385).

Adding an FC I/O Blade

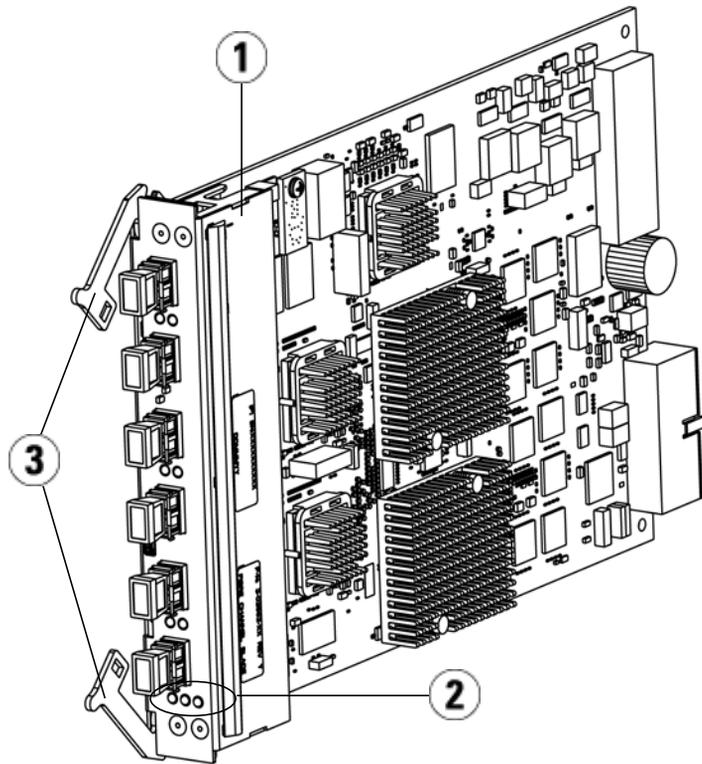
These instructions explain how to add an FC I/O blade to your library. You can add an FC I/O blade while the library is powered on.

Required tools: None

- 1 Access the back of the 9U Library Expansion Module.

Note: The recommended order of installing the FC I/O blade and fan blade in a 9U Library Expansion Module is starting from the bottom bay and moving up.

- 2 Remove the cover plate from the appropriate bay.
- 3 Press up and out to open the latch hooks on each side of the FC I/O blade.



-
- 1 FC I/O blade
 - 2 LEDs
 - 3 Latch hooks, open
-

- 4 Carefully align the FC I/O blade with the guide slots in the bay. The status LEDs must be at the bottom.

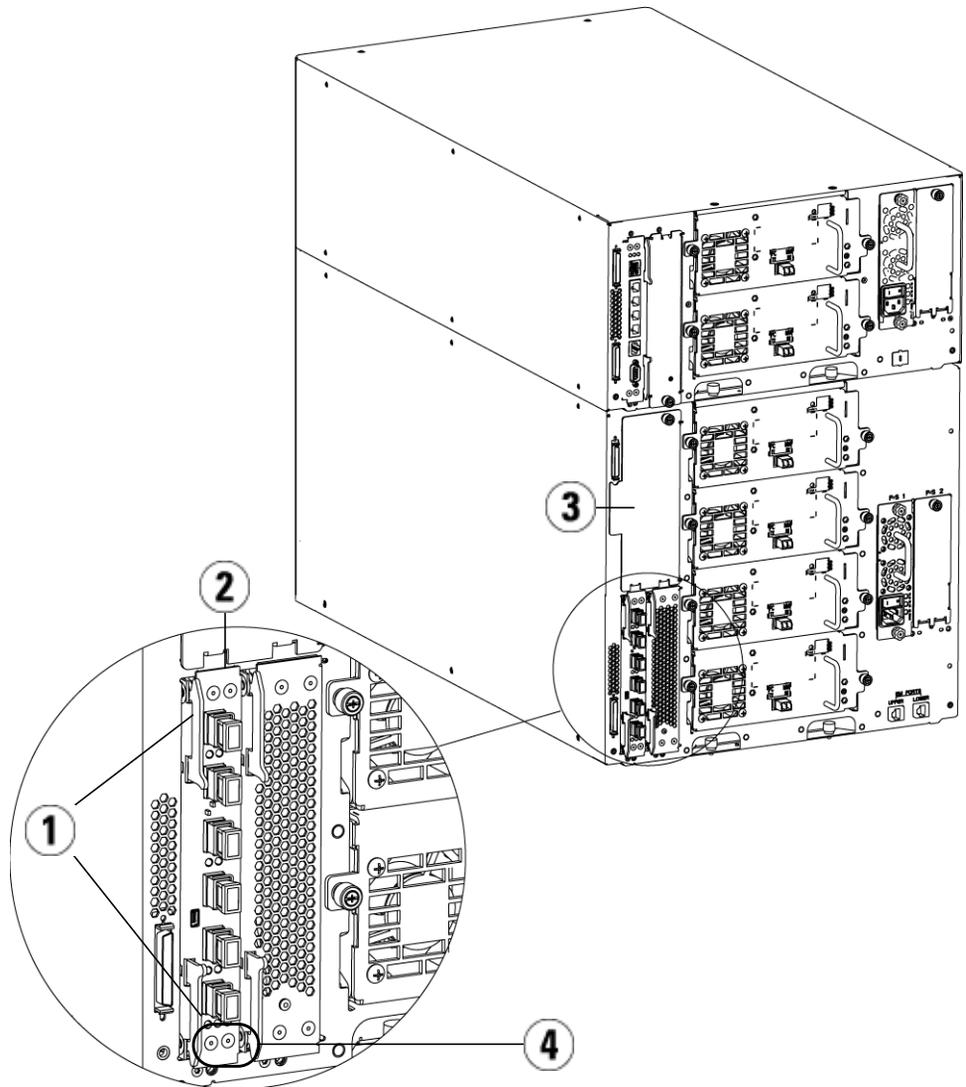
Caution: Forcing the blade into the bay can cause the pins to bend.

- 5 Evenly apply pressure to both sides of the blade and slide it into the 9U Library Expansion Module until the latch hooks begin to move toward the middle of the blade. Push the latch hooks toward the

middle of the blade and into the locked position. You will feel the blade pins connect with the 9U Library 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 9U Library 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 [Cabling Libraries With Fibre Channel Tape Drives Connected to Fibre Channel I/O Blades](#) on page 228.
- 9 Save the library configuration (see [Saving the Library Configuration](#) on page 385).

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 187.

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 393).
- 8 Save the library configuration (see [Saving the Library Configuration](#) on page 385).

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 187.

Required tools: None

- 1 Access the back of the 9U Library 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 368.
- 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 9U Library 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 9U Library 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 385).

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 [Blade Status LEDs](#) on page 396.

Adding, Removing, and Replacing the FC I/O Fan Blade

Each FC I/O blade is cooled by a fan blade. The fan blade is always installed in the bay to the right of the FC I/O blade. Each 9U Library 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 9U Library Expansion Module is starting from the bottom two bays and moving up.

[Figure 40](#) on page 361 shows the FC I/O blade and I/O fan blade installed side-by-side in the 9U Library Expansion Module.

Adding an FC I/O Fan Blade

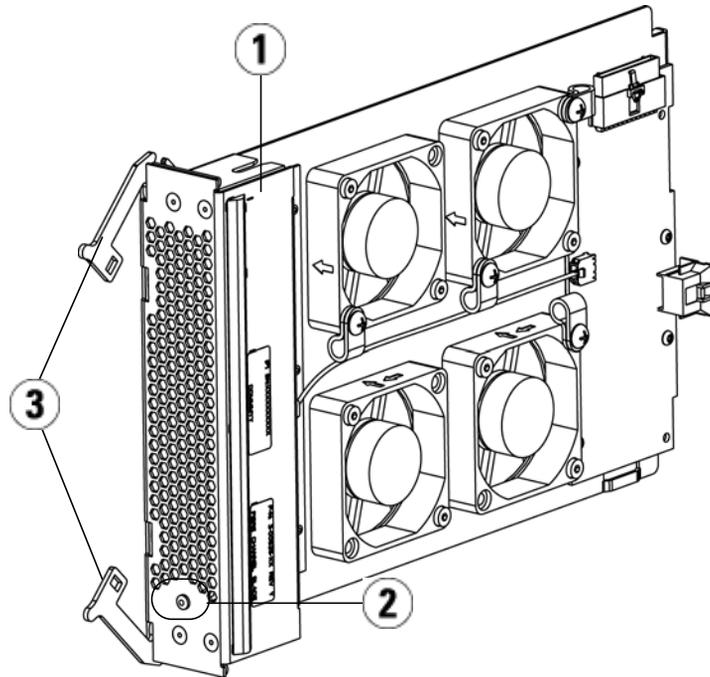
These instructions explain how to add an FC I/O fan blade to your library. You can add an FC I/O fan blade while the library is powered on.

Required tools: None

- 1 Access the back of the 9U Library 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 a 9U Library Expansion Module is starting from the bottom two bays and moving up.

- 3 Press up and out to open the latch hooks on each side of the FC I/O fan blade. The LED must be at the bottom of the blade.



-
- 1 Fan blade
 - 2 LED
 - 3 Latch hooks, open
-

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

- 4 Evenly apply pressure to both sides of the fan blade and slide it into the expansion module until the latch hooks begin to move towards the middle of the blade. Push the latch hooks towards the middle of the blade and into the locked position. You will feel the blade pins connect with the 9U Library Expansion Module's backplane as the blade locks into place.

Note: The LED for the FC I/O fan blade is on the bottom of the blade when the blade is correctly installed in the 9U Library Expansion Module.

- 5 Save the library configuration (see [Saving the Library Configuration](#) on page 385).

Removing an FC I/O Fan Blade

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

Caution: Do not permanently remove an FC I/O fan blade unless you also permanently remove the FC I/O blade to which it is associated.

Required tools: None

- 1 Access the back of the expansion module containing the FC I/O fan blade.
- 2 Lift the latch hooks out of the locked position and push them up. You will feel the FC I/O fan blade unplug from the expansion module's backplane.
- 3 Continue lifting on the latch hooks until the blade is totally unplugged from the backplane.
- 4 Slide the FC I/O fan blade out of the expansion module.
- 5 If you are permanently removing the FC I/O fan blade, place a cover on the empty bay.
- 6 Save the library configuration (see [Saving the Library Configuration](#) on page 385).

Replacing an FC I/O Fan Blade

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

Required tools: None

- 1 Access the back of the 9U Library Expansion Module.
- 2 If you have not already done so, remove the old I/O fan blade, following the directions in [Removing an FC I/O Fan Blade](#) on page 373.
- 3 Press up and out to open the latch hooks on each side of the replacement I/O fan blade.
- 4 Carefully align the FC I/O fan blade with the guide slots in the bay. The status LED must be at the bottom.

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

- 5 Evenly apply pressure to both ends of the FC I/O fan blade and slide it into the 9U Library 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 9U Library Expansion Module's backplane.
- 6 Push the latch hooks into the locked position.
- 7 Save the library configuration (see [Saving the Library Configuration](#) on page 385).

Preparing the Library for Moving or Shipping

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

Caution: When moving the library: Manufacturer-supplied packaging, whether original or purchased, is required for complete or partial de-installations. You must install the orange robot restraint assembly to protect the robot against damage. Use the original shipping carton and packaging materials to further protect your library equipment during transport.

Caution: When shipping the library: Use the shipping carton, packaging materials, and the orange robot restraint assembly that originally came with the library. This will help protect your library against damage.

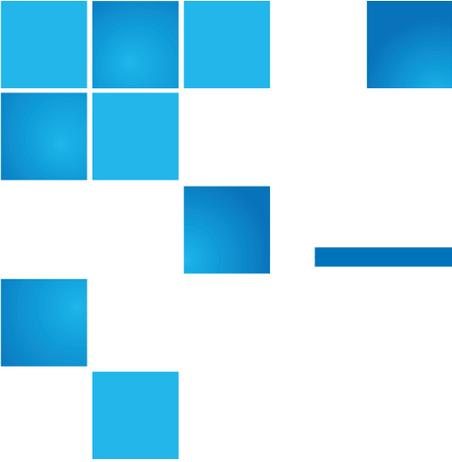
- 1 Save the library configuration (see [Saving the Library Configuration](#) on page 385).
- 2 Shut down the library using the local operator panel (**Operations > System Shutdown**). This lowers the robot to the “shipping” position on the floor of the library.
- 3 Follow instructions on the operator 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 5U Library Control Module weighs approximately 60 lbs (27.2 kg). A 9U Library Expansion Module, without tape drives, tape cartridges, or power supplies, exceeds 65 lbs (29.5 kg).

To avoid serious injury, at least two people are required to safely lift the modules.

- 10 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*.



Chapter 13 Troubleshooting

The PowerVault ML6000 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 PowerVault ML6000 library uses advanced problem detection, reporting, and notification technology to alert you of problems as soon as they occur. The library performs numerous self-tests to monitor the library's temperature, voltage and currents, and standard library operations. It performs these self-tests each time the library is powered on and during normal operation when the library is idle.

If the self-test detects a problem, the library generates a Reliability, Availability, and Serviceability (RAS) ticket that identifies the component that is likely causing the problem. The library's light emitting diodes (LEDs) may also turn on or off and flash to indicate an abnormal state. If the problem is not severe, the library continues to provide full functionality to all unaffected partitions.

RAS tickets have three severity levels:

- Severity 3 – Low severity/informational message. Indicates that an abnormal condition exists within the library that warrants investigation and correction but the nature of the condition may have little or no effect on operations.
- Severity 2 – High severity/warning message. Indicates that a condition exists within the library that impacts system performance, redundancy, or a specific host application. Typical library operations can continue without immediate corrective action, although an application may have failed and may need to be restarted. A user should investigate the condition and correct the problem soon.
- Severity 1 – Urgent severity/critical issue. Indicates that a failure has occurred or a serious condition exists within the library that requires immediate corrective action. In most cases, a hardware component is no longer functioning at an acceptable level or has failed. Typical library operations required for backup or restore operations are either not possible or are highly unreliable.

When possible, the RAS ticket provides instructions for resolving problems. You can view RAS tickets on both the operator panel and the Web client. Access the library's online Help system if you have questions about the instructions provided. To access the online Help system, click the **Help** icon at the top right of the Web client or operator panel user interface.

You can frequently resolve a simple problem yourself, but if the problem is complex or involves a field replaceable unit (FRU), you will be directed to contact service. Only qualified service technicians can service FRUs.

Caution: Do not work with RAS tickets while the library is performing an inventory. Doing so may result in inventory discrepancies, such as missing tape cartridges.

Viewing RAS Tickets

Selecting **All RAS Tickets** from the **Tools** menu on both the operator panel and the Web client opens the **All RAS Tickets** screen, which lists RAS tickets in order of last occurrence of each event, beginning with the most recent.

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

Included in the list is a brief description of the error condition captured by the RAS ticket. The **All RAS Tickets** screen allows you to view RAS ticket details and navigate to ticket resolution information.

The initial status of all RAS tickets is Unopened. Once the administrator selects the **Resolve** button on the **All RAS Tickets** screen for a ticket, its status changes to Opened. When the user closes the ticket, its status changes to Closed. You can view Opened and Unopened tickets on both the operator panel and the Web client, but you can view Closed tickets only on the Web client.

Caution: Be careful when pressing the **Close All Tickets** button. This closes all RAS tickets even if they are not resolved. It is recommended that each RAS ticket be viewed, analyzed, and closed individually.

The paths to open the appropriate screens are:

- From the Web client, select **Tools > All RAS Tickets**.
- From the operator panel, select **Tools > All RAS Tickets**.

Resolving and Closing RAS Tickets

Administrators can resolve some RAS tickets. Others must be resolved by Service personnel. Only one person at a time can resolve a ticket. Multiple users can, however, view ticket details simultaneously. If your Web client session goes down while resolving a RAS ticket, you must wait 3 minutes before you can continue resolving the RAS ticket from either the Web client or the operator panel.

- 1 Log in to the Web client.
- 2 From the **Tools** menu, select **All RAS Tickets**.
The **Tools - All RAS Tickets** screen appears.
- 3 Identify the RAS ticket you want to resolve.

Note: You can use the **Go to RAS Ticket** text box at the bottom of the screen to locate a specific RAS ticket number. In addition, if there is more than one page of RAS tickets, use the **Page 1 of x** arrows to view the additional tickets.

4 Click **Resolve**.

The **Ticket Resolution** window appears. This window contains information on how to resolve the ticket.

5 Review the description.

6 Do one of the following:

- a** To close the ticket now, click **Close**.

The **Tools - All RAS Tickets** window displays, with the RAS ticket no longer in the list. The task is complete and the RAS ticket is resolved.

- b** To leave the ticket open for future troubleshooting, click **Exit**. Then you can perform the diagnostic steps you need to resolve a related RAS ticket.

Note: To display all closed tickets, select the **Include Closed Tickets** check box at the bottom of the screen. The **Tools - All RAS Tickets** screen refreshes, with the **Resolve** button unavailable for all closed RAS tickets.

Caution: Be careful when pressing the **Close All Tickets** button. This closes all RAS tickets even if they are not resolved. It is recommended that each RAS ticket be viewed, analyzed, and closed individually.

The path to open the appropriate screen is:

- From the Web client, select **Tools > All RAS Tickets**.

Closing RAS Tickets Automatically

The library will close all currently open RAS tickets when you reboot the library. If any errors occur during the reboot, the library issues new tickets.

Automatic ticket closure will only occur when you intentionally initiate a reboot, by either restarting the library, shutting down the library, or upgrading library firmware. Automatic ticket closure will not occur if the library shuts down unexpectedly or if the power cord is unplugged.

You can always view closed tickets on the Web client by selecting **Tools > All RAS Tickets** and clicking the **Include Closed Tickets** check box. Tickets that were auto-closed are designated as “Canceled.”

Automatic ticket closure is enabled by default. You can enable or disable this feature from the operator panel.

The path to open the appropriate screen is:

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

Capturing Snapshots of Library Information

Technical support personnel may ask you to perform the Capture Snapshot operation, so they can better diagnose issues. The **Capture Snapshot** operation captures detailed information about the entire library in a single ASCII file that can be e-mailed to technical support personnel.

The logged information consists of configuration data, status information, and trace logs for library components. Trace logs collect problem data and provide support personnel with vital library information for troubleshooting and solving problems.

You can e-mail the snapshot file from both the operator panel and the Web client. On the Web client, you can also download the Capture Snapshot file to a computer. You cannot download Capture Snapshot files from the library’s operator panel, and you cannot print Capture Snapshot files from either the Web client or the operator panel.

Depending on the library configuration and your connection speed, saving the Capture Snapshot file takes approximately 30 minutes. The resulting file size can be large. Your firewall file-size limitations could prohibit you from e-mailing the file.

On the Web client, ensure that the library e-mail account is appropriately configured before you attempt to e-mail the snapshot from the library. If the library e-mail account address is not configured, an error appears. For

information on setting up the e-mail account, see [Configuring the Library E-mail Account](#) on page 92.

You can configure the library to automatically attach a library snapshot to certain RAS ticket e-mail notifications (see [Configuring the Library E-mail Account](#) on page 92). If the library is in the process of capturing an automatic snapshot, you will not be able to manually capture a snapshot via the Web client until the automatic snapshot is complete. If this happens, an error message will display. Wait about 10 minutes and try again.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Tools > Capture Snapshot**.
- From the operator panel, select **Tools > Capture Snapshot**.

Saving and E-mailing the Library Configuration Record

The library configuration record is a text file that contains details about the library's configuration. The configuration record can be saved or e-mailed to a specified e-mail address. Information in the library. The configuration record includes:

- Product information – vendor, model, product ID, product version (library firmware version), and serial number.
- Capacity on Demand (COD) license information – licensed slots and expiration date.
- Module information – vendor, module type, module serial number, and module location coordinates.
- Tape drive information:
 - SCSI tape drives – partition name, number of tape drives in partition, drive location, SCSI element address, online status, active status, ready state, vendor, model, serial number, tape drive firmware version, drive type, logical serial number, interface type, SCSI ID, and LUN.

- Fibre Channel (FC) tape drives – partition name, number of tape drives in partition, drive location, SCSI element address, online status, active status, ready state, vendor, model, serial number, tape drive firmware version, drive type, logical serial number, interface type, World Wide Node Name (WWNN) loop ID, topology, speed, and actual speed.

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

- Serial Attached SCSI (SAS) tape drives – partition name, number of tape drives in partition, drive location, SCSI element address, interface type, drive type, ready state, online status, barcode, media type, element address, vendor, model, physical serial number, logical serial number, SCSI ID, firmware level, control path status.
- I/O blade information – blade number, blade ID, location coordinates, serial number, WWNN, firmware version, and control LUN.
- Partition information – number of partitions, number of cleaning slots, number of unassigned slots, number of import/export (I/E) slots, I/E manual assignment setting, partition name, number of slots, number of tape drives, and number of cartridges.

E-mailing the Configuration Record

Administrators can use the **Tools - E-mail Configuration Record** screen on the Web client to e-mail the library configuration record.

Do not enter more than one e-mail address in the **E-mail Address** text box on the **Tools - E-mail Configuration Record** screen. If you need to send the configuration record to multiple e-mail addresses, repeat the procedure for each e-mail address.

Before you can e-mail the configuration record, the library e-mail account must be configured. For information on setting up the e-mail account, see [Configuring the Library E-mail Account](#) on page 92.

You cannot e-mail the library configuration record from the operator panel. The path to open the appropriate screen is as follows:

- From the Web client, select **Tools > E-mail Configuration Record**.

Saving the Configuration Record

Administrators can use the **Tools - Save Configuration Record** screen on the Web client to e-mail the library configuration record.

You cannot save the library configuration record from the operator panel. The path to open the appropriate screen is as follows:

- From the Web client, select **Tools > Save Configuration Record**.

Saving and Restoring the Library Configuration

The library has many configurable items, such as tape drive IDs, partitions, user accounts, Import/Export (I/E) stations, and cleaning slots. In the event of a hardware failure or firmware upgrade, the save and restore operations can be used to restore the library's firmware and configurable items to a previous state.

Note: You cannot restore a saved configuration after removing or replacing a 5U Library Control Module or 9U Library Expansion Module. After removing and/or replacing the module, save the library configuration for future use.

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

Saving the Library Configuration

Caution: Always save the library configuration after modifying a configurable item and before upgrading firmware. This allows you to restore the most current settings if necessary.

This operation saves your current library configuration and library firmware. Save your library configuration when it is in a known working state. In the event of a hardware failure, the saved configuration can be used to restore the configuration after hardware repairs are made. Before initiating a firmware upgrade, you should save the library configuration. You then have the option to restore the configuration after either a successful or an unsuccessful upgrade.

The Save/Restore Configuration operation is available only on the Web client. The path to open the appropriate screen is:

- From the Web client, select **Tools > Save/Restore Configuration**.

Restoring the Library Configuration and Library Firmware

You can restore the library's configurable items to a previous state using a saved configuration file. If you updated the library firmware since last saving the configuration, the library automatically restores the library firmware to the version that was saved with the configuration.

You can also downgrade library firmware to an earlier version using the **Tools > Update Library Firmware** command. Note that you will lose all your current library configuration information except for network settings, date and time, and license keys. You can restore the other configurable items using a configuration file that was saved when the earlier version of library firmware was installed on the library, or you can reconfigure your library's settings.

Note: The configuration file must be at the same or an earlier version of firmware than that which is currently installed on the library. You cannot restore a configuration file created with a later version of firmware.

Note: If your library is running firmware version 600G or later, you can only restore a saved configuration that was created with firmware version 410G or later. If you need to restore a configuration created with firmware that is earlier than 410G, contact Dell Technical Support (see [Appendix C, Contacting Dell](#)) for assistance.

The Configuration operation is available only on the Web client. The path to open the appropriate screen is:

- From the Web client, select **Tools > Save/Restore Configuration**.

Troubleshooting “Library Not Ready” Messages

The operator panel and Web client each include a header that contains the company logo, product name, and the three main navigation buttons **Home**, **Help**, and **Logout**. In addition, a message in the header alerts you when the library is not ready. (No message displays in the header when the library is in a ready state.)

On the operator panel, **LIBRARY NOT READY** flashes at regular intervals whenever the library robotics are not yet ready to perform library functions. To view more information about the library’s condition, select **Tools > About Library**. The **State** field on the **About Library** screen will display **Not ready**, followed, when applicable, by a brief explanation. For example, if the library door is open, the **State** field will display: **Not ready, door is open**.

The header in the Web client also alerts you when the library is not ready. For instance, if the library door is open, the header will display the following message: **Library’s door is open**.

“Library Not Ready” messages appear in the header in the operator panel and the Web client under the following circumstances:

- The robot is in the process of calibrating. When the robot has finished calibrating, the “Library Not Ready” message no longer appears.
- The robot cannot calibrate. For example, a fiducial label is missing, preventing the robot from calibrating.

- The robot requires manual intervention. For example, the picker contains a tape cartridge that it cannot unload.
- The library door is open. The robot will not operate if the door is open.
- If none of the above situations apply, but the library is still not ready to operate, the header will display a “Library Not Ready” message without additional detail. The library generates a RAS ticket whenever the library enters a “not ready” state. The RAS ticket may provide information that can help you troubleshoot the problem. See [Viewing RAS Tickets](#) on page 378 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 111).
- If more than one host is connected to a target port, you can use host mapping to tell each host which devices to see (see [Configuring Host Mapping](#) on page 118).

Duplicate Media Changer Devices Discovered

You may see one or more media changer devices (partitions) being discovered multiple times. For information on why this happens, see [FC I/O Blade Internal Virtual Port for Media Changers](#) on page 111.

To prevent this, do the following:

- Ensure that host mapping is enabled (see [Enabling/Disabling FC Host Mapping](#) on page 113).
- Assign each media changer a unique LUN and map each one to the appropriate host (see [Configuring Host Mapping](#) on page 118).

Identifying Tape Drives

You can use the operator panel and the Web client user interfaces to view information about all tape drives installed in the library. In addition, you can identify tape drives, including the control path tape drive, in selected partitions. The Web client also allows you to identify tape drives that are not assigned to specific partitions. On the Web client, you can only identify tape drives that are in a ready state.

The operator panel **Drive Information** screen lists the following information for each tape drive:

- Control path tape drive status – yes/no
- Vendor
- Model
- Type
- Serial number
- Tape drive firmware version
- Sled boot version
- Sled application version

- Mode status – online/offline, ready/not ready
- Loaded status – unloaded/loaded
- SCSI ID for SCSI tape drives
- World Wide Node Name (WWNN) for Fibre Channel (FC) tape drives
- SAS address for SAS tape drives

The Web client **Identify Drives** screen lists the following information for each tape drive:

- Location coordinates
- Mode status – online/offline
- State – ready/not ready
- Drive type
- Protocol
- Control path tape drive status – yes/no
- Vendor
- Physical serial number (P-SN)
- Logical serial number (L-SN)
- Tape drive firmware version

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

On the operator panel **Drive Information** screen, you can identify the tape drives assigned to the selected partition as well as the control path tape drive for the partition by flashing the green light-emitting diodes (LEDs) on the back of the tape drives.

- Use the **Identify All** button to flash the green LEDs on the back of the tape drives assigned to the partition. The LEDs blink 10 times per second for one minute.
- Use the **Identify Ctrl Path** button to flash the green LED on the back of the control path tape drive for the partition. The control path tape drive is used to connect each partition to the host application. Use

this button when you are cabling the library or troubleshooting the library control paths of tape drives. The green LED blinks 10 times per second for one minute.

On the Web client **Identify Drives** screen, you can identify the tape drives assigned to a particular partition, all unassigned tape drives, and the control path tape drive for each partition by flashing the green LEDs on the back of tape drives that are in a ready state:

- Use the **Identify All** button to flash the LEDs on the back of the selected tape drives. Only tape drives in a ready state will flash. If you have selected a specific partition or have only one partition configured, all the green LEDs on the tape drives within the partition will blink. If you have selected **Unassigned**, all the green LEDs on the unassigned tape drives will blink. If you have selected **All**, the green LEDs on all tape drives installed in the library will blink.
- Click **Identify Control Path** to flash the green LEDs on the back of the one or more control path tape drives. Only tape drives in a ready state will flash. The control path tape drive is used to connect each partition to the host application. Use this button when you are cabling the library or troubleshooting the library control paths of tape drives. If you have selected a partition, the green LED on the partition's control path tape drive will blink. If you have selected **All**, the green LEDs on all the ready control path tape drives will blink.

Note: There is no control path tape drive for a partition that uses FC I/O blades to connect tape drives to a host application.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Tools > Identify Drives**.
- From the operator panel, select **Tools > Drive Info**.

Retrieving Tape Drive Logs

Administrators can use the Web client to retrieve tape drive logs. Tape drive log information can be used to help troubleshoot library and tape drive issues. You can use the **Retrieve Drive Log** screen to select the appropriate tape drive.

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

Details on retrieving tape drive log files include:

- Since the log retrieval process can take up to 30 minutes, the tape drive and associated partition are automatically taken offline during the operation and brought back online when the operation completes. You will be asked to confirm that you want to take the tape drive and partition offline.

Note: If the operation does not complete successfully, the partition remains offline until you turn it back online manually or restart the library (see [Taking a Partition Online or Offline](#) on page 78).

- Tape drive logs adhere to the following naming convention: **UDS_ID_SN.dmp**, where **ID** identifies the tape drive coordinate location within the library and **SN** identifies the tape drive serial number.
- You can select the interface type (SCSI, SAS, or FC) of the tape drive from which you want to retrieve logs.

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

You cannot retrieve tape drive logs from the operator panel. The path to open the appropriate screen is as follows:

- From the Web client, select **Tools > Drive Operations**.

Retrieving Tape Drive Sled Logs

Administrators can retrieve tape drive sled logs. Tape drive sled log information can be used to help troubleshoot library, tape drive sled, and tape drive issues. You can use the **Retrieve Drive Sled Log** screen to select the appropriate tape drive sled.

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

Details on retrieving tape drive sled log files include:

- Tape drive sled logs adhere to the following naming convention: **UDS_ID_SN.LOG**, where **ID** identifies the tape drive sled coordinate location within the library and **SN** identifies the tape drive sled serial number.
- You can select the interface type (SCSI, SAS, or FC) of the tape drive sled from which you want to retrieve logs.
- A **Save** dialog allows you to specify where you want to save the tape drive sled log files file.

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

You cannot retrieve tape drive sled logs from the operator panel. The path to open the appropriate screen is as follows:

- From the Web client, select **Tools > Drive Operations**.

Identifying FC I/O Blades

Administrators can flash the green LED on a selected FC I/O blade to identify the physical location of the I/O blade in the library. After performing this blade operation, go to the back of the library and identify the I/O blade with the rapidly blinking LED at the bottom of the FC I/O blade. The LED will blink for one minute.

The paths to open the appropriate screens are as follows:

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

Permanently Removing FC I/O Blades

Library firmware monitors all FC I/O blades after they are installed in the library. Once an FC I/O blade is installed, the library expects the blade to be in the same installed location after every power cycle.

If an FC I/O blade is relocated or is permanently removed from the library, the library firmware must be configured to stop monitoring the blade. Administrators can perform this operation by selecting the FC I/O blade and performing the remove blade operation on the **Setup - FC I/O Blade Control** screen. If this is not done and the library continues to monitor a removed FC I/O blade, RAS tickets could be generated.

You do not need to configure the library to stop monitoring an FC I/O blade if the failed blade is replaced with a new blade. For instructions on how to remove and replace an FC I/O Blade, see [Adding, Removing, and Replacing FC I/O Blades](#) on page 359.

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 [Identifying FC I/O Blades](#) on page 393.

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

The paths to open the appropriate screens are as follows:

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

Resetting FC I/O Blade Ports

Administrators can reset individual ports on FC I/O blades. Resetting these ports can help troubleshoot FC I/O blade issues. The **Setup - Blade Control** screen allows you to perform the Reset Port operation on a selected FC I/O blade port.

Resetting an FC I/O blade port will cause a temporary loss of communication with connected hosts. The screen will display a warning message about the communication loss and ask you to confirm that you want to proceed.

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

Note: Before resetting FC I/O blade ports, verify the location of the FC I/O blade. See [Identifying FC I/O Blades](#) on page 393.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Setup > FC I/O Blades > FC I/O Blade Control**.
- From the operator panel, select **Setup > FC I/O Blades > FC I/O Blade Control > Reset Port**.

Viewing and E-Mailing the Command History Logs

When FC I/O blades are installed, administrators can use the **Command History Log** screens to view the most recent command and response activity that has occurred with externally addressable library devices, controller LUNs, partitions, and tape drives. This information can help you isolate the source of an issue, such as a library device or host application.

You can select any configured FC I/O blade in the library and display a list of associated library devices. For each device, you can view the command history log. You can also choose to e-mail the command history to a specific e-mail address. The log is sent as a text file attached to an e-mail message.

Before you can e-mail the command history log, the library e-mail account must be configured. For information on setting up the e-mail account, see [Configuring the Library E-mail Account](#) on page 92 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.

Blade Status LEDs

This section covers status LEDs for:

- Library control blade (LCB)
- FC I/O blade
- FC I/O fan blade

[Figure 41](#) shows the location of the blade LEDs. Use [Table 10](#) to interpret the current status of the LEDs.

Figure 41 Location of Blade LEDs

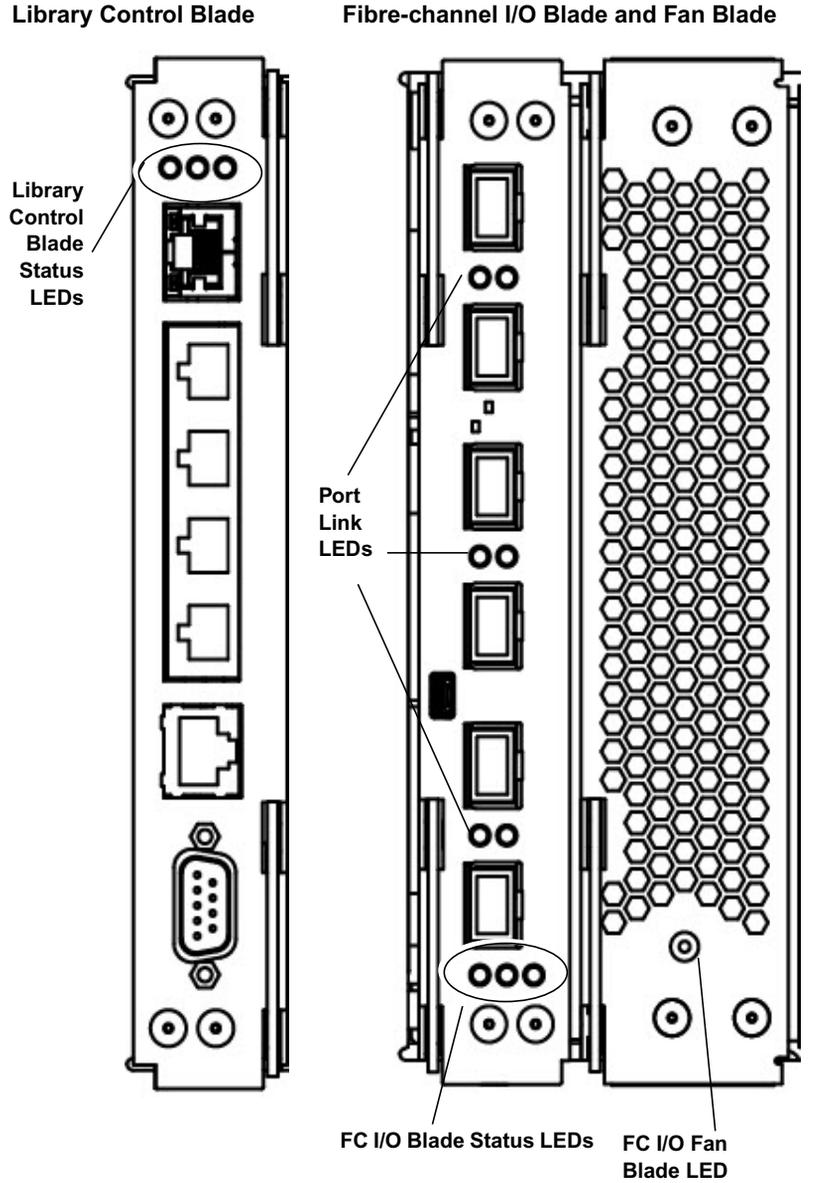


Table 10 Blade Status LEDs

LED Color	Represents	Blade Status
Green	Library application code/Blade processor status	<ul style="list-style-type: none"> • Blinks once per second – Normal operation. • Solid ON – Not operational. • Solid OFF – Not operational (or blade is booting). • Solid ON for 3 seconds, then blinks twice (FC I/O blade only) – Blade firmware is downloading. • Blinks 10 times per second (FC I/O blade only) – Identify mode (per user request, to distinguish it from other blades; see Identifying FC I/O Blades on page 393).
Amber	Health status	<ul style="list-style-type: none"> • Solid OFF – Normal operation. • Blinks once per second (LCB only) – Library application code is not operating or firmware upgrade/downgrade is in progress on existing compact flash. • Solid ON – <ul style="list-style-type: none"> • LCB – Failure OR blade is booting up or initial firmware update on new compact flash. If solid ON for more than 10 minutes, the LCB may need to be replaced. • FC I/O Blade – Failure OR blade is booting up or blade firmware is autoleveling. • FC I/O Fan Blade – There may be one or more problems, including: fan speed is too high or too low; temperature is too high; there is a faulty fan speed sensor; or there is a power control problem. <p>Note: In most cases solid ON means a failure; however, in conjunction with the blue LED blinking once every 10 seconds, an amber LED solid ON can be a normal condition for a short period of time. Autoleveling takes about three minutes per blade, and blades autolevel in series. Never remove a blade when the amber LED is solid ON unless it has been on continuously for at least 10 minutes. Never remove an LCB while the library is powered on.</p>

LED Color	Represents	Blade Status
Blue	Power Control status	<ul style="list-style-type: none"> • Blinks once every 10 seconds – Normal. Blade is powered on. • Solid ON – <ul style="list-style-type: none"> • LCB – Error condition. Power off library before removing or replacing the LCB. • FC I/O blade – Swap mode: Blade is ready to be removed or replaced. • Solid OFF – Blade is not receiving power.

Blade Port LEDs

This section describes blade port LEDs.

LCB Ethernet Hub Port LED

The LED for an Ethernet hub port is located above the port. Use [Table 11](#) to interpret Ethernet hub link activity on an LCB.

Table 11 LCB Ethernet Hub Link Activity

LED Color	Represents	Fibre Port Link Status
Amber	Link and activity	<ul style="list-style-type: none"> • Solid ON – The link is up. • Blinks – The link is up and currently transmitting commands.

Fibre Port Link LED on FC I/O Blades

A fibre port link LED on a FC I/O blade shows the current state of an FC link and indicates whether or not the link is ready to transmit commands.

The link LED for an FC I/O blade fibre port is located either below or above the port. For each link LED pair on the FC I/O blade, the LED on the left belongs to the fibre port below. The LED on the right belongs to

the fibre port above. Black lines on the FC I/O blade faceplate may indicate which LED belongs to which port.

Use [Table 12](#) to interpret Fibre Channel link activity on an FC I/O blade.

Table 12 Fibre Port Link LED
on FC I/O Blade

LED Color	Represents	Fibre Port Link Status
Green	Link and activity	<ul style="list-style-type: none"> • Blinking – Link with activity. • OFF – No link or link with constant activity*. • Solid ON – Blade is initializing.

* LED flashing increases as the activity increases and can actually appear off if the activity is high enough. Also, when the blade boots up, the link LEDs are all on until firmware initializes the ports, at which time they turn off until the port transmitter is enabled and link is acquired.

Servicing the LCB Based on LED Status

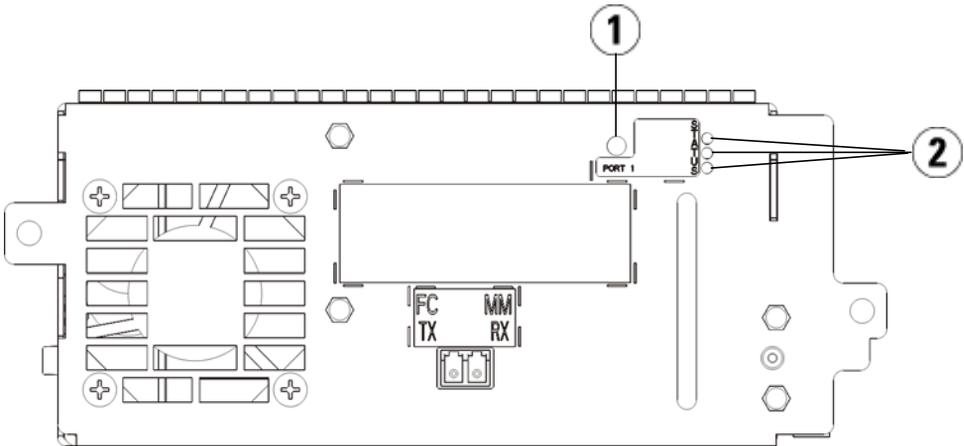
- 1 Observe the blinking patterns of the LEDs for at least 30 seconds.
- 2 Capture a snapshot of the library, and send it to Dell Technical Support for analysis.

Tape Drive LEDs

RAS tickets typically report all problems related to tape drives, including error codes and TapeAlerts. By observing the blinking pattern of LEDs on tape drives, however, you can discern which operation the tape drive is currently performing.

[Figure 42](#) shows where the tape drive LEDs and the fibre port link LED are located.

Figure 42 Location of Tape Drive LEDs



-
- 1 Fibre Port LED
 - 2 Tape Drive LEDs
-

Use [Table 13](#) to interpret tape drive activity:

Table 13 Tape Drive LEDs

LED Color	Represents	Tape Drive Status
Green	Processor activity	<ul style="list-style-type: none"> • Blinks once per second – Normal operation. • Solid ON/ Solid OFF – Tape drive’s main processor is not operating. • 10 blinks per second – Identify mode (see Identifying Tape Drives on page 388). • Blinks 3 times in 3 seconds, then pauses (solid off), and then repeats – Tape drive is initializing. • Solid on for 3 seconds, then blinks twice – Tape drive firmware is downloading. • 2 quick blinks within 1.25 seconds; then on solid for 1.25 seconds; repeat – Drive sled firmware is downloading.
Amber	Health of the tape drive	<ul style="list-style-type: none"> • Solid OFF – Normal operation. • Solid ON – Drive has failed.
Blue	Power control status	<ul style="list-style-type: none"> • Blinks once every 10 seconds – Normal operation. • Solid ON – Offline. Ready to be removed or replaced. • Solid OFF – Tape drive is not receiving power.

Tape Drive Fibre Port Link LED

The fibre port link LED shows the current state of the FC link and indicates whether or not the link is ready to transmit commands. The fibre port link LED on a tape drive is located on the rear of the tape drive, beside the fibre port.

Use [Table 14](#) to interpret FC link activity:

Table 14 Fibre Port Link Status

LED Color	Represents	Fibre Port Link Status
Green	Loop initialization protocol (LIP) and activity	<ul style="list-style-type: none"> • Solid ON – Loop initialization protocol (LIP) has occurred. • Blinks at regular intervals – Host command/ data activity is occurring.
Amber	Online and light detected	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 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 15](#) to interpret power supply activity.

Table 15 Power Supply Status

LED Color and Location	Represents	Power Supply Status
Green (top)	AC OK	<ul style="list-style-type: none"> • Solid ON – The power supply’s AC input is above the minimum requirements to operate. • Solid OFF – The power supply’s AC input is below the minimum requirements to operate.
Green (middle)	DC OK	<ul style="list-style-type: none"> • Solid ON – The power supply’s output voltage is within regulation. • Solid OFF – The power supply’s output voltage is not within regulation.
Blue (bottom)	Standby	<ul style="list-style-type: none"> • Solid OFF – Normal. • Solid ON – Swap mode: Ready to be removed or replaced.

In the RAS tickets associated with the defective power supply, record both the number of the module and the number of the power supply connected to that module.

The 9U Library Expansion Modules are numbered according to their position in relation to the 5U Library Control Module. The 5U Library Control Module is assigned the number 0. All 9U Library Expansion Modules stacked beneath the 5U Library Control Module are assigned a negative number, while 9U Library Expansion Modules stacked above the 5U Library Control Module are assigned a positive number. For example, 9U Library Expansion Module -2 is the second 9U Library Expansion Module beneath the 5U Library Control Module, while 9U Library Expansion Module +2 is the second 9U Library Expansion Module above the 5U Library Control Module.

Each module can have up to two power supplies. The power supply on the left is #1, while the power supply on the right is #2.

Using the Installation Verification Test

Administrators can run the Installation Verification Test (IVT) following a library service action to determine if the library is ready for production use. Examples of such library service actions include installing a new library or replacing a FRU or CRU.

- Note:** IVT is optimized for library firmware versions 520G and above and libraries built after July 1, 2008 (serial numbers with last four digits 8602 and above).
- If your library was built on or before July 1, 2008, and you are running firmware version 520G or above, you will not be able to run the IVT test, even though the selection is available.
 - If your library was built on or before July 1, 2008, and you are running firmware version 500G or below, you can run the test, but it is not recommended because it may produce erroneous results.

A new IVT Log is created each time you run IVT. The log reports detailed information about library readiness and indicates where specific marginal conditions and failures are located in the library subsystems if there are any.

The full IVT is divided into five subtests. You may choose to run only certain subtests depending on the amount of time available and your area of interest. The full IVT may take up to five and one-half hours to complete for a maximum configured library that includes five modules, five I/E stations and 18 drives.

- The **Robot** test evaluates the basic functionality of the library robotics assembly, including the picker assembly and the Y-carriage assembly, the barcode scanner and the calibration sensors. Time required to complete the Robot test is five minutes.

- The **Frame** test assesses the control and expansion module configuration and alignment. Time required to complete the Frame test is three minutes per module.
- The **I/E Station** test assesses the configuration and functionality of each I/E station. Time required to complete the I/E Station test is three minutes per I/E station.
- **Drives** performs functional tests on the library drives. Time required to complete the Drives test is 15 minutes per drive.
- **Tour** moves a scratch data cartridge through all storage slots in the extreme library locations. It also scans the top and bottom-most slots in the library. Time required to complete the Tour is five minutes per module.

Details on running the IVT subtests include:

- All IVT subtests are preselected by default. Clear the check box next to a subtest name to exclude that test from this IVT run. Select **Apply** when you are ready to run the IVT.
- The Robot, Drives and Tour subtests each require that you to provide a scratch data cartridge before the test can begin. If you select one of these subtests, you will be prompted to place a scratch data cartridge into the top I/E station slot. When you close the I/E station, the **Assign I/E** screen appears if the **Manual Cartridge Assignment** setting is enabled on the operator panel **System Settings** screen (**Tools > System Settings**). Assign the new scratch data cartridge to the **System** partition, and then select **Apply**.
- The Drives subtest only tests those tape drives that have the same media type as the scratch data cartridge. For example, if the scratch data cartridge is LTO-3, then all tape drives that are not LTO-3 will be skipped in the Drives test. If the tape drives in the library have different media types, you must run the Drives test multiple times with a different scratch data cartridge for each tape drive media type.
- If a subtest is missing required resources (for example, scratch data cartridges) the subtest will fail.
- The IVT starts by performing an inventory of the library. The inventory is recorded in the IVT log along with the test results.
- Select **Details** on the **Library Test Progress** screen to see the IVT results. If the IVT is still running, you will only see results for tests that have completed.

- Select **Stop** on the **Library Test Progress** screen to cancel the current IVT run between subtests. The last issued commands will complete before library control is returned.
- Once the selected tests are complete, select **Next**. You can choose to view the detailed IVT log or e-mail the detailed IVT log. Make your choice and select **Next**.

The IVT test cannot be performed from the Web client. The path to open the appropriate screen is as follows:

- From the operator panel, select **Tools > Library Tests > Installation & Verification Tests**.

Viewing the IVT Logs

A new IVT log is created each time you run IVT. The log reports detailed information about library readiness and indicates where specific marginal conditions and failures are located in the library subsystems if there are any. You can view a summary or detailed version of a log following an IVT run.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Reports > Log Viewer > Installation Verification Test Summary Log**.
- From the Web client, select **Reports > Log Viewer > Installation Verification Test Detailed Log**.
- From the operator panel, select **Tools > Library Tests > View Last Summary Log**.
- From the operator panel, select **Tools > Library Tests > View Last Detailed Log**.

Saving and E-mailing the IVT Logs

You can save and e-mail the summary and detailed IVT logs as a text file using the Web client. From the operator panel, you can e-mail the detailed IVT log as a text file.

The path to open the appropriate screens are as follows:

- From the Web client, select **Reports > Log Viewer > Installation Verification Test Summary Log**.

- From the Web client, select **Reports > Log Viewer > Installation Verification Test Detailed Log**.
- From the operator panel, select **Tools > Library Tests > E-mail Last Detailed Log**.

Running Library Demo

Administrators can run Library Demo, a simple way to test robotics functionality following a FRU or CRU replacement. It shows the library's ability to correctly move a scratch data cartridge from an I/E station to randomly selected open storage slots until the demonstration is stopped.

Details on running Library Demo include:

- Media in the storage magazines are not affected by the demonstration. The scratch data cartridge is returned to the I/E station following each cycle of 20 moves or when the demonstration is stopped.
- Before running Library Demo, ensure that no host applications are accessing the library.
- After you select **Library Demo** on the **Tools > Library Tests** screen, you will be prompted to place a scratch data cartridge into the top I/E station slot. The library robot will use this cartridge to perform its moves during the demonstration.
- When you close the I/E station, the **Assign I/E** screen appears if the **Manual Cartridge Assignment** setting is enabled on the operator panel **System Settings** screen (**Tools > System Settings**). Assign the new scratch data cartridge to the **System** partition, and then select **Apply**.
- Before the demonstration starts, the library may perform an inventory. If the screen shows the flashing "Library Not Ready" message, which indicates that an inventory is occurring, wait until the library is ready before you select **Apply** to begin Library Demo.
- The operator panel will show that the demonstration is in progress. There is an intentional delay of two seconds between move media commands to prevent unnecessary wear on the robotics
- To stop the demonstration, select **Stop** on the **Library Demo** screen. The last issued commands will complete before the demonstration is stopped and library control is returned. The operator panel will display a "Demo Being Stopped" message.

Library Demo cannot be performed from the Web client. The path to open the appropriate screen is as follows:

- From the operator panel, select **Tools > Library Tests > Library Demo**.

Restoring Factory Default Settings

Administrators can restore the default library configuration settings. Restoring the default configuration clears most of the library's configurable items, such as partitions, user accounts, I/E station slots, cleaning slots, and so on. It does not clear the following settings:

- Date and time
- Network configuration
- License keys

Once you have restored factory defaults, you can use the **Setup Wizard** or commands on the **Setup** menu to reconfigure the library. See [Configuring Your Library](#) on page 56.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Tools > Reset Factory Defaults**.
- From the operator panel, select **Tools > Factory Defaults**.

Library Diagnostics

The Diagnostics menu contains a number of tests you can run to determine if tape drives, robotics, and EKM path (if EKM is licensed) are working as they should. The following sections describe the Diagnostics tests:

- [Drive Diagnostics](#) on page 411
- [Robotics Diagnostics](#) on page 412
- [Using EKM Path Diagnostics](#) on page 156 (only available if EKM is licensed on the library)

Notes about Diagnostics include:

- Only users with Admin level privileges can access Diagnostics.
- Only one user can be logged into Diagnostics at a time. Entering Diagnostics disconnects all other library users with the same or lower privileges, on both the operator panel and the Web client. When one Admin-level user is logged into Diagnostics, all other users with Admin level privileges and below will be unable to log in to the library and will get an error message stating that Diagnostics is in progress.
- Entering Diagnostics takes all your library partitions offline. Be sure any crucial operations have stopped before you enter Diagnostics. When you exit Diagnostics, your partitions return to the online/offline status they were in previously.

Diagnostics cannot be performed from the operator panel (the only exception is the Drive Reset operation; see [Drive Reset](#) on page 411). The path to open the appropriate screen is as follows:

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

Drive Diagnostics

Drive diagnostics are separated into the following categories:

- [Drive Tests](#) – Does not require you to use a scratch tape.
- [Media Tests](#) – 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 administrators. You can access the screen, but you cannot apply changes while another administrator is performing the same operation.

The paths to open the appropriate screens are as follows:

- From the Web client, select **Tools > Diagnostics**, then select **Drives > Drive Tests > Drive Reset**.
- From the operator panel, select **Tools > Drive Mgmt > Reset drives**.

Media Tests

The Media Tests are drive tests that require you to insert a scratch or suspect tape into the library's top (uppermost) I/E station slot. The following tests are available:

- **Drive Self Test** — Performs the drive's Power On Self Test (POST) to make sure that drive hardware is working properly.
- **Read/Write Test** — Reads and writes 96 wraps worth of data in each of the scratch tape's four data sections. During the test, the drive overwrites the data on the scratch tape.
- **Fast Read/Write Test** — Reads and writes two wraps worth of data in each of the scratch tape's four data sections. During the test, the drive overwrites the data on the scratch tape.
- **Media Test** — Run this test if you suspect media damage in a tape cartridge. Since media damage usually comes from the tape edges, this test reads and writes two wraps worth of data on each of the two outside data bands on both edges of the tape for the entire length of the tape. For this test, insert the suspect cartridge in the top I/E station slot. The data will be overwritten on the suspect cartridge.

Media tests cannot be performed from the operator panel. The path to open the appropriate screen is as follows:

- From the Web client, select **Tools > Diagnostics > Drives > Media Tests**.

Robotics Diagnostics

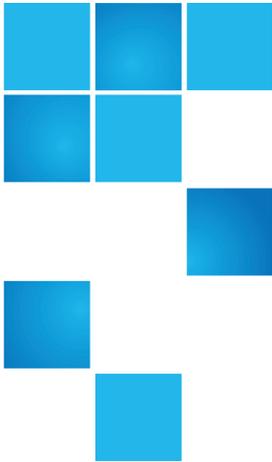
The Robotics diagnostics currently include only one test, the Get/Put Test.

Get/Put Test

The Get/Put Test requires the robot to remove one tape cartridge from the top I/E station slot, and then put the tape cartridge back into the same slot. To run this test, you must insert a tape into the library's top (uppermost) I/E station slot.

Robotics tests cannot be performed from the operator panel. The path to open the appropriate screen is as follows:

- From the Web client, select **Tools > Diagnostics > Robotics > Robotics Get/Put Test**.



Working With Cartridges and Barcodes

This chapter describes how to work with cartridges and barcodes. When working with tape cartridges, certain considerations should be taken into account. For example, all tape cartridges in the library must have a barcode label. In addition, when loading your library, you should be aware of whether or not your cartridges are write-protected.

This chapter discusses these types of items in general terms. See [Library Specifications](#) on page 421 for information on what type of tape cartridges are supported for each drive type.

This chapter covers:

- [Handling Cartridges Properly](#)
- [Write-Protecting Cartridges](#)
- [Barcode Label Requirements](#)
- [Supported Barcode Formats](#)
- [Installing Barcode Labels](#)

Handling Cartridges Properly

To ensure the longest possible life for your cartridges, follow these guidelines:

- Select a visible location to post procedures that describe proper media handling.
- Ensure that anyone who handles cartridges has been properly trained on all procedures.
- Do not drop or strike cartridges. Excessive shock could damage the internal contents of cartridges or the casings themselves, rendering the cartridges unusable.
- Do not expose cartridges to direct sunlight or sources of heat, including portable heaters and heating ducts.
- Store cartridges in a location that is as free from dust as possible. Dust can damage or degrade performance of tape media.
- For external long-term vaulted storage, store cartridges in a vertical orientation.
- If cartridges must be stacked horizontally for moving and handling, do not stack cartridges more than five high.
- The operating temperature range for Linear Tape Open (LTO) cartridges is 50°F to 113°F (10°C to 45°C). The operating relative humidity range is 10% to 80% (non-condensing). The storage temperature range is 60.8°F to 89.6°F (16° to 32°C). Temperatures above 125.6°F (52°C) can cause permanent damage.
- If cartridges have been exposed to temperatures outside the ranges specified above, stabilize the cartridges at room temperature for the same amount of time they were exposed to extreme temperatures or 24 hours, whichever is less.
- Do not place cartridges near sources of electromagnetic energy or strong magnetic fields, such as computer monitors, electric motors, speakers, or x-ray equipment. Exposure to electromagnetic energy or magnetic fields can destroy data and the embedded servo code written on the media by the cartridge manufacturer, rendering the cartridges unusable.
- Place barcode labels only in the designated slots on the cartridges.

- If you ship cartridges, ship them in their original packaging or something stronger.
- Do not insert damaged cartridges into tape drives.
- Do not touch the tape or tape leader.

For more information on determining when a tape is damaged, consult the *Dell LTO Media Handbook* (see [Other Documents You Might Need](#) on page 4).

Caution: Do not degauss cartridges that you intend to reuse.

Write-Protecting Cartridges

All cartridges have a write-protect (write-inhibit) switch to prevent accidental erasure or overwriting of data. Before loading a cartridge into the library, make sure that the write-protect switch is positioned correctly (either on or off).

Slide the red or orange write-protect switch to the right so that the padlock shows in the closed position. The switch is located on the left side of the cartridge front.

Barcode Label Requirements

Cartridges must have an external barcode label that is machine readable. Dell-supplied barcode labels provide the best results. Barcode labels from other sources can be used, but they must meet the following requirements:

Note: Checksum characters are not supported on barcode labels.

- ANSI MH10.8M-1983 Standard.
- Font: Code 39 (3 of 9).
- Allowable characters: Uppercase letters A to Z and numeric values 0 to 9.
- Number of characters: 5 to 16 (default for LTO is 6+2).

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

- Background reflection: Greater than 25 percent.
- Print contrast: Greater than 75 percent.
- Ratio: Greater than 2.2.
- Module: Minimum .254 mm (10 mil).
- Print tolerance: ± 57 μ m.
- Length of the rest zones: 5.25 mm \pm 0.25 mm.
- No black marks may be present in the intermediate spaces or rest zones.
- No white areas may be present on the bars.

Supported Barcode Formats

Dell supplies industry standard LTO barcode labels with a length of 6 + 2 corresponding to the Standard Six and Plus Six formats listed below. For advanced uses, your Dell library supports label lengths of up to 16 characters allowing you to create custom labels. Refer to [Barcode Label Requirements](#) on page 417 for label details.

The library supports the following tape cartridge barcode formats:

- **Standard** – Five to 16 characters total, including a barcode number and optional two-character media ID. If a media ID is included, the label must have a five to 14 character barcode number followed by a media ID; for example, “XXXXXXXXXXXXXXXXL4”. If a media ID is not included, the label must have a five to 16 character barcode number; for example, “XXXXX” or “XXXXXXXXXXXXXXXXXX”. Only the barcode number is reported to the host.
- **Standard Six** – Six character barcode number with or without a two-character media ID; for example, “XXXXXXL4” or “XXXXXX”. Only the six character barcode number is reported to the host.
- **Plus Six** – Six character barcode number followed by a two-character media ID; for example, “XXXXXXL4”. The six character barcode and media ID are reported to the host.
- **Extended** – Five to 16 characters total, including a barcode number and optional two-character media ID. All characters are reported to the host, regardless of the barcode label having a media ID or not. If a media ID is included, the label must have a five to 14 character barcode followed by a media ID; for example, “XXXXXXXXXXXXXXXXL4”. If a media ID is not included, the label must have a five to 16 character barcode number; for example, “XXXXX” or “XXXXXXXXXXXXXXXXXX”.
- **Media ID Last** – Five to 14 character barcode number followed by a two-character media ID, for example, “XXXXXXXXXXXXXXXXL4”. The media ID is reported to the host last, as in “XXXXXXXXXXXXXXXXL4”.
- **Media ID First** – Five to 14 character barcode number followed by a two-character media ID, for example, “XXXXXXXXXXXXXXXXL4”. The media ID is reported to the host first, as in “L4XXXXXXXXXXXXXXXX”.

Installing Barcode Labels

Each cartridge in the library must have an external label that is machine readable to identify the barcode. Most manufacturers offer cartridges with the labels already applied or with the labels included that you can attach.

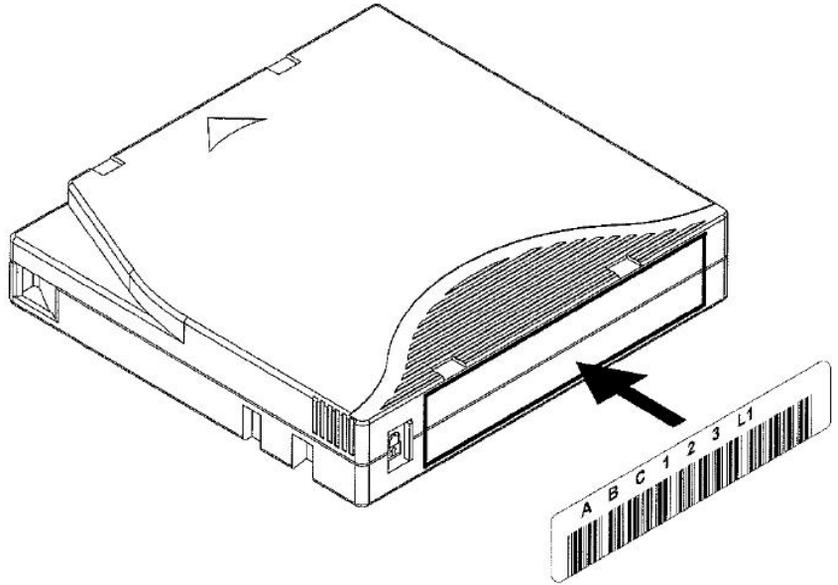
All barcode labels must be applied to the front of a cartridge. Peel off the label and place it on the cartridge. The label must be placed entirely within the recessed area on the cartridge. Verify that the label is oriented so that the numbers appear above the barcode (see [Figure 43](#) on page 420).

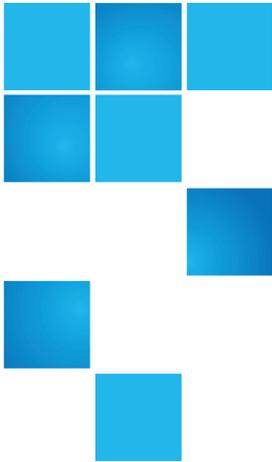
Place the barcode label as level as possible in the provided space for the label. If the label is not placed horizontally level, barcode label scan/read operations may encounter difficulties reading the label.

The cartridge cannot have any stickers or labels attached to the top or bottom because if the labels come loose, they can get caught in the tape drives or become unreadable by the scanner.

Caution: Do not place a barcode label or any labels on the top or bottom of a cartridge. Doing so can cause the tape cartridge and tape drive operations to fail.

Figure 43 Barcode Label
Orientation





Appendix A

Library Specifications

PowerVault ML6000 libraries follow the specifications described in this chapter.

Supported Components

The PowerVault ML6000 library supports the following components.

Supported Cartridges	<ul style="list-style-type: none">• LTO-1 (read-only in LTO-3 drives)• LTO-2 (read/write in LTO-3 drives; read-only in LTO-4 drives)• LTO-3 (read/write in LTO-3 and LTO-4 drives; read-only in LTO-5 drives; supports write-once, read-many (WORM) functionality)• LTO-4 (readLTO-6 drives; supports WORM functionality)• LTO-5 (read/write in LTO-6 drives; supports WORM functionality)• LTO-6 (read/write in LTO-6 drives; supports WORM functionality)
----------------------	--

Supported Tape Drive Types	<ul style="list-style-type: none"> • LTO-3 (SCSI and Fibre Channel) • LTO-4 (Fibre Channel and SAS) • LTO-4 for 7404 4GB I/O Blade (SNW) • LTO-5 Single Port Fibre Channel Tape Drive • LTO-5 Single Port for 7404 4GB I/O Blade (SNW) • LTO-5 Dual Port SAS Tape Drive • LTO-6 Single Port Fibre Channel Tape Drive • LTO-6 Dual Port SAS Tape Drive • LTO-6 Single Port for 7404 4GB I/O Blade (SNW)
Supported SAS Cable	SFF-8088
Library Robot Control	Logical Unit Number (LUN)
Connectivity	Native drive interface
Power	350W with optional redundant power supply and line cord
Library Management	<ul style="list-style-type: none"> • Operator panel touch screen • Web client • SNMP protocol • SMI-S protocol

Library Capacity

Library capacity is as follows.

Note: Slot counts in this user's guide do not include five inaccessible slots in the bottom row of any library configuration. For more information about these slots, see [Unused Slots](#) on page 171.

	ML6010 CM	ML6020 CM	ML6030 CM	ML6030 CM + 1 ML6000 EM	ML6030 CM + 2 ML6000 EMs
Maximum Available Storage Slots (Including I/E Station Slots)	41	133	225	317	409
I/E Station Slots Available	0,6	0, 6, 12, 18	0, 6, 12, 18, 24, 30	0, 6, 12, 18, 24, 30, 36, 42	0, 6, 12, 18, 24, 30, 36, 42, 48, 54
Maximum Drive Capacity	2	6	10	14	18
Maximum Power Supplies	2	4	6	8	10
Maximum Partitions	2	6	10	14	18
Maximum FC I/O Blades	0	2	4	4	4

Environmental Requirements

The environmental requirements for the library are listed below.

Note: Temperature ranges apply to product inlet temperatures, not necessarily to ambient room temperatures. Airflow restrictions or other heat-generating equipment within the rack enclosure may cause a rise over ambient room temperatures.

	Operating	Non-Operating	Storage
Altitude	Up to 10,000 ft. (3,048 m)	Up to 10,000 ft. (3,048 m)	Up to 10,000 ft. (3,048 m)
Temperature	50° to 104° F (10° to 40° C)	50° to 113° F (10° to 45° C)	-40° to 150° F (-40° to 65° C)
Relative Humidity	20 to 80%, non-condensing	10 to 90%, non-condensing	0 to 95%, non-condensing

Electrical Requirements

Electrical requirements for the library are: 100–240 VAC, 50–60 Hz

Dimensions

Library Configuration	Rack Height	Maximum Physical Height (in)
ML6010 CM	5U	8.6 in. x 17.4 in. x 31.4 in (21.9 cm x 44.2 cm x 79.8 cm)
9U Expansion Module	9U	15.8 in. x 17.4 in. x 31.4 in (40 cm x 44.2 cm x 79.8 cm)
ML6020 CM (5U Library Control Module + [1] 9U Expansion Module)	14U	24.4 in. x 17.4 in. x 31.4 in (61.9 cm x 44.2 cm x 79.8 cm)
ML6030 CM (5U Library Control Module + [2] 9U Expansion Modules)	23U	40.1 in. x 17.4 in. x 31.4 in (101.9 cm x 44.2 cm x 79.8 cm)
ML6030 CM + (1) 9U Expansion Module	32U	55.9 in. x 17.4 in. x 31.4 in (141.9 cm x 44.2 cm x 79.8 cm)
ML6030 CM + (2) 9U Expansion Modules	41U	71.6 in. x 17.4 in. x 31.4 in (181.9 cm x 44.2 cm x 79.8 cm)

Component Weights

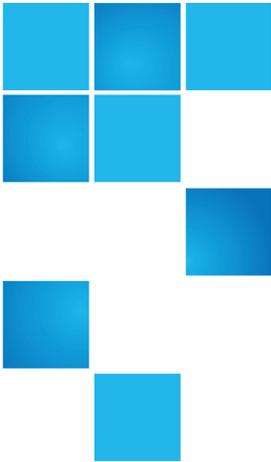
Component	Weight
Drive Sled	10 lbs (4.6 kg)
Power Supply	5 lbs (2.3 kg)
5U Chassis (empty)	60 lbs (27.2 kg)
9U Chassis (empty)	65 lbs (29.5 kg)
5U Packaging Kit	20 lbs (9 kg)
9U Packaging Kit	24 lbs (10.9 kg)
14U Packaging Kit	40 lbs (18 kg)

Library Power Consumption and Heat Output

The typical library power consumption (Watts/hour) and heat output (BTU/hour) is listed below.

Note: “Typical” values for tape drives assumes tape drives are writing.

Library Configuration	Typical Power Consumption (kW/Hour)	Typical Heat Output (BTU/Hour)
Subassembly Power Consumption:		
PowerVault ML6000 Library with Robot and LCB (no tape drives installed; robot moving; LCB installed)	0.079	269.0
LTO-3 Drive Sled Module (SCSI)	0.027	92.1
LTO-3 Drive Sled Module (Fibre Channel)	0.029	99.0
LTO-4 Drive Sled Module (Fibre Channel)	0.040	136.5
LTO-4 Drive Sled Module (SAS)	0.038	129.7
LTO-5 Drive Sled Module (Fibre Channel)	0.048	163.8
LTO-5 Drive Sled Module (SAS)	0.046	157.0
LTO-6 Drive Sled Module (Fibre Channel)	0.034	116.0
LTO-6 Drive Sled Module (SAS)	0.032	109.2
Fibre Channel I/O Blade	0.080	272.8
Control Module:		
Minimum (no drives installed; robot not moving)	0.047	160.0
Maximum (2 drives writing; robot moving)	0.166	565.0
Expansion Module:		
Minimum (no drives installed; robot not moving)	0.012	41.0
Maximum (4 drives writing; 2 Fibre-Channel I/O blades installed; robot moving)	0.256	879.0



TapeAlert Flag Descriptions

TapeAlert is an open industry standard that flags errors and provides possible solutions for storage devices and their media. This section provides information about TapeAlert flags issued by tape drives, including the identifying number, severity, recommended message, and probable cause. [Table 16](#) explains the severity codes, and [Table 17](#) 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 16 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 17 Tape Drive
TapeAlert Flag Descriptions

No.	Flag	Severity	Recommended Application Client Message	Probable Cause
1	Read warning	W	The tape drive is having problems reading data. No data has been lost, but there has been a reduction in the performance of the tape.	The drive is having severe trouble reading.
2	Write warning	W	The tape drive is having problems writing data. No data has been lost, but there has been a reduction in the capacity of the tape.	The drive is having severe trouble writing.
3	Hard error	W	The operation has stopped because an error has occurred while reading or writing data which the drive cannot correct.	The drive had a hard read or write error.
4	Media	C	Your data is at risk: 1 Copy any data you require from this tape. 2 Do not use this tape again. 3 Restart the operation with a different tape.	Media can no longer be written/read, or performance is severely degraded.
5	Read failure	C	The tape is damaged or the drive is faulty. Call the tape drive supplier help line.*	The drive can no longer read data from the tape.
6	Write failure	C	The tape is from a faulty batch or the tape drive is faulty: 1 Use a good tape to test the drive. 2 If the problem persists, call the tape drive supplier help line.*	The drive can no longer write data to the tape.

No.	Flag	Severity	Recommended Application Client Message	Probable Cause
7	Media life	W	<p>The tape cartridge has reached the end of its calculated useful life:</p> <ol style="list-style-type: none"> 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	<p>The operation has failed because the tape in the drive has experienced a mechanical failure:</p> <ol style="list-style-type: none"> 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	<p>The operation has failed because the tape in the drive has experienced a mechanical failure:</p> <ol style="list-style-type: none"> 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	<p>The tape cartridge is nearing the end of its calculated life. It is recommended that you:</p> <ol style="list-style-type: none"> 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	<p>The tape drive needs cleaning:</p> <ol style="list-style-type: none"> 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. <p>Check the tape drive user's manual for device-specific cleaning instructions.</p>	The drive thinks it has a head clog or needs cleaning.
21	Cleaning requested	W	<p>The tape drive is due for routine cleaning:</p> <ol style="list-style-type: none"> 1 Wait for the current operation to finish. 2 Then use a cleaning cartridge. <p>Check the tape drive user's manual for device-specific cleaning instructions.</p>	The drive is ready for a periodic cleaning.
22	Expired cleaning media	C	<p>The last cleaning cartridge used in the tape drive has worn out:</p> <ol style="list-style-type: none"> 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	<p>The last cleaning cartridge used in the tape drive was an invalid type:</p> <ol style="list-style-type: none"> 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: <ol style="list-style-type: none"> 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	<p>The tape drive has a hardware fault:</p> <ol style="list-style-type: none"> 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.* 	<p>The drive has a hardware fault that is not read/write related or requires a power cycle to recover.</p>
32	Primary interface	W	<p>The tape drive has a problem with the host interface:</p> <ol style="list-style-type: none"> 1 Check the cables and cable connections. 2 Restart the operation. 	<p>The drive has identified an interface fault.</p>
33	Eject media	C	<p>The operation has failed:</p> <ol style="list-style-type: none"> 1 Eject the tape or magazine. 2 Insert the tape or magazine again. 3 Restart the operation. 	<p>Error recovery action.</p>
34	Microcode update fail	W	<p>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.</p>	<p>Microcode update failed.</p>
35	Drive humidity	W	<p>Environmental conditions inside the tape drive are outside the specified humidity range.</p>	<p>Drive humidity limits exceeded.</p>
36	Drive temperature	W	<p>Environmental conditions inside the tape drive are outside the specified temperature range.</p>	<p>Cooling problem.</p>
37	Drive voltage	W	<p>The voltage supply to the tape drive is outside the specified range.</p>	<p>Drive voltage limits exceeded.</p>
38	Predictive failure	C	<p>A hardware failure of the tape drive is predicted. Call the tape drive supplier help line.*</p>	<p>Predictive failure of drive hardware.</p>

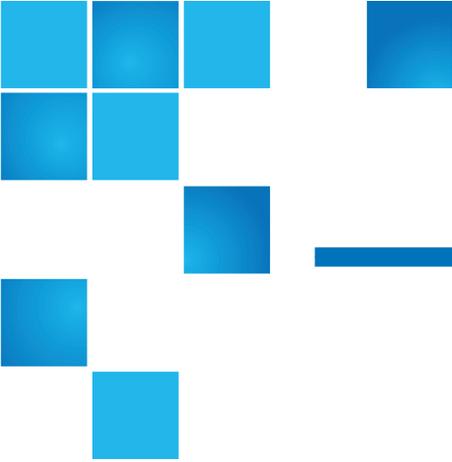
No.	Flag	Severity	Recommended Application Client Message	Probable Cause
39	Diagnostics required	W	The tape drive may have a hardware fault. Run extended diagnostics to verify and diagnose the problem. Check the tape drive user's manual for device-specific instructions on running extended diagnostic tests.	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	<p>The operation has failed because the media cannot be loaded and threaded:</p> <ol style="list-style-type: none"> 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	<p>The operation has failed because the medium cannot be unloaded:</p> <ol style="list-style-type: none"> 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	<p>The tape drive has a problem with the automation interface:</p> <ol style="list-style-type: none"> 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	<p>An attempt had been made to overwrite user data on a WORM medium:</p> <ol style="list-style-type: none"> 1 If a WORM medium was used inadvertently, replace it with a normal data medium. 2 If a WORM medium was used intentionally: <ol style="list-style-type: none"> 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			

* Go to <http://support.dell.com> for Dell technical support information.

** 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).



Appendix C Contacting Dell

For customers in the United States, call 800-WWW-DELL (800-999-3355).

Note: If you do not have an active Internet connection, you can find contact information on your purchase invoice, packing slip, bill, or Dell product catalog.

Dell provides several online and telephone-based support and service options. Availability varies by country and product, and some services may not be available in your area. To contact Dell for sales, technical support, or customer service issues:

- 1 Visit <http://support.dell.com>.
- 2 Select your country or region from the drop-down menu at the top left of the page.
- 3 Click **Contact Us** on the top left of the page.
- 4 Select the appropriate service or support link based on your need.
- 5 Choose the method of contacting Dell that is convenient for you.